

KONGR45GPEN

DESIGN OF FAULT DETECTION, ISOLATION AND RECOVERY IN THE ACUBESAT NANOSATELLITE

DRAFT SPACEDOT (THE TITLE PAGE WILL CHANGE)

Copyright © 2021 kongr45gpen

PUBLISHED BY DRAFT SPACEDOT (THE TITLE PAGE WILL CHANGE)

TUFTE-LATEX.GITHUB.IO / TUFTE-LATEX /

Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

The AcubeSAT project is carried out with the support of the Education Office of the European Space Agency, under the educational Fly Your Satellite! programme.

The views expressed herein by the authors can in no way be taken to reflect the official opinion, or endorsement, of the European Space Agency.

First printing, 2021

Contents

1	<i>Reliability Engineering in CubeSat Systems</i>	13
1.1	<i>Kalispera</i>	13
2	<i>The AcubeSAT mission</i>	15
2.1	<i>CubeSat</i>	15
2.2	<i>Subsystems</i>	15
2.2.1	<i>Attitude Determination and Control Subsystem (ADCS)</i>	15
2.2.2	<i>Communications (COMMS)</i>	16
2.2.3	<i>Electrical Power Subsystem (EPS)</i>	17
2.2.4	<i>On-Board Data Handling (OBDH)</i>	18
2.2.5	<i>On-Board Software (OBSW)</i>	18
2.2.6	<i>Operations (OPS)</i>	18
2.2.7	<i>Structural</i>	19
2.2.8	<i>Systems Engineering (SYE)</i>	20
2.2.9	<i>Science Unit (SU)</i>	20
2.2.10	<i>Thermal</i>	22
2.2.11	<i>Trajectory</i>	22
2.3	<i>Tools used</i>	22
3	<i>The SAVOIR Fault Detection, Isolation and Recovery (FDIR) concept</i>	23
3.1	<i>The ECSS Packet Utilisation Standard</i>	23
3.1.1	<i>The ECSS services</i>	23
3.2	<i>The SAVOIR standard</i>	25
4	<i>Fault Detection, Isolation and Recovery (FDIR) in AcubeSAT</i>	27
4.1	<i>Fault Detection, Isolation and Recovery (FDIR) principles</i>	27

4.2	<i>Failure causes and recovery actions</i>	27
4.2.1	<i>Failure causes</i>	27
4.2.2	<i>Preventive actions</i>	27
4.2.3	<i>Corrective actions</i>	27
4.3	<i>Fault Detection, Isolation and Recovery (FDIR) operating modes</i>	27
5	<i>Practical demonstration of Fault Detection, Isolation and Recovery (FDIR)</i>	
	29	
5.1	<i>System Description</i>	29
5.1.1	<i>Hardware</i>	29
5.1.2	<i>Flight Segment Software</i>	30
5.1.3	<i>Ground Segment Software</i>	31
5.2	<i>Fault Detection, Isolation and Recovery (FDIR) setup</i>	31
5.3	<i>Test results</i>	31
	<i>Bibliography</i>	35
	<i>Source code</i>	37

List of Figures

- 2.1 The SatNOGS COMMS board 16
- 2.2 Dynamic power budget analysis. Left: Power consumption & generation for the orbit. Right: Battery discharge level throughout the mission 17
- 2.3 Safe mode functional flow 20
- 2.4 The CubeSat's 3U 20
- 2.5 Example mission image output Arampatzis *et al.*, *AcubeSAT Pay-load DDJF* 20
- 2.6 The microfluidic chip and its separation into 3 subexperiments and 1 test line. The fluid inlets are shown on the left side of the chip, while the outlets are on the right. *Green*: flow layer. *Blue*: control layer. 21
- 2.7 Ground track of an example AcubeSAT orbit, generated using NASA'S General Mission Analysis Tool 22

- 3.1 The Packet Utilisation Standard (PUS) data transfer model 23
- 3.2 blablabla 26

- 5.1 High-level block diagram of the demonstration system 29

List of Tables

2.1	Maximum Attitude Determination and Control Subsystem (ADCS) error values after stabilisation	16
2.2	AcubeSAT nominal mode power budget	17
2.3	Overview of AcubeSAT functionality on different modes	19
5.1	List of new software developed for this thesis	30
5.2	List of used software libraries	31
5.3	List of ST[20] parameters	31

Acronyms

<i>ADCS</i> Attitude Determination and Control Subsystem	<i>15–18</i>
<i>CAN</i> Controller Area Network.....	<i>18</i>
<i>CCSDS</i> The Consultative Committee for Space Data Systems	<i>16</i>
<i>CDR</i> Critical Design Review	<i>15</i>
<i>COMMS</i> Communications	<i>16, 17</i>
<i>COTS</i> Commercial Off-The-Shelf	<i>15, 17</i>
<i>ECSS</i> European Cooperation for Space Standardization	<i>23, 29</i>
<i>EMC</i> Electromagnetic Compatibility	<i>16</i>
<i>EPS</i> Electrical Power Subsystem.....	<i>16, 17</i>
<i>ETL</i> Embedded Template Library	<i>30</i>
<i>FDIR</i> Fault Detection, Isolation and Recovery	<i>25, 31, 33</i>
<i>FDIR</i> Fault Detection, Isolation and Recovery ..	<i>13, 15, 16, 21, 23, 25,</i> <i>27, 29, 30</i>
<i>GS</i> Ground Station.....	<i>15, 16, 24</i>
<i>I²C</i> Inter-Integrated Circuit	<i>30</i>
<i>ISM</i> Industrial, Scientific, Medical	<i>16</i>
<i>LEO</i> Low Earth Orbit	<i>20</i>
<i>MCU</i> microcontroller (MicroController Unit)	<i>18, 29, 30</i>
<i>MPPT</i> Maximum Power Point Tracking	<i>17</i>
<i>MRAM</i> Magnetoresistive Random-Access Memory	<i>18</i>
<i>OBC</i> On-Board Computer	<i>17, 18</i>
<i>OBDH</i> On-Board Data Handling.....	<i>17</i>
<i>OBSW</i> On-Board Software	<i>18</i>
<i>OPS</i> Operations	<i>18</i>
<i>PA</i> Product Assurance	<i>15</i>
<i>PCB</i> Printed Circuit Board	<i>20</i>

