AE3534 – Spacecraft Technology

Command & Data Handling

Jasper Bouwmeester

Lecture Notes

TUDelft

# 1.1 | Introduction to Command & Data Handling

What is a Command & Data Handling?

Definition

The function of a Command and Data Handling Subsystem (CDHS) is to perform onboard operations and internal communication

The function of a command and data handling subsystem is to perform onboard operations and internal communication. The task of managing the operations of the spacecraft subsystems is nowadays performed mostly by software in an autonomous manner and is generally categorized as onboard operations. The software is also responsible preparing the data to be downlinked and handling any commands that are received from operators on the ground. Lastly, the command and data handling subsystem is in control of, and facilitates, all internal communications (consisting of commands and data) between the spacecraft subsystems.

The term "command and data handling" is a legacy of the past in which many satellite functions were still performed by analog circuits. With the current shift towards the digital domain, the term does not fully cover the topic anymore. However, due to lack of any better alternatives, the term is still widely used. An appropriate analogy to describe this subsystem, is to regard it as the brain and nervous system of the spacecraft.
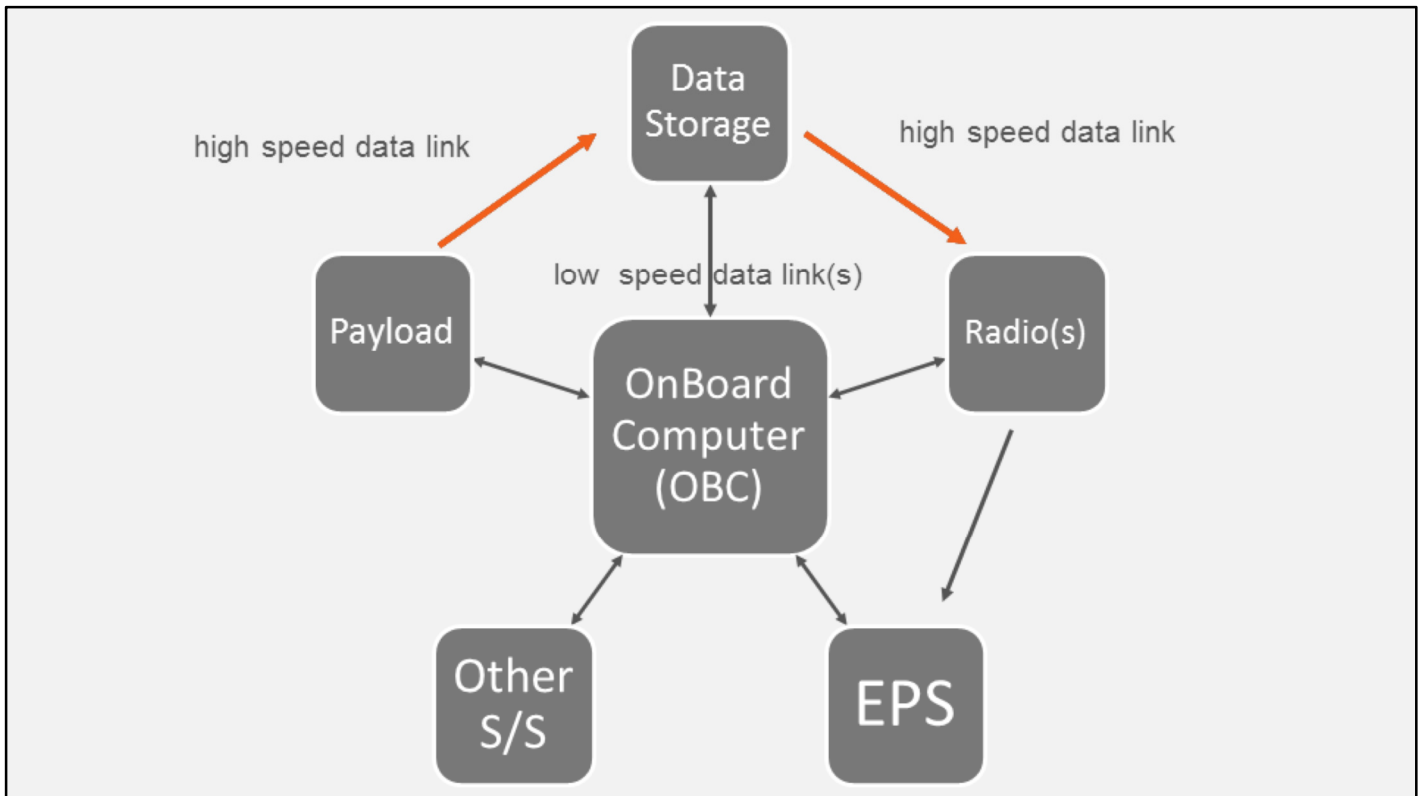
This figure provides an overview of the architecture of the Command and Data Handling Subsystem (CDHS) in a typical spacecraft. The heart of the system is the Onboard Computer (OBC) which runs the software responsible for managing the onboard operations. The OBC is tightly linked to the Electrical Power Subsystem (EPS). The primary reason for the close relationship between the OBC and EPS is the importance of the available and consumed power for managing onboard operations. For instance, by continuously querying the EPS on the available power, the OBC can decide to turn off non-critical subsystems to prevent vital systems from shutting down. Secondly, the OBC must be able to command the EPS to disable or enable different subsystems throughout the various phases of the mission. Since, the amount of data transmitted between these two subsystems is small, a low speed data link is used.

The OBC is also responsible for receiving, interpreting and executing commands from ground operators via the radio receiver. Using low speed radio transmitters, the OBC also sends packets of housekeeping data to the ground station. The purpose of the housekeeping data is to give the operators an overview of the spacecraft health and general condition. Some small satellites only have a single low speed transmitter and the housekeeping and payload data are combined over the same link.

For larger satellites with payloads capable of producing vast amounts of data, a dedicated high speed data link is used to store the data onto the onboard storage system. When the satellites passes over a ground station, the OBC commands the high speed radio transmitter to retrieve and transmit the previously stored payload data through another dedicated high speed link from the onboard storage system. This approach frees the OBC from having to process large amounts of data and allows it to devote its internal resources for time critical operations.

The OBC also communicates to the payload and all other subsystems through low speed data links. This is required to retrieve information on their health, perform critical interventions as well as to command these subsystems to perform various actions according to the operational scheme of the mission.

Note that the figure just provides an example and the true architecture differs from satellite to satellite.

Command Handling

- Nominal commanding
  - Digital data link to OBC
  - Parameter change
  - Operational mode change
  - Software uplink
- High Priority Commanding (HPC)
  - Only for limited functions
  - Analogue components
  - Sequence of pulses or tones
  - Direct link to subsystems
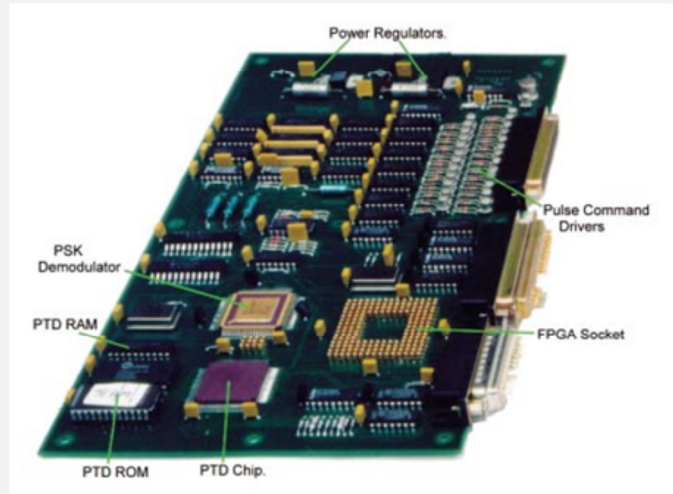

TEAM Telecommand Board © ESA

Larger spacecraft are equipped with a dedicated command controller system. Under normal conditions, the command decoder forwards the received commands to the OBC using a data link. These commands are used to change the software parameters, the operational mode or to even provide a complete revision of the onboard software. However, as a result of severe anomalies or failures, the OBC may not be able to receive commands or communicate with other subsystems through the nominal data links. To circumvent these issues and to improve the ability of ground operators to recover the subsystems from these modes, many satellites have implemented an alternative command route called high priority commanding. High priority commands can only be used to control a limited set of critical functions such as switching a subsystem on or off or resetting its parameters to the default configuration.

