NTNU – Trondheim
Norwegian University of
Science and Technology

Mission Event Planning & Error-Recovery for CubeSat Applications

Magnus Haglund Arnesen

Christian Elias Kiær

Problem Description

The NTNU Test Satellite (NUTS) is an ongoing project which aims to build, launch and operate a double CubeSat by 2015. The project is close to a pre-flight test model, and the software and hardware must be integrated in order to complete this model.

The thesis should focus on error handling and recovery specifications for the NUTS project. The planning of error and recovery modes should be documented with block diagrams and evaluated with respect to quality and simplicity. Different fail safe systems are to be evaluated, after which some of them can be chosen for implementation. Such systems can be reboot procedures, current consumption monitoring and backup. Different ways of removing power and planning for a delayed start of the satellite should be evaluated. Necessary self-tests and their reliability should also be documented.

The main results of this Master Thesis should be:

- A detailed mission event plan aimed to minimize error and fault consequences and maximize the probability of mission success.

- A new reliable hardware watchdog for removing lasting faults/failures by toggling power to all subsystems.

- Defined modes of operation to tackle unforeseen events, lack of battery power and/or loss of communication.

- A detailed and as accurate as possible power budget with the aim of creating a solid basis for battery estimation and mission event planning.

- Provide a foundation for helping NUTS meet its goal of a 2015 launch.

Assignment given: 16. January 2014
Supervisor: Bjørn B. Larsen
Co-supervisor: Roger Birkeland

Abstract

NTNU Test Satellite (NUTS) is a student-built double CubeSat with a scheduled launch in 2015. The project is multidisciplinary where students from all specialities can apply both for thesis assignments and volunteer work. The satellite will be in a low earth orbit (LEO) where radiation creates a challenging environment for electronics and on-board systems. To counter the effects of space radiation, a thorough and detailed mission event plan, as well as battery estimation and methods for removing lasting faults have been evaluated and implemented.

Two watchdog solutions have been suggested, a global watchdog with triple modular redundancy (TMR) on the backplane and a solution with a local watchdog on each master module. Both solutions have the capability to remove single event latchups (SEL) by temporarily removing power to the affected module. Based on results and analysis, the solution with two local watchdogs are the preferred solution due to the increased complexity of the TMR solution. Furthermore, the voter necessary in a TMR implementation is a single point of failure which if malfunctioning, will leave the satellite unresponsive. Guidelines for choosing a new watchdog system's parameters are given. This includes the watchdog's time-out period, power-on-reset (POR) delay and a threshold voltage for the voltage supervisory function.

Mission event plans are proposed for initial power-up, in-orbit power monitoring, payload verification and satellite self-tests. A flowchart defining a software watchdog responsible for maintaining an operational satellite is also presented.

An adjustable beacon rate enables power conservation by defining three different transmission rates; low, normal and full rate. For the full rate, the power consumption is estimated to 2200 mW, 233.33 % higher than in low rate and 100 % higher than normal rate. A battery management framework has been proposed in order to avoid a low battery condition.

Sammendrag

NTNU Test Satelitt (NUTS) er en studentbygget satellitt med planlagt oppskytning i 2015. Prosjektet er et samarbeidsprosjekt mellom flere studiespesialiteter på NTNU, og både masterkandidater og frivillige kan være med å utvikle satellitten. Satellitten vil operere i lav jordbane (LEO) der stråling skaper utfordringer for elektronikken og systemene ombord. For å håndtere strålingseffektene er det gjennomført batteriestimering, laget en detaljert oppdragsplan og metoder for å fjerne varige feil.

