ECSS-E-HB-20-21A
15 May 2019

Space engineering

Guidelines for electrical design and interface requirements for actuators

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

Foreword

This Handbook is one document of the series of ECSS Documents intended to be used as supporting material for ECSS Standards 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.

The material in this Handbook is defined in terms of description and recommendation how to organize and perform the work of electrical actuators, in terms of electrical design and interface requirements (both source and load side).

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

Disclaimer

Published by: ESA Requirements and Standards Division
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands

Table of contents

Figures

Tables

Change log

ECSS-E-HB-20-21A 15 May 2019	First issue

Introduction

The present handbook, and the relevant standard ECSS-E-ST-20-21, have been produced in a general context to provide stable electrical interface specifications (both for the source and the load, for functional and performance aspects).

The convergence within ECSS among agencies, of Large System Integrators and of a representative group of electronic manufacturers on the identified requirement set can provide an effective way to get more recurrent products for generic use, both for the actuator electronics (power source), and for the actuators themselves, in a rather independent way from the final application.

The standard ECSS-E-ST-20-21 has therefore to be intended as a standard for product development, and the present handbook as a guideline to understand the relevant requirements, the typical issues of the actuators interfaces both at system and at equipment level.

This handbook complements ECSS-E-ST-20-21, and it is directed at the same time to power system engineers, who are specifying and procuring units supplying and containing electrical actuators, to power electronics design engineers, who are in charge of designing and verifying actuator electronics, and to electrical actuators designers.

For the system engineers, this document explains the detailed issues of the interface and the impacts of the requirements for the design of the actuator chain.

For design engineers, this document gives insight and understanding on the rationale of the requirements on their designs.

It is important to notice that the best understanding of the topic of Actuators Electrical Interfaces is achieved by the contextual reading of both the present handbook and the ECSS-E-ST-20-21.

1 Scope

In general terms, the scope of the consolidation of the electrical interface requirements for electrical actuators in the ECSS-E-ST-20-21 and the relevant explanation in the present handbook 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 European space agencies, 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.

In particular, the scope of the present handbook is:

- To explain the type of actuators, the principles of operation and the typical configuration of the relevant actuator electronics,
- To identify important issues relevant to electrical actuators interfaces, and
- To give some explanations of the requirements set up in the ECSS-E-ST-20-21.

2 References

ECSS-S-ST-00-01	ECSS system - Glossary of terms
ECSS-E-ST-20-21	Space engineering - Electrical design and interface requirements for actuators
ECSS-E-ST-33-11	Space engineering - Explosive subsystems and devices
ECSS-Q-ST-30-11	Space product assurance - Derating – EEE components
ECSS-Q-ST-40	Space product assurance - Safety
CSG-NT-SBU-16687-CNES Ed/Rev 01/01	Payload safety handbook

3 Terms, definitions and abbreviated terms

3.1 Terms from other documents

a. 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

b. 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

c. For the purpose of this document, the terms and definitions from ECSS-E-ST-20-21 apply.

3.2 Abbreviated terms

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

Abbreviation	Meaning
AIT	assembly, integration and test
CEO	chief executive officer
CSG	Centre Spatial Guyanais
DC	direct current
DIS	disable
EEE	electric, electro-mechanic and electronic
EMC	electro-magnetic compatibility
EMI	electro-magnetic interference

Abbreviation	Meaning
EN	enable
FO	fail operational
FMEA	failure mode effect analysis
FMECA	failure mode effect and criticality analysis
FPGA	field programmable logic array
FS	fail safe
N	nominal
NEA	non-explosive actuators
OBC	on-board computer
PCB	printed circuit board
PCDU	power conditioning and distribution unit
R	redundant
SCSW	spacecraft central software
SMA	shape memory alloy
SW	software
TM	telemetry
WC	worst case

4 Explanations

4.1 Explanatory note

The present handbook refers to the electrical interface requirements defined in the ECSS-E-ST-20-21.

The ECSS-E-ST-20-21 requirements are referred to in this handbook by using following convention and are indicated in italic font:

[requirement number]

For example:

Requirement 5.2.3.2.1a.

→ [Req. 5.2.3.2.1.a.]

See also, for more information, Annex A of ECSS-E-ST-20-21.

In addition:

- each requirement (i.e. any statement containing a "shall" in the standard) is marked with red text.
- each recommendation (i.e. any statement containing a "should" in the standard) is marked with blue text.

Keywords are highlighted in **bold**. A keyword is a word that either has a special meaning in the contest of the section in which it appears, or highlight a concept.

4.2 How to use this document

For the best utilisation of this document, it is recommended to print it together with the ECSS-E-ST-20-21 and to consult both of them contextually.

In this way, the discussion and the rationale explanation of each individual requirement are clearer and there is the minimum risk of misunderstanding.

5 Actuators Interface

5.1 Type of actuators

Electro-mechanic actuators of different types are used for space applications as part of hold down and release mechanisms and deployment mechanisms.

The technologies used in electro-mechanic actuators are varied:

a. Based on pyrotechnic devices (release nuts/bolt cutter, separation nut, cutters, brazing melt, wire cutter, cable cutter, valves),

b. Split spool devices (Fusible wire, SMA wires),

c. Solenoid actuated nuts,

d. SMA triggered release nuts,

e. SMA actuators (pin pullers and pushers),

f. Paraffin actuators (pin pullers and pushers),

g. Electro-magnetic, solenoid pin puller and pusher actuators,

h. Electromagnets, and magnetic clamps,

i. Thermal cutters and knife,

j. Piezoelectric actuators.

The actuation can be performed by provision of heat thanks to a hot head or a filament, causing mechanical action, ignition of explosive powder, deformation of SMA or paraffin expansion, or by direct electro-magnetic action (solenoids, electro-magnets), or by effects induced by piezo-electric means.

Interfaces to electrical motors (for example solar array drive mechanisms, reaction wheels, and other mechanisms) are not covered by the present handbook and standard ECSS-E-ST-20-21.

Actuators can be classified according to different criteria: from electrical point of view, they can be classified as voltage-driven or current-driven types.

A typical example of voltage-driven actuator is a thermal knife, a typical example of current-driven actuator is a pyro device.

Another interesting classification of actuators is according to their level of reusability, according to Table 5-1.

Table 5-1: Actuators reusability

NON-REUSABLE	PARTIALLY REUSABLE (need for refurbishment)	REUSABLE (manually resettable)	REUSABLE (self-resetting)
Pyro cutters Initiators Pyrotechnic bolt, wire cutters and pyro-cutters	Pyro nuts Fusible wire actuated nuts SMA direct actuators Spool based devices separation nut Thermal cutters	Solenoid actuated nuts SMA actuated nuts Paraffin actuators SMA actuators Wire triggers Thermal cutters	Electro-magnetic actuators and triggers Magnetic clamps

The database of actuators used for the drafting of the ECSS-E-ST-20-21 is reported in Annex A.

Some figures of actuators are hereby provided.

Figure 5-1: Dassault pyro initiator

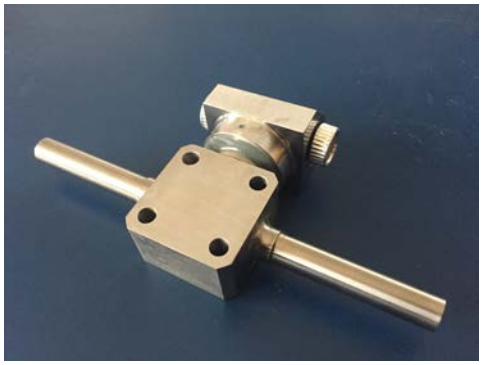


Figure 5-2: Pyro-valve (to be equipped with pyro initiators)

Figure 5-3: Thermal knife (partially reusable – needing refurbishment)

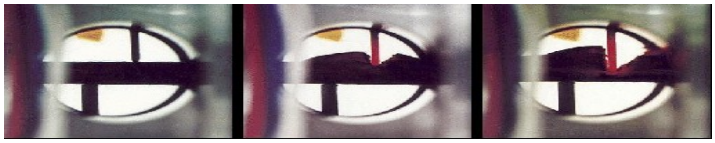


Figure 5-4: Thermal knife activation (partially reusable – needing refurbishment)

Figure 5-5: Thermal knife (with thermal heads visible)

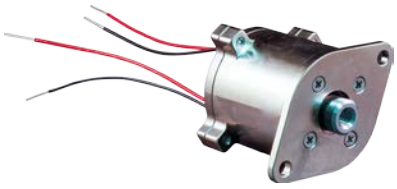


Figure 5-6: Glenair heavy duty HDRM (partially reusable – needing refurbishment)

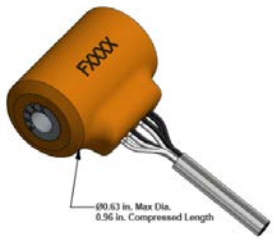


Figure 5-7: TINI Aerospace Frangibolt (reusable – manually resettable)

Figure 5-8: NEA split-spool based HDRM (partially reusable – needing refurbishment)

Figure 5-9: Arquimea pin-puller family (reusable – manually resettable)

5.2 Coverage assumptions

[Assumption 4.2a]

> *"This standard applies to satellites; launchers and human space applications are not included."*

For launchers and human space applications, the actuator system needs normally to be two failure tolerant to avoid human injury, and therefore more stringent requirements are necessary to avoid spurious actuators activation (for example, it is necessary to disconnect both hot and return line from ground to actuators, as per *[Req.5.2.2d]* without alternatives as expressed in *[Req.5.2.2e.1]* and *[Req.5.2.2e.2]*).

[Assumption 4.2b]

> *"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."*

The actuator electronics provides the requested functionality after any single failure thanks to the provided redundancy (see [*Req.5.2.2a]*).

[Assumption 4.2c]

> *"Interfaces to electrical motors (for example solar array drive mechanisms, reaction wheels, other mechanisms) are not covered by the present standard."*

While electrical motors can indeed be used in actuators, the complete specification of motor drive electronics is not subject of the present standard.

[Assumption 4.2d]

> *"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"*

The actuator electronics covered by ECSS-E-ST-20-21 is single point failure tolerant: the coverage of premature and unwanted actuation having catastrophic consequences is achieved by system provisions (avoidance of mechanical interference, additional barriers like skin connectors at spacecraft level operated during integration activities, etc.).

[Assumption 4.2e]

> *"Current-driven actuators covered by this standard have an inductance of 1 μH max, not including harness."*

[Assumption 4.2f]

> *"Voltage-driven actuators covered by this standard have an inductance of 20 mH max."*

Current-driven actuators normally drive loads characterised by small parasitic inductance (the limit is set to 1 μH). Normally current regulators are not well suited to drive large inductive loads, otherwise important stability issues can arise.

Voltage-driven actuators can base their operation on electro-magnetic effects (solenoid pin puller and pusher, electromagnets, and magnetic clamps), characterised by large inductance (the limit is set to 20 mH).

In any case, it is necessary to limit the actuator inductance to a reasonable limit to have a chance to procure generic actuator electronics, e.g. applicable to many actuators types without any design change.

[Assumption 4.2g]

> *"The actuators electronics nominal input voltage (excluding transients) is assumed to be within a range of 21 V to 100 V."*

This is the typical range from regulated and unregulated buses used in European satellites (28 V regulated or unregulated, 50 V regulate or unregulated, 100 V regulated).

5.3 Actuators electronics, general architecture

5.3.1 Overview

A typical block diagram for explosive or non-explosive actuator electronics is shown in Figure 5-10.

A variant of the actuators electronics block diagram is shown in Figure 5-11.

For brevity, explosive or non-explosive actuator electronics are referred as Actuator Electronics in this document.

Note that the diagram in Figure 5-10 or Figure 5-11 is given only as a reference, without losing generality, and some of the features thereby reported can be actually realised differently.