The high priority commanding route typically uses only analogue components which are less prone to radiation effects. Instead of relying on digital communication channels, a sequence of pulses or tones are transmitted to the subsystems over simple electrical links.
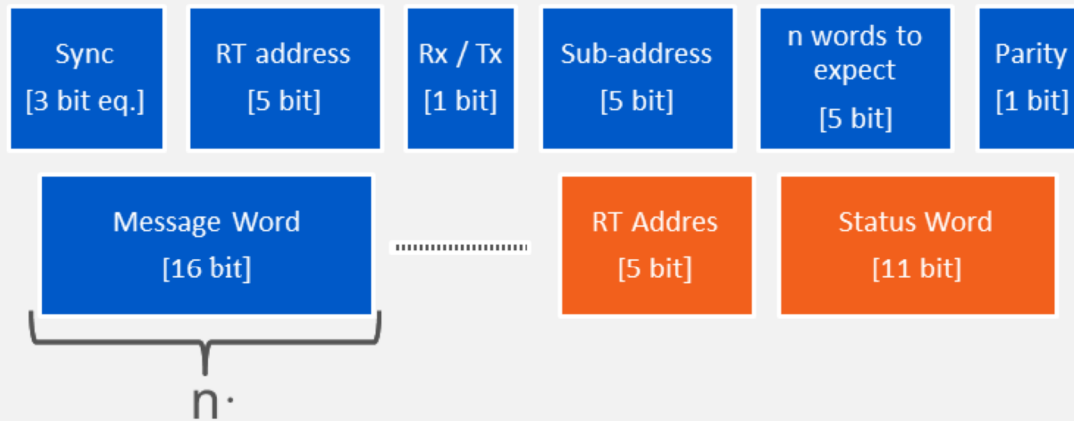
1.2 | Data Busses
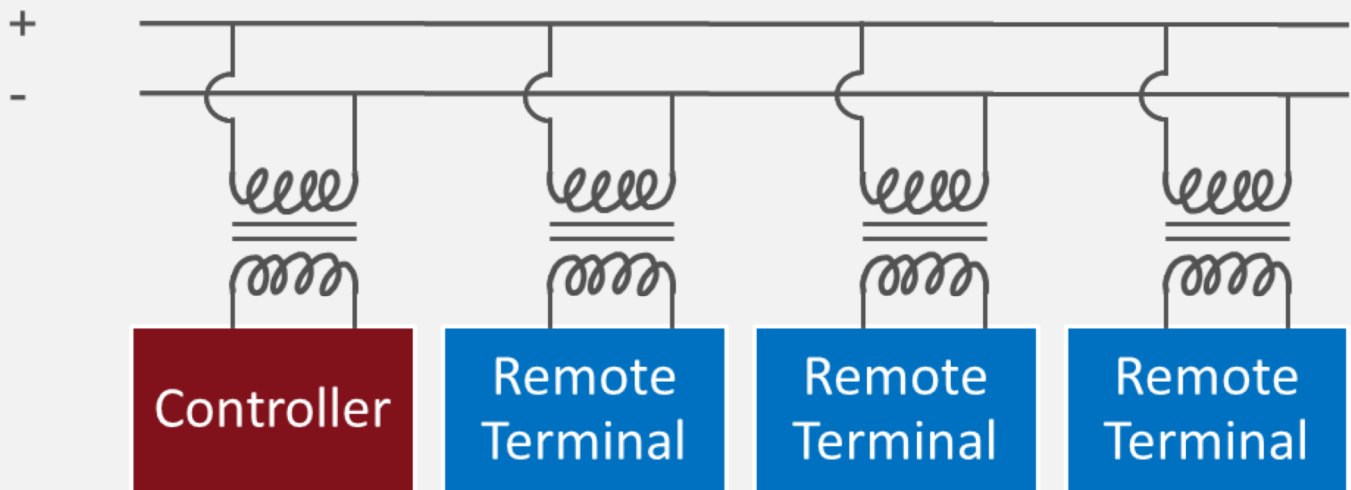
The MIL-STD-1553, commonly found in large spacecraft, is a data bus comprising of a single bus controller and up to thirty-one remote terminals. The bus controller is responsible for managing all communications on the bus, a role which is generally accomplished by the OBC. A remote terminal can be the controller of a subsystem or it can be a router connected to multiple other subsystems.

The MIL bus uses a pair of wires using differential signaling. All remote terminals tap in to the same physical bus using a bus topology referred to as a linear bus. Furthermore, since all data bits are transmitted sequentially, the MIL bus can be considered a serial bus which can support data-rates of up to 1 Mb/s.

All devices (controller and remote terminals) use coupling transformers, which only couples alternating currents (the desired signals) but does not pass through direct current, so the bus cannot be shorted. The figure provides a simplified overview of the MIL bus. In practice, several passive elements may be required (depending on the distance between the tapping point and the remote terminal) to complement the single transformer. The primary function of the transformer coupling is to protect the shared bus against short circuits which can occur at subsystems.

MIL-STD-1533 Data Protocol (transmission)

Sync [3 bit eq.]	RT address [5 bit]	Rx / Tx [1 bit]	Sub-address [5 bit]	n words to expect [5 bit]	Parity [1 bit]

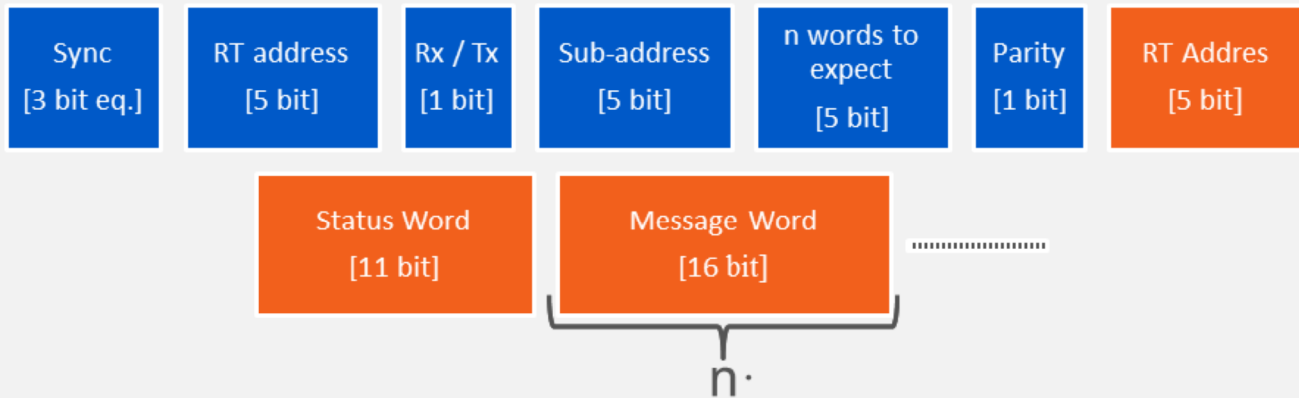| Message Word [16 bit]	....	RT Addres [5 bit]	Status Word [11 bit]

n·

The figure provides an overview of the data message protocol for a transmission from the bus controller to a remote terminal unit. The transmission begins with a synchronization signal that lasts for a period equivalent to 3 bits. This synchronization sequence is required by the remote terminal in order to synchronize its internal clock to that of the bus controller which makes it possible to distinguish sequential bits.

Following synchronization sequence, the address of the remote terminal is transmitted. The address indicates intended recipient (remote terminal) of the message. A single RS/TX bit follows the address field. The purpose of this bit is to indicate if the controller will send a message to the receiver or expects a message back.

Similarly to the address field, the sub-address field is used to indicate the receiving device connected to a router. The length of the message (in terms of words) is transmitted after the sub-address. The 20 bit long message header ends with a single parity bit which can be used to detect a single bit flip. When the controller wants to transmit a message to a remote terminal, the header is followed by the actual message. The receiver subsequently acknowledges the reception by transmitting its address and providing a status word to indicate good reception or faults.

MIL-STD-1533 Data Protocol (reception)

Sync [3 bit eq.]	RT address [5 bit]	Rx / Tx [1 bit]	Sub-address [5 bit]	n words to expect [5 bit]	Parity [1 bit]	RT Addres [5 bit]

| Status Word [11 bit]	Message Word [16 bit]

n·

For receiving a message, the remote terminal first responds with its address and status word, followed by the message.

Various other sequences, containing only status words, or communication between two remote terminals can occur. But in all cases the bus controller leads the transaction.

MIL-STD-1533 Signals (1)

differential signal pair   + noise   signal
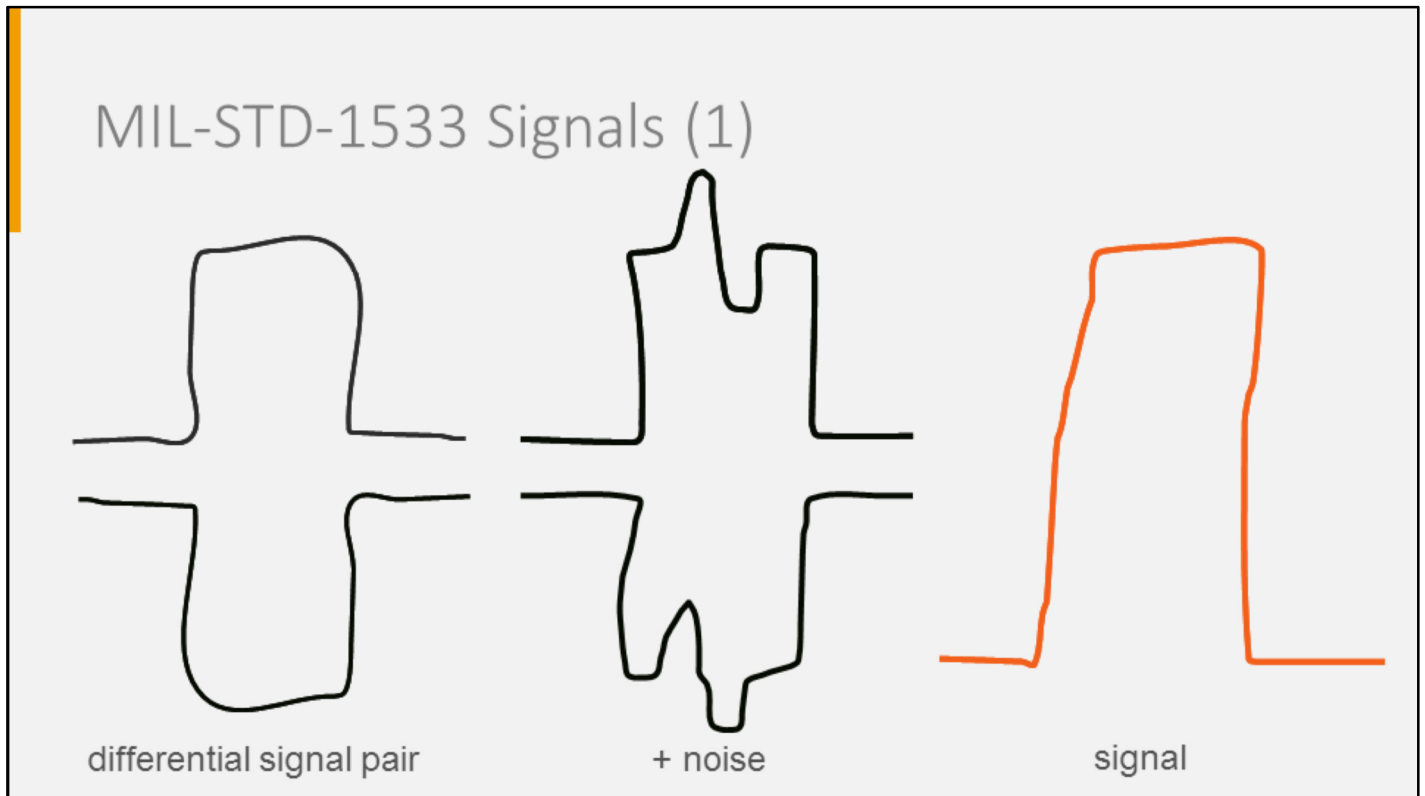
To understand the purpose of differential signaling, we need to visualize the signals on the pair of wires. A differential signal, as shown on the left, simply means that the signal on one of the two wires is identical to the signal on the other wire, but opposite in direction. The intended signal is a difference between two signals, as shown on the right. For digital communication, typically high (1) and low (0) are the binary states. Since the differential pair of wires are routed close to each other, any external electromagnetic noise will distort both signal equally and in the same direction, as shown in the middle. Since, the data is contained in the difference between the signals on both wires, the noise is cancelled out and the original data is fully preserved. This is referred to as common mode noise rejection.

