

This draft is distributed to the ECSS community for Public Review.

(Duration: 8 weeks, taking into account the summer break)

START of Public Review: 3 July 018

**End of Parallel Assessment: 28 September 2018**

NOTE: In parallel the Public Review of supporting Handbook "ECSS-E-HB-20-21A-DIR1" is taking place.

**DISCLAIMER** (for drafts)

This document is an ECSS Draft Standard. It is subject to change without any notice and may not be referred to as an ECSS Standard until published as such.

Space engineering

**ECSS Secretariat**

**ESA-ESTEC**

**Requirements & Standards Division**

**Noordwijk, The Netherlands**

Electrical design and interface requirements for actuators

**Foreword**

This Standard is one of the series of ECSS Standards intended to be applied together for the management, engineering and product assurance in space projects and applications. ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards. Requirements in this Standard are defined in terms of what shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

This Standard has been prepared by the ECSS-E-ST-20-21 Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

**Disclaimer**

ECSS does not provide any warranty whatsoever, whether expressed, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item are error-free. In no respect shall ECSS incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or in any way connected to the use of this Standard, whether or not based upon warranty, business agreement, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by ECSS.

Published by: ESA Requirements and Standards Division

ESTEC, P.O. Box 299,

2200 AG Noordwijk

The Netherlands

Copyright: 2018© by the European Space Agency for the members of ECSS

Change log

|  |  |
| --- | --- |
| **Previous steps** |  |
| ECSS-E-ST-20-21C 2.0 FINAL\_OZ\_FT\_8May\_macro FT | Draft provided by WG. |
| ECSS-E-ST-20-21C DIR1  18 May 2018 | Draft for Parallel Assessment  18 May – 1 June 2018 |
| **Current Step** |  |
|  | Public Review  3 July – 28 September 2018  NOTE: To avoid additional work will the tables of Annex A be updated only after the Public Review has taken place.  All listed requirements along with their text will then be created through cross-references.  Therefore it can be that the text of the requirement in the Table does not match the text of the referenced requirement. |
| **Next Steps** |  |
|  | DRR implementation |
|  | DRR Feedback |
|  | TA Vote for publication and  DOORS conversion |
|  | Publication |

Table of contents

[Change log 3](#_Toc514403309)

[Introduction 6](#_Toc514403310)

[1 Scope 7](#_Toc514403311)

[2 Normative references 8](#_Toc514403312)

[3 Terms, definitions and abbreviated terms 9](#_Toc514403313)

[3.1 Terms from other standards 9](#_Toc514403314)

[3.2 Terms specific to the present standard 9](#_Toc514403315)

[3.3 Abbreviated terms 10](#_Toc514403316)

[3.4 Nomenclature 11](#_Toc514403317)

[4 Principles 12](#_Toc514403318)

[4.1 General 12](#_Toc514403319)

[4.2 Standard assumptions 12](#_Toc514403320)

[5 Requirements 13](#_Toc514403321)

[5.1 Functional general interface requirements 13](#_Toc514403322)

[5.1.1 General 13](#_Toc514403323)

[5.1.2 Reliability 13](#_Toc514403324)

[5.2 Functional source interface requirements 14](#_Toc514403325)

[5.2.1 General 14](#_Toc514403326)

[5.2.2 Reliability 14](#_Toc514403327)

[5.2.3 Commands 15](#_Toc514403328)

[5.2.4 Telemetry 15](#_Toc514403329)

[5.3 Functional load interface requirements 17](#_Toc514403330)

[5.3.1 General 17](#_Toc514403331)

[5.3.2 Reliability 17](#_Toc514403332)

[5.4 Performance general interface requirements 17](#_Toc514403333)

[5.4.1 General 17](#_Toc514403334)

[5.5 Performance source interface requirements 18](#_Toc514403335)

[5.5.1 General 18](#_Toc514403336)

[5.5.2 Reliability 18](#_Toc514403337)

[5.5.3 Telemetry 18](#_Toc514403338)

[5.5.4 Recurrent products 19](#_Toc514403339)

[5.6 Performance load interface requirements 19](#_Toc514403340)

[5.6.1 General 19](#_Toc514403341)

[5.6.2 Reliability 19](#_Toc514403342)

[5.6.3 Recurrent products 20](#_Toc514403343)

[Annex A (informative) Requirements mapping 21](#_Toc514403344)

[Bibliography 38](#_Toc514403345)

**Tables**

[Table A-1 : Functional general requirements list 22](#_Toc514403346)

[Table A-2 : Functional source requirements list 24](#_Toc514403347)

[Table A-3 : Functional load requirements list 31](#_Toc514403348)

[Table A-4 : Performance general requirements list 32](#_Toc514403349)

[Table A-5 : Performance source requirements list 33](#_Toc514403350)

[Table A-6 : Performance load requirements list 36](#_Toc514403351)

Introduction

This standard identifies the requirements needed to specify, procure or develop the electronics needed for driving release actuators (bot explosive like pyrotechnic devices or non-explosive like thermal knives) and gives the relevant electrical interface specification, both from source and load perspective.

The present standard covers explosive or non-explosive actuators electronics required to comply with single fault tolerance with respect to actuation success.

For a reference architecture description, it is possible to refer to ECSS-E-HB-20-21.