To forskjellige watchdog-system er foreslått hvor en er implementert på et testkort. Det er foreslått en trippel modulær redundans (TMR) watchdog og en lokal watchdog på hver mastermodul. Begge løsningene kan fjerne single event latchup ved å midlertidig skru av spenningen til den berørte modulen. Basert på oppnådde resultat er en lokal watchdog å foretrekke grunnet økt kompleksitet i en TMR-løsning. Dessuten skapte TMR-løsningen et single point of failure (SPF) i majoritetsvelgeren, noe som vil sette satelliten ute av drift hvis den skulle svikte. Et nytt watchdog-system har flere parametere som må velges, nemlig time-out-periode, oppstartsforsinkelse (power-on-reset delay) og en terskelspenning. Oppgaven presenterer retningslinjer for valg av disse parameterne.

Forslag til oppdragsplaner for første oppstart, effektforbruk, payload-kontroll og selvtester er presentert. Flytdiagram for en software watchdog ansvarlig for å opprettholde en fungerende satellitt er også presentert.

En justerbar senderate gir muligheten for å spare energi ved å bruke tre nivåer; lav, normal og høy. I høyeste tilstand er effektforbruket 2200 Wm, 233.33 % høyere enn i laveste tilstand og 100% høyere enn i normal tilstand. Et batteri monitorinssystem har blit foreslått for å unngå laveste batteritilstad.

Preface

This thesis has been written at the Norwegian University of Science and Technology during spring of 2014. It has been a collaborative effort between Magnus Haglund Arnesen and Christian Elias Kiær. Work has been divided in equal parts and we have both participated in every aspect of the thesis. The assignment was given by NUTS' project management in collaboration with our supervisor, Bjørn B. Larsen.

A challenging task for both of us was to create a suitable mission event plan. Assistance from project management and the entire NUTS team has been invaluable in order to create a plan usable for the satellite. Researching theory necessary for forming a solid foundation and creating a reliable system was time consuming, yet rewarding as all the pieces fell into place. The constant need for redundancy and reliability when designing were a new and challenging task. We had to consider this throughout the design process and when proposing a new solution for the project.

Being a part of the NUTS project and working together towards a common goal with so many committed and resourceful members were especially rewarding. This was also invaluable when work progressed slowly and new input from members helped us move forward. We contributed with volunteer work by recruiting new members at stands and presenting our master thesis for students in lower classes.

We would like to thank our supervisor, Associate Professor Bjørn B. Larsen, project manager Roger Birkeland and project coordinator Amund Gjersvik for guidance and help during this semester.

- Magnus Haglund Arnesen
Trondheim, 11.06.2014

- Christian Elias Kiær
Trondheim, 11.06.2014

Contents

List of Figures

List of Tables

List of Acronyms

LEO   Low Earth Orbit

NTNU Norwegian University of Science and Technology

NUTS NTNU Test Satellite

NAROM Norwegian Center for Space-Related Education

P-POD Poly Pico-Satellite Orbital Deployer

OBC   On-Board Computer

MCU   Microcontroller Unit

VHF   Very High Frequency

UHF   Ultra High Frequency

ADCS Attitude Determination and Control System

EPS   Electrical Power System

SAA   South Atlantic Anomaly

SEE   Single Event Effects

SEU   Single Event Upset

SET   Single Event Transient

SEL   Single Event Latchup

SEB   Single Event Burnout

TID   Total Ionizing Dose

MeV   Megaelectronvolt

I^{2}C   Inter Integrated Circuit

TMR   Triple Modular Redundancy

RBF   Remove Before Flight

IR   Infrared

ACK   Acknowledgement

COTS   Commercial Off-The-Shelf Components

POR   Power-On-Reset

BOD   Brownout Detector

IC   Integrated Circuit

CH   Channel

PCB   Printed Circuit Board

SPF   Single Point of Failure

FRAM   Ferroelectric Random Access Memory

WDT   Watchdog Timer

GPIO   General-Purpose Input/Output

PA   Power Amplifier

NTC   Negative Temperature Coefficient

Chapter 1

Introduction

This chapter presents the thesis' motivation, problem description and disposition, as well as relevant previous work.