<i>PCDU</i> Power Conditioning & Distribution Unit	17
<i>PDMS</i> Polydimethylsiloxane	20, 22
<i>PUS</i> Packet Utilisation Standard	23, 25, 30
<i>RF</i> RadioFrequency	16, 23
<i>RTOS</i> Real-Time Operating System	18, 30
<i>SAVOIR</i> Space AVionics Open Interface aRchitecture	29
<i>SRAM</i> Static Random Access Memory	29
<i>SU</i> Science Unit	17, 20
<i>SYE</i> Systems Engineering	20
<i>TC</i> Telecommands	16, 23–25
<i>TM</i> Telemetry	16, 24
<i>UHF</i> Ultra-High Frequency	16, 19

Abstract

Space is not a welcoming environment; while the aerospace engineering community has managed to reliably operate thousands of satellites in orbit, CubeSats, the most popular class of nanosatellite, only have a 50% success rate. Low costs, lack of strict technical requirements and scarcity of publicly available documentation often drives up the risks for educational, scientific and commercial CubeSats. This thesis investigates a configurable and modular Fault Detection, Isolation and Recovery (FDIR) architecture that uses the ECSS Packet Utilisation Standard. This FDIR concept, along with the provided open-source software implementation, can be used by CubeSat missions to increase the reliability of their design and chances of mission success, by autonomously responding to on-board errors. The thesis also includes background information regarding CubeSat reliability, and explores the software and hardware used to implement the proposed FDIR design on the AcubeSAT mission, currently under design by students of the Aristotle University of Thessaloniki.

KAPOU EDW tha mpei kai to abstract sta ellhniKa

1

Reliability Engineering in CubeSat Systems

1.1 Kalispera

space is very important¹ Fault Detection, Isolation and Recovery (FDIR)

¹ Durou *et al.*, “Hierarchical Fault Detection, Isolation and Recovery Applied to Cof and Atv Avionics.”

2

The AcubeSAT mission

2.1 CubeSat

2.2 Subsystems

The AcubeSAT nanosatellite is technically and programmatically split into **N** different subteams or **subsystems**, each responsible for a different section of the satellite, and made up out of **M** dedicated members.

In the following sections, a brief introduction on the function and design of each subsystem is presented. As the Systems Engineering and Product Assurance process is inherently connected to the function of all subsystems, the details relevant to FDIR are also mentioned. For more detailed information, the reader is encouraged to refer to [AcubeSAT's website¹](#), or to the publicly available [Critical Design Review \(CDR\) documents²](#).

2.2.1 Attitude Determination and Control Subsystem (ADCS)

The ADCS subteam is responsible for controlling the **attitude** and orientation of the spacecraft in orbit. This is achieved using a series of Commercial Off-The-Shelf (COTS) control actuators (one 3-axis magnetorquer board, one 1-axis reaction wheel), sensors for attitude determination (1 gyroscope and 2 magnetometers), and filtering, determination & control algorithms.³

The ADCS can operate under different pointing profiles for different attitude needs:

1. **Detumbling**, where the satellite is attempting to minimize its angular acceleration close to 0, to ensure a stable communications link, prevent detachment of parts and allow easier regaining of pointing.

Detumbling mode is implemented in the simplest possible way, using only one of the 2 redundant magnetometers and a simple control algorithm. It is activated when there is no need to apply any of the specific pointing modes, or if the spacecraft angular rate is too high. In AcubeSAT, system-wide *Safe Mode*, *Commissioning Mode* and *Science Mode* apply detumbling.

¹ <https://acubesat.spacedot.gr/subsystems/>

² <https://gitlab.com/acubesat/documentation/cdr-public>

³ Savvidis *et al.*, [AcubeSAT AOCS DDJF](#).

2. **Nadir pointing**, where the satellite points the $+X$ side towards the Earth. This profile is used during *Nominal Mode* on passes over the Ground Station, where the directional patch antenna needs direct visibility.
3. **Sun pointing**, where the satellite points two sides to the sun with a 45° angle of incident each, in order to maximise solar panel input. This profile is used during *Nominal Mode*, between GS passes, in order to ensure a positive power budget.

The performance of the ADCS system can be summarised using performance metrics such as the ones presented in Table 2.1.

Table 2.1: Maximum ADCS error values after stabilisation

Error	Value
Absolute Performance Error	$< 30^\circ$
Absolute Knowledge Error	$< 1^\circ$

2.2.2 Communications (COMMS)

The communications subsystem is responsible for transmitting data between the Earth and the spacecraft in orbit. The transmitted data is split into 3 different categories:⁴

- **Telecommands (TC):** Commands from the Earth to the satellite. They can be used to request information, or to perform specific spacecraft actions.
- **Telemetry (TM):** Information sent from the satellite towards Earth, typically including vital information such as sensor values, system status, timestamps and events.
- **Science data:** The scientific data generated by the payload. These are the highest-volume data and represent the main scientific output of the mission.

It is important to mention that the satellite orbit only allows for a very short visibility duration every day, increasing the needs for on-board autonomy and the importance of a correctly implemented FDIR method.

The main component of the COMMS subsystem is the **SatNOGS COMMS board**,⁵ an open-source RF transceiver developed by the **LibreSpace Foundation**, based on CCSDS telecommunications standards.

Communication will take place using 2 frequency bands on the ISM range, namely 436.5 MHz and 2.425 GHz, supported by a deployable turnstile and a directional patch antenna respectively. The use of ISM frequencies allows easy radio-amateur access to the satellite. The first (UHF) band also emits a periodic **beacon**, listing information about satellite status.

The communications subsystem is also responsible for the Electromagnetic Compatibility (EMC) analysis and interference mitigation, as well as the design and construction of the satellite Ground Station. The Ground Station will be part of **SatNOGS**,⁶ a global network of satellite ground stations based on open technologies and open data.

⁴ Kapoglou and Chatziargyriou, *Acube-SAT TTC DDJF*.

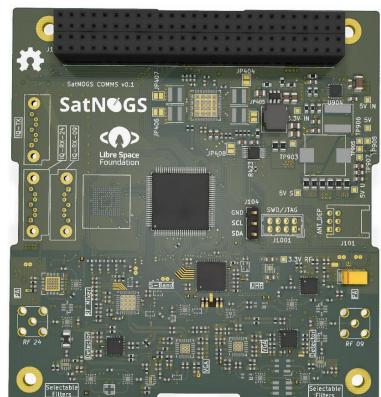


Figure 2.1: The SatNOGS COMMS board

⁵ Surligas, "SatNOGS-COMMS."

