TXMISSION

Improving Smallsat Reliability

Technology White Paper

Industry analysis shows that up to 15% of smallsats do not complete their missions successfully. Ambitious, enterprising business models and longer operational lifetimes are driving the need for ever more reliable smallsats. Lifetime reliability engineering is a well-understood discipline but generally comes with a hefty price tag. We describe a cost-effective, novel architecture for enhancing the reliability of smallsat communications systems. By adding intelligent dynamic monitoring and handling of abnormal operational events, failures can be mitigated and reliability increased. The techniques are described in relation to Software Defined Radios (SDRs) but have wider application across all smallsat subsystems.

Overview

MissionCast™ is the name we have given to the sophisticated watchdog monitor function that runs on all our Software Defined Radios (SDRs). This comprises:

- Dedicated hardware in the form of an independent watchdog processor, memory, clock source and power supply. The standard devices that implement the watchdog can optionally be replaced with radiation hardened components to provide reliable operation even in harsh electromagnetic environments.
- Software that continually monitors all power supplies, clocks, sensors, interfaces, alarms and main processor operation for abnormal events and responds with various remedial strategies ranging from reprogramming of devices to soft and hard resets of individual devices, subsystems or the whole SDR.

In many designs, failure mode analysis is used to increase understanding of potential system failures and thereby facilitate the creation of designs where the main perceived risks of failure have been ameliorated or eliminated. By contrast, the philosophy embedded in MissionCast™ is quite different and complementary – it is no less than the intelligent active management of all undesirable events that happen in real operation. As such, it does not rely on pre-conceived ideas of what may go wrong.

'... New Space applications require new thinking: increasing reliability through the intelligent active management of all undesirable events that happen in real life ...'

While the concept of a watchdog monitoring function is not new, historically, they have often been based on simple logic and have been implemented using the same hardware and software resources that the watchdog itself is tasked with monitoring, rather than being an independent component of the design.

In this whitepaper, we describe how the humble watchdog can be transformed into a modern thoroughbred with much more bite.

MissionCast™ Operation

The function of the MissionCast™ watchdog is to perform automated status monitoring, fault reporting and fault mitigation. Status information and fault messages are stored in the watchdog's non-volatile memory, meaning that historical information continues to be available even after an interruption to the power supply. Status and fault messages can be output in real time via the watchdog's internal CAN bus, which is a robust interface that can be connected to the flight computer or other management system. Other forms of reporting using interfaces that lie outside of the watchdog circuit, such as Ethernet, are also supported.

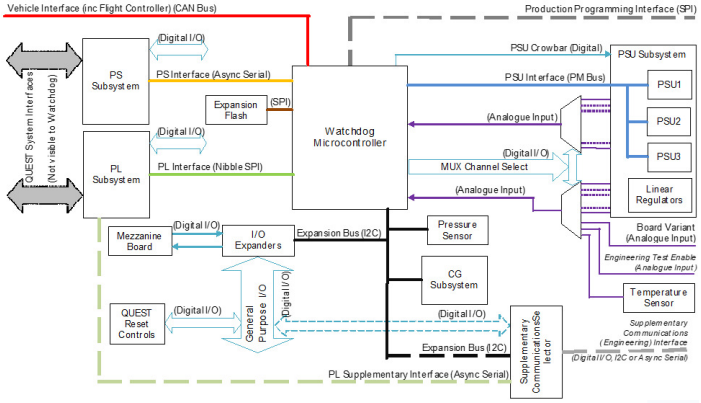
Customization

During manufacture, the watchdog's executable image and configuration data is programmed into the hardware. Nothing further is required other than to power on the SDR, at which point the watchdog runs completely autonomously from all other SDR subsystems and will manage all other system resources such as power supplies and clocks. A key design goal has been to ensure that when faults arise, they cannot interfere with or subvert the operation of the watchdog.

The watchdog subsystem will recognize any customization of the SDR that has taken place and will automatically adapt its fault detection and remedial action strategy to suit the capabilities of the individual platform. This is designed to ensure maximum system availability in all circumstances.

Watchdog Services

The watchdog subsystem provides the following services:



MissionCast™ Watchdog Monitoring Subsystem

- Active operational configuration of multiple pre-defined variants of the SDR platform to ensure consistency between the operational feature set and the continuous monitoring being performed by the watchdog.
- Controlling the detailed startup sequence based on the underlying interdependencies of the various SDR subsystems.
- Monitoring and reporting of the SDR status
- Taking remedial action when subsystem failures are detected. Any remedial action taken by the watchdog, such as forcing a restart, will be recorded and stored in the watchdog's non-volatile memory.
- Performing a safe, controlled shutdown of defective circuitry when no remedial action is possible, thereby eliminating the potential for faults to propagate to other smallsat subsystems and minimizing power consumption.

When power is applied to the SDR, initially only the watchdog is powered up. Power supply voltages, permissible currents, power ratings, warning and fault recognition threshold levels are then applied by the watchdog to the rest of the SDR, along with the settings for all system clock generation.

Monitoring and Diagnostics

The watchdog monitors key parameters of the SDR and will:

- Identify and generate warning reports on subsystems that are approaching their operational limits.
- Identify and generate fault reports with respect to key performance indicators that have reached or exceeded their operational limits.
- Monitor a 'heartbeat' message to provide confidence that the SDR processor subsystem is behaving normally.
- Generate a periodic report on the key parameters for internal and external logging purposes.

When generating diagnostics, the watchdog uses various measurements:

- Input voltage, current and power for each PSU subsystem
- Output voltage, current and power for each voltage rail
- Internal temperature of each PSU subsystem
- Voltage and temperature measurements

Periodic measurements of key parameters are made by the watchdog, with more volatile signals being measured more frequently. Diagnostics are generated from the measurements based on the acceptable range of values and the variation in the values that are read. The diagnostics are stored in non-volatile memory and are forwarded to the main processor system at least once a second.

Each subsystem of the SDR is responsible for its own performance management. Consequently, if the watchdog detects a parameter as being out of bounds then it indicates that the relevant subsystem has malfunctioned and requires the intervention of the watchdog to correct the situation. Failure to acknowledge receipt of the heartbeat message also indicates a subsystem failure.

Summary

A small investment in additional onboard diagnostic monitoring capabilities can significantly enhance smallsat reliability by taking the appropriate remedial action when faults occur. Reliability is further enhanced by implementing the monitoring function as an independent subsystem using radiation hardened devices.