ECSS-E-HB-20-21 includes a clarification of the principles of operation of the actuator electronics, identifies important issues related to actuators and explains the requirements of the present standard.

# Scope

In general terms, the scope of the consolidation of the electrical interface requirements for electrical (hold down and release or deployment) actuators in the present ECSS-E-ST-20-21 and the relevant explanation in the handbook ECSS-E-HB-20-21 is to allow a more recurrent approach both for actuator electronics (power source) and electrical actuators (power load) offered by the relevant manufacturers, at the benefit of the system integrators and of the Agency, thus ensuring:

* better quality,
* stability of performances, and
* independence of the products from specific mission targets.

A recurrent approach enables manufacturing companies to concentrate on products and a small step improvement approach that is the basis of a high quality industrial output.

This standard applies to satellite electrical design.

This standard does not apply to launchers and human space applications.

# Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revision of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the more recent editions of the normative documents indicated below. For undated references, the latest edition of the publication referred to applies.

|  |  |
| --- | --- |
| ECSS-S-ST-00-01 | ECSS system - Glossary of terms |
| ECSS-Q-ST-30-02 | Space product assurance - Failure modes, effects (and criticality) analysis (FMEA/FMECA) |
| ECSS-E-ST-33-11 | Space engineering - Explosive subsystems and devices |

# Terms, definitions and abbreviated terms

## Terms from other standards

1. For the purpose of this document, the terms and definitions from ECSS-S-ST-00-01 apply, in particular for the following terms:
   1. redundancy
   2. active redundancy
   3. hot redundancy
   4. cold redundancy
   5. fault
   6. fault tolerance
2. For the purpose of this document, the terms and definitions ECSS‐Q‐ST-30-02 apply, in particular for the following terms:
   1. failure propagation
3. For the purpose of this document, the terms and definitions from ECSS-E-ST-33-11 apply, in particular for the following terms:
   1. no fire
   2. all fire

## Terms specific to the present standard

1. actuator

<CONTEXT: electrical actuator> component of a machine that is responsible for triggering the movement of a mechanism or a system

1. actuator electronics

electronics supplying an actuator

1. actuators group

set of actuators sharing the same ARM and the same FIRE block

1. The term “actuators group” is synonymous to the term “group” in this standard
2. all-fire current

current giving a probability of actuation higher than a specified limit, at a confidence level higher of a specified limit

1. no-fire current

current giving a probability of actuation lower than a specified limit, at a confidence level higher than a specified limit

1. maximum fire current

maximum current allowed in an actuator in nominal conditions

1. minimum actuation current

all-fire current plus a margin defined by the system integrator

1. The current margin is calculated to guarantee in worst case the required reliability with a given confidence level when the actuation time is above the minimum actuation time.
2. minimum actuation time

actuation time in the all-fire current reference conditions, plus a margin established by the manufacturer or by the system integrator

1. The margin is calculated to guarantee in worst case the required reliability with a given confidence level when the actuation current is above the minimum actuation current.
2. inhibition strap

hardware feature that does not allow firing of the actuator

1. current-driven actuator

actuator that is commanded by a current pulse within a certain range of values and duration

1. voltage-driven actuator

actuator that is commanded by a voltage pulse within a certain range of values and duration

## Abbreviated terms

For the purpose of this Standard, the abbreviated terms and symbols from ECSS-S-ST-00-01 and the following apply:

| Abbreviation | **Meaning** |
| --- | --- |
| DC | direct current |
| EEE | electrical, electronic and electromechanical |
| FMEA | failure modes and effects analysis |
| FMECA | failure modes, effects and criticality analysis |
| RoD | review of design |
| SSE | space segment element |
| SSS | space segment subsystem |

## Nomenclature

The following nomenclature applies throughout this document:

1. The word “shall” is used in this Standard to express requirements. All the requirements are expressed with the word “shall”.
2. The word “should” is used in this Standard to express recommendations. All the recommendations are expressed with the word “should”.
3. It is expected that, during tailoring, recommendations in this document are either converted into requirements or tailored out.
4. The words “may” and “need not” are used in this Standard to express positive and negative permissions, respectively. All the positive permissions are expressed with the word “may”. All the negative permissions are expressed with the words “need not”.
5. The word “can” is used in this Standard to express capabilities or possibilities, and therefore, if not accompanied by one of the previous words, it implies descriptive text.
6. In ECSS “may” and “can” have completely different meanings: “may” is normative (permission), and “can” is descriptive.
7. The present and past tenses are used in this Standard to express statements of fact, and therefore they imply descriptive text.

# Principles

## General

The indicated requirements verification (see Annex A) identifies the overall applicable methods to confirm compliance to the requirements, without explicitly explaining how the verification is split at applicability level (equipment, SSE, SSS or any combination thereof).

## Standard assumptions

1. This standard applies to satellites and does not apply to launchers and human space flight applications.
2. According to requirement 4.4g of ECSS-E-ST-33-11 this standard covers explosive or non-explosive actuators electronics required to comply with single fault tolerance with respect to actuation success.
3. It is assumed that the two fault tolerance approach (as per ECSS-Q-ST-40 clause 6.4.2.1), with respect to premature and unwanted actuation having catastrophic consequences, when required according to requirement 4.4h of ECSS-E-ST-33-11, is implemented as a system (SSE and SSS) level provision and not at equipment level. See ECSS-E-HB-20-21 section 5.5.1.
4. Current-driven actuators covered by this standard have an inductance of 1 µH max.
5. Voltage-driven actuators covered by this standard have an inductance of 20 mH max.
6. The actuators electronics input voltage is assumed to be within a range of 21 V to 100 V.