1.1 Motivation

Norwegian University of Science and Technology's (NTNU) Test Satellite (NUTS) project has a goal of launching a Low Earth Orbit (LEO) satellite by 2015. A LEO satellite operates at heights of 500 km to about 2000 km [15], and it is estimated that NUTS will operate at approximately 600 km.

The project aims at giving students hands-on training with cooperation between specialities and to increase interest for science and technology in lower education levels. This will hopefully help recruit candidates to higher education [16]. The satellite is designed following the CubeSat standard where one cube must not exceed 1.33 kg and measure only 10x10x10 cm [1], of which a satellite may combine up to three such cubes. NUTS has decided to make a double CubeSat with a maximum weight of 2.66 kg and maximum dimensions of 10x10x20 cm. The project initially aimed at carrying an infrared (IR) camera to capture air glow phenomena, but due to cost and complexity both in hardware and engineering, it has been decided to replace the IR-camera with a visual range camera.

1.2 Problem Description

The NTNU Test Satellite (NUTS) is an ongoing project which aims to build, launch and operate a double CubeSat by 2015. The project is close to a pre-flight test model, and the software and hardware must be integrated in order to complete this model.

The thesis should focus on error handling and recovery specifications for the NUTS project. The planning of error and recovery modes should be documented with block diagrams and evaluated with respect to quality and simplicity. Different fail safe systems are to be evaluated, after which some of them can be chosen for implementation. Such systems can be reboot procedures, current consumption monitoring and backup. Different ways of removing power and planning for a delayed start of the satellite should be evaluated. Necessary self-tests and their reliability should also be documented.

The main results of this Master Thesis should be:

- A detailed mission event plan aimed to minimize error and fault consequences and maximize the probability of mission success.

- A new reliable hardware watchdog for removing lasting faults/failures by toggling power to all subsystems.

- Defined modes of operation to tackle unforeseen events, lack of battery power and/or loss of communication.

- A detailed and as accurate as possible power budget with the aim of creating a solid basis for battery estimation and mission event planning.

- Provide a foundation for helping NUTS meet its goal of a 2015 launch.

1.3   Thesis Outline & Contributions

A brief outline of this thesis can be given as follows:

Chapter 2 presents the given CubeSat standard and requirements, as well as NUTS' mission goals and mission lifetime. Theory presented in Chapter 3 will form the thesis' foundation and Chapter 4 introduces the current NUTS system. Chapter 5 presents estimates to solar cells' charging power and the satellite's power consumption. Chapter 6 sets the requirements for NUTS' mission plans and is the foundation the planning results in Chapter 7. Chapter 8 presents the design of two new watchdog solutions. Chapter 9 proceeds with watchdog testing and presents achieved results. It also presents battery management for different levels of remaining battery capacity. Results are discussed throughout Chapter 10 before conclusions are made in Chapter 11.

Work presented in this thesis will aim at providing NUTS with a new watchdog system, a mission event plan, defined battery and operation modes, as well as an initial power budget. These are all necessary parts of NUTS' pre-flight test model, which is scheduled for completion during fall 2014.

1.4 Previous Work

The NUTS project was started in September 2010 and is part of the Norwegian Student Satellite Program run by Norwegian Center for Space-Related Education (NAROM).