Without losing in generality, the general architecture of **Actuator Electronics** is hereby explained in reference to in Figure 5-10.

Actuator Electronics receive power from the Power Conversion and Distribution Electronics (either directly from a battery or from a regulated power bus).

The power lines from the Power Conversion and Distribution Electronics can be provided or not with over-current protection to safeguard the power bus from short-circuits or overloads generated in the Actuator Electronics.

In case over-current protections are not provided by the Power Conversion and Distribution Electronics, it is important that Actuator Electronics failures do not cause short circuit or overload of input power lines *[Req.5.1.2b].*To this respect, the relevant harness or connector lines double insulation is applied.

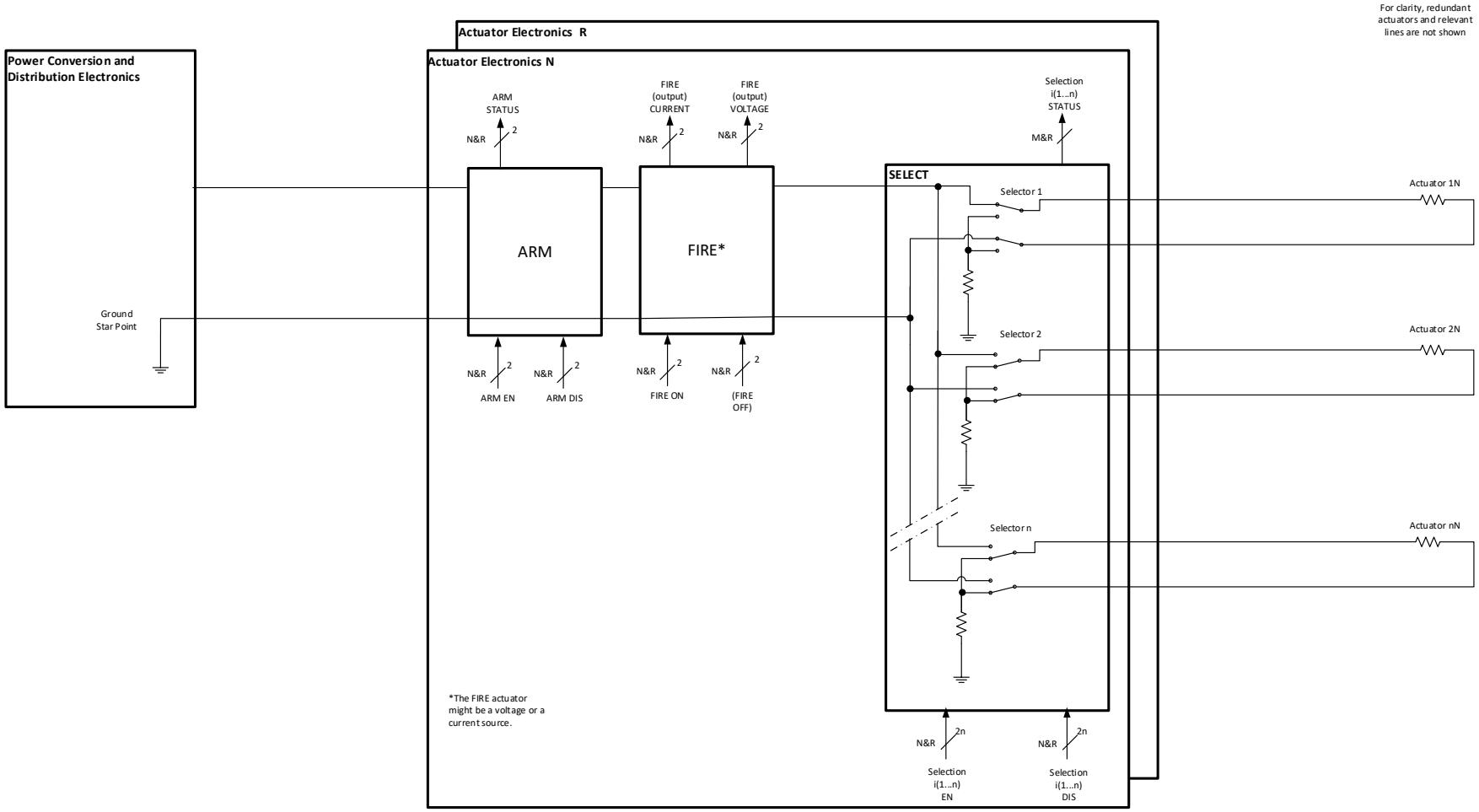
To comply with the required single failure tolerance requirement *[Req.5.2.2a]*, the Actuator Electronics are duplicated, with a nominal (N) and a redundant (R) side.

In Figure 5-10 explosive or non-explosive actuators are just called Actuators (for clarity, only Actuators and power and command and telemetry lines relevant to nominal side are shown).

There are three physical barriers against spurious or untimely activation of Actuators *[Req.5.2.1a]*, represented in Figure 5-10 by **ARM, FIRE** and **SELECT** blocks.

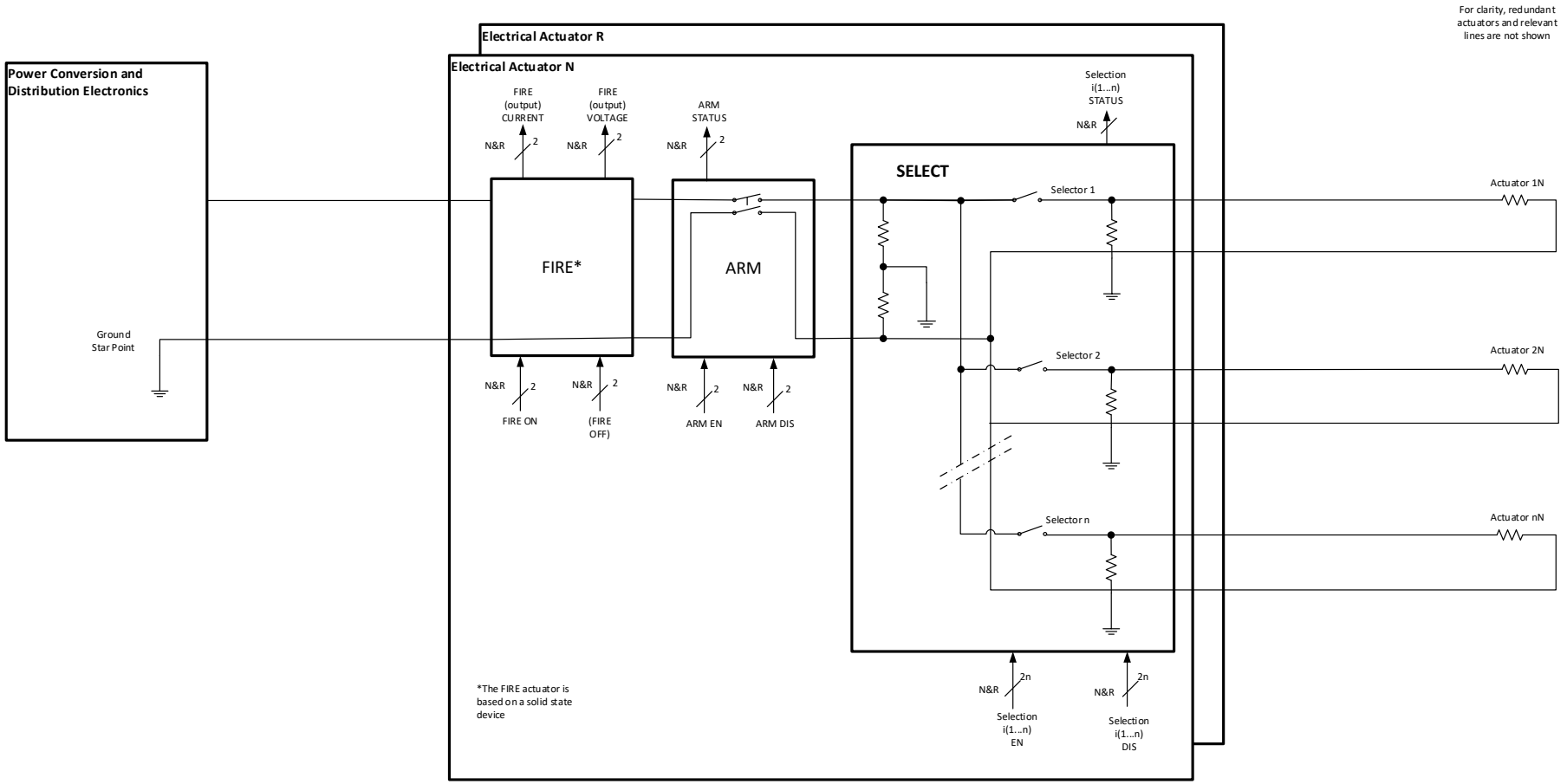
The need for three barriers is explained in section 5.5.1.

In accordance with best practices, any internal conductor (for example, and referring to Figure 5-11, disconnected hot line between ARM and SELECT switches when they are both open, or disconnected return line between ARM switch and actuators return) is grounded to power return to avoid any build-up of potential due to electrostatic phenomena *[Req.5.2.2h]*.



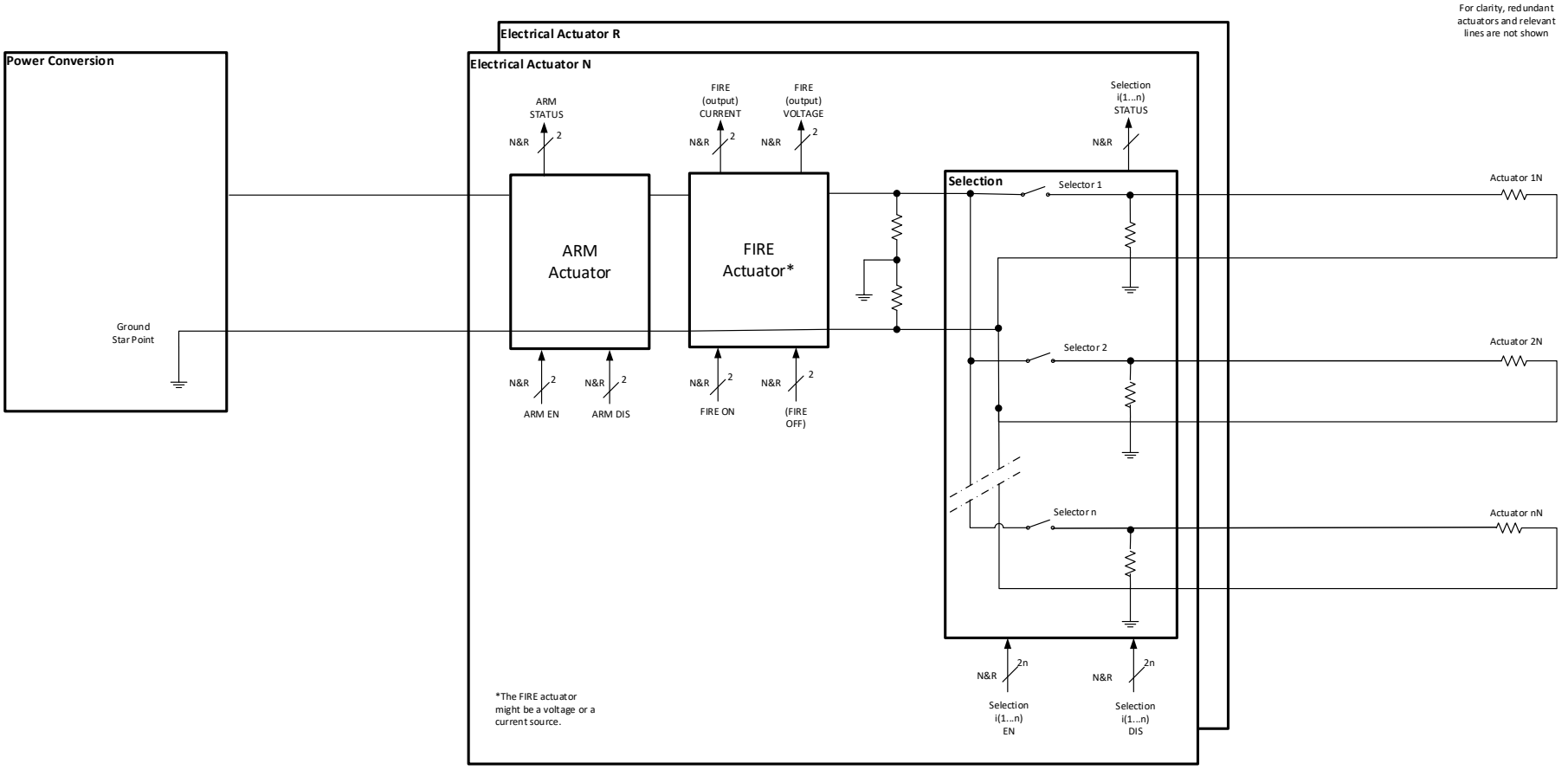
Key: DIS = disable EN = enable N = nominal R = redundant

Figure 5-10: Typical actuators electronic block diagram



Key: DIS = disable EN = enable N = nominal R = redundant

Figure 5-11: Typical actuators electronic block diagram, variant 1



Key: DIS = disable EN = enable N = nominal R = redundant

Figure 5-12: Typical actuators electronic block diagram, variant 2

5.3.2 ARM block

The ARM block is usually implemented by bi-stable relays or by solid state switches (typically MOSFETs).