# Requirements

## Functional general interface requirements

### General

With regards to actuation sequence, the FIRE event shall be contained within the SELECT event of the specific actuator line i (i=1…n), and the SELECT event is contained within the ARM one.

With regards to actuation sequence, the selection of different SELECT lines may be executed within the same ARM event, but with different FIRE pulses occurrences.

An end to end test shall be performed to ensure that the actuator pulses are effectively present at actuator interface when a system level verification is done.

### Reliability

No single failure shall result in unwanted actuator firing.

1. For example, in the configuration where one actuation electronic failure can lead to unwanted actuation, leading to catastrophic consequences, the selection switch status is processed by the system to avoid unwanted actuation.

In case over-current protections are not provided by the Power Conversion and Distribution Electronics, Actuator Electronics failures, including relevant harness and connector lines, shall not cause short circuit or overload of input power lines.

The system engineering function shall analyse the effect of anomalies in the selection configuration, and use the SELECT statuses information to stop the FIRE command to the main or redundant actuator electronics to avoid catastrophic or undesired consequences.

1. See ECSS-HB-20-21 section 5.5.2 and requirement 5.2.2h of the standard.

## Functional source interface requirements

### General

Actuator electronics shall implement at least three independent safety barriers ARM, SELECT and FIRE necessary to be released before a deployment device is actuated.

The design of the actuator electronics shall allow testing the functionality of each single barrier.

ARM, FIRE and SELECT switching functions shall be located in the hot power line of the actuation path.

The actuator electronic shall control the FIRE actuation duration as specified in requirements 5.2.2j, 5.2.3f, 5.3.1c and 5.6.3b.

Separate connectors dedicated to the actuators electronics outputs shall be implemented.

At power up, the three stages barriers shall be in open state.

Each initiator power line shall be distributed to the relevant user with dedicate return wire except for non-explosive actuators implemented on satellites with power return on structure.

### Reliability

To comply with single fault tolerance, with respect to ability to perform the desired activation, the Actuator Electronics shall be duplicated in a Main and a Redundant section.

1. Including duplication (main and redundant) of all relevant commands and telemetries.

With respect to the needed level of segregation among main and redundant sides of electrical actuator circuits, no common failure mechanism between main and redundant part shall exist.

No single failure in the actuator electronics shall cause more than one of the safety barriers to be spuriously or permanently enabled.

The actuator electronics shall meet one of the two conditions:

Disconnect both the hot and the return lines to the actuators when ARM and SELECT lines are disabled, or

Comply with 5.2.2e.1 and 5.2.2e.2.

In case the return lines to the actuators cannot be disconnected as specified in 5.2.2d, then two following conditions shall be met:

The relevant actuator group does not share connectors with other groups or with other electronic functions.

The harness of the relevant actuator group are not bundled together with any other wire or bundle carrying a positive or negative potential sufficient to trigger the relevant actuators.

The Actuator Electronics shall not be stressed in case of an output short circuit.

To ensure that no other selector is in short circuit failure and therefore that no unwanted actuation is taking place, the actuator electronics shall allow the possibility to check the SELECT statuses before issuing the FIRE command.

Any line that remains floating shall be connected to structure ground internally to the actuator electronics via bleeding resistors 100 kΩ to 1 MΩ.

Insulation among actuator output lines shall be tested.

No single failure in the actuator electronic shall lead to the loss at the same time of the current or voltage limitation and of the actuation duration control.

### Commands

Main and redundant actuator electronics shall accept commands from both main and redundant command chain.

ARM, FIRE and SELECT switching shall be actuated by separate commands.

The enable and disable commands for ARM and for SELECT/FIRE shall follow completely independent physical paths, such that no single failure in the complete command chain can result in a fire action.

1. For example, ARM driven by high power command while SELECT and FIRE driven by serial command interface.

The activation of the ARM switch shall be performed by:

Direct execution of a dedicated and independent discrete command.

Without any other interaction from an actuator electronic function.

The activation of the SELECT and FIRE switches shall be performed by execution of standard serial commands.

For long duration actuators more than 1 s, in addition to 5.2.1d, the FIRE OFF commands shall be implemented by a standard serial line.

The fire commands of the actuator electronics shall be inhibited by dedicated external inhibition straps, acting on the firing function.

1. strap closed = commands disable,
   * + 1. strap open = commands enable.

### Telemetry

Telemetries from the main and the redundant actuator electronics shall be provided to both the main and the redundant acquisition chain.

The actuator electronics shall provide the indication of the status of each selection switch.

Status telemetries shall indicate the effective condition of the relevant functionality) and not provide indirect information.

* 1. 1 Effective condition includes for example state when the switch is effectively ON or OFF, if the line is effectively enabled or disabled, etc.
  2. 2 For example, in case there is only one selection switch per line, the circuitry providing status of the selection switch is fully independent from the monitored circuit.