⁶ White et al., "Overview of the Satellite Networked Open Ground Stations (SatNOGS) Project."

2.2.3 Electrical Power Subsystem (EPS)

The EPS is the subsystem responsible for the generation, distribution and storage of electrical power of the spacecraft. It is a critical aspect of the spacecraft due to the direct dependence of all subsystems to the high power needs of many CubeSat subsystems, and is theorised to be the most common reason for CubeSat failure.⁷

AcubeSAT has opted for a COTS subsystem approach for the EPS.⁸

- **Solar panels** are procured from EnduroSat. Four 3U panels cover the X and Y faces of the satellite, and one 1U panel covers the -Z face.
- The **Power Conditioning & Distribution Unit (PCDU)** is procured from NanoAvionics and offers 10 switched channels with overcurrent protection over 4 voltage rails, as well as 4 Maximum Power Point Tracking (MPPT) converters.
- The **battery pack**, also procured from NanoAvionics, contains 4 18650 Li-Ion cells in a 2S2P⁹ configuration.

A dynamic approach is taken with regards to power budget calculation:

1. The in-orbit power generation is calculated for the duration of the mission using the **STK** software, taking into account satellite orientation, pointing profiles and eclipse, with a 1 min resolution.
2. The power consumption of the system is calculated on average for each different operational mode.
3. MPPT efficiencies and battery charge level are calculated for each timepoint, assuming worst-case thermal and electrical conditions
4. A system-wide 10% margin is applied to the results

We have created a Python library consolidating the above steps¹⁰ and producing the necessary outputs to prove the adequacy of the design.

⁷ Langer and Bouwmeester, "Reliability of CubeSats – Statistical Data, Developers' Beliefs and the Way Forward."

⁸ Anastasios-Faidon *et al.*, *AcubeSAT System DDJF*.

⁹ 2 series, 2 parallel

Table 2.2: AcubeSAT nominal mode power budget

Consumer	Power
ADCS	1.10 W
COMMS	0.85 W
EPS	0.99 W
OBC	0.12 W
SU	0.25 W
Total	3.30 W
Orbit Average Power	4.24 W

¹⁰ <https://gitlab.com/acubesat/eps/power-budget>

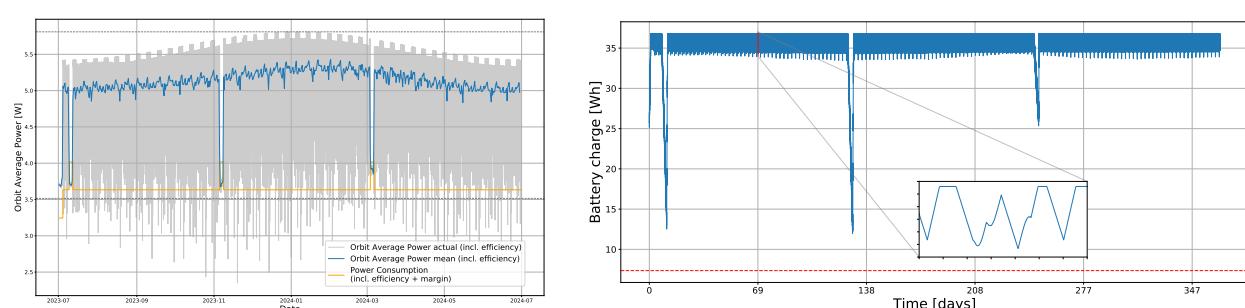


Figure 2.2: Dynamic power budget analysis. Left: Power consumption & generation for the orbit. Right: Battery discharge level throughout the mission

2.2.4 On-Board Data Handling (OBDH)

The OBDH subsystem is responsible for the design of the spacecraft's data interfaces, as well as the design of the **On-Board Computer (OBC)** board, tasked with controlling the basic spacecraft functions.¹¹

The OBC board contains the main OBC logic, and is based around a **Microchip SAMV71Q21RT**¹² radiation-tolerant microcontroller and an MRAM memory, used to store critical data. The board also hosts the in-house implemented components of the ADCS subsystem, as a space-saving measure.

AcubeSAT's data interface is using a cold-redundant Controller Area Network (CAN) bus to facilitate cross-subsystem communication, selected due to its robustness and reliability.¹³ AcubeSAT boards implement the PC/104 mechanical interface.¹⁴

2.2.5 On-Board Software (OBSW)

The OBSW subsystem is responsible for the design and development of the nanosatellite's software. The language chosen to be used in the system's 4 microcontrollers (MCUs) is a reduced form of C++, and the code is guarded under a number of standards, static checkers and unit tests.¹⁵ All software runs under the FreeRTOS operating system.

2.2.6 Operations (OPS)

The operations subsystem is responsible for the devising the operational modes & procedures of the spacecraft, and ensuring the functionality, commandability and observability of the satellite before and during its mission.

During flight, AcubeSAT can remain within one of the following **system modes**:¹⁶

- **Launch/Off mode:** During this mode, the satellite is turned completely off, and no subsystems are energised. This is used to represent the state of the spacecraft inside the deployer, where no electronics are allowed to be energised,¹⁷ and the CubeSat is in a completely dormant state.
- **Commissioning mode:** This mode is initiated as soon as the CubeSat exits the deployer, meaning that launch is complete. It contains the initial startup actions of the spacecraft, including detumbling and antenna deployment. No science takes place during commissioning mode.
- **Nominal mode:** This mode represents the state where the CubeSat will spend most of the time on. Apart from the necessary autonomy functions and battery charging, the CubeSat will also downlink telemetry and science data. No science takes place during nominal mode, except for health checks commanded from the ground. Nominal mode is also the only mode where the satellite performs nadir or sun pointing (Section 2.2.1).

¹¹ Kanavouras and Pavlakis, *AcubeSAT OBDH DDJF*.

¹² <https://www.microchip.com/wwwproducts/en/SAMV71Q21RT>

¹³ Bouwmeester *et al.*, "Survey on the Implementation and Reliability of CubeSat Electrical Bus Interfaces."

¹⁴ PC/104 Embedded Consortium, *PC/104 Specification*.

