

UTN-FRC

TECOM 2023

CONSIDERACIONES PARA EL DISEÑO DE LA AVIONICA DE UN SATELITE

Daniel Caruso

Contenidos

◆ Introducción

◆ Entornos

- Terrestre - Lanzamiento - De la Tierra - Solar - Espacial

◆ Aviónica

- TT&C - C&DH - Almacenamiento a bordo - Generación de Potencia - Control de Actitud - Propulsión

◆ Electrónica de Vuelo

- Características particulares - Márgenes - Partes EEE - Mitigación de riesgos asociados a las partes EEE -

◆ Diseño Confiable

◆ Sistema Tolerante y Sistema Autónomo de Protección frente a Fallas

Introducción

- Si bien un vehículo espacial se diseña para que pueda sobrevivir en las condiciones extremas del ambiente espacial, existen otros ambientes (Entornos) por los que ese vehículo pasará durante el ciclo de desarrollo del proyecto que deben considerarse. Es así necesario conocer la naturaleza de las condiciones en cada entorno a fin de evitar fallas en órbita.
- El espacio se caracteriza por
 - un alto vacío (aunque no total)
 - una muy baja (pero no nula) resultante de las fuerzas másicas
 - posibles aceleraciones no gravitatorias intermitentes o impulsivas
 - radiación ionizante
 - fuentes y sumideros extremos de radiación térmica, gradientes térmicos considerables
 - micro meteoritos y restos "basura" espaciales.

Entornos

TERRESTRE

Temperatura - Humedad - Limpieza - Contaminación controladas
Solo adhesivos y lubricantes especiales
~~Gadmio Zinc Magnesio Plásticos~~
Transporte y “handling” controlados - Uso de “savers”

LANZAMIENTO

Excitaciones mecánicas - cargas cuasiestáticas, aleatorias, sinusoidales, acústicas y de shock
Despresurización rápida - Compatibilidad electromagnética
Ambiente radioeléctrico hostil en la base de lanzamiento

SOLAR

Drag función de la altitud y de la actividad solar
Densidad de flujo 3 veces mayor (1400 vs 500 w/m²)
Sin medidas especiales t° del material entre -270°C y + 130°C
Radiación UV provoca la polimerización de moléculas orgánicas

De la TIERRA

Atmósfera (capas con diferente densidad, composición de gases y distintas temperaturas) - No esfericidad de la Tierra
Campo Magnético Terrestre
Anomalía Sudamericana y Cinturones de Van Allen

ESPACIAL

Hostil: Extremos de temperatura - Vacío (no hay convección; soldaduras requieren plomo) - Radiación TID y SEU/SEL - Oxígeno molecular - Meteoritos y micro meteoritos
A favor: viento - vapor de agua - limpieza - gravedad efectiva 0

Aviónica

Aviónica

- Subsistemas electrónicos utilizados en aviones, satélites y vehículos lanzadores
- Según wikipedia “avionic systems include communications, navigation, the display and management of multiple systems, and the hundreds of systems that are fitted to aircraft to perform individual functions”
- El alcance de lo que incluye depende de la definición y de los objetivos de la misión en la que aplique el satélite a cuya aviónica se refiere
 - Subsistema de Comunicaciones —> TT&C y otro tipo de comunicaciones
 - Subsistema de Manejo de Datos —> C&DH / OBDH
 - Almacenamiento de datos a bordo
 - Subsistema de Potencia —> Generación, Almacenamiento de Energía, Electrónica de Regulación y de Distribución
 - Subsistema de Control de Actitud —> electrónica asociada a sensores/actuadores/ctrl
 - Subsistema de Control de Orbita —> electrónica asociada

Subsistema TT&C

- ★ TT&C —> Telemetry, Tracking and Control
- ★ Su objetivo primario es proporcionar los canales de comunicaciones, uno ascendente (TC) y otro descendente (TM), para el control y el conocimiento del estado de todas las unidades funcionales del satélite
- ★ Se implementa generalmente con redundancia funcional, es decir contar con “camino” redundantes para satisfacer las dos funciones.
- ★ Funciones:
 - ✓ Recepción y Detección de Comandos
 - ✓ Modulación y Transmisión de la Telemetría (de Housekeeping)
 - ✓ Tracking de portadora – Seguimiento del satélite por parte de una estación terrestre
 - ✓ Facilitar la detección y medición de la portadora en tierra
 - ✓ La variación de la frecuencia de portadora por el efecto Doppler proporciona el rango con baja precisión
 - ✓ La medición de retardos entre subida-bajada permite determinar rango con mayor precisión (distancia). Si se cuenta con un transponder, que no introduce variaciones de fase entre la recepción-demodulación-modulación-transmisión.
 - ✓ Los ángulos de acimut y elevación de la antena de tierra, cuando se encuentra en modo auto-track, también permite determinar la ubicación angular del satélite