The ARM block can disconnect only the hot power line in the scheme of Figure 5-10, while on the alternative scheme in Figure 5-11 it disconnects both the hot and the return power lines.

In the option shown in Figure 5-12, the ARM block disconnects the hot line only.

The reason of disconnecting both hot and return power lines is to avoid that any potential that can couple with the hot line of the actuator (due to a failure, loss of insulation or similar reasons) can trigger a spurious activation of the device *[Req.5.2.2d]*.

In case the return lines cannot be disconnected, additional care needs to be paid to avoid coupling to any potential that can trigger the actuator action, separating actuator groups in different connectors and adding sufficient isolation of actuator hot lines to avoid the problem: requirements *[Req.5.2.2e.1]* and *[Req.5.2.2.e.2]* apply.

The commands to the ARM block are ARM enable (ARM EN) and ARM disable (ARM DIS).

Both ARM EN and ARM DIS are duplicated into nominal (N) and redundant (R) commands *[Req.5.2.2a]*, and are provided by dedicated commands (e.g. commands that are not included in a single general serial command flow) – *[Req.5.2.3d]*.

The telemetry for the ARM block is the ARM STATUS, which according to *[Req.5.2.4c]* shall indicate the effective condition of the ARM output (if enabled or disabled).

Both the nominal and the redundant ARM STATUS telemetries are provided to both to the nominal and the redundant acquisition chains *[Req.5.2.4a]*.

5.3.3 SELECT block

Apart being an electrical barrier, the SELECT block provides the specific power connection to one of the actuators connected to the same group.

It can disconnect the hot and the return line to the actuator (as it is shown in Figure 5-10) or just the hot line (as it is shown in Figure 5-11) in case the ARM block provides disconnection of the (common) return line to all actuators in the same group (according to *[Req.5.2.2d]*).

It is also allowed that the ARM block provides just the disconnection of the hot line, but in this case:

a. It is important that the relevant actuator group does not share connectors with other groups or with other electronic functions (*[Req.5.2.2e.1]*);

b. It is important that the harness of the relevant actuator group is not bundled together with any other wire or bundle carrying a positive or negative potential sufficient to trigger the relevant actuators (*[Req.5.2.2e.2*]);

The provision expressed by *[Req.5.2.2e.1]* and *[Req.5.2.2e.2]* is intended to avoid any premature actuator firing due to unpredictable causes (see also section 6.2.2).

The SELECT block takes care of providing a resistive path for connecting the actuators to structure *[Req.5.2.2h]*.

The commands to the SELECT block are Select (1…n) enable (EN) and Select (1…n) disable (DIS).

Both Select EN (1…n) and Select DIS (1…n) are duplicated into nominal (N) and redundant (R) commands *[Req.5.2.2a]*, and are generally included in a single general serial command flow.

The telemetries for the SELECT block are the Select (1…n) STATUSes, which according to *[Req.5.2.4c]* indicate the effective condition of the relevant SELECT output (if enabled or disabled).

Both the nominal and the redundant Select (1…n) STATUS telemetries are provided to both to the nominal and the redundant acquisition chains *[Req.5.2.4a]*.

5.3.4 FIRE block

The fire block is in charge of providing to the selected actuator controlled current (for current-driven actuators) or controlled voltage (for voltage driven ones).

The FIRE blocks accepts a redundant FIRE ON command and can accept a redundant FIRE OFF command. In any case the FIRE ON duration is limited (few tenths of milliseconds for pyro actuators, few tens of seconds for thermal knives or for non-explosive actuators), meaning that if the FIRE OFF command is not sent, the FIRE ON commands act on a monostable function to provide the requested FIRE duration *[Req.5.2.1d]*.

Both FIRE ON and FIRE OFF is duplicated into nominal (N) and redundant (R) command *[Req.5.2.2a]*, and is generally included in a single general serial command flow.

The telemetries for the FIRE block are different depending on the duration of the FIRE pulse.

For actuators characterised by a long duration of the FIRE pulse (e.g. more than 1 second), the telemetries of the FIRE block are the FIRE (output) current and the FIRE (output) voltage *[Req.5.2.4e]*.

For actuators characterised by a short duration of the FIRE pulse (e.g. less than 1 second), the telemetry of the FIRE block is a peak FIRE status, providing a bi-level digital signal identifying if the monitored fired current was larger than a given threshold of the expected firing current during a period of time greater than a given fraction of the expected FIRE current *[Req.5.2.4d]*.

The reason for the different implementation for long and short FIRE duration cases depends on the need to simplify the electronics for short pulses: the recording of the FIRE event voltage and current with the due time resolution can require memory storage capabilities, fast current and voltage acquisition circuits, etc.

It is considered that such effort does not make sense in general for recurrent actuator electronics products: for generic products, the peak FIRE status approach seems more than adequate to have a confirmation of a successful FIRE pulse being transferred to the relevant actuator.

Both the nominal and the redundant FIRE telemetries are provided to both to the nominal and the redundant acquisition chains *[Req.5.2.4a]*.

During AIT, when actuators are implemented and actuator electronics is operational, an inhibition strap is normally present to avoid that incorrect procedure or operator error results in unwanted firing.

The inhibition strap normally acts on the FIRE block to disable the FIRE ON command to be executed *[Req. 5.2.3g]*.

5.4 Actuators electronic, timing sequence

The typical timing sequence of actuators electronics is provided in Figure 5-13.

The FIRE event is contained within the SELECT action of the specific actuator line i (i=1…n), which is contained within the ARM action *[Req.5.1.1a]*, *[Req.5.1.1b].*

In other words, and referring to Figure 5-13, if t0 is the time when ARM is enabled,

$$t0 < t1 < t2 < t3 < t4 < t5$$

where

- t0 is the time when ARM is enabled,
- t1 is the time when SELECT (specific line) is enabled,
- t2 is the time when FIRE ON pulse is executed,
- t3 is the time when FIRE OFF pulse is executed,
- t4 is the time when SELECT (specific line) is disabled,
- t5 is the time when ARM is disabled.

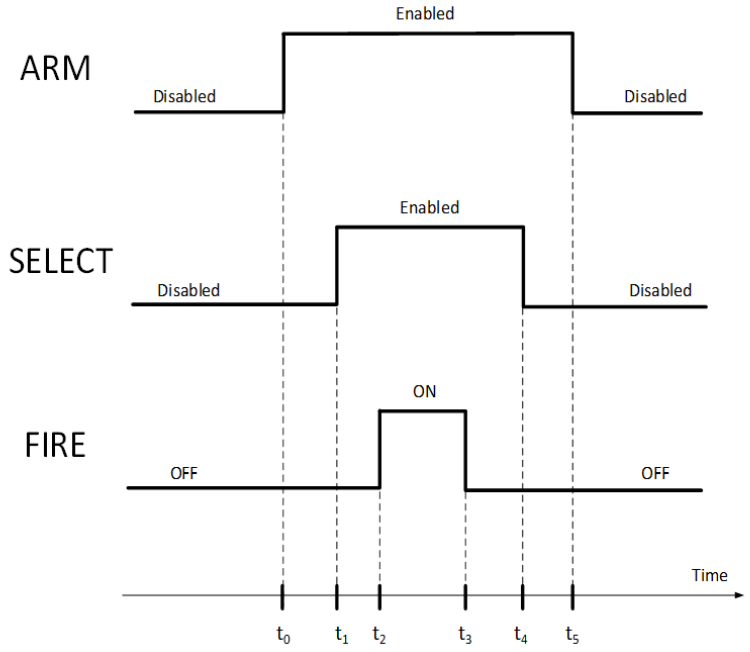


Figure 5-13: Actuators electronics timing sequence

The selection of different SELECT lines can be executed within the same ARM event, but with different FIRE pulses occurrences *[Req.5.1.1c]*, as shown in Figure 5-14.

The reason for *[Req.5.1.1a]*, *[Req.5.1.1b]* and *[Req.5.1.1c]* is to switch the ARM and SELECT lines at zero current: current into the lines will only appear when FIRE is commanded.

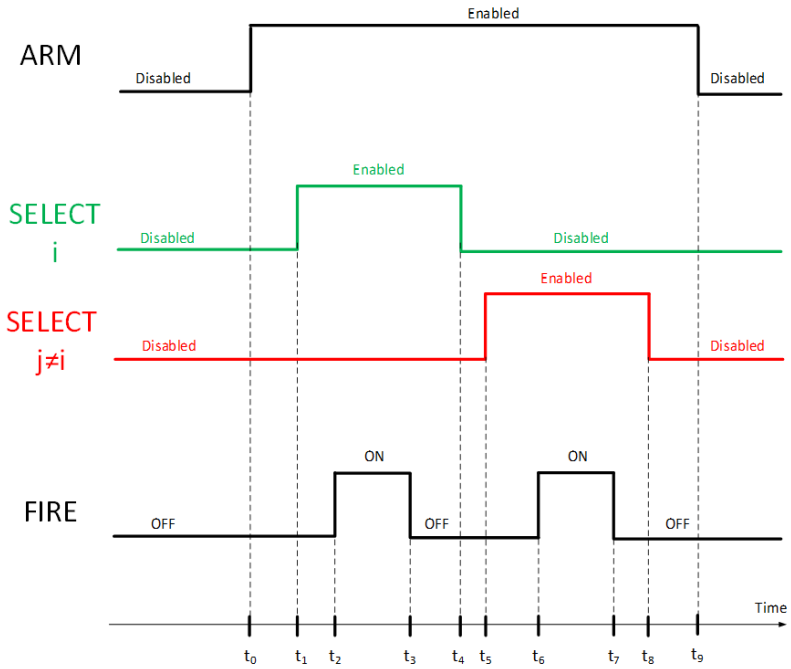


Figure 5-14: Actuators electronics timing sequence, different selected lines

It is important that before authorising a FIRE execution, it is possible to check the status of the SELECT lines to ensure that no other line is enabled apart the intended one for firing (*[Req.5.2.2g]*): if for any reason any other line is short circuited, enabled or connected (due to a failure or any spurious effect), it is important to take measures such that the FIRE execution does not take place, unless it is acceptable from system point of view (e.g. it does not result in critical mechanical interferences or other unwanted effects).