¹⁵ Kanavouras, Kozaris, *et al.*, *AcubeSAT OBSW DDJF*.

¹⁶ Zaras *et al.*, *AcubeSAT Mission Description & Operations Plan*.

¹⁷ California Polytechnic State University, *CubeSat Design Specification Rev.*

¹³, req. 3.3.3.

- **Science mode:** This is where the main experiment takes place and payload data are generated. This mode includes operation of the fluidic system, control of the microfluidic chip, reinvigoration of the cells, and periodic acquisition of pictures using the miniaturised microscope.

AcubeSAT has split science mode into **3 distinct occurrences**, termed sub-experiments α , β and γ , lasting 72 hours each, and taking place at different points of the mission to investigate the time-dependence of the observed results.

- **Safe mode:** It is common for spacecraft systems to include a *safe mode*,¹⁸ where the spacecraft switches off all non-essential systems and function, in order to respond to major malfunctions that cannot be corrected by autonomous procedures. Safe mode is intended as a well-defined and well-tested mode which is easy to maintain and reduces risk of any malfunction.

On AcubeSAT, spacecraft functionality is significantly reduced, and the attitude profile includes pointing only. However, UHF communication and beacon transmission are still active for observability purposes.

¹⁸ Aguirre, *Introduction to Space Systems*, p. 385.

Function	Launch	Commissioning	Nominal	Science	Safe
ADCS	Off	Detumbling	Pointing	Detumbling	Detumbling
COMMS	Off	UHF only	UHF and S-Band	UHF only	UHF only
EPS	Off	On	On	On	On
OBC	Off	On	On	On	On
SU	Off	Off	Maintenance & data only	On	Maintenance only

Each mode is associated with a **functional flow diagram**, showing a high-level description of the spacecraft operation during this mode.¹⁹

Table 2.3: Overview of AcubeSAT functionality on different modes.
¹⁹ *AcubeSAT Functional Architecture*.

2.2.7 Structural

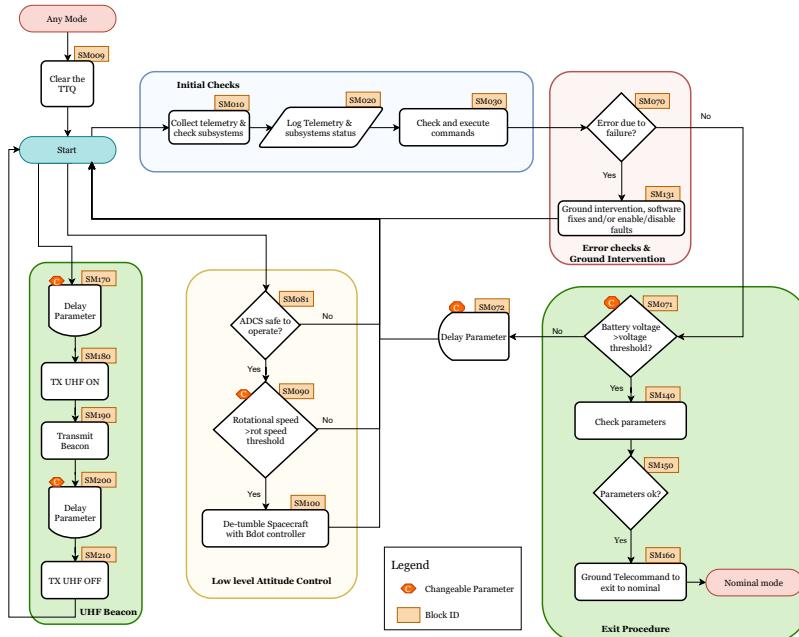


Figure 2.3: Safe mode functional flow

20

2.2.8 Systems Engineering (SYE)

2.2.9 Science Unit (SU)

The Science Unit subteam is responsible for the conceptualisation and implementation of the mission's scientific payload, namely the high-throughput study of the effects of Low Earth Orbit (LEO) environments on yeast cells.

The payload is composed of the following functional parts:²²

- The **payload container**, an almost 2U aluminum structure, pressurised at standard atmospheric pressure, and designed to host all the payload instrumentation. The container also accommodates a unibody which mechanically supports all SU components.
- A **microfluidic chip** based on Polydimethylsiloxane (PDMS), hosting 384 chambers capable of probing 190 distinct strains of *Saccharomyces Cerevisiae* for each subexperiment.
- A **fluidic system** composed from 2 pumps, 8 latching solenoid valves, 6 non-latching solenoid valves, and 3 fluid medium containers
- An **imaging system** operating as a microscope, containing a camera and a series of lights, filters and a lens
- A number of **heaters** to control component operational temperatures
- A number of redundant **sensors** for environmental measurements

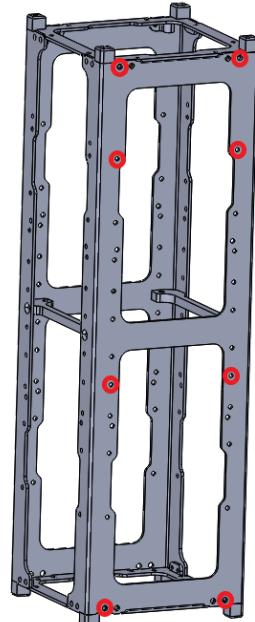


Figure 2.4: The CubeSat's 3U

²⁰ Like a toast

²¹ Toast is awesome

²² Arampatzis et al., *AcubeSAT Payload DDJF*.