Subsistema C&DH / OBDH

- ★ C&DH → Command and Data Handling // OBDH → On Board Data Handling
- ★ Objetivo primario:
 - ✓ Recepción (a nivel digital), validación, decodificación y ejecución y/o distribución de comandos, ya sea de tiempo real o diferido (time-tagged)
 - ✓ Recolección, procesamiento y formateo de la telemetría de ingeniería (housekeeping) del satélite
 - ✓ Generación/distribución de las señales de sincronismo a bordo – Gestión del tiempo a bordo [OBT]
 - ✓ Ejecuta la secuencia de operaciones de misión según la secuencia de comandos almacenados (time-tagged) o de los automatismos definidos
 - ✓ Es uno de los S/S responsables del mantenimiento de la autonomía del satélite a través de la detección de fallas y generación de las acciones/comandos de mitigación o recuperación frente a esas fallas

Subsistema C&DH / OBDH - Automatismos / Detección de fallas y generaron de acciones correctivas - Uno de los ejemplos en SAC-D/Aquarius

Si luego del reset, C&DH detectara que el satélite se encuentra acoplado al lanzador y confirmara además este hecho por el estado inactivo de un flag llamado “omitir secuencia inicial” (es decir, si la lógica de votación indicara acoplamiento y además el flag “omitir secuencia inicial” se encontrara inactivo), realizará las siguientes acciones:

- Relevar, en base a la lectura de las TMYs de cada equipo, el estado actual del sistema y comenzar las tareas de supervisión conforme a ello.
- Rechazar todo comando relacionado con acciones de despliegue (Paneles / Aquarius / Rosa) y con el encendido de TXs.
- En caso de encontrar alguna TCE (thruster control electronics) encendida comandar su apagado.
- En caso de encontrar algún TX encendido, ya sea de banda S o de banda X, comandar su apagado

Luego de detectar la separación, las acciones de rechazo de comandos y de análisis anteriores dejarán de efectuarse y se ejecutarán las siguientes:

- A los 60 segundos: Ejecutar el automatismo de encendido del TX nominal de banda S
- A los 90 segundos: Ejecutar el automatismo de apertura de Paneles Solares
- A los 100 segundos: Comandar la transición de AOCS a “safe-hold”, a partir de la habilitación de la supervisión correspondiente.