5.5 Actuator electronics, failure tolerance

5.5.1 Double failure tolerance

Double failure tolerance relates to safety.

The double failure tolerance is demonstrated at overall system level (including hardware failure and also operator error) when the associated consequences is catastrophic; this is required and defined in the ECSS standard but also in launcher requirement such as:

a. CSG safety regulations, see Payload Safety handbook, CSG-NT-SBU-16687-CNES (see Annex B);

b. ECSS-Q-ST-40 (requirements 6.4.2.1a to 6.4.2.1e).

This double failure requirement applies for ground activities only: for examples within the large system integrator facilities or in the launch site - clean room, and on the launcher on the launch pad.

During the ascent phase, any propagation from spacecraft to the launcher is considered as “severe” or “critical” or “serious” (consequences) requiring only one-failure tolerant design.

Therefore, the electrical actuator circuitry shall be designed based on the safety analysis regarding the severity, which is made at system level, considering that extra barriers can be constituted and added to this analysis.

Historically, only explosive pyrotechnic devices were used for deployment devices; these devices have systematically catastrophic consequences with respect to human injuries, in the case of inadvertent pyro activation or inadvertent deployment (solar array, antenna, …) likely to kill AIT people.

For this reason, the electrical design on the activation line implements three barriers or switches (SELECT, ARM and FIRE).

On top, inhibition strap (to inhibit physically the activation of commands as long as the spacecraft is on the launcher), was introduced as an additional barrier considering that the software is by nature planned to start automatically the complete deployment sequence.

Even with the implementation of 3 barriers there may be cases where double failure tolerance is not met by the electrical actuator circuitry itself.

For example a failure in the commanding chain using the same physical interface could lead to activate more than one barrier or to select more than one output.

Nowadays, a larger variety of actuators are considered (such as non-explosive actuator or release system based on heating concept); the safety classification of inadvertent activation of such devices can be discussed and criticality can decrease below catastrophic. In principle, it can open the door for adapting the electrical design of the actuation system, compared to state of the art.

Considering that the only event to consider is the "inadvertent release and associated consequences" because of failure or operation occurrence, the process is the following:

a. To identify the "severity" associated to risk-related activity in spacecraft large system integrator facilities and on the launch pad; it is important that this assessment considers the operations (e.g. pyro safe plug is one barrier as long as it is connected) and the different phases; it is important that this assessment also considers the personnel presence (and potential impacts) depending on the AIT operations. For example, "restricted area" around appendices that deploy can be put in place during specific phase of the satellite integration and test, in order to protect people from injuries.

b. To specify per phase, per activity, per function the level of failure tolerance required

c. To sum up all the barriers per phase,

d. To demonstrate how these barriers are managed and controlled.

It appears that such process can lead to different solutions, satellite and mission dependent, which is counterproductive in the frame of a standardisation effort.

Then, the conclusion of the working group and the resulting standard was to consider a single interface (for standardisation reason) based on the "worst case" consequence of inadvertent release of actuator, i.e. to implement 3 barriers as it is currently. This has the benefit of:

a. Standardised circuitry for many possible actuator types, which gives also the flexibility for allocation of the lines,

b. Single SW elementary module

c. Single operational procedure

d. Safety file and justification nearly reusable (i.e. best practice)

5.5.2 Single failure tolerance

Generally speaking, the actuator electronics is designed to be one failure tolerant, both **for no actuation case** and **for unwanted actuation case**:

- **For no actuation case**: it means that after any single failure in the actuator electronics, the actuation pulse is delivered at least to the nominal or to the redundant actuator. Such requirement is normally implemented by actuator electronics full redundancy (duplication of all circuitries into nominal and redundant part).
- **For unwanted actuation case**: it means that after any single failure in the actuator electronics, no unwanted actuation pulse is delivered nor to the nominal nor to the redundant actuator (*[Req. 5.1.2.a]*).
  Such requirement is normally implemented in the actuator electronics by the presence of the three physical barriers (ARM, SELECT, FIRE) and a careful design of the circuits driving them.

[Req. 5.2.3c] specifies that the single failure tolerance requirement includes also the complete command line to the actuator electronics.

Note that the complete command line includes the receiver part of the commands in the actuator electronics but also the transmitter issuing the commands to the actuator electronics (Remote Terminal Unit or other).

To fulfil *[Req. 5.2.3c]*, the circuits delivering the commands to each of the nominal and redundant barriers (ARM, SELECT, FIRE) are segregated in a way that no common failure mechanism exists, for being unable to transfer both the nominal or the redundant command (*[Req. 5.2.2b]*, *[Req.5.2.2k]*).

Note that a spurious command, determined for example by a failure in the command line, can activate one of the barriers (for example ARM), but that is generally allowed due to the presence of the other barriers (in this case, SELECT and FIRE).

An exception to the previous statement appears if a failure in the SELECT barrier happens (causing a short circuit of a selection switch): this can cause the actuation of the intended line (as requested) but also of the line where the selection switch is shorted.

This situation can prove to be unacceptable at system level (causing mechanical interferences, blocking the release of critical deployments, creating hazardous situation, etc.).

It is important that as a consequence, the equipment or subsystem where the actuator electronics resides offers the possibility to check the SELECT statuses before issuing the FIRE command (*[Req. 5.2.2h]*).

On the other side, it is important to assess the need of checking the SELECT statuses before issuing the FIRE command by the system responsible depending on the severity of the consequences of a spurious actuation on any other actuator line (*[Req. 5.1.2c]*).

6 Explanation of ECSS-E-ST-20-21 Interface Requirements

6.1 Functional general

6.1.1 General

[Req. 5.1.1a]

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

[Req. 5.1.1b]

"The SELECT event is contained within the ARM event."

The requirements are explained in detail in section 5.4.

[Req. 5.1.1c]

"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."

The requirement is explained in detail in section 5.4.

[Req. 5.1.1d]

"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."

The end-to-end verification of the presence of the actuator firing pulses at actuator interface is necessary to avoid any issues with incorrect interface specification or with as built versus as design status. Such verification becomes paramount in case the test of actuators firing is not done with the actual flight actuators (which is the normal case for non-resettable ones).

The end-to-end test is performed with the actual flight actuator if resettable and safe.

Alternatively, it is performed with a flight representative actuator or – if not possible for safety or practical reasons – with a load of the same impedance as the flight actuator.

6.1.2 Reliability

[Req. 5.1.2a]

"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."

Unwanted actuator firing can result in unacceptable event; on ground, this can lead to human safety or hardware damage issues; in flight, this can lead to loss of the mission.

On ground, human safety or other catastrophic issues require tolerance to two failures, which has to be demonstrated at system level. This is covered by the overall assumption of this standard.

In flight, unwanted actuator firing can lead to mission loss, in the case that actuation of release mechanisms in wrong order can lead to mechanical damage of the appendices to be deployed and finally to unsuccessful deployment (example: a solar array stack release prior a primary deployment). Other case can be the activation of passivation devices planned for end of mission, (example: battery by-pass activation, leading to battery passivation).

As clarified by the requirement note, unwanted actuation can be the consequence of a wrong activation of a selection switch.

Such failure tolerance is proposed to be managed at system level and not at actuator electronic level: first this avoids unnecessary constraint on the electronic itself and second it is not wished by the system that the electronic itself take decision to interrupt an actuation sequence when this is not necessary. In this case, unwanted actuation can be avoided by checking telemetries of the selection status at software level, before performing firing of an actuator. It supposes that the status is relevant to the actual selection switch position, and not to the image of the commanded state (see *[Req.5.2.4c]*).

Unwanted actuation can also be the consequence of loss of insulation between a power line and an actuator supply line, when the return supply line of this actuator is not isolated from main bus return (as it can be in some actuator electronics architecture in flight configuration, refer to Figure 5-12). In this case, it is important that all dispositions of connector pin segregation, actuator line double isolation with respect to other power lines are taken to avoid any propagation of a single isolation failure.

Note that in some cases unwanted actuation can be tolerated, in the case of a very simple deployment sequence, consisting in releasing nominal and redundant hold down system in any order and where finally the objective is to achieve a straight forward nominal and redundant path actuation, maximising chance of success.

[Req. 5.1.2b]

"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 requirement is intended to avoid short circuiting unprotected power lines from the Power Conversion and Distribution Electronics: either a current protection is available upstream the Actuator Electronics, or it is important that the Actuator Electronics itself is designed in a way that such short circuit is not possible.

[Req. 5.1.2c]

"The system engineering function shall analyse the effect of anomalies in the selection configuration, and use the SELECT statuses information not to start execution of the FIRE command to the nominal or redundant actuator electronics to avoid catastrophic or undesired consequences.

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

The requirement is explained in detail in section 5.5.2.

In the case the firing sequence order of the actuators is not an issue and if several actuators can be fired at the same time without catastrophic consequences (failure case), the system analysis required here can conclude that there is no need to verify at system level the select statuses during the actuation sequence.

Example, the deployment strategy can be to fire nominal and redundant actuation lines sequentially without verifications, resulting in having fired all actuators at the end, the overall system being one failure tolerant to non-actuation.

6.2 Functional source

6.2.1 General

[Req.5.2.1a]

"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 need of three independent safety barriers is explained in section 5.5.

[Req.5.2.1b]

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

The functional testability of each single barrier is required to ensure that the presence of the effective number of barriers as per *[Req.5.2.1a]*, and to avoid possible unexpected events (especially the ones of catastrophic nature like mission loss or human injury) deriving from mistakes in the as designed or as built configuration of the actuator electronics.

[Req.5.2.1c]

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

The main reason for having the fire and selection switch in the hot power line is that otherwise the power line of the actuator itself can fall in short circuit to the ground after it has been actuated, leading to the impossibility to switch off the actuator if the return path is solely open.

The Arm function shall act on the hot power line to effectively act as an effective isolation protection in the direct path from the main bus supply to the actuator power line.

[Req.5.2.1d]

"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."

The requirement intends to specify that no additional command to the actuator electronics is necessary to terminate the firing event.

However, for contingency operations, it is possible to interrupt the FIRE action by sending an OFF command via serial line [Req.5.2.3f].

[Req.5.2.1e]

"Dedicated connectors dedicated to the actuators electronics outputs shall be implemented."

This is a general design requirement aiming to avoid:

- EMC coupling between actuator electrical lines and other lines,
- that single isolation failure between actuator line and other active or power line is leading to failure propagation and unwanted actuation.

[Req.5.2.1f]

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

This requirement requires that the three barriers are in open state at power up of the equipment. In fact in case of one barrier is already in close state at power ON, the three barriers become equivalent functionally to two barriers only. Thus this requirement is essential to have a reliable operation and to guarantee the correct use of the three barriers.

All the barriers states are open at power up of the equipment without system intervention except in case of latching relays are used. In this case, the state of the latching relay is under system responsibility (think about solid state solution…).

[Req.5.2.1g]

"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."

The reason of this requirement is to reduce EMC perturbations (due to equal currents flowing in the hot and in the return line). It does not apply of course for platforms where the structure is used as a common return.

6.2.2 Reliability

[Req.5.2.2a]

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

NOTE Including duplication (nominal and redundant) of all relevant commands and telemetries."

The requirement is self-explaining. The note is key to explain that the redundancy includes also all commands and telemetries, and it is important to read the note in conjunction to *[Req.5.2.3a]*, *[Req.5.2.3c]*, *[Req.5.2.4a]*, such that the overall command chain (at equipment but also at system level) is Single Point Failure Free with respect to the execution of an unwanted FIRE command.

[Req.5.2.2b]

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

This requirement is essential to have a reliable operation of the actuators, nominal or redundant.