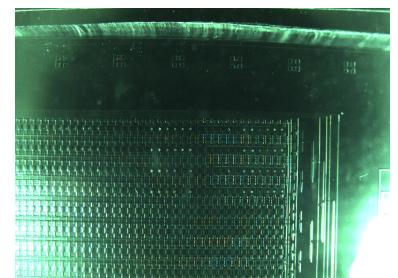
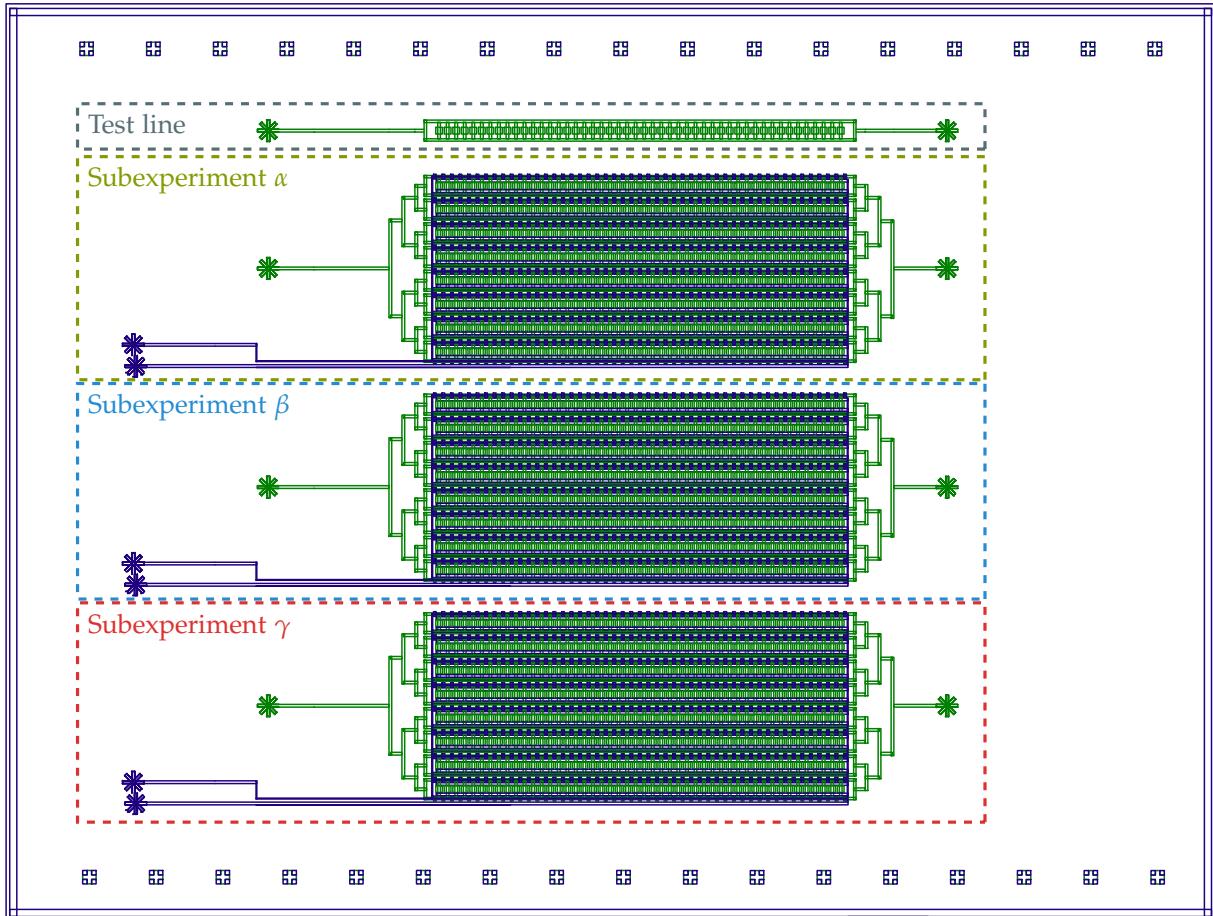


Figure 2.5: Example mission image output Arampatzis et al., *AcubeSAT Payload DDJF*

- A Printed Circuit Board (PCB) containing the microcontroller and rest of the control components of the payload



There is a number of constraints that the payload imposes on FDIR design:

1. **Interruption** of one of the three 72-hour subexperiments during execution may mean complete loss of the subexperiment. The impact of such an event depends on the duration and timepoint of its occurrence. In any case, adequate observability will allow the ground-control experiment to mimic the in-orbit conditions as much as possible.
2. **Freezing** of liquids inside the chip and fluidic tubes may lead to permanent damage on the setup. As such, heater operation may be required even during safe mode, after the first sub-experiment has been performed and liquid has flown into the system. This characteristic imposes further restrictions on the minimum availability of the system, depending on the thermal conditions.

Figure 2.6: The microfluidic chip and its separation into 3 subexperiments and 1 test line. The fluid inlets are shown on the left side of the chip, while the outlets are on the right. *Green*: flow layer. *Blue*: control layer.

2.2.10 Thermal

The Thermal subteam is responsible for the thermal analysis of the satellite, where the solar and earth albedo conditions are combined with the components' heat dissipation to determine the worst-case temperatures experienced by the satellite in hot and cold conditions.

The results of thermal analysis typically lead to implementation of passive or active thermal control methods. Notably, in AcubeSAT, 3 electronically-controlled heaters are used for the batteries, PDMS chip and valves.

2.2.11 Trajectory

The Trajectory subteam is responsible for the analysis of the space-craft's orbit, the calculation of radiation effects, the satellite's compliance to space debris regulations, and the estimation of its orbital lifetime.

AcubeSAT's requirements do not dictate use of thrusters, meaning that the satellite's orbit will be determined solely by the launcher, and cannot be altered in flight. As the selected launcher opportunity is unknown until some time before satellite delivery, a number of sensitivity analyses are executed to determine the allowed orbits.

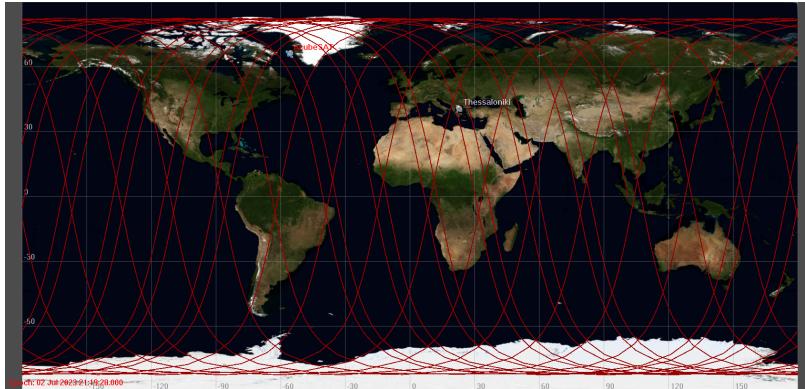


Figure 2.7: Ground track of an example AcubeSAT orbit, generated using NASA'S General Mission Analysis Tool

2.3 Tools used

3

The SAVOIR FDIR concept

3.1 The ECSS Packet Utilisation Standard

3.1.1 The ECSS services

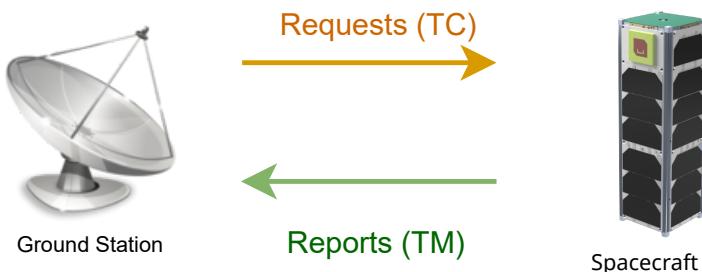


Figure 3.1: The PUS data transfer model

blablablab¹

- **ST[01]: Request verification**

Provides acknowledgement or failure reports for executed commands. This service essentially informs the operators about the status of TC sent to the spacecraft, and reports any occurred errors during parsing or execution.