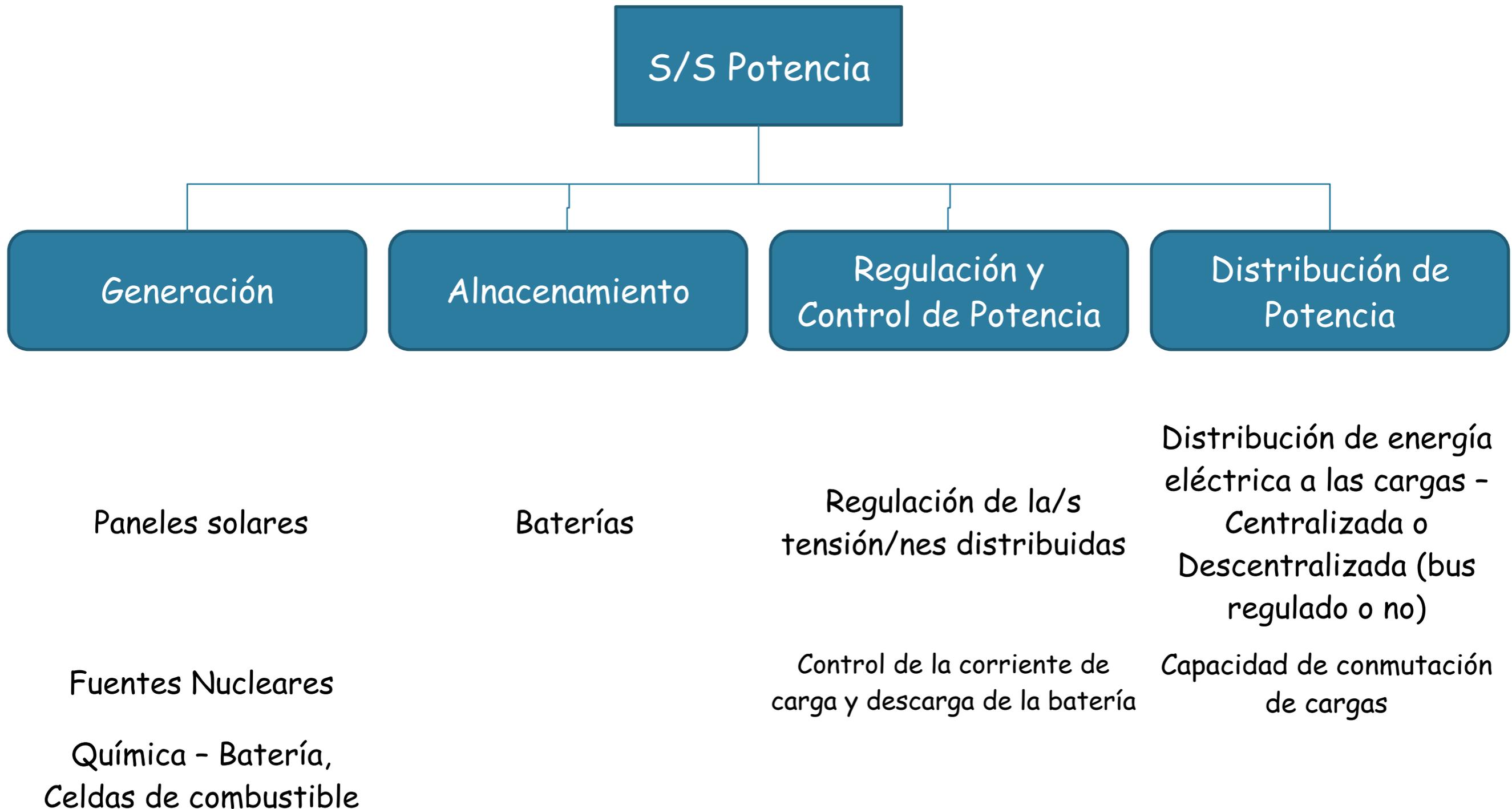
Almacenamiento a bordo

- Tecnología de memorias —> FLASH, SDRAM, EEPROM
- Paginado de la memoria, accesos
- Compresión de datos en caso de necesidad
- Margen por degradación —> se debe dimensionar EOL
- Capacidad de detección y corrección de errores