MIL-STD-1533 Signals (2)
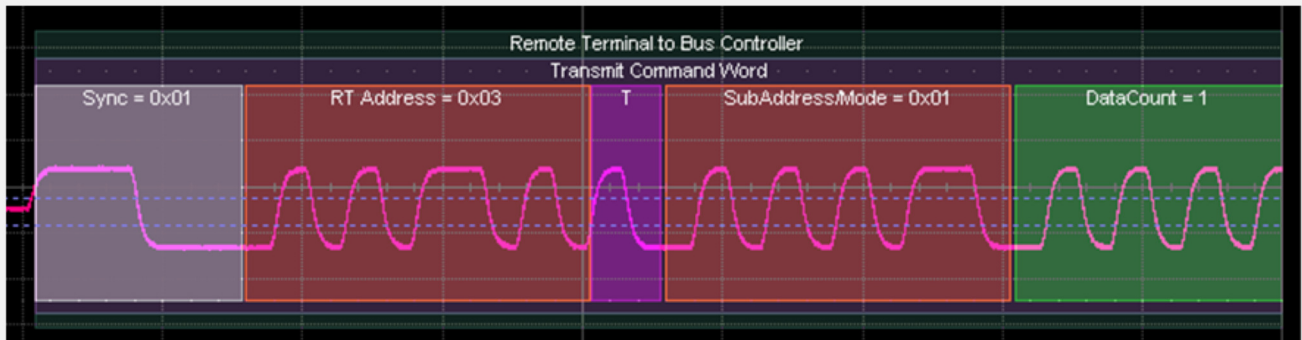
This figure shows a measurement of the differential signal (so the voltage difference between the pair of wires). In case of the MIL bus, the peak-to-peak differential voltage (high) is about 28 V. Although such a high voltage increases the power consumption, it also makes this data bus extremely robust against electromagnetic interference. To enhance reliability further, this bus is typically implemented in a dual, triple or even quadruple redundant configuration.

Even today, many expensive spacecraft use the ageing MIL data bus due to its high reliability and legacy. It will for instance be used in the JUICE mission of ESA, set to explore Jupiter's moons in ~2022.
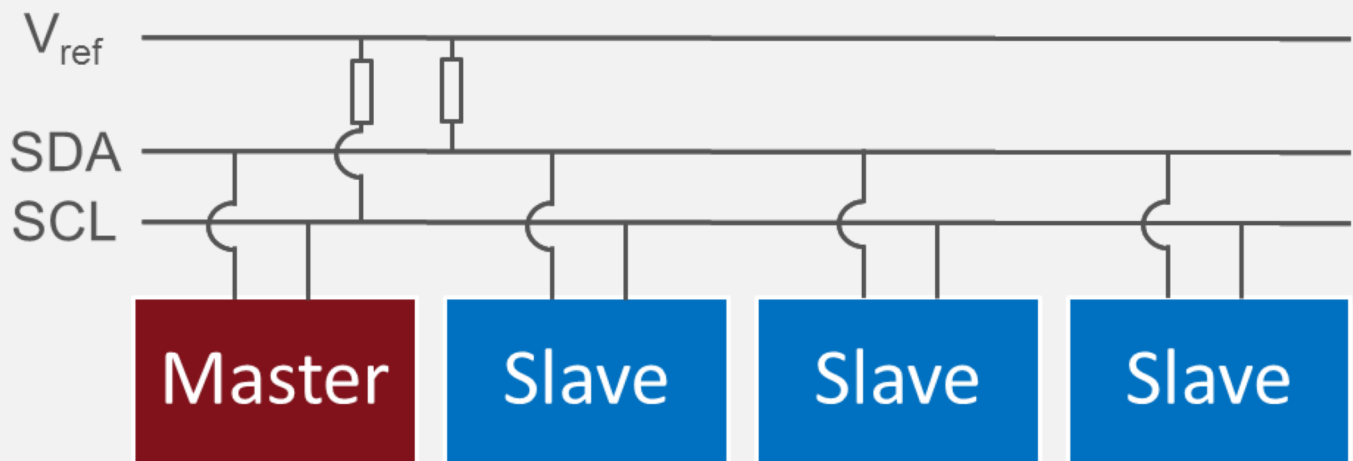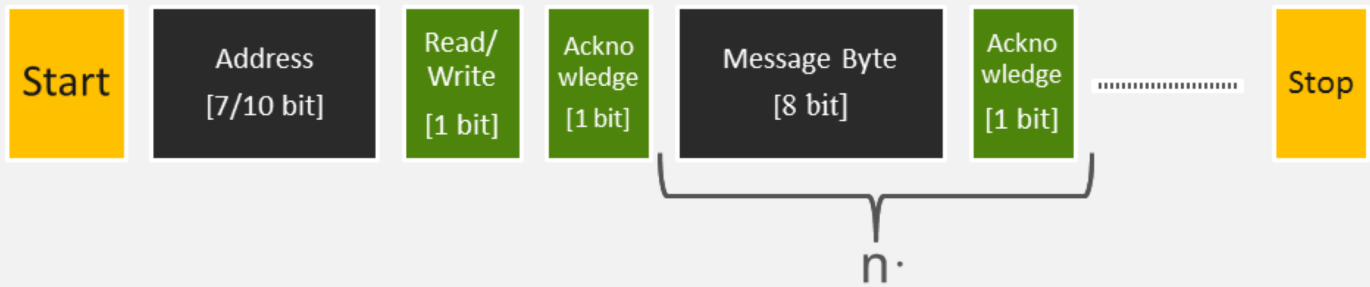
The I^2C data bus is another example of a serial data bus with a linear bus topology. Unlike the MIL bus, this bus uses one wire for the data signal and one for the clock signal. Simple resistors are used to pull-up the signals to the reference voltage (typically 3.3V or 5V).

The master device controls the bus and can communicate with up to 112 slave devices. The signal is generated by pulling down the lines to the ground. The data rate is for most practical cases limited to 400 Kb/s. Even higher data rates are supported by the bus, but their support in hardware is limited.

Thousands of integrated circuits have implemented an I^2C controller ranging from microcontrollers to special purpose devices. Compared to other busses, I^2C consumes very little power. The maximum length of the bus is however limited to about 30cm, making this bus unsuitable for large spacecraft.

However, as a result of the availability and the low power consumption, I^2C is currently the most popular PocketQubes and CubeSats. I^2C is also implemented in the successful Delfi-C^3 and Delfi-n3Xt CubeSats which are developed and operated at TU Delft.

I^{2}C Data Protocol

| Start | Address [7/10 bit] | Read/ Write [1 bit] | Acknowledge [1 bit] | Message Byte [8 bit] | Acknowledge [1 bit] | .... | Stop |

n·

Each transaction begins with a start condition from the master. Following the start condition, 7 or 10 bit address of the slave device is transmitted. Similar to the MIL bus, the read/write bit informs the slave to prepare to receive or transmit data. The slave then needs to acknowledge that it is addressed and ready for the next action.

The actual message (to or from the slave) is then transmitted onto the bus. The recipient must acknowledge the data after each byte. The message can be up to 255 bytes long and ends with a stop condition from the master.

I²C Signals
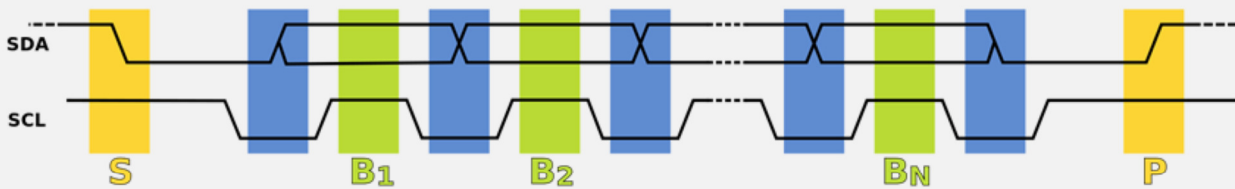
This figure gives a graphical representation of the data and clock signals. By separating the data and the clock signals, the slaves do not to synchronize their own internal clocks to the master's clock based on data transmission frequency. This should in principle increase the reliability of the data bus. However, due to the unshielded, low voltage (typically 3.3 V) and non-differential nature of the bus, both lines are very susceptible to electromagnetic interference and radiation events. A signal distortion on one of the lines can lead to a bit flip which might not be too problematic. However, it can also lead to a missing address bit or a false start or stop condition. In practice, the handling of such anomalies are often poorly implemented in integrated circuits which can cause bus lockups to occur.

SpaceWire is a data bus that is specifically designed for space applications by the European Space Agency (ESA). It is a point-to-point bus which directly connects two devices (as opposed to a linear bus which can connect multiple devices). One of these devices can however be a router which connects several other devices via SpaceWire or other data busses. The bus uses differential signaling like the MIL bus and supports data rates of up to 400 Mb/s. It has separate data and strobe signal similar to the I^2C bus. Unlike the previously discussed busses, the SpaceWire bus is a full duplex bus, meaning that there are dedicated outgoing lines for data transmission as well as incoming lines for reception which can be operated simultaneously. The eight lines, together with a shield line, are wired via 9 pin connectors.