The obvious alternative is to keep the nominal and redundant part of the actuator electronics well segregated in individual assemblies (separated PCBs or modules), ensuring that no possible common failure mechanism exists.

For compactness and mass saving reasons, the nominal and redundant part of the actuator electronics can be implemented in the assemblies (PCB or module): in this case the attention to common failure mechanisms becomes of paramount importance and it needs to be scrutinised to the highest level of attention, applying all best practices in terms of double isolation, lack of combined thermal-electrical effects that can jeopardise the nominal to redundant part segregation (like possible explosion of tantalum capacitors), absolute confirmation of the long-term reliability of the common parts (especially PCBs), etc.

It is then necessary that some independent review can ensure the quality of the combined solution, with an assessment of all technologies used down to the highest level of possible visibility.

[Req.5.2.2c]

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

The safety barriers are ARM, FIRE and SELECT functions.

A spurious command, determined for example by a failure in the command line, can activate one of the barriers which is allowed due to the presence of the other barriers.

In the case a single hardware failure of the actuator electronic can lead to enable two of these functions, an additional failure at system level, such as operator error, can lead to fire the actuator firing.

Depending on the way the system has provided the justification with respect to two failures tolerance, this can be not acceptable or can require additional system barrier which are not available in all cases.

Therefore a failure tolerance with respect to actuation of two barrier is requested.

Note that *[Req.5.2.2c]* implies that no single failure in the actuator electronics leads to the permanent connection of a deployment device to the main power bus, even in case of short circuit between positive and return, or structure at actuator device output interface.

A permanent connection of the deployment device can lead to permanent power consumption and dissipation for which the power system is not designed for.

[Req.5.2.2d]

"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."

This set of requirements assures no unwanted actuator activation in case of spurious application of a positive potential to the actuator hot line. This can happen in the actuator electronics, in the connectors or in the harness.

The requirement is mandatory for actuation lines where unwanted firing can have catastrophic consequences, but it is considered sensible to apply it to all cases in order to have consistent, generic products. Figure 5-10, and Figure 5-11 above show configuration that disconnect the return lines either at the SELECT or the ARM function.

In case the return lines cannot be disconnected, requirements *[Req.5.2.2e]* applies.

[Req.5.2.2e]

> *"In case the return lines to the actuators cannot be disconnected as specified in 5.2.2d, then two following conditions shall be met to avoid failure propagation due to loss of insulation:*
>
> *1. The relevant actuator group does not share connectors with other groups or with other electronic functions having source capability to trigger the relevant actuators.*
>
> *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. "*

Those two requirements assure that short circuits in connectors (pin-to-pin, or via connector housing) or a failure of cable isolation do not cause unwanted actuator activation.

For pyro actuators the ECSS Pyro (ECSS-E-ST-33-11) and Electrical Standards (ECSS-E-ST-20) define special measures for pyro lines (EMI safety margin, shielding, isolation and connectors), but this is not the case for non-explosive actuators. This is in order to avoid EMI coupling into pyro wires sufficient to cause explosive actuation.

[Req.5.2.2e.1] is intended to avoid failures in connectors that can cause connection of an actuator hot or return line to a potential sufficient for unwanted actuation. Typical examples of this are pin-to-pin short circuits or pin-housing-pin shorts that can be caused by debris shorting pins, wrong connector mating or bent pins. It has to be noted that even a grounded row of pins separating actuator lines from other potentials cannot be sufficient in case of bent pins that provide potential to the actuator hot line via the connector housing, especially for non-shielded lines where the connector housing is not grounded.

[Req.5.2.2e.2] has the intention to assure sufficient isolation between actuator wires and other potential carrying wires, such that isolation failures cannot short the lines and cause unwanted firing. This can be achieved by separate routing, separate harness bundles (no common clamping), or by shielding of the lines, such that failures in wire isolation only generate shorts to the shielding.

[Req.5.2.2f]

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

For all types of power outlets it is required or at least good design practice to be protected against a short to return or to structure; this also counts for actuator interfaces as it is for some actuators (for example, pyros) even likely to end up shorted to structure while for others it cannot be excluded to happen.

An output short circuit is also likely to happen during AIT process, not necessarily in the actuator device only but also in attached AIT equipment.

[Req.5.2.2g]

"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."

This requirement combined with *[Req.5.1.2a]* ensures the availability of the status of the selected line and the others selection lines belonging to the same group.

The main issue is the unwanted firing of an actuator due to a wrong or faulty selection: to avoid this, the actuator electronics gives the possibility to verify the relevant SELECT statuses and understand the presence of an issue before issuing a FIRE command.

[Req.5.2.2h]

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

The purpose of this requirement is to avoid electrostatic charging and discharging, especially for actuator circuits where both hot and return lines are disconnected by relays, that can otherwise remain floating and can pick-up electrostatic charge. And the bleeding resistors allow a relatively high-ohmic connection to ground, that does not violate the single point grounding concept (preventing ground loops).

In case the actuator return lines are not disconnected by relays, the single point grounding concept prevents electrostatic charge.

See also ECSS-E-ST-33-11, 4.8.2.5b to 4.8.2.5d.

[Req.5.2.2i]

"Insulation among actuator output lines shall be tested."

The insulation among actuator output lines is required to avoid the spurious activation of different actuators; testing at equipment level is required to ensure that no issue of insulation is found later in the satellite development.

[Req.5.2.2j]

"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."

The rationale behind this requirement is to ensure that the any fault does not lead to any failure propagation, especially in the harness and its associated connectors, inside as well as outside of the actuators electronics. With this requirement the complete path of harness and connectors can be sized to sustain any failure mode when the level or duration is controlled.

[Req.5.2.2k]

"No cross-strapping shall be present between electronics of nominal and redundant actuators chains."

To avoid possible catastrophic failures leading to mission loss or human hazards, the nominal and redundant actuators electronic chains are kept separate, with no cross-strapping between them.

See also *[Req.5.2.2b].*

6.2.3 Commands

[Req.5.2.3a]

"Nominal and redundant actuator electronics shall accept commands from both nominal and redundant command chain."

It is important that the actuator electronics accepts commands from both nominal and redundant acquisition chain (at system level) to ensure the relevant commandability irrespective of combined failures in the command circuits of the actuator electronics and in the system level nominal or redundant command acquisition chain.

[Req.5.2.3b]

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

This requirement intends to avoid common failure that can actuate ARM FIRE and SELECT simultaneously. This contributes to the justification of the two failures tolerance with respect to unwanted actuation having catastrophic consequences.

At the end, in flight, all command are sent and managed by the on board software sequence, for example to ensure appendices deployment. It is important that the physical path itself of the command is segregated by using different media not prone to possible common failure; one way to do so, based on the state of the art, is to send arm command through a discrete high power command and select and fire commands through the communication bus.

Refer also to *[Req.5.2.3c]*.

[Req.5.2.3c]

"The 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 enable is driven by high power command while SELECT, FIRE and ARM disable are driven by serial command interface."

This requirement asks for a full separation of the command chain for ARM and for SELECT/FIRE, not only in the Actuator Electronics, but also on the units or unit that provide the relevant commands to the Actuator Electronics.

The issue to be avoided is that the failure of a single chip on the command chain – for example a FPGA – or a common function on the command chain – for example a common power supply for generation of both ARM and of SELECT and FIRE commands – or other can result in an unwanted FIRE action.

[Req.5.2.3d]

"The activation of the ARM switch shall be performed:

1. By direct execution of a dedicated and independent command.

2. Without any other interaction from an actuator electronic function.

NOTE Req. 5.2.3d2 stresses that within the actuator electronics there is no additional logical conditioning of the signal leading to the activation of the ARM switch."

To avoid any chance of spurious actuator firing due to failures or errors in the command chain (at system, subsystem and equipment level), it is important to separate completely the ARM activation from the SELECT and FIRE one, and to make sure that no on board logic is shared for commanding,

supply or protect the command section of the three barriers.
With respect to point 1, the typical implementation of a dedicated and independent command is by a discrete command, but it can be implemented also otherwise.

[Req.5.2.3e]

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

The common choice for commands separation of the three barriers is to transmit SELECT configuration and FIRE commands by (standard) serial line, while ARM is enabled/disabled by dedicated discrete command. *[Req.5.2.3e]* confirms the standard approach to allow the development of recurrent solutions for the actuator electronics.

Note that there is no requirement to use a specific serial command type, it could be any of the ones normally used on spacecraft (MIL-STD-1553, CAN bus, Spacewire or other).

[Req.5.2.3f]

"For long duration actuators, in addition to 5.2.1d, the FIRE OFF commands should be implemented by a standard serial interface."

This requirement is asking for a FIRE OFF command that is needed in case the actuation time for the actuator is variable enough to potentially lead to a negative effect. As an example, this can be the case of a Launch Lock mechanism located in the Instrument perimeter. If this is powered for too long, it can outgas and pollute the Instrument.

In this situation, the only possibility is to command the actuation for the WC long actuation time and, in case of need, leave to the SCSW the option to stop the FIRE based on information available at System level from other TMs. In the example of the Launch Lock mechanism, this can be the temperature TM for the unit.

[Req.5.2.3g]

"The fire commands of the actuator electronics shall be inhibited by dedicated external inhibition straps.

NOTE strap closed = commands disable,
strap open = commands enable."

This requirement identifies an important feature to prevent untimely activation of the actuator lines. A physical strap shall be foreseen to inhibit the execution of a FIRE command. A single strap is enough to cope with the number of Safety barriers, as the second barrier is available in OBC (which also features separation straps).

6.2.4 Telemetry

[Req.5.2.4a]

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

It is important that the telemetries of the actuator electronics are provided to both nominal and redundant acquisition chain (at system level) to ensure the possibility to acquire them correctly irrespective of combined failures in the telemetry circuits of the actuator electronics and in the system level nominal or redundant acquisition chain.

[Req.5.2.4b]

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

This requirement identifies an important feature of the Actuator Electronics, so that to offer the satellite or system operator the information of the actual status of the selection switches, to be used both for nominal confirmation and for detection of failure conditions.

For failure conditions, and also thanks to *[Req.5.2.4c]* and *[Req.5.2.2g]*, the information about the actual status of each selection switch allows the detection of any anomaly in the SELECT block configuration, that can be used by the system to inhibit the FIRE action on that redundant half of the Actuator Electronics if necessary.

This inhibit can prevent that selection switches in incorrect enabled state can deliver the FIRE pulse to other actuator than the one intended.

[Req.5.2.4c]

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

NOTE 1 Effective 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.

NOTE 3 In case a relay is used, spare contacts are used to provide direct status information."

This requirement identifies an important implementation rule of telemetry circuits, so that to guarantee that they indicate correctly the effective (direct) condition of the relevant functionality to the signal output (e.g. if the switch is effectively ON/OFF, if the arming function is ENABLED or DISABLED) to be read out by the satellite Data Handling Subsystem.

The requirement is meant to avoid the occurrence of monitoring signals from intermediate circuit blocks (for example, the output of a status flip-flop) that cannot provide the actual output that that it is important to monitor in case of failure of the circuits or components downstream the intermediate circuit itself (in the example mentioned, a sort circuit failure of the switch that it is important to be commanded by the flip-flop).

It is important to be compliant to this requirement as this sort of information is used during satellite operational phase for determination which actuator e.g. has been selected for firing. False information due to failure in the TM signal "repeater" network can allow satellite operators or on board FDIR logic to understand the exact nature of a failure that can have occurred, and therefore impair or make extremely difficult relevant recovery actions.

In particular, the note to this requirement identifies the need to have an independent status circuitry for non-serial redundant selection switches.

In the note, independent means that all what is needed for monitoring do not share the same resources needed for the activation of the selection switch itself (secondary supply line, common components or features), so that no single failure causes an unwanted status without having the possibility to discover it by telemetry information.