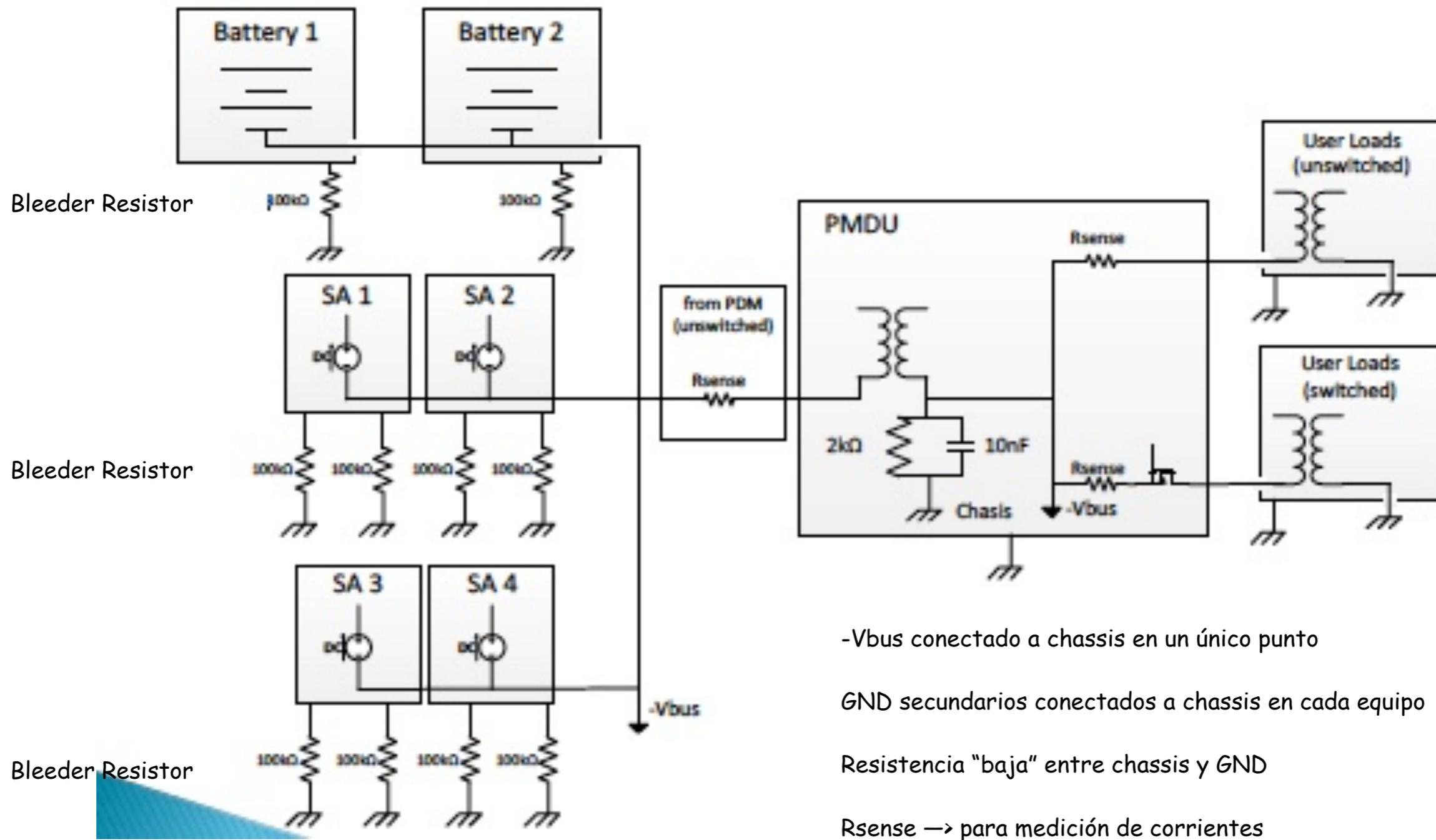
Ejemplos

- ➔ Memoria de “masa” del SAC-D (telemetría de HK almacenada, tablas de configuración de subsistemas de plataforma, copias parciales de las memorias de programa de subsistemas para su posterior bajada a Tierra)
- ➔ Memoria SSR del SABIA-Mar (datos generados por los instrumentos, telemetría de HK