When redundant links and routers are available, SpaceWire can automatically reroute the data in case of single link failures. The combination of high data rates and high reliability make this bus a very popular bus for modern spacecraft. On the other hand, the SpaceWire is typically implemented in FPGA's and ASICs, which increases the effort required to implement it in existing systems. Furthermore, it has a higher power consumption when compared to I^2C and other low power busses, making it less suitable for PocketQubes and CubeSats.
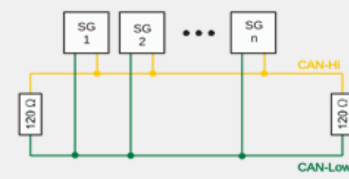
Space Wire Signals
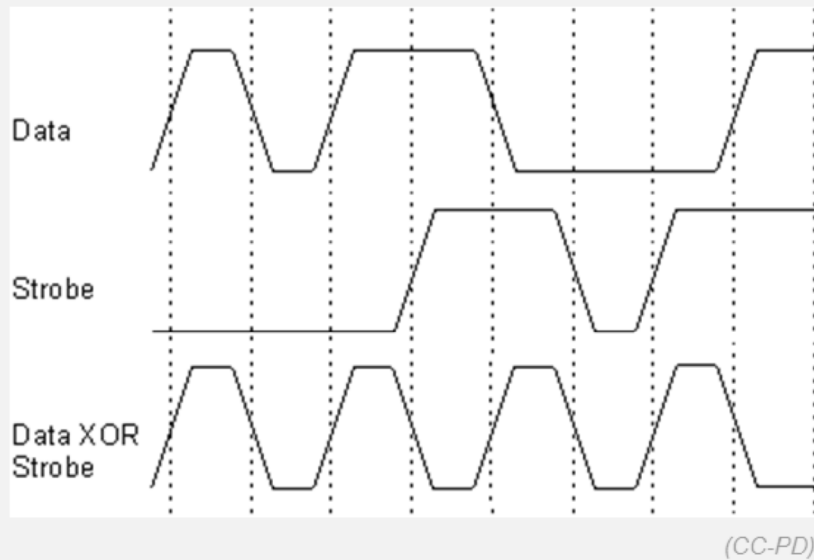
The strobe signal is designed to alternate its logic level when two consecutively identical data bits are transmitted. This is referred to as data strobe encoding. This means that for each bit, either the data or the strobe signal changes its logic level, but never both at the same time. From the figure, we can see that performing a simple exclusive-or operation on the two signals, recovers the pure clock signal. This approach has the advantage of being more robust against external and mutual interference in both signal lines. For instance, a change of both signals during the same bit interval is not allowed and can thus be determined as an anomaly and handled appropriately.
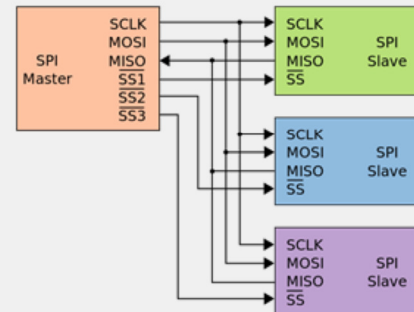
Other Implemented Busses

- CAN
- SPI
- Time Triggered Ethernet
- RapidIO
- etcetera

by Stefan-XP (CC-BY-SA)

by D. Monniaux (CC-BY-SA)

by C. Burnet (CC-BY-SA)

Controller Area Network (CAN)

The Controller Area Network, or CAN-bus is a differential bus developed for the automotive industry. It is designed for time critical functions and can support data rates of up to 5 Mb/s. In terms of performance, power consumption and reliability this bus takes the middle ground compared to the previously discussed busses.

Serial Peripheral Interface (SPI)

Serial Peripheral Interface, or SPI, is a data bus with close resemblance to I^2C. One of the differences between the two busses is that SPI uses a dedicated slave select wire per device, as opposed to digital addressing, to select individual devices. Secondly, the SPI is a full duplex bus.

The data rate of SPI is limited by the maximum clock speeds of the master or slave device and can be up to several hundreds of megabits per second. For robustness it is best to stay at least one order of magnitude below the slowest controller clock speed. Also the length of the wire can lay a role due to capacitance of the bus. The advantages and disadvantages of this bus are similar to I^2C.

(Time Triggered) Ethernet

The Ethernet bus is widely used in wired computer networks around the globe. Time Triggered Ethernet is a modification of the standard implementation to make this bus more robust and to allow time critical operations. However it remains compatible with the standard Ethernet bus and can thus be connected to terrestrial Ethernet devices such as a personal computers. Compatibility with a widely adopted standard for terrestrial applications is one of the advantages of this bus and allows the satellite systems to be addressed through the internet like a network of devices. This bus can support data rates of up to 100 Mb/s and may be implemented in future satellites.

Other Implemented Busses (cont'd)

- CAN
- SPI
- Time Triggered Ethernet
- RapidIO
- etcetera

Rapid-I-O

Rapid-I-O is a data bus for time critical computer systems with extreme performance requirements. The throughput of this bus is up to 10 Gb/s for a single lane and can be multiplied by increasing the number of lanes.

It is most commonly used in the terrestrial telecommunications industry, for instance in equipment at cellular towers. The performance and its robustness make this point-to-point data bus interesting for some dedicated space instrumentation with very high performance requirements.

There are many more data busses which can and/or are implemented in spacecraft. However, the most common at present and in the near future or dealt with.

1.3 | OnBoard Computing

Processors

- Focus on computation
- Requires peripheral ICs
- Fastest for generic computation
- Typical power consumption >10 Watt

Processors (nowadays typically microprocessors, have been around since the dawn of the personal computer and primarily focus on computation. Processors typically lack internal peripheral integrated circuits and require external work memory and data bus controllers in order to function.

Processors are considered the fastest general computing platform and have a typical average power consumption of between 10 W and 150 W. General computing platforms can serve a wide range of applications. They are good at performing arithmetic operations (calculating the outcome of an equation) as well as logic operations (if/else conditional execution).

Due to reliability, flight heritage, decades of mission design and radiation environment testing, very old processors are still flown onboard large and expensive spacecraft. For instance, the radiation hardened variant of the famous Intel 386 (introduced in 1985) is still being used for the command computers in the international space station.

Note that the term 'microprocessors' are used as synonym to processors. The latest (micro-)processors still have computation as main function, but they do include some peripherals functions. They are however not to be confused with microcontrollers, as is discussed on the next page.

Microcontrollers

- Focus on embedded systems
- Memory integrated
- Integrated peripheral functions: ADC, DAC, PWM, I^2C, UART, etc
- Typical power consumption < 1 Watt

Microcontrollers are computing platforms that are primarily intended for embedded systems. As such, they lack the computational power of (micro)processors, but they have integrated memory and a plethora of peripherals. Some of these peripherals are Analogue to Digital Converters (ADC), Pulse Width Modulators (PWM) and data bus controllers. The average power consumption of microcontrollers is much less than processors and is typically well below 1 W (recent advancements has reduced the power consumption of some microcontrollers to less than 1 μW).

Even though the computational performance of state-of-the-art microcontrollers is much less than state-of-the-art processors, they still outperform older processors such as the Intel 386 while consuming several orders of magnitude less power. Since the need for computational power for many spacecraft functions has not grown as fast as processors speeds, there is a trend in the space sector to move towards microcontrollers, especially for smaller spacecraft.

Field Programmable Gate Array (FPGA)

- Re-programmable logic
- IP-cores for specific functions and complete microcontrollers
- Fast and low power for specific functions
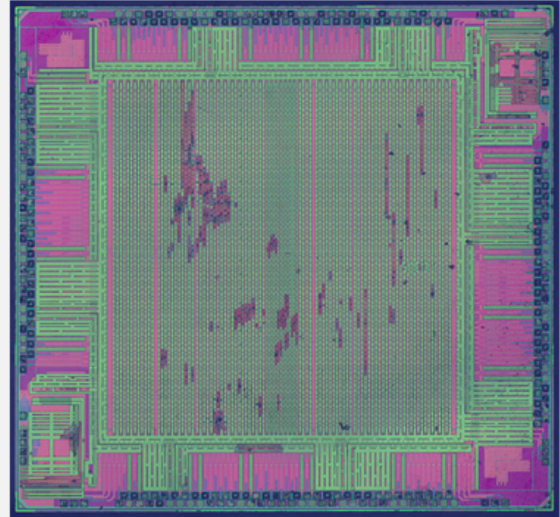- Higher power for microcontrollers

A Field Programmable Gate Array (FPGA) is an integrated circuit with reprogrammable logic. A hardware descriptive programming language is used to simplify the process and reduce the cost of designing integrated circuits. Predesigned Intellectual Property (IP) cores for specific functions can also be downloaded and used. IP cores are used as building blocks for FPGAs and contain designs as simple as counters or as complex as complete microcontrollers. The reprogrammable logic makes the FPGA special. Their internal structure can be reprogrammed on the go so their architecture is not predetermined when it is manufactured.

FPGAs are relatively fast and low power when designed for specific functions. However, a microcontroller implemented within an FPGA (using IP cores) consumes more power than a regular microcontroller (because of the more generic, less efficient lay-out of transistors).

The LEON microprocessor family is an IP core developed by the European Space Agency and can be integrated into FPGAs. There are various peripheral IP cores such as SpaceWire bus controllers designed for it. Furthermore, since it was designed specifically for space application, it has failure tolerant logic, redundant critical functions as well as intensive error detection and correction mechanisms. This microprocessor has become very popular on modern spacecraft.

Future of onboard computers

Application Specific IC (ASIC)

- Complete hardware solution for specific application
- IP-cores for specific functions
- Fast and power efficient

System-on-Chip (SoC)

- Complete hardware solution for specific and generic applications
- Smallest complete systems

The Application Specific Integrated Circuits (ASIC)

The Application Specific Integrated Circuits (ASIC) are the logical step after FPGAs. An ASIC is a complete integrated hardware solution for a specific application. It requires designing a new chip from scratch or IP core blocks. The advantages of ASICs over FPGAs is that the circuit structure can be optimized to be as fast and power efficient as possible.