- **ST[02]: Device access**

Allows toggling, controlling and reconfiguring any on-board peripherals that do not support the PUS paradigm, but rely on simpler protocols to communicate.

- **ST[03]: Housekeeping**

Produces periodic reports containing values of on-board parameters. This service essentially composes the periodic RF **beacon** of the satellite, by storing and transmitting parameter values without any prior TC request.

- **ST[04]: Parameter statistics reporting**

Allows reporting statistics (min, max, mean, standard deviation) for specific parameters over specified intervals. This is a memory-efficient alternative to the ST[03] housekeeping service.

¹ ECSS Secretariat, *ECSS-E-ST-70-41C – Telemetry and Telecommand Packet Utilization*; ECSS Secretariat, *ECSS-E-70-41A – Telemetry and Telecommand Packet Utilization*; Kaufeler, “The ESA Standard for Telemetry and Telecommand Packet Utilisation.”

- **ST[05]: Event reporting**

Generates reports when notable occurrences take place on-board, such as:

- Autonomous on-board actions
- Detected failures or anomalies
- Predefined steps during an operation

- **ST[06]: Memory management**

Allows writing and reading directly from an on-board memory unit. This can be useful for debugging and investigative purposes, fetching mission data, or uploading new software to the spacecraft avionics. The service also provides for downlinking and uplinking files in a file system.

- **ST[07]: Task management (*deprecated*)**

Allows stopping, suspending or resuming software tasks in case of contingency. This service has been removed from the standard and is only mentioned as a reference.

- **ST[08]: Function management**

Provides the capability of running predefined actions that can receive further parameters. These actions can correspond to payload, platform, or any other functionality.

- **ST[09]: Time management**

Allows periodic reporting of the current absolute spacecraft time for observability and correlation purposes.

- **ST[10]: Time packet (*deprecated*)**

Used in the past for time packet generation. This service has been removed from the standard and is only mentioned as a reference.

- **ST[11]: Time-based scheduling**

Allows the operators to "time-tag" telecommands for execution at future timestamps, instead of immediately.

- **ST[12]: On-board monitoring**

This service allows checking parameter values to ensure that they remain within configurable limits. Whenever a violation occurs, an ST[05] can be optionally generated for further processing.

- **ST[13]: Large packet transfer**

Provides a method of message segmentation, for message payloads that are too large to fit within the maximum allowed length for TC or TM.

- **ST[14]: Real-time forwarding control**

This service is responsible of controlling which types of generated reports are immediately transmitted to the Ground Station.

- **ST[15]: On-board storage and retrieval**

This service allows storing generated report on-board, as well as their commanded mass retrieval when the spacecraft has Ground Station visibility.

- **ST[16]: On-board traffic management (*deprecated*)**

Allows monitoring the status and load of an on-board data bus and provides commands for resolution of errors. This service has been removed from the standard and is only mentioned as a reference.

- **ST[17]: Test**

This service allows performing on-board connection and "are-you-alive" checks.

- **ST[18]: On-board operations procedure**

Allows loading, controlling (start, suspend, resume, abort) and configuring On-Board Control Procedures, which are sequences of commands written in an application-specific language.

- **ST[19]: Event-action**

Provides the operators with the capability of autonomously executing TCs when an ST[05] event is triggered.

- **ST[20]: On-board parameter management**

Provides the capability of reading and setting on-board parameters. Parameters are some of the most important entities defined in the PUS, and can represent:

- Read-write configuration variables for the system or lower-level components
- Read-only sensor and other telemetry values
- FDIR results and diagnostics

- **ST[21]: Request sequencing**

Allows operators to load series of TCs to be executed in a sequential order.

- **ST[22]: Position-based scheduling**

Provides the capability of executing TCs when the spacecraft reaches a specific point in its orbit.

- **ST[23]: File management**

Provides the capability of managing on-board file systems, with functions such as *copy*, *move*, *delete*, or *create directory*.