almacenada, tablas de configuración, copias parciales de las memorias de programa de PM-OBC y SM-OBC), con capacidad de 64 Gbytes BOL, hot redundant. El plan de misión prevé una necesidad de alrededor de 16 Gbytes EOL.

Subsistema de Generación de Potencia



Grounding



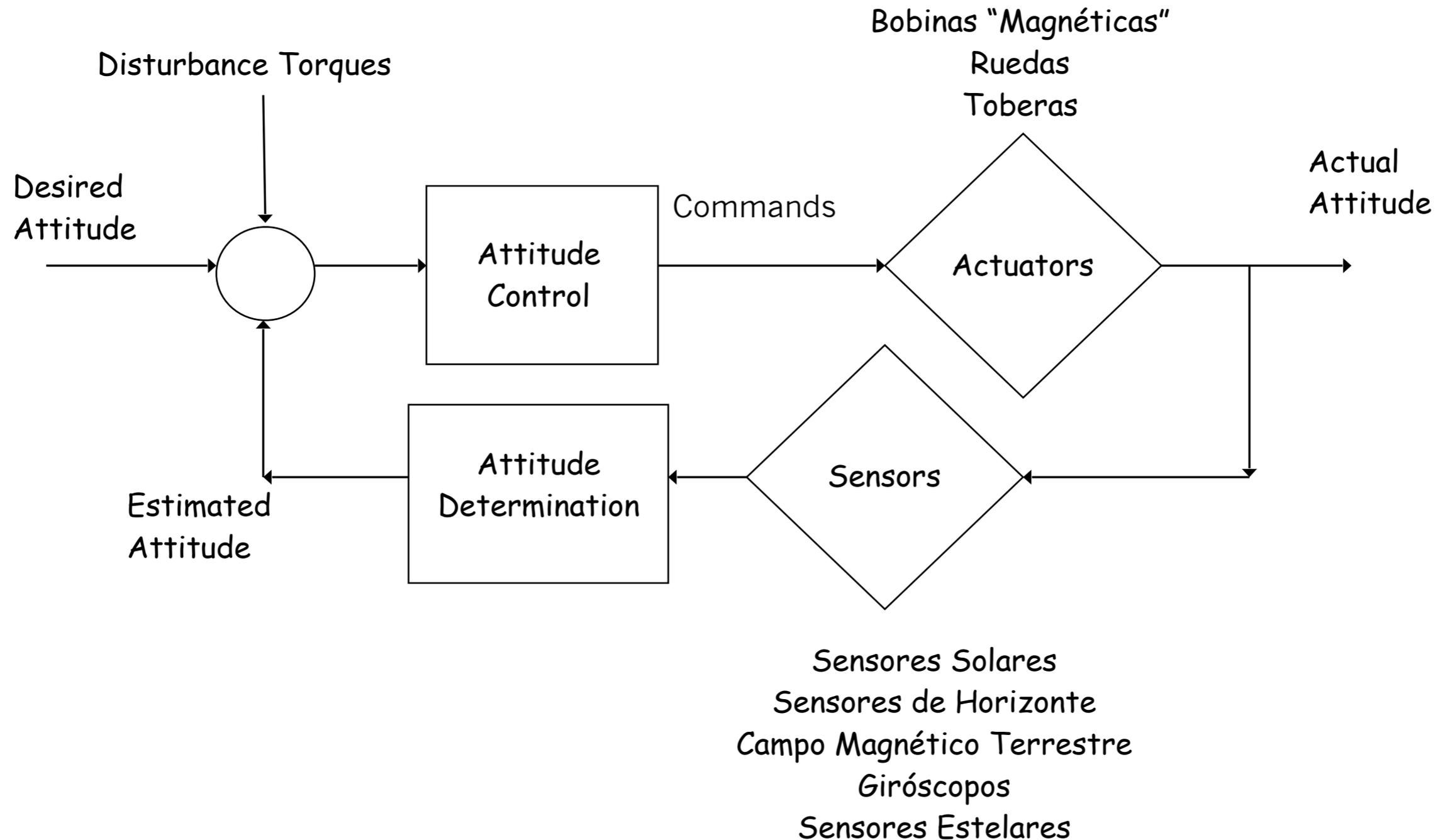
-Vbus conectado a chassis en un único punto