NTNU has previously been part of two other CubeSats, NCUBE-1 and NCUBE-2. These projects were in collaboration with different universities and university colleges across Norway. None of the satellites were able to initialize contact with a ground station after launch. NCUBE-2 was launched on October 27, 2005, and was successful in reaching orbiting, but radio contact with the satellite was never achieved. NCUBE-1 was launched on July 26, 2006, but a problem with the second stage of the rocket prevented the satellite from reaching orbit [11]. Figure 1.1 shows the complete NCUBE-2 before launch.
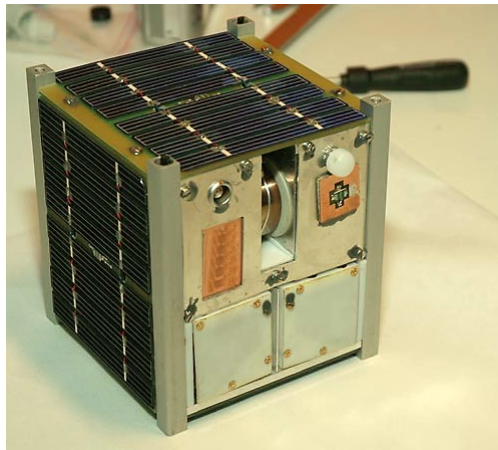
Figure 1.1: NCUBE-2. Photo by: Bjørn Pedersen, NTNU

NUTS consists of both volunteer and project/master thesis work. NUTS is handled by the Department of Electronic and Telecommunication (IET) at NTNU, and master students from several departments may apply to the project. The project is currently lead by project manager Roger Birkeland and project coordinator Amund Gjersvik. NUTS is a multidisciplinary project where an open dialogue is required to achieve common goals.

Since the beginning in 2010, several students have committed a large amount of work and research. The most notable contributions related to this thesis are present below.

1.4.1 2013 Master Thesis

Error Detection and Correction for Low-Cost Nano Satellites - Kjell Arne Ødegaard

K.A. Ødegaard [17] focused on different low level software solutions to deal with error detection and correction. This thesis will focus on hardware solutions and more application level implementations in order to minimize fault probability and consequences.

1.4.2 2012 Master Thesis

Electrical Power System of the NTNU Test Satellite - Lars Erik Jacobsen

L. E. Jacobsen focuses on the power system of the satellite and finalization of the Electrical Power System (EPS) module [18]. This thesis has been a foundation for the solar panels and the batteries, as well as how the power distribution is intended.

1.4.3 2011 Master Thesis

Power Distribution and Conditioning for a Small Student Satellite - Dewald De Bruyn

The thesis from D. D. Bruyn serves as a main specification for the current backplane design [11]. The backplane prototypes are still being used in testing today and interconnects the satellite's modules.

Chapter 2

Background

This chapter provides a brief overview of the CubeSat standard, requirements and mission goals for the NUTS project.

2.1 CubeSat Standard

The CubeSat standard began as a collaborative project between California Polytechnic State University (CalPoly) and Stanford University. The purpose of the project was to develop a standard design for picosatellites in order to reduce cost, shorten development time and make frequent launches into space possible [1].

2.1.1 Electrical Requirements

The standard has a list of electrical requirements and some of the most important are [1]:

- *No electronics shall be active during launch to prevent any electrical or RF interference with the launch vehicle and primary payloads.*

- *All systems shall be turned off, including real time clocks.*

- *The CubeSat shall include at least one deployment switch on the designated rail standoff to completely turn off satellite power once actuated.*

2.1.2 Operational Requirements

The operational requirements for the satellite are [1]:

- *All deployables such as booms, antennas and solar panels shall wait to deploy a minimum of 30 minutes after the CubeSat's deployment switches are activated from the P-POD ejection.*

- *RF transmitters greater than 1 mW shall wait to transmit a minimum of 30 minutes after the CubeSat's deployment switches are activated from the P-POD ejection.*