The primary disadvantage of ASICs is that it takes a lot of time and money (in the order of 100,000 Euros) to produce. However, as technology advances the cost of production of these devices will decrease substantially in the near and become more cost effective.

System on Chips (SoC)

ASICs with various different integrated functions are generally called System on Chips (SoC). These devices can have integrated generic processors, microcontroller, radio frequency circuits, power amplification, power handling and even Micro Electro-Mechanical (MEMS) sensors within the same chip package. These complete systems, represent the smallest level of miniaturization achievable by our current technology and may one day lead to a complete satellite on a chip.

Examples of Onboard Computers

Spacecraft	Type	Environment	Launch Year	Onboard Computer
International Space Station	Space Station	LEO	1998	Intel 386 (rad-hard)
Spirit & Opportunity	Rover	Mars surface	2003	BAE RAD6000
Delfi-C3 & Delfi-n3Xt	CubeSats	LEO	2008 & 2013	MSP430
GOCE	Satellite	LEO	2009	ERC 32
JUICE	Satellite	Jupiter Moon	2020	LEON 2
Ariane 6	Launch Vehicle	LEO/GEO	2020	LEON 3 (?)

Photo by Ashlyak (CC-BY-SA)

As previously stated, the international space station uses the very old radiation hardened Intel 386 processors. The Spirit and Opportunity Mars rovers of NASA use an IBM made radiation hardened B-A-E processor. The radiation hardened variant of this processor has a clock speed of 25 MHz and costs 200,000 Euros. In comparison, the TI MSP-430 microcontrollers used by the Delfi-C^3 and Delfi-n3Xt CubeSats of TU Delft, run at a clock speed of 8 MHz and cost only 2 Euros. The large discrepancy in price is caused by the fact that the MSP430 is designed and intended for terrestrial applications.

The GOCE satellite uses a radiation tolerant variant of the ERC-32 processor from Atmel. This processor is discontinued but has been used as the basis for the previously mentioned LEON microprocessor family.

The JUICE satellite planned to visit Jupiter's moons, will use a LEON 2 microcontroller while the Ariane 6 launch vehicle will most likely use a LEON 3 microcontroller. It is interesting to note that, even though LEON 4 processors was already released in 2010, both JUICE and Ariane 6 (both planned for >2020) are using the previous versions of this microprocessor family. This shows that the space industry is extremely conservative when it concerns major missions. The reasons for this is mainly attributed to inability to replace faulty devices once launched, high cost of spacecraft (compared to most terrestrial equipment) and challenging and harsh conditions of launch and space.

# 1.4 | Failures in electrical systems and software

Failure Root Causes

- Software bugs
- Electrical design flaws
- Radiation effects
- Corrosion during pre-launch storage
- Thermal-electrical stress
- Thermal-mechanical stress
- Mechanical stress during launch
- Manufacturing and assembly errors

Typical failure root causes for satellite devices are:
- Software bugs and electrical design flaws. These failures are considered human errors and are a major source of onboard failures.
- Radiation damage of electrical devices.
- Component corrosion as a result of humid environments (prior to launch).
- Thermal-electrical and thermal-mechanical stresses as a result of the extreme thermal environment in space. These phenomena can lead to open or short circuits or change the electrical properties of a device.
- Mechanical damage as a result of the extreme vibrations during the launch.
- Component manufacturing and assembly errors.

Most failures are related to software and electrical systems. While these failures are seen throughout the entire spacecraft, failure detection, isolation and recovery is typically a major task of the OBC and should be well thought through when designing the CDHS. Therefore this subtopic is addressed within this first major topic of CDHS.
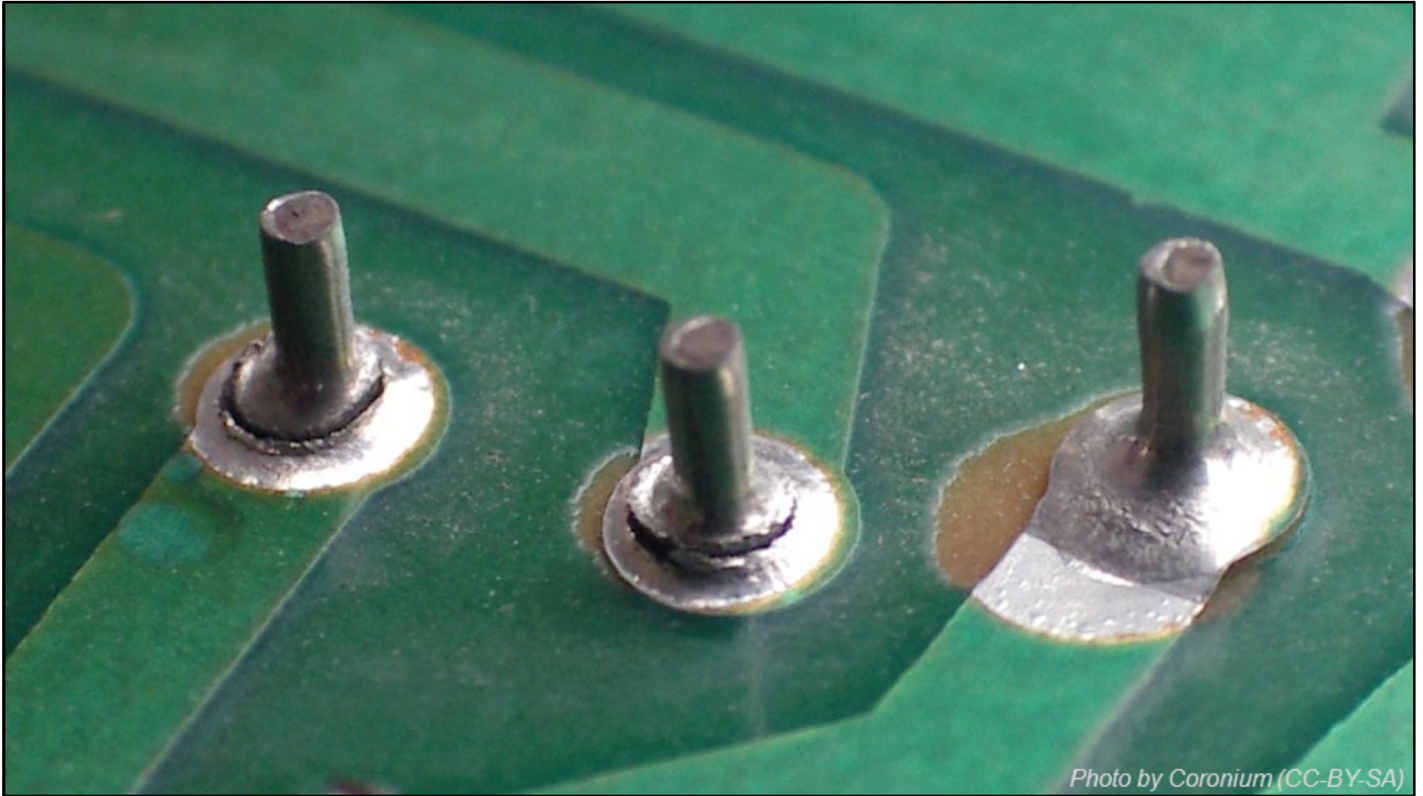
This photo provides an example of what thermal-mechanical stress can do to a bad solder joint. This may actually be a combination of a design flaw (solder joints should be free of stress) and a production flaw (bad soldering). Like in this example, most failures are rather trivial to understand. A special type of root cause for failures, radiation effects, are however treated more elaborate next.
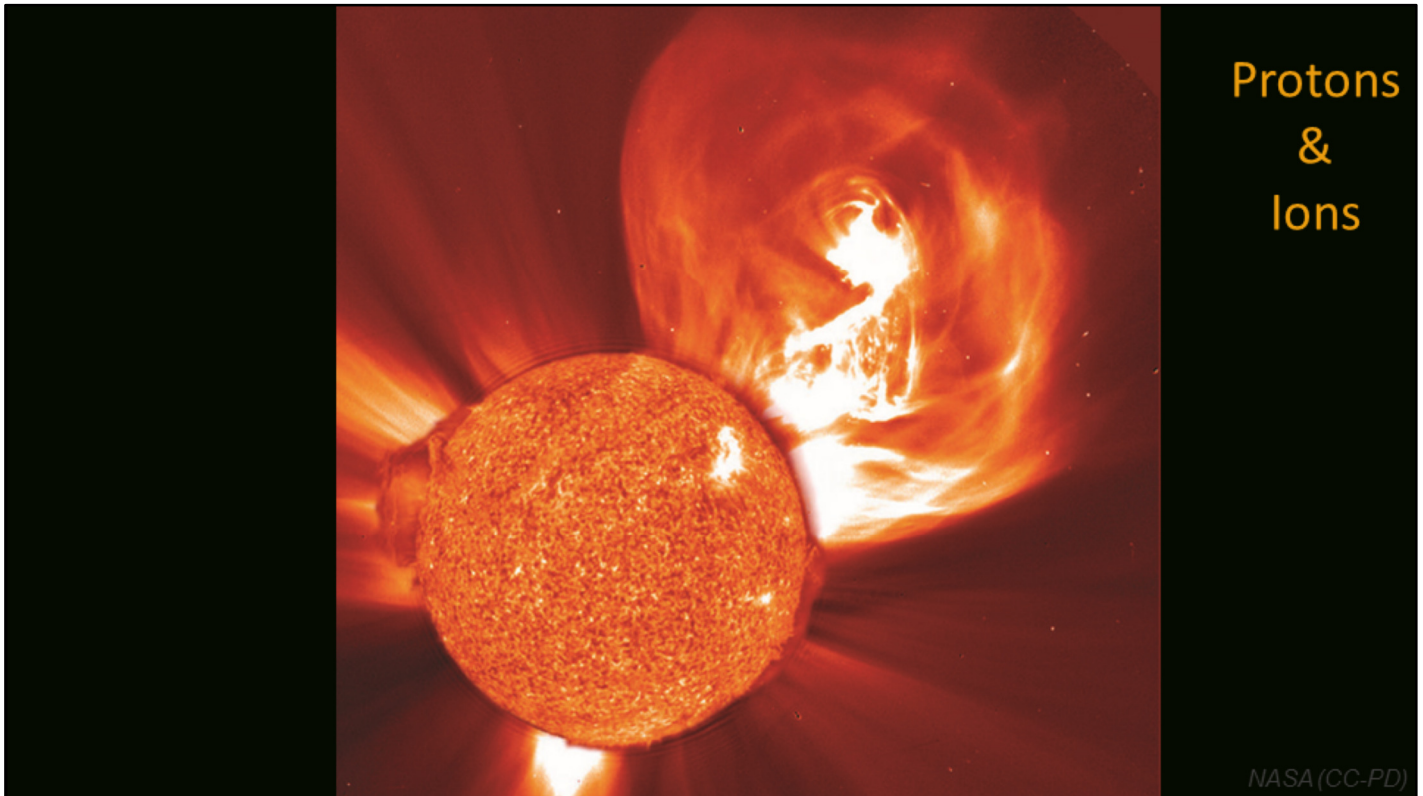
There is an abundance of particle radiation in space. Particles such as protons and ions are blasted into space in all directions by solar eruptions. Even though the Sun experiences an 11 year cycle of active maximum and a passive minimum, the rate, direction and occurrence of these eruptions are incredibly hard to predict.
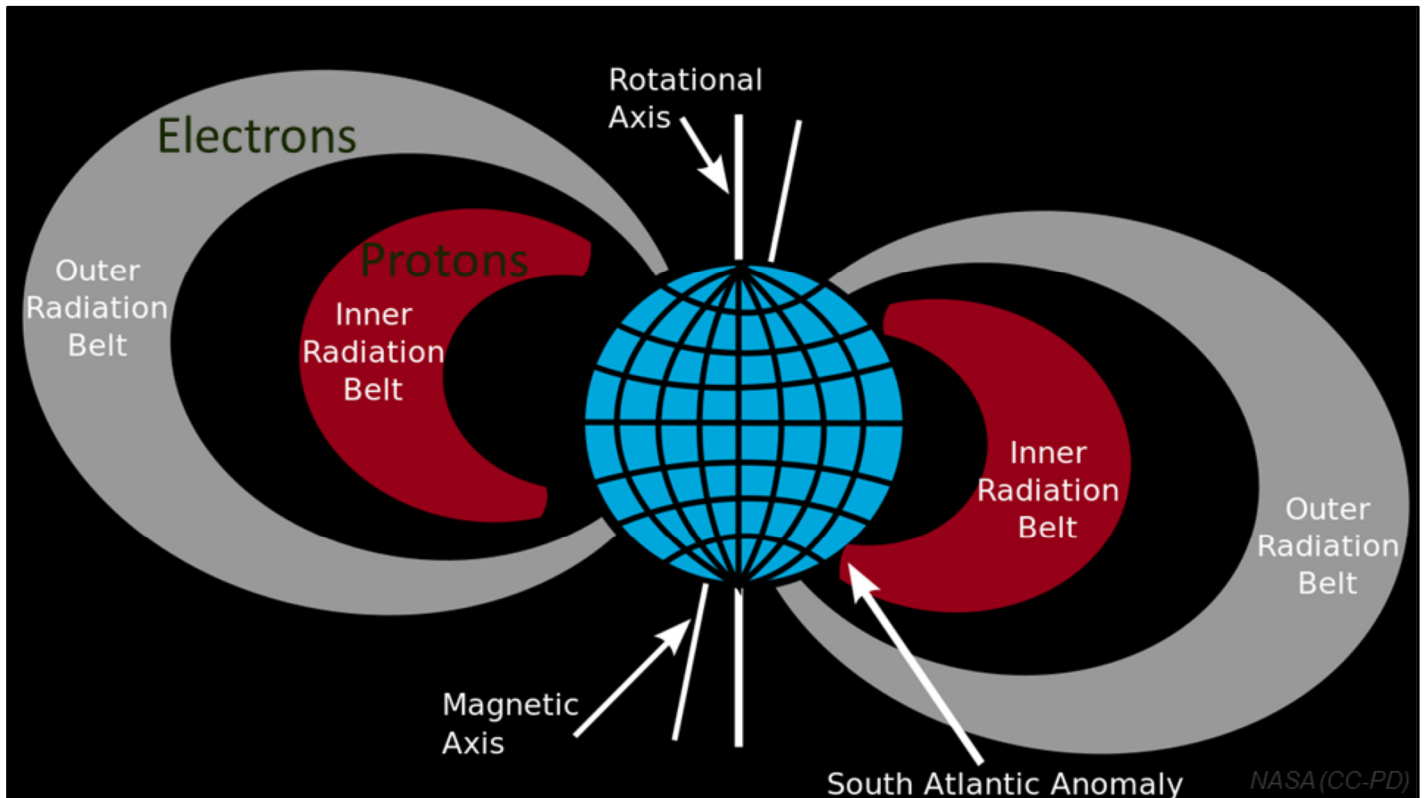
This picture depicts the famous Van Allen belts. The Earth's magnetic field traps the more energetic protons in the inner belt and the electrons in the outer belt. The higher energy levels of the protons make it harder to implement effective shielding. The South Atlantic Anomaly (SAA) is an area above the South Atlantic where the inner Van Allen belt comes very close to the Earth's surface and crosses low Earth orbits. Satellites experience a higher number of radiation events when they are passing through the South Atlantic Anomaly.