GND secundarios conectados a chassis en cada equipo

Resistencia "baja" entre chassis y GND

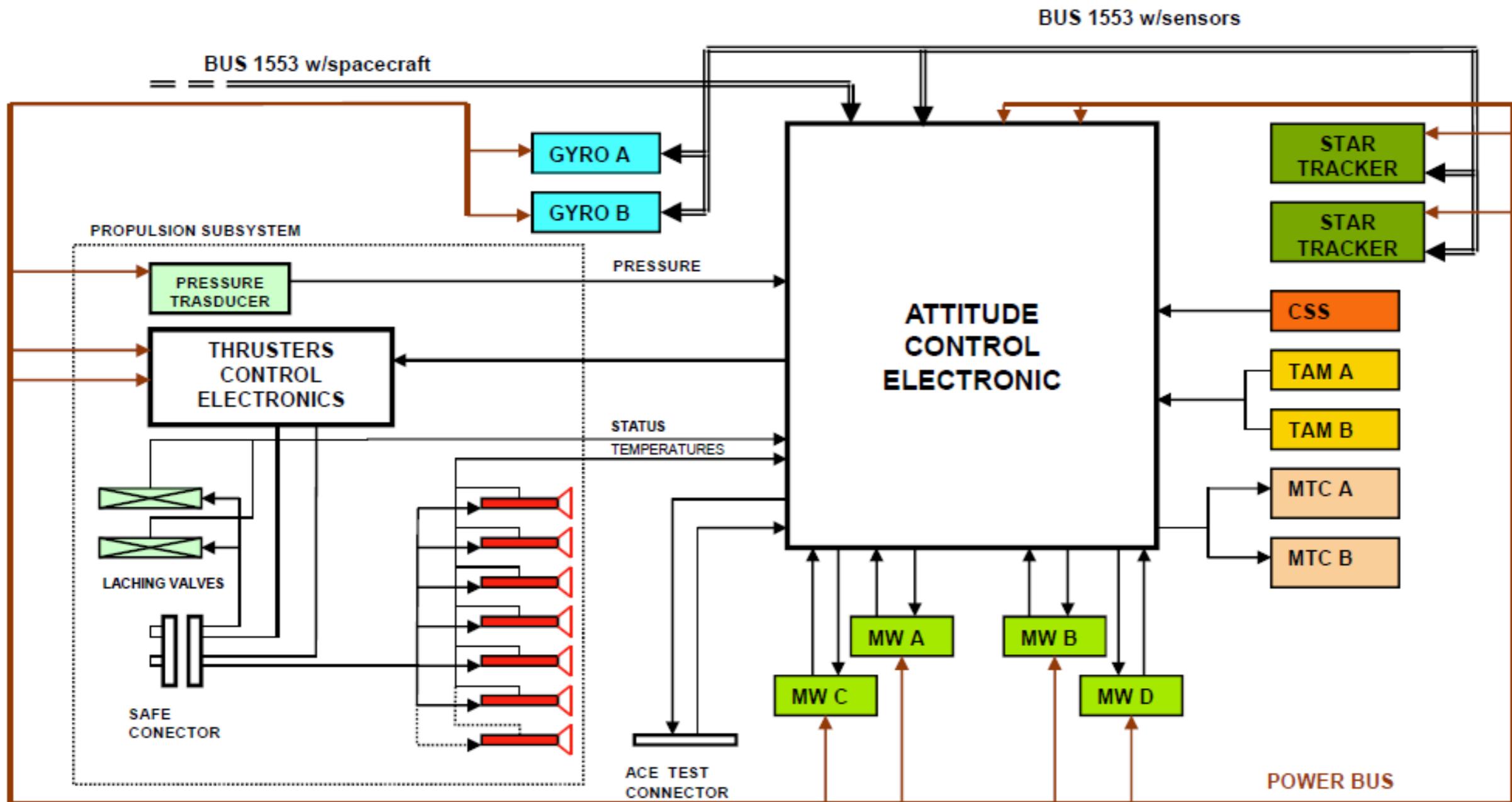
R_{sense} → para medición de corrientes

Subsistema de Control de Actitud



Subsistema ADOCS

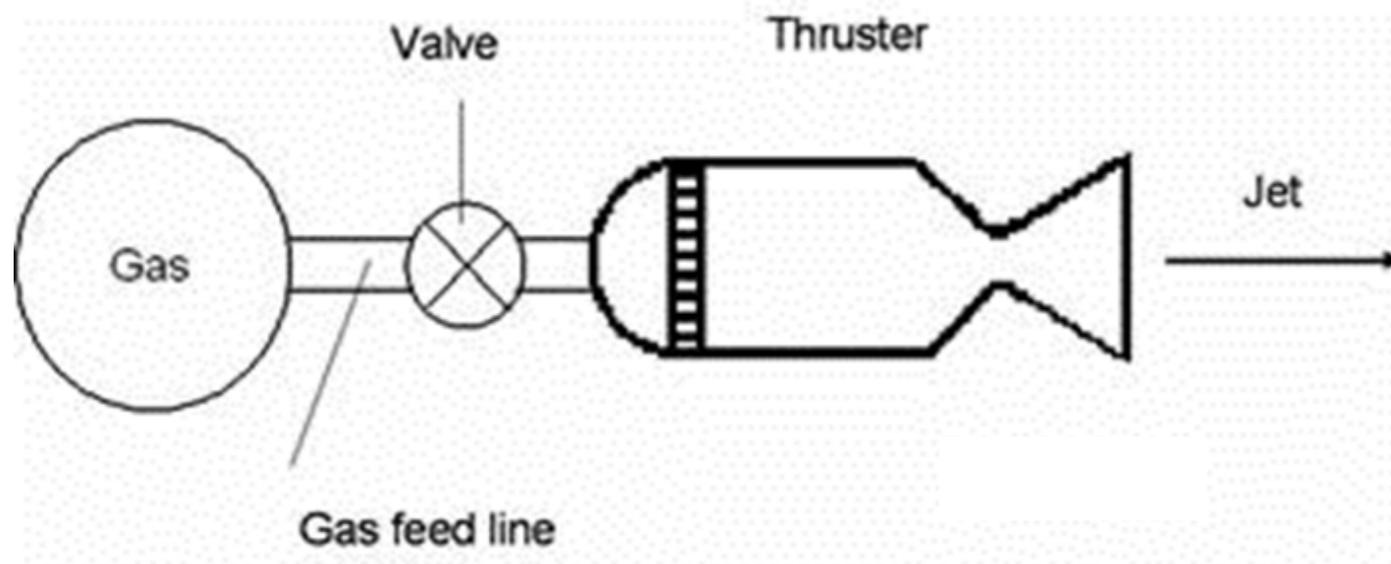
Attitude Determination & Orbit Control Subsystem



SAC-D

Subsistema Propulsión

- Corrección de la órbita inicial - Adquisición de la órbita
- Mantenimiento de la órbita
- Maniobras de evasión frente a posibilidad de colisiones
- Maniobra de "de-orbit"
- Control de actitud