For short duration actuators less than 1 s, the actuator electronics shall provide a peak firing status which is valid when the monitored firing current is larger than a threshold of 60 % to 80 % of the expected firing current during a period of time greater than 1 ms to 10 ms.

1. The exact current threshold and time duration are established by trimming in the actual application.

For long duration actuators more than 1 s, a current and voltage telemetry shall be provided.

The status of each inhibition strap shall be available as a standard telemetry of the actuator electronics.

1. Standard telemetry of the actuator electronics is for example serial standard telemetry.

For on-ground test purposes the status of each inhibition strap shall be available from the actuator electronics as a physical connection or disconnection.

One status telemetry shall be provided for the main inhibition strap, and another for the redundant one.

A short circuit between the output of the actuator electronics and the ground shall not affect the telemetry of the actuated line.

A status telemetry should be provided via serial telemetry line, to identify if nominal output current or voltage ranges have been exceeded.

If requirement 5.2.4j is applied, the following conditions shall be fulfilled:

The requested status is based on a latch to identify the abnormal conditions even at the end of the firing.

The status latch is resettable through serial command.

## Functional load interface requirements

### General

For current-driven actuators the following shall be specified:

The no-fire current and the relevant duration,

The maximum fire current,

The all-fire current.

For voltage-driven actuators, the voltage range for all fire action shall be specified.

The minimum all fire actuation time shall be specified.

### Reliability

The nominal and redundant electrical actuator paths shall be independent such that no failure mechanism can cause the loss of the actuation function.

Any abnormal voltage or current emission applied on the main respectfully redundant electrical interface of the actuator shall not propagate failure to the redundant respectfully main electrical interface.

1. See actual limit specified in requirements 5.5.2a and 5.5.2b.

## Performance general interface requirements

### General

For current-driven actuators, one of the following two conditions shall be met:

If the actuator maximum resistance as per requirement 5.6.1a is specified, the actuators electronics is able to provide the specified current when the load resistance, including actuator plus harness, is equal to the maximum value not to exceed the voltage as per requirement 5.5.1b.

Otherwise, the system ensures that the minimum current and voltage as qualified is applied at actuator level.

For voltage-driven actuators, the maximum overall harness resistance of the actuator line shall guarantee that the voltage into the actuator is above the specified limit.

Parasitic capacitance to structure seen by the actuator electronics, load plus relevant harness, shall be limited to 1 µF.

Parasitic inductance seen by the actuator electronics (load plus relevant harness) shall be limited to

10 µH for current-driven actuators

20 mH for voltage-driven actuators.

The current timing profile for voltage-driven actuators shall be provided by the system integrator.

## Performance source interface requirements

### General

The nominal current delivered to an actuator shall be verified within the specified limits.

For current-driven actuators, the output maximum voltage, at which the minimum actuation current is guaranteed, shall be specified.

For current-driven actuators, the minimum margin of electronics actuator current on top of “all-fire current” shall be established to calculate the minimum actuation current.

Any monitor current in an actuator system fire line shall be limited to 5 mA or to one tenth of the no-fire current to the actuator whichever is less.

The total leakage current of an armed, selected, but not fired, deployment actuator power outlet shall not exceed 5 mA.

The leakage current to any unselected actuator output line (hot side) to the relevant return shall be lower than 1 mA while any other output line is fired.

### Reliability

For voltage-driven actuators, the abnormal output voltage emission of the actuator electronics shall be limited by the voltage of the input power source of the actuator electronics.

For current-driven actuators, the maximum fault current emission from the actuator electronics to the actuator shall not exceed two times the maximum nominal specified value according to requirement 5.3.1a.2.

### Telemetry

For long duration actuators more than 1 s, the current and voltage telemetries should be provided with 8 Hz sample rate or higher.

If requirement 5.2.4j is applicable, a status telemetry shall be provided via serial telemetry line, to identify if nominal current or voltage ranges have been exceeded by 10 % to 50 % of their maximum nominal value.

### Recurrent products

The power capability of a generic design of actuator electronics should be 50 W DC.

For current-driven actuators, the actuator electronics should supply a current up to 6 A.

1. Specific current capability is trimmed in production.

For current-driven actuators, the actuator electronics should supply the requested current during duration up to 100 ms.

1. Specific current pulse duration is trimmed in production.

For voltage-driven actuators, the actuator electronics should supply a voltage up to 21 V ±1 V, providing the current is lower than the limit defined in requirement 5.5.4e.

1. Specific voltage capability is trimmed in production.

For voltage-driven actuators, the actuator electronics should limit the maximal current to one actuator to 2,5 A.

For voltage-driven actuators, the actuator electronics should be able to supply the requested current during an indefinite duration.

The actuator electronics should be able to support a repetition rate for FIRE pulses down to 100 ms.

## Performance load interface requirements

### General

The maximum actuator resistance shall be specified in the operative conditions range, including temperature.

The maximum actuator resistance need not be specified if the actuators qualification conditions, meaning the minimum voltage source to get all-fire current, is specified.

1. To specify, or otherwise, the maximum actuator resistance has an impact on requirements for current-driven actuators, see 5.4.1a.

No-fire current shall be greater than 50 mA.

### Reliability

It shall be possible to apply to the main, respectively redundant, actuator voltages up to the ones applicable to the input of the actuator electronics without affecting the functionality and performance of the redundant, respectively main, actuator.