Single Event Upsets UOSAT-3
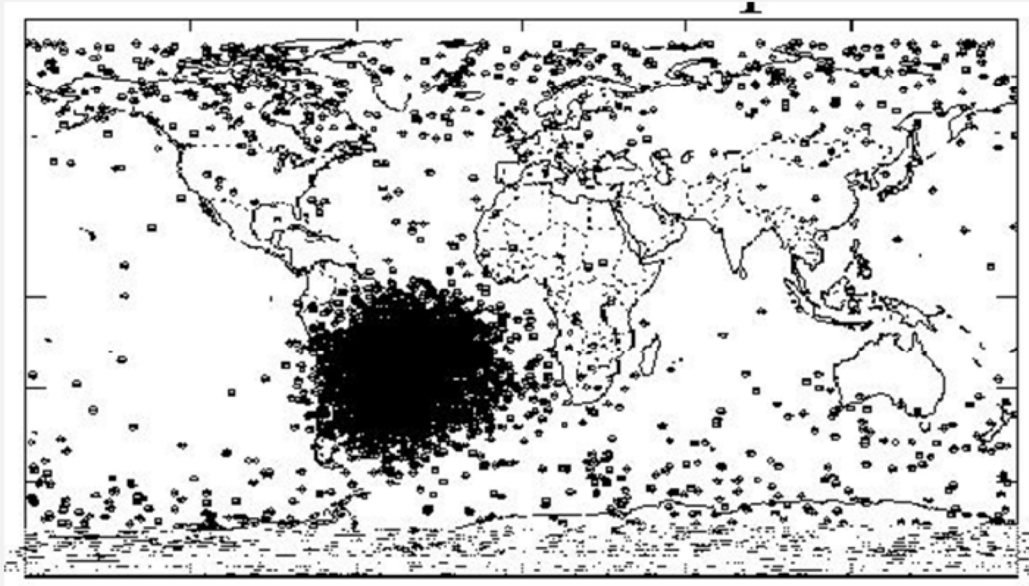
(c) ESA

In this graph all the detected radiation events of a satellite called UOSAT-3 are plotted. This clearly shows the impact of the SAA.
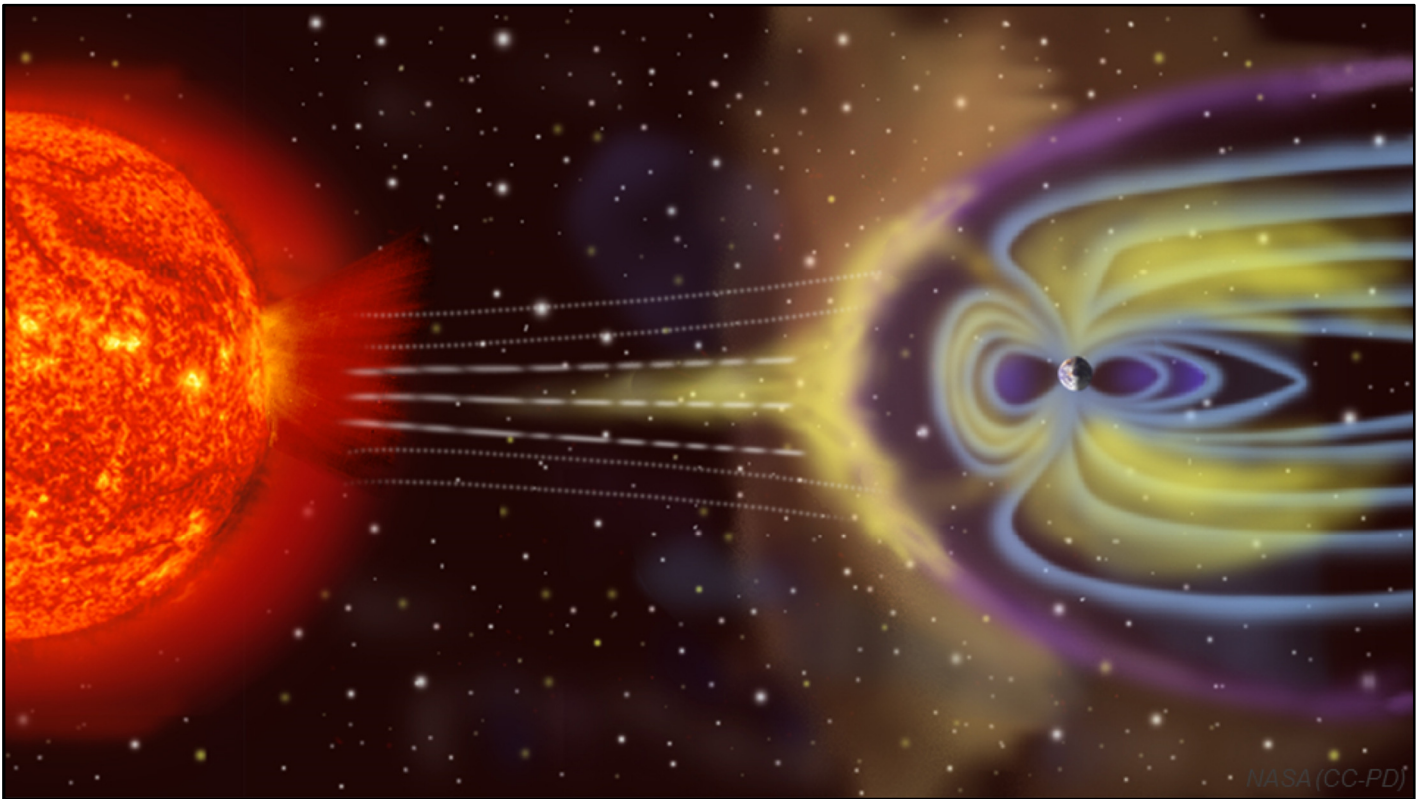
While the magnetic field of the Earth is to blame for the van Allen belts, I should also note the this same magnetic field protects the Earth and low Earth orbits from the majority of particle radiation coming from the Sun.