[Req.5.2.4d]

"For short duration actuators, the actuator electronics shall provide a peak firing status which is valid when the monitored firing current is larger than a threshold of 20 % to 80 % of the expected firing current during a period of time greater than 0,5 ms to 10 ms.

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

[Req.5.2.4e]

"For long duration actuators, a current and voltage telemetry shall be provided."

The telemetries for the FIRE block are different depending on the duration of the FIRE pulse.

For actuators characterised by a long duration of the FIRE pulse (e.g. more than 1 second), the telemetries of the FIRE block are the FIRE (output) current and the FIRE (output) voltage (*[Req.5.2.4e]*).

For actuators characterised by a short duration of the FIRE pulse (e.g. less than 1 second), the telemetry of the FIRE block is a peak FIRE status, providing a flag identifying if the monitored fired current was larger than a given threshold of the expected firing current during a period of time greater than a given fraction of the expected FIRE pulse duration (*[Req.5.2.4d]*).

The reason for the different implementation for long and short FIRE duration cases depends on the need to simplify the electronics for short pulses: the recording of the FIRE event voltage and current with the due time resolution can require memory storage capabilities, fast current and voltage acquisition circuits, etc.

It is considered that such effort does not make sense in general for recurrent actuator electronics products: for generic products, the peak FIRE status approach seems more than adequate to have a confirmation of a successful FIRE pulse being transferred to the relevant actuator.

In particular, the peak firing status telemetry current and time ranges (respectively 20 % to 80 % of the expected firing current and during a period of time greater than 0,5 ms to 10 ms) are defined for facilitating the relevant product development: on the specific application, the precise values will be specified within the applicable range and achieved by trimming at equipment level.

Note that *[Req.5.2.4d]* requires the identification of a correct firing of the pulse before the relevant actuator can go to open circuit (otherwise the telemetry cannot indicate a correct fire event). The open circuit is a common outcome of the actuation of pyro explosive devices, or other actuators based on fuses operation (some NEA for example).

[Req.5.2.4f]

"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."

[Req.5.2.4g]

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

Observability of the inhibition strap status (*[Req.5.2.4f]*) is needed by on board software to confirm deployment chain status after satellite separation.

In addition, when the strap are fit (or removed) on ground, there is a need for on ground AIT personnel to check that the complete end to end line (strap – harness – internal PCDU lines) is actually inhibiting (or not) the firing block (*[Req.5.2.4g]*). This allows a verification while the satellite being OFF.

[Req.5.2.4h]

> *"One status telemetry shall be provided for the nominal inhibition strap, and another for the redundant one."*

Considering that the actuator electronics is duplicated in a nominal and a redundant section *[Req.5.2.2a]* and also that inhibition straps are provided for the fire commands *[Req.5.2.3g]*, the observability of the inhibition straps related to nominal section and also to redundant section is provided.

[Req.5.2.4i]

> *"A short circuit between the output of the actuator electronics and the ground or structure shall not affect the validity of the telemetry of the actuated line."*

Essentially for explosive pyrotechnic lines supply, it is possible that the actuation results temporarily or definitively in short circuit to ground; it is important that this does not lead to a wrong reading of the telemetry.

[Req.5.2.4j]

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

The overvoltage and the overcurrent is detected during the firing based upon the threshold specified by *[Req.5.5.2a]* and by *[Req.5.5.2b]*. It is recommended that the detection status telemetry is implemented and is provided via serial telemetry line.

In case of repetitive firing, the reset of the status is done by serial command.

The threshold for the status telemetry is set between the maximum nominal current or voltage, and the maximum allowable fault current or voltage emission.

[Req.5.2.4k]

> *"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."*

To allow the observability of this abnormal behaviour even after the firing or after disappearance of the abnormal conditions, this status is based on a latch. The latch is resettable via serial command in order to allow other firing actions under monitoring an eventual abnormal conditions.

6.3 Functional load

6.3.1 General

[Req.5.3.1a]

"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."

[Req.5.3.1c]

"The minimum all fire actuation time shall be specified."

To ensure the activation of current-driver actuator, it is important that the actuator electronic provides a current higher than all fire current for duration higher than a minimum time, all these values being specified by the actuator supplier.

In addition, in order to ensure a proper functioning of the actuator, it is needed to specify a maximum current to be applied to the actuator.

It is important that no fire current is specified, below which no actuation is guaranteed, providing that the duration is lower than the one specified.

[Req.5.3.1b]

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

[Req.5.3.1c]

"The minimum all fire actuation time shall be specified."

To ensure the activation of voltage-driver actuator, the actuator electronic shall provide a voltage within a given voltage range for duration higher than a minimum time, all these values being specified by the actuator supplier.

6.3.2 Reliability

[Req.5.3.2a]

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

The requirement is important to ensure that no common failure mechanism (of electrical, thermal, mechanical or combined nature) can result in the loss of the desired actuation in spite of the split of the electrical actuator path in nominal and redundant side.

For example, it is important that the mechanical configuration of a thermal knife or of a non-explosive actuator is such that either nominal (redundant) actuation is ensured even when a failure appears on the redundant (nominal) side, such that the electrical parameters (voltage, current) are not in their nominal range.

[Req.5.3.2b]

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

NOTE See actual limit specified in requirements 5.5.2a and 5.5.2b."

As the upstream actuator electronics can fail and provide up to twice of nominal maximum current or voltage up to the one applied at the input of the actuator electronics itself, the actuator design shall ensure no propagation to the redundant actuator function in such case. See also *[Req.5.5.2a]* and *[Req.5.5.2b]*.

6.4 Performance general

6.4.1 General

[Req.5.4.1a]

> *"For current-driven actuators, one of the following two conditions shall be met:*
>
> *1. 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.*
>
> *2. Otherwise, the system ensures that the minimum current and voltage as qualified is applied at actuator level."*

The typical situation for current-driven actuators (Pyros, NEA, etc.), is that the actuator resistance is defined by the manufacturer in non-operative mode and at ambient conditions. The actuator resistance cannot have been characterised during operation (actuation) and in temperature.

Such resistance, if added to the harness resistance and multiplied by the minimum activation current to be guaranteed by the actuator electronics, can result into a voltage higher than the one the actuator electronics can provide, with the result that the worst case current can be lower than specified, with the risk of not being able to get an effective actuation.

Hence the requirement identified above (together with the "companion" requirements performance, source *[Req.5.5.1b]* and performance, load *[Req.5.6.1a]* and *[Req.5.6.1b]*).

It is necessary to check the power interface to the actuator to identify if the actuator electronics can indeed provide the required (minimum) actuation current for a voltage at the interface (actuator electronic output) equal to the following product:

- (minimum) actuation current x (max operative actuator resistance + relevant max harness resistance).

Example

Let us imagine that an actuator electronic output (line i) has the {V,I} characteristic shown in Figure 6-1 (it can be a typical case of a current actuator for pyros based on a FIRE linear regulator).

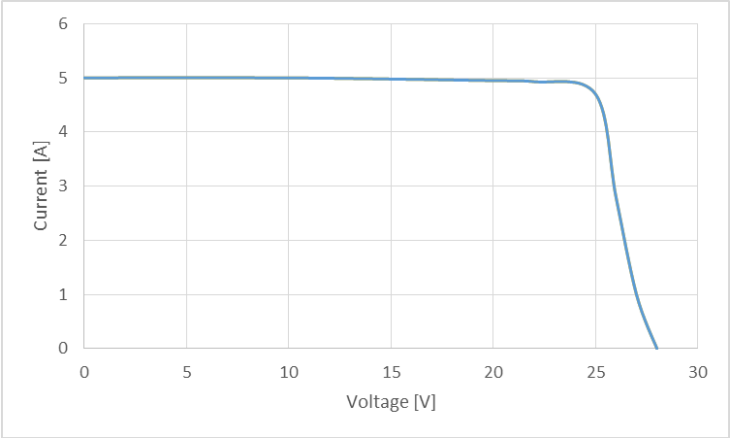


Figure 6-1: Actuator electronics {V, I} characteristic

Let us assume the two cases shown in Figure 6-2 and in Figure 6-3.

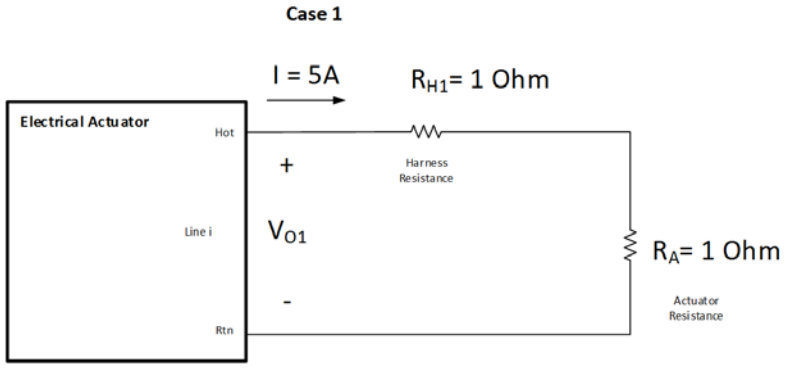


Figure 6-2: Example - case 1

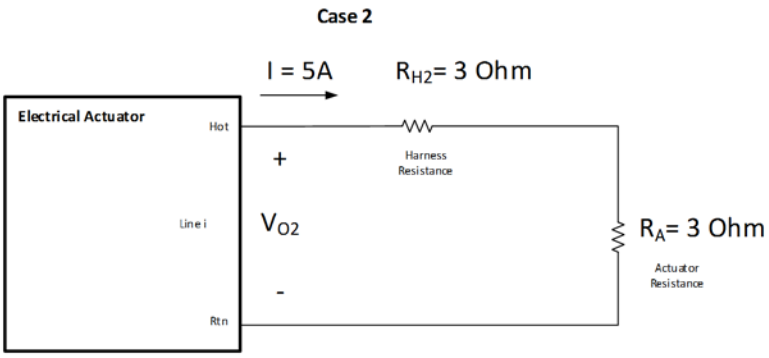


Figure 6-3: Example - case 2

In case 1, the voltage VO1 developed at the electronic actuator output interface is low enough (10 V) to guarantee that the current drive is at the specified value (5 A).

In case 2, the voltage VO1 developed at the electronic actuator output interface is such that the current driven is below the specified one (it is about 4,2 A, below the specified value of 5 A).

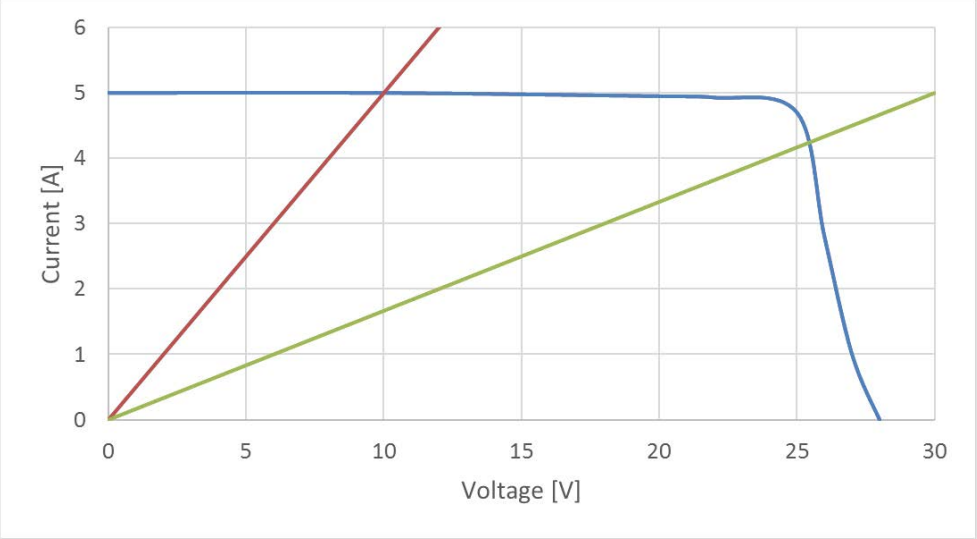


Figure 6-4: Example - case 1 and 2

In case the actuator resistance, within the full temperature and operation range is not known, *[Req. 5.4.1a]* gives another solution, e.g. to ensure that the minimum current and voltage as qualified is applied at actuator level: this can require to the system integrator an analysis to confirm that the minimum voltage and current at actuator interface respect the limits of actuator qualification as per *[Req. 5.6.1b]*, taking into account of the actuators electronic capability obtained thanks to the requirement performance, source *[Req.5.5.1b]*.