3.2 The SAVOIR standard

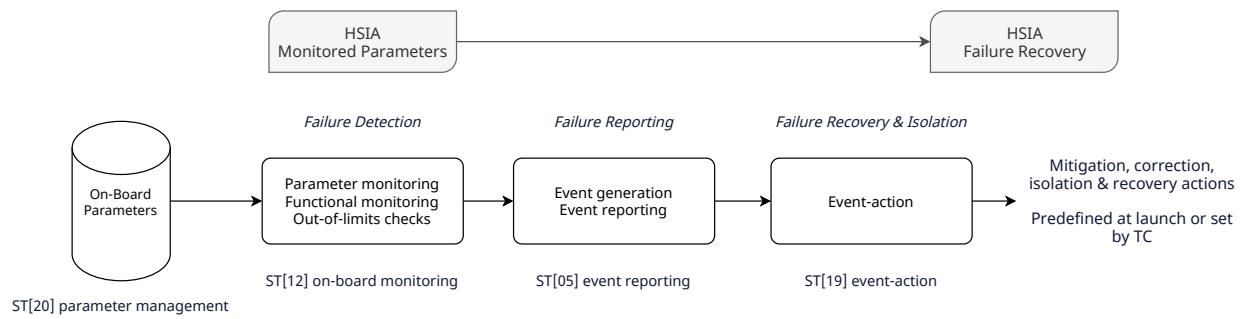


Figure 3.2: blablabla

4

FDIR in AcubeSAT

4.1 FDIR principles

- The 7 AcubeSAT FDIR principles
- SAVOIR FDIR requirements and compliance

4.2 Failure causes and recovery actions

4.2.1 Failure causes

4.2.2 Preventive actions

4.2.3 Corrective actions

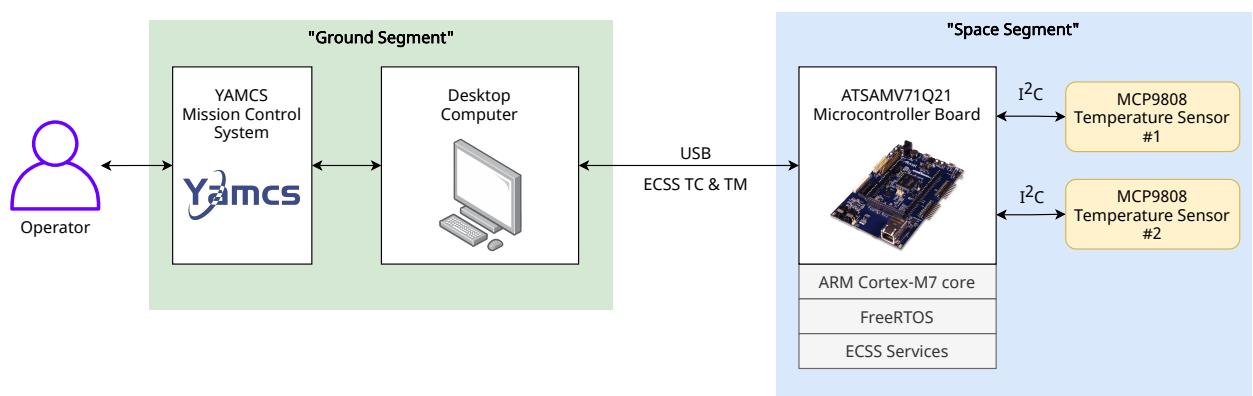
4.3 FDIR operating modes

5

Practical demonstration of FDIR

As a proof of concept for AcubeSAT's FDIR implementation, a practical setup to simulate the satellite's behaviour was prepared (Figure 5.1). Key elements of the setup are:

- A Cortex-M7 **microcontroller**, used to simulate a **satellite subsystem**
- A number of redundant **sensors** used as the potential failure points
- The accompanying **software** that includes an implementation of the ECSS services and the Space AVionics Open Interface aRchitecture (SAVOIR) FDIR methodology
- A desktop computer, serving as the **ground station** to provide the necessary commanding and observing capabilities



5.1 System Description

5.1.1 Hardware

The centre of the demonstration system is the MCU used to simulate the design and functionality of one of AcubeSAT's subsystems (Section 2.2.4). The selected MCU is the Atmel ATSAMV71Q21 hosted on the **ATSAMV71-XULT¹** development board. This MCU is functionally identical to the one that will be used in orbit, featuring a 32-bit ARM

Figure 5.1: High-level block diagram of the demonstration system

¹ <https://www.microchip.com/Developmenttools/ProductDetails/ATSAMV71-XULT>

Cortex-M7 core with 2 MiB of flash and 384 KiB of SRAM memory, and a maximum clock speed of 300 MHz.

The MCU is accompanied by two **temperature sensors** which are used to simulate subsystem components which are prone to failure. The selected sensor is the Microchip **MCP9808**² which offers an accurate and frequent temperature readout over an Inter-Integrated Circuit (I²C) bus.

The two sensors are wired in a **hot-redundant**³ configuration, due to their extremely low operating power. The two sensors are connected to different I²C buses, so that the failure of one bus will not affect the operation of the other sensor.

5.1.2 Flight Segment Software

All FDIR operations and functionality are developed using the C++ language⁴ on the MCU. All developments rely on free and open source software which is freely available for download and modification. The **Git**⁵ version control is used for all software projects.

The FDIR functionality is structured around the **ECSS-E-ST-70-41C PUS implementation created by the AcubeSAT team**⁶, which offers a modular implementation of the standard utilising modern C++.

The MCU software and business logic are built on **FreeRTOS**⁷, a low-footprint real-time operating system targeted towards embedded devices. FreeRTOS provides the capability of safe concurrency, along with support for well-controlled tasks and a number of synchronisation primitives.

To ensure high reliability and a low resource footprint of the software, the following **constraints** are enacted in C++ development:

1. Dynamic memory allocation⁸ is banned completely from the code
2. Item 1 means that standard C++ containers cannot be used. Instead, the **Embedded Template Library (ETL)**⁹ is integrated in the software.
3. "Expensive" features such as Run-Time Type Inference or exceptions are also prohibited.

All software developed in the scope of this thesis is available online, and listed in Table 5.1. The most critical parts of the developed software are expanded in Section 5.3. A summary of used libraries can also be found in Table 5.2.

5.1.3 Ground Segment Software

5.2 FDIR setup

5.3 Test results

² <https://www.microchip.com/wwwproducts/en/MCP9808>

³ Meaning they are both operating and generating measurements at the same time

⁴ The C++17 standard has been selected

⁵ <https://git-scm.com/>

⁶ <https://gitlab.com/acubesat/obc/ecss-services>

⁷ <https://www.freertos.org/>

⁸ Use of `malloc`, `new` etc.

⁹ <https://www.etlcpp.com/>

Library name	Description	URL
fdir-demo	Full microcontroller code for the demonstration	https://github.com/kongr45open/fdir-demo
fdir-demo-yamcs	Ground segment software: files and source code for YAMCS integration and MCU communications	https://github.com/kongr45open/fdir-demo-yamcs

Table 5.1: List of new software developed for this thesis

Library name	Description	Modifications
FreeRTOS	Real-time operating system for embedded devices	
ecss-services	C++ implementation of the ECSS-E-ST-70-41C PUS	Missing services were implemented and some interface improvements were made to improve integration with the MCU https://gitlab.com/kongr45open/ecss-services/-/tree/fdir
ETL	C++ library (including containers, algorithms and other utilities) for applications with embedded constraints	
YAMCS	Software framework for mission & spacecraft control	
cobs-c	Implementation of Consistent Overhead Byte Stuffing	

Table 5.2: List of used software libraries

Param. ID	Parameter	Units	Type
0	Temperature 1	°C	float
1	Temperature 2	°C	float
2	Δ Temperature	°C	float
3	Temperature 1 Status		Enumerated
4	Temperature 2 Status		Enumerated