1. See assumption in 4.2e.

### Recurrent products

For current-driven actuators, the actuator all-fire current should be lower than 5 A.

For short duration actuators, the actuator minimum all fire actuation time should be lower than 50 ms.

For voltage-driven actuators, the minimum voltage for all fire action should be lower than 19 V with a current lower than 2,5 A respecting duration specified according requirement 5.3.1c.

The maximum inductance of voltage-driven actuators should be 20 mH.

The maximum inductance of current-driven actuators should be 1 µH.

The maximum capacitance of actuators should be 1 µF.

1. (informative)  
   Requirements mapping

Table A-1 to Table A-6 provide a compact view of the requirements of the present standard, including the verification method suggested for each of them. According to ECSS-E-ST-10-02, the verification is accomplished by one or more of the following verification methods:

* Test (T),
* Analysis (A),
* Review-of-design (RoD), and
* Inspection (I).

In addition to the methods of verification specified in ECSS-E-ST-10-02, the present annex includes the test verification at design qualification level (T\*).

The test verification at design qualification level (T\*) is intended to be performed on a representative version of the hardware, on a set up not necessarily equal to the final flight one, to be established by the relevant manufacturer or user.

1. If not stated otherwise, any reference to the handbook inside the tables, is a reference to ECSS-E-HB-20-21.

The suggested applicability level indicated in Table A-1 to Table A-6 (SSE/SSS/Equipment) is intended in and-option (SSE and/or SSS and/or Equipment).

**NOTE:**

**To avoid additional work will the tables of this Annex be updated only after the Public Review has taken place.**

**All listed requirements along with their text will then be created through cross-references.**

**Therefore it can be that the text of the requirement in the Table does not match the text of the referenced requirement.**

: Functional general requirements list

| Ref. | Paragraph | Text of the requirement | | Conditions | Applicability | Applicability level | Verification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A = analysis  RoD = review of design | | | T = test  T\* = test verification at design qualification level | | | | |
| 5.1.1a | General | With regards to actuation sequence, the FIRE event shall be contained within the SELECT event of the specific actuator line i (i=1…n), and the SELECT event is contained within the ARM one. | | Nominal | All | SSE/SSS/Equipment | T |
| 5.1.1b | General | With regards to actuation sequence, the selection of different SELECT lines may be executed within the same ARM event, but with different FIRE pulses occurrences. | | Nominal | All | SSE/SSS/Equipment | T |
| 5.1.1c | General | An end to end test shall be performed to ensure that the actuator pulses are effectively present at actuator interface when a system level verification is done. | | Nominal | All | SSE/SSS | T |
| 5.1.2a | Reliability | No single failure shall result in unwanted actuator firing.  NOTE For example, in the configuration where one actuation electronic failure can lead to unwanted actuation, leading to catastrophic consequences, the selection switch status is processed by the system to avoid unwanted actuation. | | Failure | All | SSE/SSS/Equipment | RoD, A |
| 5.1.2b | Reliability | In case over-current protections are not provided by the Power Conversion and Distribution Electronics, Actuator Electronics failures (including relevant harness and connector lines) shall not cause short circuit or overload of input power lines. | | Failure | All | SSS/Equipment | A |
| 5.1.2c | Reliability | The system engineering function shall analyse the effect of anomalies in the selection configuration, and use the SELECT statuses information to stop the FIRE command to the main or redundant actuator electronics to avoid catastrophic or undesired consequences.  See ECSS-HB-20-21 section 5.5.2 and requirement 5.2.2h of the standard. | | Failure | All | SSE | A |