Only near the poles, some of the Solar particle radiation still protrudes leading to the beautiful light phenomenon known as Aurora Borealis.

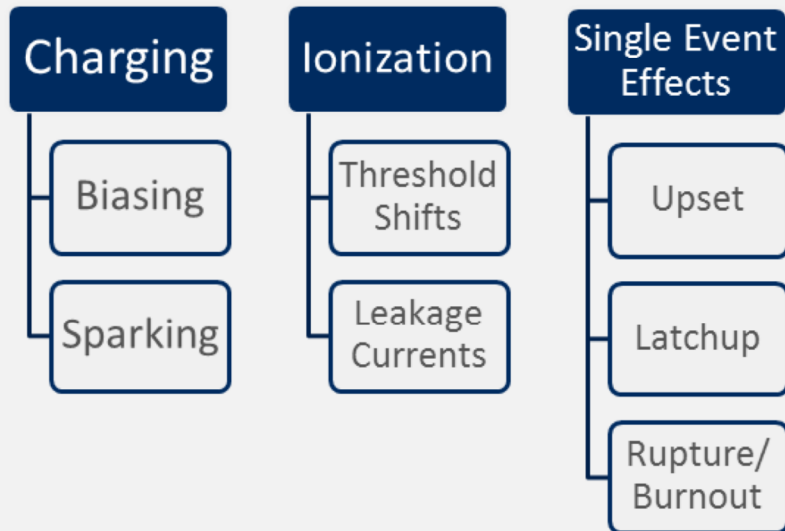Cosmic rays are a third source radiation (primarily protons and ions) and come from all kinds of sources in the universe. Radiation hitting the surface of a spacecraft structure or component can also lead to secondary radiation. Similarly, a high energy particle can also create bremsstrahlung radiation (comprising electromagnetic radiation, electrons and ions) as it decelerates inside the structure of the spacecraft.
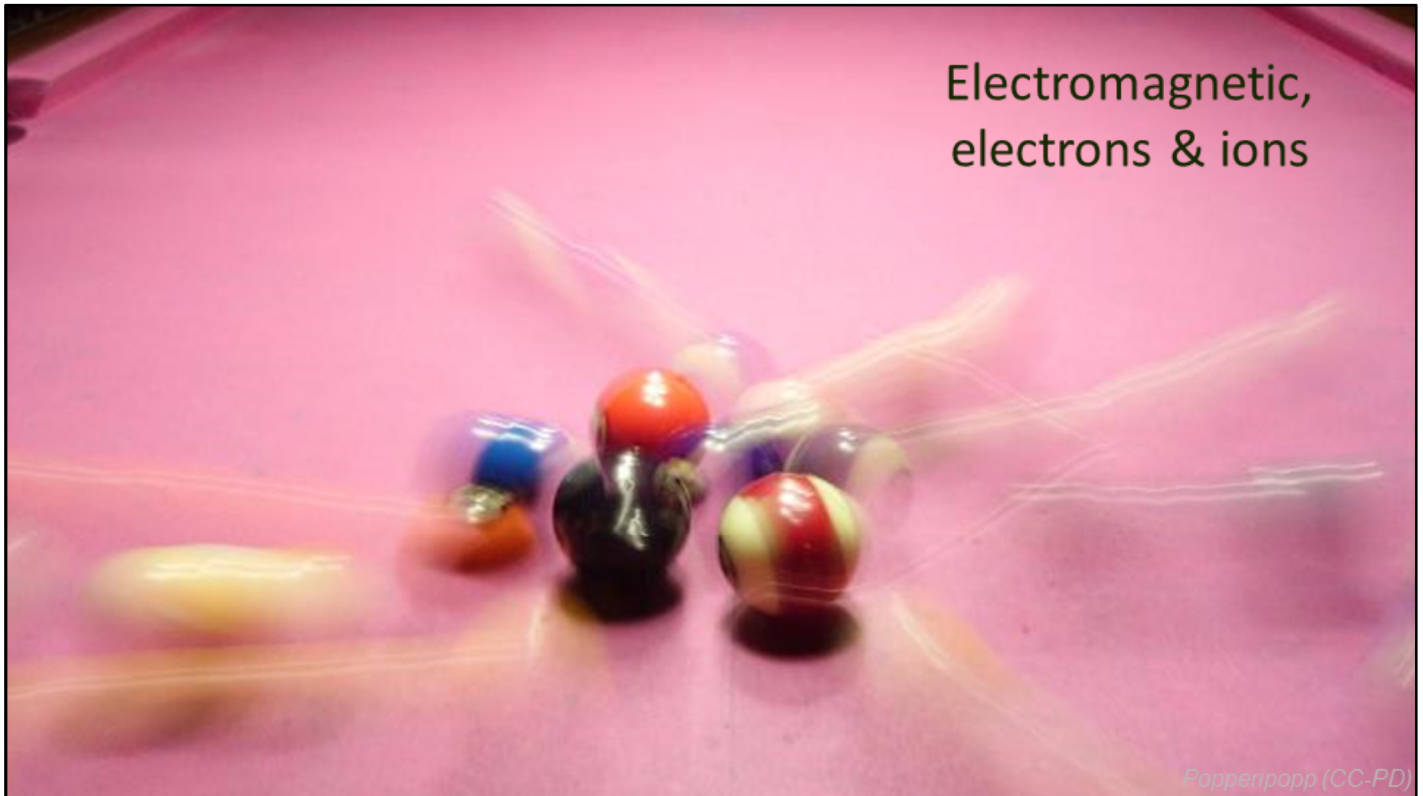
The word bremsstrahlung is German and means "braking radiation," since it involves high energy particles braking down. If a free electron encounters the nucleus of a heavy atom head-on (such as, for example, a semiconductor atom) the negatively charged electrons on the outside of the nucleus force the electron to lose kinetic energy. By the law of conservation of energy, this kinetic energy can't disappear into thin air, so a photon of a certain energy is emitted, generating bremsstrahlung. This phenomenon is actually an important generator of x-rays.

Radiation Effects

Charging
- Biasing
- Sparking

Ionization
- Threshold Shifts
- Leakage Currents

Single Event Effects
- Upset
- Latchup
- Rupture/Burnout

Charging
When an insulator prevents the flow of electrons, a buildup of electrons can occur. This is referred to as charging and can create a voltage potential which can lead to biasing of transistors. It can also lead to sparking if the voltage level becomes too high for the insulator to withstand. Sparking can lead to transients in the circuit with potentially harmful consequences. A proper grounding of the body and the solar panels can prevent most charging issues.

Ionization
Ionization occurs when the atoms or molecules within the electronics lose or gain an electron as a result of impact with a radiation particle. A single ionization event does not significantly change the properties and behavior of electrical components, however over time ionization can change the threshold values or lead to high leakage currents.

Single event effects
Single event effects are events which occur immediately after a radiation particle impact. Single event upset causes a logic state change within a digital component and results in a bit-flip in the memory or software. If the heat released by a particle changes the properties of the material locally, a short circuit can occur in the component. This is called single event latch-up and if it persists, it can have a cascading effect on other parts of the circuit or integrated circuit eventually resulting in permanent fault. A rupture or burnout is direct destruction of the component or logic unit in an integrated circuit. Countermeasures for this type of failure are limited but luckily so is the probability of occurrence.

Ionization

- Cumulative effect; Total Ionization Dose (rad)
- COTS integrated circuits: 1 – 10 krad
- Radiation hardened electronics: 100 krad – 1Mrad
- Aluminium (structure) is a good shielding material

A measure to quantify ionization is the Total Ionization Dose (TID) which is expressed in the radiation absorbed dose (rad). Radiation hardened electronics can operate up to much higher doses of ionization. Commercial Of The Shelf (COTS) integrated circuits can typically sustain less than 10 kilorad before they start to malfunction. Since, hardly any radiation testing is performed on these devices, the exact radiation tolerance figure is never available. Radiation hardened electronics can sustain between 100 and 1000 kilorad and are generally accompanied by extensive radiation testing figures.

Radiation hardening is a combination of local shielding and a different transistor layout. The transistors are larger and consume more power than their commercial equivalents. Since the market is orders of magnitude smaller and the production process is more complex, prices are between 100 and 100,000 times higher.