Table 5.3: List of ST[20] parameters

Bibliography

- [1] O. Durou, V. Godet, L. Mangane, D. Pérarnaud, and R. Roques, "Hierarchical fault detection, isolation and recovery applied to cof and atv avionics," *Acta Astronautica*, vol. 50, no. 9, pp. 547–556, May 1, 2002, ISSN: 0094-5765. DOI: [10.1016/S0094-5765\(01\)00212-0](https://doi.org/10.1016/S0094-5765(01)00212-0). [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0094576501002120> (visited on 04/03/2021).
- [2] G. Savvidis, R. Voulgarakis, T. Papafotiou, V. Moustakas, E. Mylonas, and V. Pappa, *AcubeSAT AOCS DDJF*, 2021. [Online]. Available: https://gitlab.com/acubesat/documentation/cdr-public/-/blob/master/DDJF/DDJF_AOCS.pdf.
- [3] K. Kapoglis and E. Chatziargyriou, *AcubeSAT TTC DDJF*, 2021. [Online]. Available: https://gitlab.com/acubesat/documentation/cdr-public/-/blob/master/DDJF/DDJF_TTC.pdf.
- [4] M. Surligas, "SatNOGS-COMMS," presented at the CubeSat Developers Workshop, Apr. 12, 2021, p. 22.
- [5] D. White, C. Shields, P. Papadeas, A. Zisisimatos, M. Surligas, M. Papamatthaiou, D. Papadeas, and E. Kosmas, "Overview of the Satellite Networked Open Ground Stations (SatNOGS) Project," *Small Satellite Conference*, Aug. 8, 2018. [Online]. Available: <https://digitalcommons.usu.edu/smallsat/2018/all2018/313>.
- [6] M. Langer and J. Bouwmeester, "Reliability of CubeSats – Statistical Data, Developers' Beliefs and the Way Forward," *Proceedings of the 30th Annual AIAA/USU Conference on Small Satellites*, 2016. [Online]. Available: <https://repository.tudelft.nl/islandora/object/uuid%3A4c6668ff-c994-467f-a6de-6518f209962e> (visited on 05/20/2021).
- [7] R. Anastasios-Faidon, K. Kanavouras, and G. Pavlakis, *AcubeSAT System DDJF*, 2021. [Online]. Available: https://gitlab.com/acubesat/documentation/cdr-public/-/blob/master/DDJF/DDJF_SYS.pdf.
- [8] K. Kanavouras and G. Pavlakis, *AcubeSAT OBDH DDJF*, 2021. [Online]. Available: https://gitlab.com/acubesat/documentation/cdr-public/-/blob/master/DDJF/DDJF_OBDH.pdf.
- [9] J. Bouwmeester, M. Langer, and E. Gill, "Survey on the implementation and reliability of CubeSat electrical bus interfaces," *CEAS Space Journal*, vol. 9, no. 2, pp. 163–173, Jun. 1, 2017, ISSN: 1868-2510. DOI: [10.1007/s12567-016-0138-0](https://doi.org/10.1007/s12567-016-0138-0). [Online]. Available: <https://doi.org/10.1007/s12567-016-0138-0> (visited on 05/20/2021).
- [10] PC/104 Embedded Consortium, "PC/104 Specification," Aug. 13, 2008. [Online]. Available: https://pc104.org/wp-content/uploads/2015/02/PC104_Spec_v2_6.pdf.
- [11] K. Kanavouras, I. Kozaris, A. Theocharis, G. Pavlakis, and D. Stoupis, *AcubeSAT OBSW DDJF*, 2021. [Online]. Available: https://gitlab.com/acubesat/documentation/cdr-public/-/blob/master/DDJF/DDJF_OBSW.pdf.

- [12] A. Zaras, K. Kapoglou, M. Georgousi, T. Papafotiou, M. Chadolias, A. Anthopoulos, A.-F. Retselis, A. Arampatzis, K.-O. Xenos, and E. Christidou, *AcubeSAT Mission Description & Operations Plan*, 2021. [Online]. Available: <https://gitlab.com/acubesat/documentation/cdr-public/-/blob/master/MD0%20file/MD0.pdf>.
- [13] California Polytechnic State University, “CubeSat Design Specification Rev. 13,” Feb. 20, 2014. [Online]. Available: https://www.cubesat.org/s/cds_rev13_final2.pdf.
- [14] M. A. Aguirre, *Introduction to Space Systems: Design and Synthesis*, ser. Space Technology Library. New York: Springer-Verlag, 2013, ISBN: 978-1-4614-3757-4. DOI: [10.1007/978-1-4614-3758-1](https://doi.org/10.1007/978-1-4614-3758-1). [Online]. Available: <https://www.springer.com/gp/book/9781461437574> (visited on 05/23/2021).
- [15] (May 8, 2021). AcubeSAT Functional Architecture, [Online]. Available: <https://gitlab.com/acubesat/systems-engineering/functional-architecture>.
- [16] A. Arampatzis, A. Zaras, P. Matsatsos, O. Ousoultzoglou, D. Nikolopoulou, and E. Sandaltzopoulou, *AcubeSAT Payload DDJF*, 2021. [Online]. Available: https://gitlab.com/acubesat/documentation/cdr-public/-/blob/master/DDJF/DDJF_PL.pdf.
- [17] ECSS Secretariat, “ECSS-E-ST-70-41C – Telemetry and telecommand packet utilization,” European Space Agency, Apr. 15, 2016. [Online]. Available: <https://ecss.nl/standard/ecss-e-st-70-41c-space-engineering-telemetry-and-telecommand-packet-utilization-15-april-2016/>.
- [18] ——, “ECSS-E-70-41A – Telemetry and telecommand packet utilization,” European Space Agency, Jan. 30, 2003. [Online]. Available: <https://ecss.nl/standard/ecss-e-70-41a-ground-systems-and-operations-telemetry-and-telecommand-packet-utilization/> (visited on 05/24/2021).
- [19] J.-F. Kaufeler, “The ESA standard for telemetry and telecommand packet utilisation: PUS,” Nov. 1, 1994. [Online]. Available: <https://core.ac.uk/download/pdf/42783096.pdf> (visited on 05/24/2021).

Source code

here we write code