: Functional source requirements list

| Ref. | Paragraph | Text of the requirement | | Conditions | Applicability | Applicability level | Verification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A = analysis  RoD = review of design | | | T = test  T\* = test verification at design qualification level | | | | |
| 5.2.1a | General | Actuator electronics shall implement at least three independent safety barriers ARM, SELECT and FIRE necessary to be released before a deployment device is actuated. | | Nominal | All | SSS/Equipment | RoD |
| 5.2.1b | General | The design of the actuator electronics shall allow testing the functionality of each single barrier. | | nominal | all | SSE/SSS/Equipment | RoD, T |
| 5.2.1c | General | ARM, FIRE and SELECT switching functions shall be located in the hot power line of the actuation path. | | Nominal | All | Equipment | RoD |
| 5.2.1d | General | The actuator electronic shall control the FIRE actuation duration as specified in this standard. | | Nominal | All | SSS/Equipment | RoD |
| 5.2.1e | General | Separate connectors dedicated to the actuators electronics outputs shall be implemented. | | Nominal | All | SSS/Equipment | RoD |
| 5.2.1f | General | At power up, the three stages barriers shall be in open state. | | Nominal | All | SSS/Equipment | RoD, T |
| 5.2.1g | General | Each initiator power line shall be distributed to the relevant user with dedicate return wire except for non-explosive actuators implemented on satellites with power return on structure. | | Nominal | All | SSE/SSS/Equipment | RoD |
| 5.2.2a | Reliability | To comply with single fault tolerance, with respect to ability to perform the desired activation, the actuator electronics shall be duplicated in a main and a redundant section.  NOTE Including duplication (main and redundant) of all relevant commands and telemetries. | | Failure | All | Equipment | RoD |
| 5.2.2b | Reliability | With respect to the needed level of segregation among main and redundant sides of electrical actuator circuits: no common failure mechanism between main and redundant part shall exist. | | Failure | All | Equipment | RoD, A |
| 5.2.2c | Reliability | No single failure in the actuator electronics shall cause more than one of the safety barriers to be spuriously or permanently enabled. | | Failure | All | SSS/Equipment | RoD, A |
| 5.2.2d | Reliability | The actuator electronics shall meet one of the two conditions:  1. Disconnect both the hot and the return lines to the actuators when ARM and SELECT lines are disabled, or  2. Comply with 5.2.2e.1 and 5.2.2e.2. | | Nominal | All | Equipment | RoD, T |
| 5.2.2e | Reliability | In case the return lines to the actuators cannot be disconnected as specified in 5.2.2d, then two following conditions shall be met:  1 The relevant actuator group does not share connectors with other groups or with other electronic functions.  2 The harness of the relevant actuator group are not bundled together with any other wire or bundle carrying a positive or negative potential sufficient to trigger the relevant actuators. | | Nominal | All | 1 SSE/SSS/Equipment  2. SSE/SSS | RoD |
| 5.2.2f | Reliability | The Actuator Electronics shall not be stressed in case of an output short circuit. | | Nominal / Failure | All | Equipment | A, T |
| 5.2.2g | Reliability | To ensure that no other selector is in short circuit failure and therefore that no unwanted actuation is taking place, the actuator electronics shall allow the possibility to check the SELECT statuses before issuing the FIRE command. | | Nominal / Failure | All | SSS/Equipment | T |
| 5.2.2h | Reliability | Any line that remains floating shall be connected to structure ground internally to the actuator electronics via bleeding resistors, 100 kΩ to 1 MΩ. | | Nominal | All | Equipment | RoD, T |
| 5.2.2i | Reliability | Insulation among actuator output lines shall be tested. | | Nominal | All | SSE/Equipment | T |
| 5.2.2j | Reliability | No single failure in the actuator electronic shall lead to the loss at the same time of the current or voltage limitation and of the actuation duration control. | | Nominal | All | Equipment | A |
| 5.2.3a | Commands | Main and redundant actuator electronics shall accept commands from both main and redundant command chain. | | Nominal | All | SSE/SSS/Equipment | RoD, T |
| 5.2.3b | Commands | ARM FIRE and SELECT switching shall be actuated by separate commands. | | Nominal | All | SSE | RoD |
| 5.2.3c | Commands | The enable and disable commands for ARM and for SELECT/FIRE shall follow completely independent physical paths, such that no single failure in the complete command chain can result in a fire action.  NOTE For example, ARM driven by high power command while SELECT and FIRE driven by serial command interface. | | Nominal / Failure | All | SSE/SSS/Equipment | RoD, A |
| 5.2.3d | Commands | The activation of the ARM switch shall be performed by:  1. Direct execution of a dedicated and independent discrete command.  2. Without any other interaction from an actuator electronic function. | | Nominal | All | SSS/Equipment | RoD |
| 5.2.3e | Commands | The activation of the SELECT and FIRE switches shall be performed by execution of standard serial commands. | | Nominal | All | SSE/SSS | RoD |
| 5.2.3f | Commands | For long duration actuators, >1s, in addition of req. 5.2.1d, the FIRE OFF commands shall be implemented by a standard serial line. | | nominal | all | SSS/Equipment | RoD, T |
| 5.2.3g | Commands | The fire commands of the actuator electronics shall be inhibited by dedicated external inhibition straps: strap closed = commands disable, strap open = commands enable, acting on the firing function. | | Nominal | All | SSE/SSS/Equipment | RoD/T |
| 5.2.4a | Telemetry | Telemetries from the main and the redundant actuator electronics shall be provided to both the main and the redundant acquisition chain. | | Nominal | All | SSE/SSS/Equipment | RoD, T |
| 5.2.4b | Telemetry | The Actuator Electronics shall provide the indication of the status of each selection switch. | | Nominal / Failure | All | SSS/Equipment | RoD, A, T |
| 5.2.4c | Telemetry | Status telemetries shall indicate the effective condition of the relevant functionality and not provide indirect information.  NOTE 1Effective condition includes for example state when the switch is effectively ON or OFF, if the line is effectively enabled or disabled, etc.  NOTE 2 For example, in case there is only one selection switch per line, the circuitry providing status of the selection switch is fully independent from the monitored circuit. | | Nominal / Failure | All | SSS/Equipment | RoD |
| 5.2.4d | Telemetry | For short duration actuators (less than 1s), the actuator electronics shall provide a peak firing status which is valid when the monitored firing current is larger than a threshold of 60% to 80% of the expected firing current during a period of time greater than 1 ms to 10 ms.  NOTE The exact current threshold and time duration are established by trimming in the actual application. | | Nominal / Failure | Short duration actuators (<1s) | SSS/Equipment | RoD, A, T |
| 5.2.4e | Telemetry | For long duration actuators (more than 1s), a current and voltage telemetry shall be provided. | | Nominal / Failure | Long duration actuators (>1s) | SSS/Equipment | RoD, A, T |
| 5.2.4f | Telemetry | The status of each inhibition strap shall be available as a standard telemetry of the actuator electronics  NOTE Standard telemetry of the actuator electronics is for example serial standard telemetry | | Nominal | All | SSS/Equipment | RoD/T |
| NOTE | Telemetry | For on ground test purposes the status of each inhibition strap shall be available from the actuator electronics as a physical connection or disconnection. | | Nominal | All | SSS/Equipment | RoD/T |
| 5.2.4g | Telemetry | One status telemetry shall be provided for the main inhibition strap, and another for the redundant one. | | Nominal | All | SSS/Equipment | RoD |
| 5.2.4i | Telemetry | A short circuit between the output of the actuator electronics and the ground shall not affect the telemetry of the actuated line. | | Nominal | All | SSS/Equipment | A,T |
| 5.2.4j | Telemetry | A status telemetry should be provided via serial telemetry line, to identify if nominal output current or voltage ranges have been exceeded. | | nominal / failure | All | SSS/Equipment | RoD, T |
| 5.2.4k | Telemetry | If requirement 5.2.4j is applied, the following conditions shall be fulfilled:  1.The requested status is based on a latch to identify the abnormal conditions even at the end of the firing.  2.The status latch is resettable through serial command. | | nominal / failure | All | SSS/Equipment | RoD, T |