(c) ESA
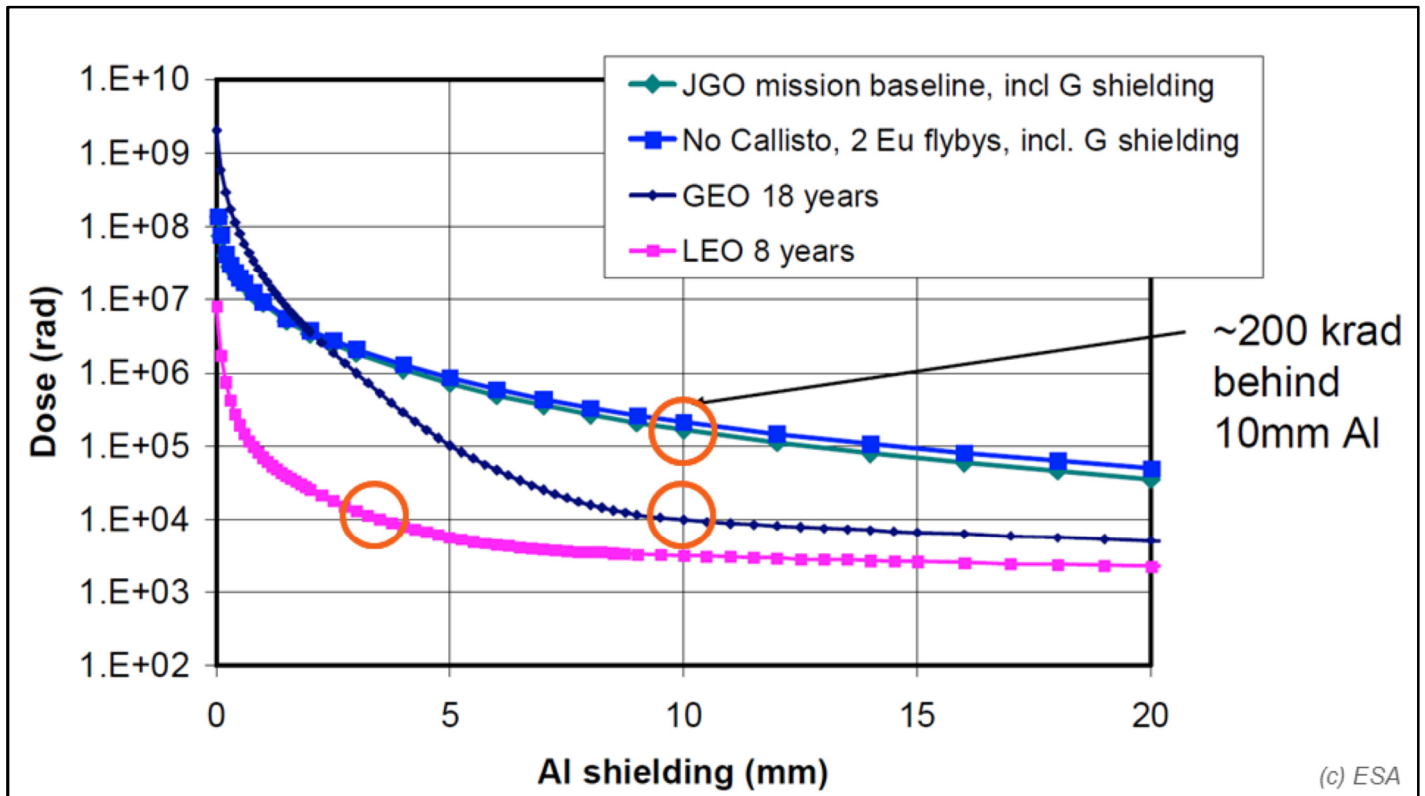
The most commonly used material for radiation shielding in space applications is aluminium. This lightweight material can be used for the outer structure of the spacecraft and will simultaneously shield the electronics inside. The thickness of the panel is directly proportional to the amount of radiation shielding. Multiple layers of shielding can be applied around the electronics to increase the effect. It is however important to note that shielding in close proximity to the actual electronics can lead to a larger flux of Bremsstrahlung.

The figure illustrates the relationship between the thickness of the aluminum shielding and the total ionization dose on a logarithmic scale. The lower purple plot, indicating a Low Earth Orbit mission with a duration of 8 years, illustrates that a shielding thickness of 3 mm will ensure that the total ionization dose would remain below 10 kilorad. If the mission time is sufficiently small and a small measure of risk is allowed, commercial of the shelf electronics can be used for such a mission. For a geostationary orbit and a mission lifetime of 18 years, a shielding thickness of at least 10 mm is required to be able to safely use commercially of the shelf electronics. Although not impossible, due to the high cost and critical functions of geostationary satellites, commercial of the shelf components are typically avoided on these missions.

The radiation levels near Jupiter (as experienced by the JUICE mission) indicate that even 10 mm of shielding will still result in 200 kilorad of total ionization. For these types of missions, commercial of the shelf electronics will simply not suffice.

Latchups

- Integrated circuits are short circuited due to a parasitic structure
- Triggered by heavy ions, protons, neutrons
- CMOS technology most susceptible
- Silicon-on-Insulator (SoI) makes ICs immune
- Fast and adequate detection and power cycling can resolve a major part of latchups

A latch-up occurs when a radiation particle creates a parasitic structure in an integrated circuit. In some locations this can lead to a short circuit. Latch-ups are triggered by heavy ions, protons and neutrons. Complementary Metal Oxide Semiconductor (CMOS) is one of the most popular semiconductor technologies. High noise immunity and very low power consumption are the primary reason for their popularity. Unfortunately, this technology is also highly susceptible to latch-ups. This susceptibility can be mitigated by using silicon-on-insulator substrates for the integrated circuits. The insulator in the substrate prevents parasitic structures which can cause a latch-up. Furthermore, the produced integrated circuits are generally faster and more efficient than CMOS on bulk silicon substrates. The manufacturing cost for silicon-on-insulator is approximately 10% higher which represents the barrier that prevents major availability. Fortunately, further miniaturization and speed improvements resulting from the use of this substrate, means that more commercial electronics will make the step towards silicon-on-insulator.

Aside from the previously discussed manufacturing techniques, fast and adequate detection and power cycling can also resolve latch-ups in time. Power cycling electronic devices can eliminate the parasitic structure caused by radiation particles. This mechanism can be designed around the integrated circuit or as part of the integrated circuit itself.

Measures to mitigate failures

- Redundancy
- Failure Detection, Isolation and Recovery (FDIR)
- Component selection
    - Radiation hardened
    - Fault tolerant
    - Screening of COTS
    - Flight heritage
- Conformal coating
- **Testing!**

Redundancy

A "simple" method of dealing with failures is to provide redundancy. The concept is that spare systems or components can replace the function of faulty ones. Although simple in theory, in practice the following challenges must be considered:

- For some applications the state of the spare system has to mirror the state of the primary system. This can be complex and power consuming.
- Redundancy does not eliminate failures caused by human errors in design and testing.
- The total ionization dose on the spare system will be equal to the primary system regardless of which system is currently in use.

Some of these challenges can be overcome with the use of a backup solution instead. A backup system is different in design and/or performance from the primary system. It could be used to protect against human errors and/or radiation effects (even TID) as it uses a different (often more simple) circuit. It will however increase the complexity of the overall design.

Regardless of the technique, if properly implemented, redundancy can lower the probability of system failure. To properly implement redundancy, onboard autonomy is required to detect a failure on a subsystem or component, isolate it and switch over to the backup system.

Failure Detection, Isolation and Recovery (FDIR)

Failure Detection, Isolation and Recovery (FDIR) can also be used to deal with soft errors such as data bus lockup or anomalous behavior of software. FDIR can also be used for graceful degradation. Graceful degradation is the concept of balancing performance and available resources. For instance, graceful degradation policies can implemented in the onboard computer to apply lower duty cycles of a payload to deal with less available solar power as a result of partial solar array failure. This approach allows the satellite to continue and accomplish the critical objectives of the mission at a reduced performance level.

Measures to mitigate failures (cont'd...)

- Redundancy
- Failure Detection, Isolation and Recovery (FDIR)
- Component selection
    - Radiation hardened
    - Fault tolerant
    - Screening of COTS
    - Flight heritage
- Conformal coating
- **Testing!**

Component Selection

Proper component selection can prevent a large number of failure types. Aside from radiation hardened electronics, fault tolerant components are also important for space applications. These devices can sometimes include integrated circuits which compute the same step multiple times and compare the outcome to determine its validity. Internal latch-up protection and FDIR are also often implemented in fault tolerant integrated circuits.

Unfortunately, most if not all commercial of the shelf electronics do not provide the specifications of radiation tolerance and internal failure measures. Some of these specifications can be obtained by manually screening these components by testing them in a radiation particle accelerator facility and thermal cycling chambers.

A very popular measure to improve reliability is to select components with flight heritage. Although limited flight heritage does not provide significant statistical output to quantitatively assess the reliability, many potential design flaws become less of a concern. For large expensive spacecraft, the need for flight heritage results in a conservative attitude towards technology and prevents innovation. Even for CubeSats, flight heritage is sometimes used as a major trade-off criterion.

Conformal coating

Conformal coating is a thin polymeric film which is applied over a fully assembled electronic board. It protects the board against the environment such as moisture, provides extra structural rigidity to the circuit and improves the thermal handling capability. The improvement in reliability may be subtle, but the low cost and easy process makes conformal coating an attractive solution for most high reliability applications.

Measures to mitigate failures (...cont'd)

- Redundancy
- Failure Detection, Isolation and Recovery (FDIR)
- Component selection
    - Radiation hardened
    - Fault tolerant
    - Screening of COTS
    - Flight heritage
- Conformal coating
- **Testing!**

Testing

The most important measure to improve reliability is testing. Unfortunately, as testing is the final stage before delivery to the integrator or the launch provider, it often falls victim to time and budget mismanagements. To improve and facilitate the testing procedures, it is vital to take testing into account when designing a spacecraft. For instance, when designing software or electrical circuits, it is important to allow each part to be testable both individually and as a whole. It is also important to note that, redundancy and FDIR have the potential to become hazards if not properly tested and often require the most comprehensive testing regimes.