Subsistema Propulsión

Trade-offs and Layout

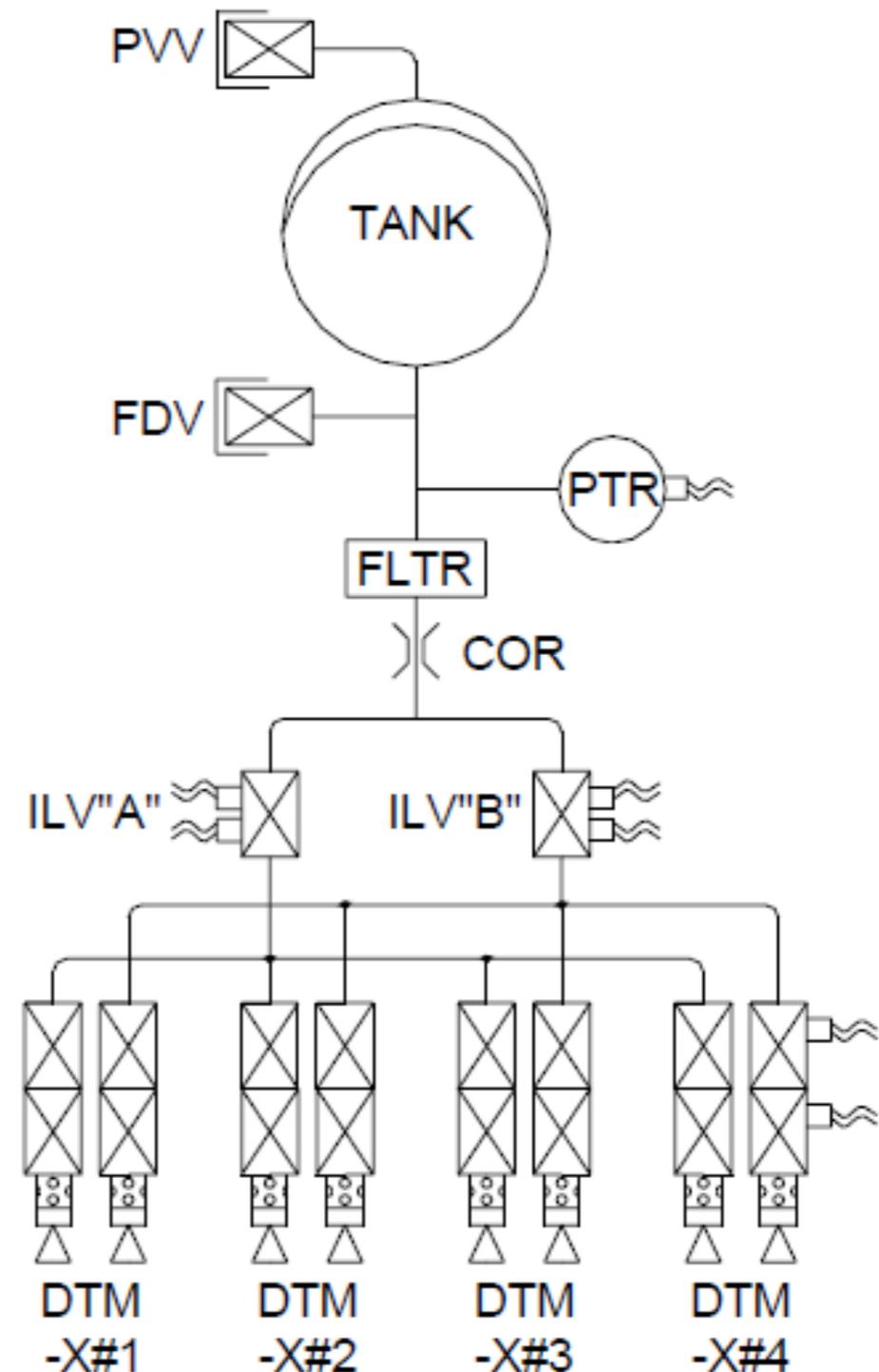
Monopropellant vs. Bipropellant

Blowdown vs. Regulated

Nitrogen vs. Helium

Result: A monopropellant hydrazine system with nitrogen blowdown operation is selected

Two totally redundant branches downstream COR.



Electrónica de Vuelo

Características Particulares de la Electrónica para Vuelo

- Diseño siguiendo una política de márgenes
- Calidad de Partes EEE → específica y costosa, screening, obsolescencia, disponibilidad de Modelos de Ingeniería para ensayos "tempranos" y reemplazos transitorios
- Diseños minimizando SWaPs (Size, Weight and Power), PCBs multicapa
- Vacío → ~~encapsulado plástico~~; soldaduras con plomo (evitar la formación de whiskers); disipación solo por conducción (diseño térmico lleva generalmente a incluir capas para disipación que "conecten térmicamente" la placa al chasis)
- Mínimo momento dipolar magnético del satélite minimizando loops de corrientes → cableado ((conexión entre celdas de la batería, twisted pairs); aislación de retornos en sistemas de alimentación descentralizados (retorno primario conectado a estructura en un solo punto, retornos secundarios conectados a chasis en cada equipo)
- Compatibilidad Electromagnética → filtrado y terminaciones de interfaces (minimizar susceptibilidad y emisión conducida); hermeticidad electromagnética del housing de los equipos (minimizar susceptibilidad y emisión radiada); arquitectura de "grounding" que aisle y/o minimice interferencias); necesidad de realizar ensayos en cámara anecoica y blindada (tanto a nivel equipo como a nivel satélite) utilizando equipamiento específico (medición de emisiones conducidas y radiadas, y excitación de niveles por conducción y radiación para determinar susceptibilidades)
- Radiación → endurecimiento (tecnologías), blindaje, SEUs y Latch-Ups
- Confiabilidad → diseños considerando confiabilidad, FMEA, Fault Tree, Fault Tolerance (redundancias), FDIR (Failure Detection Isolation & Recovery)

Ningún Sistema es mejor que el peor de sus componentes

Política de Margenes

Nivel Equipo (SABIA-Mar)

Nivel Satélite (NASA)

POWER DESIGN MATURITY	PHASE B [%]	PHASE C [%]
New units containing new technologies	20--25	15
New units containing existing technologies	15--20	15
Major modification to existing units	10--15	10
Minor Modification to existing unit New units with Engineering models	5--10	5
Off the shelf Flight qualified units	3--5	5

Resource	Pre-Phase A	Phase A	Phase B	Phase C	Phase D	Phase E
Mass	≥30%	≥25%	≥20%	≥15%	0	
Power (wrt EOL capacity)	≥30%	≥25%	≥15%	≥15%	≥10% *	
Propellant	3σ***				3σ	
Telemetry and Command hardware channels**	≥25%	≥20%	≥15%	≥10%	0	
RF Link	3 dB	3 dB	3 dB	3 dB	3 dB	
$\text{Margin (in percent)} = (\text{Available Resource} - \text{Estimated Value of Resource}) / \text{Estimated Resource} \times 100$						
<p>* At launch there shall be 10% predicted power margin for mission critical, cruise and safing operating modes as well as to accommodate in-flight operational uncertainties.</p> <p>** Telemetry and command hardware channels read data from hardware such as thermistors, heaters, switches, motors, etc.</p> <p>*** The 3 sigma variation is due to the following: 1. Worst-case spacecraft mass properties 2. 3-sigma low launch vehicle performance 3. 3-sigma low propulsion subsystem performance (thruster performance/alignment, propellant residuals) 4. 3-sigma flight dynamics errors and constraints 5. Thruster failure (applies only to single-fault-tolerant systems)</p>						

Partes EEE

- ★ En general los ICs podrían diferenciarse en dos categorías básicas:
 - Calificados para el espacio “Space-qualified” – que pueden o no ser endurecidos a la radiación
 - Industriales / Comerciales, incluyendo los utilizados en la industria automotriz