[Req.5.4.1b]

"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."

For voltage-driven actuators, the presence of the harness resistance degrades the accuracy of the voltage appearing at the actuator side, when considering the current flowing during the actuation event. The system responsible needs therefore to ensure that the harness resistance is within a maximum limit.

[Req.5.4.1c]

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

[Req.5.4.1d]

"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."*

To avoid bus perturbations during the firing and after the Pyro blowing, it is important that the Pyro devices including harness are characterized by:

a. a parasitic inductance lower than 10 µH (for current-driven actuators) and 20mH (for voltage driven actuators);

b. a parasitic capacitance (to the structure) lower than 1uF.

[Req.5.4.1e]

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

Taking account the requirement 5.5.4e where the firing current shall be limited to 2,5 A during the start-up, it is important that the full current timing profile for voltage-driven actuators are provided in order to optimise the firing circuit implementation (design and analyses).

6.5 Performance source

6.5.1 Overview

Note that a number of recommendations are given in this clause of the standard (e.g. in form of "should" requirements).

The idea is on one side to promote the development of recurrent actuators electronics able to supply a wide range of actuators, and on the other to give standard, reference interface definition for future actuators development.

In particular, consider the following requirements:

[Req.5.5.4a]

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

[Req.5.5.4b]

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

NOTE Specific current capability is trimmed in production"

[Req.5.5.4c]

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

NOTE Specific current pulse duration is trimmed in production"

[Req.5.5.4d]

"For voltage-driven actuators, the actuator electronics should supply a voltage with an initial set point selectable from 19 V to 21V, and with an overall accuracy of ±1 V, providing the current is lower than the limit defined in requirement 5.5.4e.

NOTE Specific voltage capability is trimmed in production."

[Req.5.5.4e]

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

[Req.5.5.4f]

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

[Req.5.5.4g]

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

The objective of these requirements is an attempt to standardise the actuator electrical interface in view of power electronic reuse for universal usage. These requirements are worded with "should" as

far as it cannot be prevented that an actuator supplier will propose a specific interface; also, specific application can be needed and can require bespoke development.

The proposed standardisation aims to answer the need of most of actuators, trying to find the most common performances, and excluding the extreme cases that can oversize the actuator electronics. The state of the art of actuators is given in Actuators database, Annex A.

Two categories can be identified and are reflected in this standard:

a. voltage driven actuators: these actuators are generally composed of heating systems, such as thermal knives, shape memory alloy, paraffin, that require a voltage to be applied during a "long" duration, higher than seconds.

b. current driven actuators: these actuators are generally composed of fusing elements that is blown with current during a short period (tens of milliseconds)

Other actuators, based on magnetic actuation for example, can be used in one or the other way, with intermediate duration.

The power sizing of actuator electronic is driven by "long" duration actuation, higher than seconds, which is considered a DC steady state power. The actuator table suggests that 50W covers most of the application.

This gives an envelope of heating capability to be used by actuator supplier for their design.

It is important that the nominal initial set point of the actuation voltage can be selected between 19 V and 21 V, considering that 21 V correspond to a voltage value just below typical unregulated bus voltage (22 V minimum). Heaters, part of the actuator, can be adjusted to perform with such voltage.

The ±1 V accuracy requested to the actuation voltage (*[Req.5.5.4d]*) covers temperature, radiation and ageing effects.

It is important that the actuator electronic current is limited to avoid excessive dissipation above the 50 W sizing and to avoid trip off in case the actuator inrush exceeds the actuator electronic capability.

The current capability of actuation electronics, for current driven actuator has to be considered in transient, typically up to several tens of milliseconds. The maximal current value adequate to fire equipment listed in the actuation table is 6 A.

Trimming (for firing voltage, current and duration) shall be understood as a capability to configure the actuator electronics hardware before the manufacturing of the unit, in order to cope with the desired actuator specification. Note that several types of actuators can be used on a given mission, to release different appendices and passivate different items.

6.5.2 General

[Req.5.5.1a]

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

This requirement identifies the need to verify the maximum and minimum current deliverable to an actuator (nominal operation). It is not the maximum (or minimum) fault current that can be provided after a failure.

The check of the maximum nominal current is necessary because an excessive current can impair the functionality of the actuator itself: for example, the current into the filament of a pyro device can be interrupted in open circuit before igniting the explosive, resulting in missed actuation.

[Req.5.5.1b]

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

For current-driven actuators, if the actuator plus the harness resistance is too high, it cannot possible to transfer enough power to the actuator itself during firing event.

In other words it is necessary to define the maximum voltage at the output of the actuator electronics when the delivered current is still within the specified range.

Typically, if the voltage at the actuator electronics exceeds a given value, the relevant power regulator saturates and is not able to guarantee the delivered current to be over the specified minimum limit.

See also the explanation of *[Req.5.4.1a]*.

[Req.5.5.1c]

"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."

A margin is added by the system on the actuation current depending on the knowledge and available data of the actuator firing conditions (voltage, current, impedance, firing probability).

This margin intends to increase the actuation event probability, while keeping the actuation current within the specified limit (maximal actuator current as specified in *[Req.5.3.1a.2]*).

As a practical example based on state of the art, for an explosive pyrotechnic actuator where all fire current is specified at 3,5 A, the system will set the actuator electronic current to 5 A, giving a margin of 1,5 A.

[Req.5.5.1d]

"Any monitor current in an actuator system fire line shall be limited to 5 mA."

A way to detect the presence and actual selection of actuator device is to let the drive function inject a low current into the selector function and by TM monitor the resulting voltage at drive output.

This injected current is with very good margin lower than the manufacturer specified no-fire current. In practical actuator drive designs an injected current of few mA is sufficient for detection and monitoring which is lower than one tenth of no-fire of current applied actuators.

[Req.5.5.1e]

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

The leakage current is set to 5mA to allow the implementation of clever circuits to identify if selection switches are abnormally in ON state (due to any failure).

Normally currents lower than 5 mA can be conveniently used to have such information, and on the other side the no fire current for all types of actuators normally used at present in Europe is much higher than 5mA.

To ensure consistent specification of actuators, the no fire current has been specified to be at least 50mA in performance, load *[Req.5.6.1c]*.

[Req.5.5.1f]

> *"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."*

This requirement is to ensure that the actual leakage current is far below no-fire current level of any available actuators (to check the performance aspect relevant to functional *[Req.5.2.2i]*).

It is important that it acceptance testing of the drive function foresees the check of the actual leakage current to ensure that it is safely under the specified limit: the check is made systematically for all lines.

[Req.5.5.1f] identifies a convenient way to check reciprocal insulation among actuators output lines: note that it does not necessarily require to measure directly a current, but for example the voltage appearing across an external resistor to the select circuit or to an internal one.

6.5.3 Reliability

[Req.5.5.2a]

> *"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."*

This requirement gives a maximum envelope to the voltage that can appear at the output of the actuator electronics after a failure or when the actuator ends up in an open circuit (typical case for a pyro device).

Performance, load *[Req.5.6.2a]* ensures consistence of the actuator interface with *[Req.5.5.2a]*.

[Req.5.5.2b]

> *"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."*

To avoid failure propagations, and to avoid stress on any element in series with the actuator (switches, sense resistors, PCB tracks, wires, harness, connector contacts), that can be used to fire other actuator lines, it is necessary to limit the maximum fault current emission from the actuator electronics to the actuator.

This current limit has been conveniently set to 2 times the maximum nominal specified value to give the possibility of implementing simple design solutions in the actuator electronics on one side (like additional indefinite current limitation or removal of current after a given time duration in case of fault current emission), and on the other to ensure limited stress conditions to all series elements.

Note that the current limit is set to 2 times the actual maximum (nominal) current after trimming by the equipment manufacturer.

The important rationale behind this requirement is to ensure that the fault emission current or voltage does not lead to any failure propagation, especially in the harness and its associated connectors, inside as well as outside of the actuator electronics. With this requirement the complete path of harness and connectors can be sized to sustain such failure mode when the level is controlled.

6.5.4 Telemetry

[Req.5.5.3a]

> *"For long duration actuators, the current and voltage telemetries should be provided with 8 Hz sample rate or higher."*

For long duration actuators, the knowledge of the current (for voltage driven actuator) or the voltage (for current driven actuator) are needed for the observability of the firing event.

8 Hz is a typical sampling rate for such telemetry and is enough to assess transient event and understand the physics behind this kind of actuators (for example the evolution of the actuator resistance for a heating device).

[Req.5.5.3b]

"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."

It shall be possible to detect if the actuation has been terminated due to an overcurrent or overvoltage generation.

Even though actuation has been terminated, the actuation can have occurred, especially in current driven actuators. This requirement ensures that it will be visible in telemetry to the operator that the regulator is not working correct, such that it can be decided to switch to the redundant actuator electronics.

The reason to set the detection limit to maximum 50% is to have margin to the 100% limit specified in *[Req.5.5.2b]*.

6.5.5 Recurrent products

[Req.5.5.4a]

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

The particular rationale behind this requirement is the following:

A generic drive can be designed as a dc/dc converter able to act in two modes:

- Current limited voltage source for voltage driven actuators
- Voltage limited current source for current driven actuators.

A generic driver able to deliver up to 20 volt for voltage driven actuators and up to 5 ampere for current driven actuators is expected to cover the actual available and today applied actuators.

For voltage driven actuators a current capability of 2,5 A is needed, which will demand 20V x 2,5A = 50 watt.

For current driven actuators the necessary available voltage is determined by the resistance of the actuator plus the spacecraft harness. Available data shows that a total of two ohms (one ohm for device, one ohm for harness) comprises actual designs. The generator therefor is required to deliver $5A^2 \times 2\Omega = 50$ watt.

[Req.5.5.4b]

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

NOTE Specific current capability is trimmed in production."

The requirement is explained at the beginning of section 6.5.

[Req.5.5.4c]

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

NOTE Specific current pulse duration is trimmed in production."

The requirement is explained at the beginning of section 6.5.

[Req.5.5.4d]

"For voltage-driven actuators, the actuator electronics should supply a voltage with an initial set point selectable from 19 V to 21V, and with an overall accuracy of ±1 V, providing the current is lower than the limit defined in requirement 5.5.4e.

NOTE Specific voltage capability is trimmed in production."

The requirement is explained at the beginning of section 6.5.

[Req.5.5.4e]

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

From evaluation of the voltage driven actuators presently used in Europe (see Annex A), it results that a current limit of 2,5 A is sufficient to power them correctly.

In case the actuator internal resistance at low temperature can draw higher current than the limit (when the nominal activation voltage range is applied), the only result can be that the heating up phase of the actuator thermal head will last slightly longer than with the current limit applied.

[Req.5.5.4f]

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

Although voltage driven actuators typically do not need the drive active for more than approximately one minute, it is important that the drive circuit is able to operate continuous because in this way the actuation can be repeated with no limitations.

[Req.5.5.4g]

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

This requirement is needed to have a quasi-simultaneous activation of more actuators (for example, to address the hold down and release mechanisms of a large solar array).