: Functional load requirements list

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Ref. | Paragraph | Text of the requirement | | Conditions | Applicability | Applicability level | Verification |
| A = analysis  RoD = review of design | | | T = test  T\* = test verification at design qualification level | | | | |
| 5.3.1a | General | For current-driven actuators the following shall be specified:  1 The no-fire current and the relevant duration.  2 The maximum fire current  3 The all-fire current. | | Nominal | Current-driven actuators | Equipment | RoD |
| 5.3.1b | General | For voltage-driven actuators, the voltage range for all fire action shall be specified. | | Nominal | Voltage-driven actuators | Equipment | RoD |
| 5.3.1c | General | The minimum all fire actuation time shall be specified. | | Nominal | All | Equipment | RoD |
| 5.3.2a | Reliability | The nominal and redundant electrical actuator paths shall be independent such that no failure mechanism can cause the loss of the actuation function. | | Nominal/Failure | All | Equipment | RoD, A |
| 5.3.2b | Reliability | Any abnormal voltage or current emission applied on the main (redundant) electrical interface of the actuator shall not propagate failure to the redundant (main) electrical interface. NOTE See actual limit specified in requirements 5.5.2a and 5.5.2b. | | Failure | All | Equipment | T\* |

: Performance general requirements list

| Ref. | Paragraph | Text of the requirement | | Conditions | Applicability | Applicability level | Verification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A = analysis  RoD = review of design | | | T = test  T\* = test verification at design qualification level | | | | |
| 5.4.1a | General | For current-driven actuators, one of the following two conditions shall be met: 1. If the actuator maximum resistance as per req. 5.6.1a is specified, the actuators electronics is able to provide the specified current when the load resistance, including actuator plus harness, is equal to the maximum value not to exceed the voltage as per req. 5.5.1b. 2. Otherwise, the system ensures that the minimum current and voltage as qualified is applied at actuator level. | | Nominal | Current-driven actuators | SSE/SSS/Equipment | A,T |
| 5.4.1b | General | For voltage-driven actuators, the maximum overall harness resistance of the actuator line shall guarantee that the voltage into the actuator is above the specified limit. | | Nominal | Voltage-driven actuators | SSS/SSE | A,T |
| 5.4.1c | General | Parasitic capacitance to structure seen by the actuator electronics (load plus relevant harness) shall be limited to 1µF. | |  | All | SSS/SSE | A |
| 5.4.1d | General | Parasitic inductance seen by the actuator electronics (load plus relevant harness) shall be limited to 1,10 µH for current-driven actuators 2,20 mH for voltage-driven actuators. | |  | All | SSS/SSE | A |
| 5.4.1e | General | The current timing profile for voltage-driven actuators shall be provided by the system integrator. | | Nominal | Voltage-driven actuators | Equipment | RoD |