- ★ Los criterios de selección pueden resumirse en 4:
 - **Confidence**, confianza de acuerdo con el historial de la parte y del fabricante, incluyendo experiencias previas en proyectos/usos similares - Intente utilizar partes EEE con historia — Si se necesita una parte sin historia previa, nueva, entonces habrá que “pagar” por su calificación o screening, o asumir el riesgo.
 - Nivel de calidad **requerida** por la misión para la función
 - Compromiso **costo-calidad** - mayor costo en los dispositivos endurecidos a la radiación y calificados MIL-Aero — una posibilidad de menor costo es considerar dispositivos de menor calidad y menor resistencia a la radiación pero sumando ensayos de screening, y diseños de sistemas tolerantes a fallas y, en cierto grado, a la radiación
 - **SWaP** “Size, Weight, and Power”

Estrategias de Mitigación de los riesgos asociados a las Partes EEE

- **Simplificación de la dimensión del problema**
 - Búsqueda de información
 - Herencia / Base de datos "abiertas y accesibles"
 - Ensayos
 - Radiación - Confiabilidad aumentada por las horas de testing
 - Análisis de Confiabilidad y/o Criticidad (WCA - PSA - Derating - FMEA - FMECA)
- **Protección**
 - Blindajes frente a la radiación
 - Diseño térmico optimizado
 - Derating
- **Mitigación**
 - Tolerancia frente a fallas (ejemplo: redundancias)
 - FDIR [Failure Detection Isolation & Recovery]

Diseño Confiable

El proceso de diseño e implementación de un sistema confiable no depende solo de “sumar” redundancias: la tolerancia a fallas es solo una parte de ese proceso.

Existen herramientas que permiten controlar diferentes aspectos de este proceso para mejorar la confiabilidad de un sistema, intentando no solo que tolere fallas sino también que las evite.

- Algunas de estas herramientas, que se han utilizado en los proyectos satelitales de CONAE:
 - ✓ Contar con un Plan de Aseguramiento que defina planes de control de partes y procesos
 - ✓ Contar con herencia (documentada), utilizando diseños anteriores validados
 - ✓ Simplicidad en el diseño
 - ✓ Incluir consideraciones que aumenten la confiabilidad de los diseños: a nivel equipo: derating del rango térmico, espesor de aluminio del “housing”; a nivel diseño circuital / software: limitación de corrientes, sumar EDAC, scrubbing de dispositivos de memoria por medio de un dispositivo externo al procesador, redundancias funcionales; a nivel parte: triple-voting, preferiblemente con lógica interna del dispositivo; Implementar los pasivos con calidad MIL (R,C, cables, conectores, ...) y pinturas y adhesivos con bajo nivel de sublimación
 - ✓ Efectuar Análisis de Confiabilidad (Worst Case, Failure Mode Effects, Single Event Effects)
 - ✓ Construcción de Arbol Funcional y Arbol de Fallas que permitan determinar las funciones que sí o sí debieran redundarse para garantizar una mínima operación del satélite

Diseño Confiable - Cont.1

- Otras herramientas que hemos utilizado en los proyectos satelitales de CONAE:
 - ✓ Realizar revisiones independientes del diseño
 - ✓ Selección y control de partes y control de procesos;
 - ✓ Utilizar márgenes explícitos en los diseños
 - ✓ Derating de partes
 - ✓ Utilizar técnicas de protección ambiental
 - ✓ Utilizar técnicas de diseño y codificación de software siguiendo standards de diseño de Software (ESA y/o NASA tienen documentación al respecto)
 - ✓ Screening de partes, en casos específicos en los que no se cuenta con suficiente información
 - ✓ Diseñar un sistema que, por un lado sea tolerante a fallas y por otro se proteja frente a fallas
 - ✓ Definir un Programa de Verificación (análisis y ensayos) consistente con el nivel de calidad de la misión del satélite que se requiera.

Sistema Tolerante y Sistema Autónomo de Protección frente a Fallas

- Un diseño **Tolerante** a fallas es aquel que, ante la falla de algún subsistema, ensamble, o parte de un sistema, permite que dicho sistema continúe operando, probablemente con un desempeño reducido, pero que evite la falla completa. Las características de una arquitectura tolerante a fallas incluyen: redundancias, cross-strapping, detección de fallas y mecanismos de corrección.
- En cambio, un **Sistema Autónomo de Protección** frente a fallas es aquél que, luego de ocurrida una falla, coloque al satélite (sistema) en un estado operativo “seguro” y “comandable”, y que dicho estado pueda mantenerse por un período de tiempo prolongado sin necesidad de comandos generados en tierra para continuar operando.
- El estado “seguro” mencionado está íntimamente vinculado a asegurar una orientación del satélite (Actitud) que arroje un balance energético positivo “power positive” (mayor generación que consumo), que el balance térmico resulte en rangos de temperatura permitidos para los equipos con margen, y que la comunicación con tierra se encuentre garantizada.
- La mayoría de las funciones de detección, aislación y corrección frente a fallas son implementadas a través del Software, aunque algunas se implementan a través de lógica cableada sin intervención de software (WatchDogs, EDAC based on triple voting, Power cycling due to latch-up, etc.)