6.6 Performance load

6.6.1 General

[Req.5.6.1a]

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

This requirement corresponds to the case where we have the knowledge of the actuator resistance, otherwise *[Req.5.6.1b]* applies.

For an extensive explanation, see *[Req.5.4.1a]*.

[Req.5.6.1b]

"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."

This requirement applies if the actuator resistance in the operative conditions range, including temperature, is not known.

Note that if neither *[Req.5.6.1a]* nor *[Req.5.6.1b]* can be complied, it is considered necessary to get information either on the actuator resistance, or on the minimum voltage and current able to guarantee the firing event, with a sufficient probability and confidence level on a representative sample of the actuators.

For an extensive explanation, see *[Req.5.4.1a]*.

[Req.5.6.1c]

"No-fire current shall be greater than 50 mA."

The no fire current limit is specified to be consistent with the relevant source specification, see *[Req.5.5.1d]*, *[Req.5.5.1e]* and *[Req.5.5.1f]*, with a reasonable margin.

6.6.2 Reliability

[Req.5.6.2a]

"It shall be possible to apply to the nominal, 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 nominal, actuator.

NOTE See assumption in clause 4.1g."

This requirement is formulated to provide consistency with performance, source *[Req.5.5.2a]*.

For the present known type of actuators compliance to this requirement is not critical: the nominal (redundant) actuator can be provided with voltages in (reasonable) excess of the nominal range, and possibly be damaged by this event, but the redundant (nominal) actuator is not affected.

6.6.3 Recurrent products

[Req.5.6.3a]

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

[Req.5.6.3b]

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

All fire current is compatible with the source capability as defined *[Req.5.5.4b]* and *[Req.5.5.4c]*.

[Req.5.6.3c]

"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."

All fire action is compatible with the source capability as defined in *[Req.5.5.4d]* and *[Req.5.5.4e]*, accounting a margin for harness voltage drop.

[Req.5.6.3d]

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

[Req.5.6.3e]

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

[Req.5.6.3f]

"The maximum capacitance of actuators should be 1 μF."

This requirements are specified according to the assumptions made in section 5.2.

Annex A
Actuators database

While preparing this handbook a research was made about possible actuators available on the market. The information contained in the Table A-1, Table A-2, Table A-3 of this Annex is not exhaustive, and it has been produced at the time the present handbook has been drafted.

Therefore there is no guarantee that such information is up-to-date, including the provided web links to the relevant manufacturers.

Table A-1: Current driven, non-explosive actuators

Type / Feature	Non Explosive Actuator 1,2,3,4	Non Explosive Actuator 5	Non Explosive Actuator 6	Non Explosive Actuator 7	Non Explosive Actuator 8	Non Explosive Actuator 9	Non Explosive Actuator 10	Pin Puller 1,2	Pin Puller 3,4	Split spool Non Explosive Actuator	Hold down and release mechanism 1	Battery bypass Actuator 1,2,3	Non-Pyrotechnic Valve
Minimum actuation current (A)	4	3,5	3,5	4,5	3,5	3,5	3,5	4,1	2,8-3,2	4,5	3,5	4	2
Minimum actuation current (All fire current) (A)													
Nominal firing current (A)													
Maximum firing current (A)		6,5	6,5	6,5	6,5	6,5	6,5						
Maximum firing current duration (ms)		250	250	250	250	250	250						
Maximum actuation duration (ms)	25							2200	3500-4000	25	45-100	25	30
Nominal firing duration (ms)													
Minimum actuation duration (ms)		40	40	30	40	40	40						
Maximum actuation duration (Functioning time)													
No fire current 1 (A)	0,25	0,25	0,6	0,4	0,5	0,5	0,25			0,6		0,5	
No fire current condition 1		ambient	ambient	ambient	ambient	ambient	ambient						
No fire current 2 (A)		0,25	0,6	0,4	0,4	0,4	0,25						
No fire current condition 2		vacuum	vacuum	vacuum	vacuum	vacuum	vacuum						
No fire power (W)													
No fire duration (s)	infinite	300	300	300	300	300	300					infinite	
Number of bridgewire													
Min resistance (Ω)	1,2						1,1-1,7 +10%		11-12 +10%	1		0,95	
Max resistance (Ω)	2	2	2	2	2	2	2					1,6	

Type / Feature	Non Explosive Actuator 1,2,3,4	Non Explosive Actuator 5	Non Explosive Actuator 6	Non Explosive Actuator 7	Non Explosive Actuator 8	Non Explosive Actuator 9	Non Explosive Actuator 10	Pin Puller 1,2	Pin Puller 3,4	Split spool Non Explosive Actuator	Hold down and release mechanism 1	Battery bypass Actuator 1,2,3	Non-Pyrotechnic Valve
R conditions	25°C	ambient	ambient	ambient	ambient	ambient	ambient	23°C	23°C			25°C	
Isolation with ground (MΩ)										1-5			
Test voltage for isolation (V)													
Min insulation resistance (MΩ)													
NEA 1 to 10, Battery Bypass actuator 1 to 3, Non pyrotechnic valve: see www.neaelectronics.com/products Pin Puller 1 to 4: see www.arquimea.com/?q=products-services/9 Split spool NEA: see http://www.cooperindustries.com/content/public/en/wiring_devices/interconnect/products/non_explosive_actuator1.html HDRM 1: see https://cdn.glenair.com/catalogs/hold_down_release_mechanism_technology.pdf													

Table A-2: Current driven, explosive actuators

Type / Feature	Pyro element 1	Pyro element 2	Pyro element 3	Pyro element 4	Pyro cable cutter 1	Pyro assembly 1	Pyro assembly 2	Pyro assembly 3	Pyro valve 1	Pyro valve 2	Pyro valve 3	Pyro valve 4
Minimum actuation current (A)	4,1	5	5		5							
Minimum actuation current (All fire current) (A)		3,1	3,1		3,5	> 3,5A / 40ms	3,5A	3,5A		> 3,5A / 40ms		
Nominal firing current (A)		≥5	≥5		>5	5	5		4,5	4,1 to 5		
Maximum firing current (A)												
Maximum firing current duration (ms)												
Maximum actuation duration (ms)	15	10	10		4							
Nominal firing duration (ms)						10	4		10			
Minimum actuation duration (ms)												
Maximum actuation duration (Functioning time)						< 5ms	< 2ms / 5A	< 6ms / 3,5A min		15 to 10		
No fire current 1 (A)	1	1	1	1	1	1	1	1				
No fire current condition 1												
No fire current 2 (A)												
No fire current condition 2												
No fire power (W)						1	1	1				
No fire duration (s)	300	300	300	300	300	300	300	300	5ms	5		
Number of bridgewire						1	1	1				
Min resistance (Ω)	0,9	0,9	0,9		0,95	0,9	0,95	0,95	0,95	0,9		
Max resistance (Ω)	1,2	1,2	1,2		1,15	1,2	1,15	1,15	1,15	1,2		
R conditions					no info							
Isolation with ground (MΩ)	100	2	100	5	1000							
Test voltage for isolation (V)	500	250		500	500	500	250	500		500		
Min insulation resistance (MΩ)						100	1000	50		>100		
Pyro element 1, Pyro assembly 1: see www.dassault-aviation.com/en/space/pyrotechnics-catalogue/ Pyro element 2,3, Pyro assembly 2: see www.ariane.group/en/about-us/subsidiaries-and-affiliates/pyroalliance/												

Table A-3: Voltage driven actuators

Type / Feature	Thermal knife 1	Thermal knife 2	Thermal knife 3	Thermal knife 4	Thermal knife 5	Thermal knife 6	Low shock release unit	Release Unit	Hold down and release 1	Frangibolt 1	Frangibolt 2
Minimum actuation voltage (V)	19	tbd	tbd	tbd	tbd	tbd	20,2	18,5	6	28	18,5
Typical actuation voltage (V)	20,25	20	28	35	50	100	21,3				
Maximum actuation voltage (V)	21,5	tbd	tbd	tbd	tbd	tbd	22,4	21,5	20		21.5
Maximum actuation duration (s)	120	120	120	120	120	120	23	0,025			145
Typical actuation duration (s)	30	60	60	60	60	60	22				
Operating current (A)	< 0,8	< 1	< 1	< 1	< 1	< 1	0,7A to 2,07 A	2,5		1,75-5,0	0,88 at 18,5V
Maximum inrush current (A)	4,03	tbd	tbd	tbd	tbd	tbd					
No fire current (A)	n/a	n/a	n/a	n/a	n/a	n/a		0,25			
Min resistance (Ω)	7,5	tbd	tbd	tbd	tbd	tbd	14,8		1,4+10%		19
Max resistance (Ω)	8,1	tbd	tbd	tbd	tbd	tbd	35		24+10%		23
R conditions	25°C	25°C	25°C	25°C	25°C	25°C	min at -40°C, max at +40°C				20°C
Isolation with ground (MΩ)	2	100	100	100	100	100	100				
Test voltage for isolation (V)	10	500	500	500	500	500	250				

Thermal knife 1 to 6: see www.airbusdefenceandspacenetherlands.nl/activities/others/

HDRM 1: see www.arquimea.com/?q=products-services/9

Frangibolt 1,2: see tiniaerospace.com/products/

Annex B
Extract from CSG-NT-SBU-16687-CNES

B.1 EXTRACT from CSG-NT-SBU-16687-CNES Ed/Rev 01/01

3.1. CLASSES OF RISKS RELATIVE TO ACTIVITIES ON THE GROUND

The satellite customer, for each risk-related activity it intends to perform on the ground:

✍ identifies and assesses the risks according to two categories defined by the severity of the potential damage:

Risk classes	*Definition of damage*
Risk of catastrophic consequences	**Loss of human life, immediately or later** **Permanent disability** **Irreversible harm to public health**
Risk of serious consequences	**Serious injury to people not leading to loss of human life, nor to permanent disability** **Reversible harm to public health** **Significant damage to property**: total or partial destruction of public or private property total or partial destruction of a critical facility for the launch operation **Significant damage to the environment**

…

3.2. REQUIREMENTS RELATIVE TO ACTIVITIES ON THE GROUND

Any risk-related system identified and implemented in the framework of ground activities must meet a reliability goal that is clearly identified and compatible with the qualitative and quantitative requirements below. This goal of reliability must explicitly contribute to the safety of people or property, public health and the environment.

The demonstration that the goal of reliability has been met must take into account the aspects related to the equipment and their implementation, and can be based on recognised dependability rules and methods.

Qualitative requirements:

1. For any risk-related activity performed inside the perimeter of the CSG or from the CSG, space systems, safety systems, integrated launcher stages and corresponding GROUND systems must meet the following requirements:

- activity implying risks with serious consequences: Single point of failure criterion

No failure (either simple equipment failure or human error) must generate a risk of serious or *a fortiori* catastrophic consequences (referred to as "Fail Safe" or FS).

However, there is no obligation to comply with the single point of failure criterion for the structural elements of a payload if this is not possible under acceptable economic conditions, given the state of knowledge and current practices and the vulnerability of the environment in which the payload is likely to be placed.

- activity implying risks with catastrophic consequences: double point of failure criterion

No combination of two failures (equipment failure or human error) must generate a risk of catastrophic consequence (referred to as FS/FS or FO/FS).

This double point of failure criterion does not apply in the case of two human errors.

2. The above-mentioned quality requirements do not apply to structural elements, which are designed in compliance with standards and according to appropriate engineering methods, in order to ensure an equivalent level of safety. These standards and methods are laid down in a regulatory statement issued by the CEO of CNES.

Quantitative requirements:

For any activity with a risk of catastrophic consequences carried out inside the perimeter of the CSG, the maximum acceptable probability of there being at least one victim (collective risk), taken into account for the sizing of launch systems, test benches and the corresponding technical equipment, is 10-6 per campaign for the preparation of a launch or test.