: Performance source requirements list

| Ref. | Paragraph | Text of the requirement | | Conditions | Applicability | Applicability level | Verification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A = analysis  RoD = review of design | | | T = test  T\* = test verification at design qualification level | | | | |
| 5.5.1a | General | The nominal current delivered to an actuator shall be verified within the specified limits. | | Nominal | All | SSS/Equipment | A,T |
| 5.5.1b | General | For current-driven actuators, the output maximum voltage, at which the minimum actuation current is guaranteed, shall be specified. | | Nominal | Current-driven actuators | SSS/Equipment | A,T |
| 5.5.1c | General | For current-driven actuators, the minimum margin of electronics actuator current on top of “all-fire current” shall be established to calculate the minimum actuation current. | | Nominal | Current-driven actuators | SSS/Equipment | A,T |
| 5.5.1d | General | Any monitor current in an actuator system fire line shall be limited to 5 mA or to one tenth of the no-fire current to the actuator whichever is less. | | Nominal | All | SSS/Equipment | A, T |
| 5.5.1e | General | The total leakage current of an armed, selected, but not fired, deployment actuator power outlet shall not exceed 5 mA. | | Nominal | all | SSS/Equipment | A,T |
| 5.5.1f | General | The leakage current to any unselected actuator output line (hot side) to the relevant return shall be lower than 1 mA while any other output line is fired. | | Nominal | All | SSS/Equipment | T |
| 5.5.2a | Reliability | For voltage-driven actuators, the abnormal output voltage emission of the actuator electronics shall be limited by the voltage of the input power source of the actuator electronics. | | Failure | Voltage-driven actuators | SSS/Equipment | A |
| 5.5.2b | Reliability | For current-driven actuators, the maximum fault current emission from the actuator electronics to the actuator shall not exceed two times the maximum nominal specified value according to req. 5.3.1b. | | Failure | Current-driven actuators | SSS/Equipment | A, T\* |
| 5.5.3a | Telemetry | For long duration actuators (> 1s), the current and voltage telemetries should be provided with 8Hz sample rate or higher. | | Nominal / Failure | All | SSE/SSS/Equipment | RoD, A, T |
| 5.5.3b | Telemetry | If Req.5.2.4j is applicable, a status telemetry shall be provided via serial telemetry line, to identify if nominal current or voltage ranges have been exceeded by 10 to 50% of their maximum nominal value. | | Nominal / failure | All | SSS/Equipment | A,T |
| 5.5.4a | Recurrent products | The power capability of a generic design of actuator electronics should be 50W DC. | |  | All | SSS/Equipment | A, T |
| 5.5.4b | Recurrent products | For current-driven actuators, the actuator electronics should supply a current up to 6 Amp.  NOTE Specific current capability is trimmed in production. | | Nominal | Current-driven actuators | SSS/Equipment | A,T |
| 5.5.4c | Recurrent products | For current-driven actuators, the actuator electronics should supply the requested current during duration up to 100ms.  NOTE Specific current capability is trimmed in production | | Nominal | Current-driven actuators | SSS/Equipment | A,T |
| 5.5.4d | Recurrent products | For voltage-driven actuators, the actuator electronics should supply a voltage up to 21 V +/-1 V, providing the current is lower than the limit defined in Req. 5.5.4e.  NOTE Specific current capability is trimmed in production. | | Nominal | Voltage-driven actuators | SSS/Equipment | A,T |
| 5.5.4e | Recurrent products | For voltage-driven actuators, the actuator electronics should limit the maximal current to one actuator to 2,5 A. | | Nominal | Voltage-driven actuators | SSS/Equipment | A,T |
| 5.5.4f | Recurrent products | For voltage-driven actuators, the actuator electronics should be able to supply the requested current during an indefinite duration. | | Nominal | Voltage-driven actuators | SSS/Equipment | A,T |
| 5.5.4g | Recurrent products | The actuator electronics should be able to support a repetition rate for FIRE pulses down to 100ms. | | Nominal | All | SSS/Equipment | A,T |

: Performance load requirements list

| Ref. | Paragraph | Text of the requirement | | Conditions | Applicability | Applicability level | Verification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A = analysis  RoD = review of design | | | T = test  T\* = test verification at design qualification level | | | | |
| 5.6.1a | General | The maximum actuator resistance shall be specified in the operative conditions range (including temperature). | | Nominal | All | Equipment | A or T |
| 5.6.1b | General | The maximum actuator resistance need not be specified if the actuators qualification conditions, meaning the minimum voltage source to get all-fire current, is specified. NOTE To specify, or otherwise, the maximum actuator resistance has an impact on requirements for current-driven actuators, see 5.4.1a. | | Nominal | All | Equipment | A,T |
| 5.6.1c | General | No fire current shall be greater than 50mA. | | Nominal | All | Equipment | A,T |
| 5.6.2a | Reliability | It shall be possible to apply to the main, respectively redundant, actuator voltages up to the ones applicable to the input of the actuator electronics without affecting the functionality and performance of the redundant, respectively main, actuator.  See assumption in clause 4.2 bullet e. | | Failure | All | Equipment | A or T |
| 5.6.3a | Recurrent products | For current-driven actuators, the actuator all fire current should be lower than 5A. | | Nominal | Current-driven actuators | Equipment | RoD,T |
| 5.6.3b | Recurrent products | For short duration actuators, the actuator minimum all fire actuation time should be lower than 50ms. | | Nominal | Short duration actuators | Equipment | RoD,T |
| 5.6.3c | Recurrent products | For voltage-driven actuators, the minimum voltage for all fire action should be lower than 19V with a current lower than 2.5A respecting duration specified according req.5.3.1e. | | Nominal | Voltage-driven actuators | Equipment | RoD,T |
| 5.6.3d | Recurrent products | The maximum inductance of voltage-driven actuators should be 20mH. | | Nominal | Voltage-driven actuators | Equipment | A,T |
| 5.6.3e | Recurrent products | The maximum inductance of current-driven actuators should be 1 µH. | | Nominal | Current-driven actuators | Equipment | A,T |
| 5.6.3f | Recurrent products | The maximum capacitance of actuators should be 1 µF. | | Nominal | All | Equipment | A,T |

Bibliography

|  |  |
| --- | --- |
| ECSS-S-ST-00 | ECSS system - Description, implementation and general requirements |
| ECSS-Q-ST-40 | Space product assurance - Safety |
| ECSS-E-ST-10-02 | Space engineering - Verification |
| ECSS-E-HB-20-21 | Space engineering - Electrical design and interface requirements for actuators handbook |