2.1.3 CubeSat Mechanisms

Figure 2.1 shows the Poly Picosatellite Orbital Deployer (P-POD). NUTS will be inserted into this orbital deployer together with a single CubeSat from a different party. At the bottom railing of each satellite there is two deployment switches which breaks the connection between the battery and the electrical systems, causing the satellite to be disabled while inside the P-POD. Figure 2.2 shows the railing deployment switch in a single CubeSat.
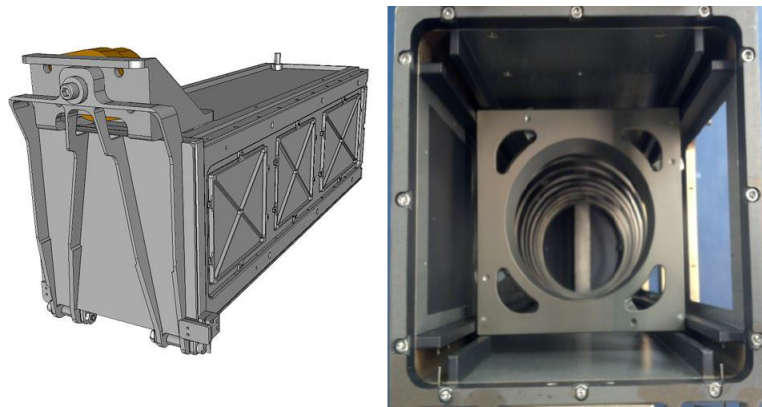
Figure 2.1: Poly Picosatellite Orbital Deployer [1]
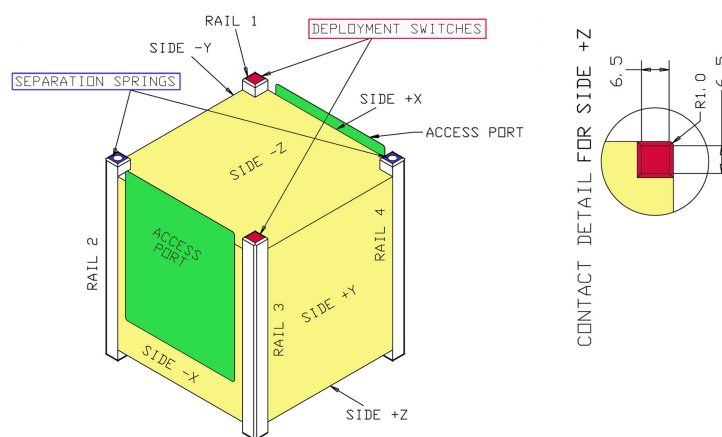
Figure 2.2: Railing deployment switch [1]

2.2 Mission Goals

NUTS' mission statement is to design, develop, test, launch and operate a double CubeSat.

A mission success is given by the following criteria [19]:

- Deliver a tested satellite according to mission specification

- Transmit a beacon signal receivable for radio amateurs

- Confirm successful de-tumbling - i.e. stabilize the satellite after ejection from the P-POD

- Establish two-way communication and receive full telemetry

- Initiate camera pointing and capture an image

- Receive a valid image

The mission is consider successful if one or several of the above criteria are fulfilled. The main goal is to identify the NUTS beacon signal and thereby having a positive confirmation of an operational satellite. If the satellite is able of capturing and transmitting an image, the mission is a complete success. As given by the project management, the desired mission lifetime for NUTS is 3 months.

Chapter 3

Theory

This chapter focuses on theory which is necessary for forming a solid background for the rest of the thesis. This includes space radiation, redundancy, as well as background on solar panel charging and battery estimation.

3.1 Definitions

Throughout this thesis, terms and expressions will be used to describe different phenomenons. This section will provide the definitions of these.

- Failure - When a system deviates from its intended state and does not presented a desirable result.

- Faults - Defects or abnormal conditions in software and/or hardware which may cause failures.

- Errors - Unexpected problems internal to a system which manifests themselves externally as failures.

3.2 Space Radiation

One of the biggest concerns in space is radiation. For most low earth orbits (LEO), the radiation environment is harsher compared to the Earth's surface, but not as harsh as the higher orbits or deep space. Radiation is particles emitted from various sources which may lead to degradation and even cause failure of the electronics and the electrical system [20]. Solar flares, galactic cosmic rays and particles trapped in Earth's magnetic field are all sources of space radiation. Galactic cosmic rays are high energy particles, most of which are atomic nuclei, but also high energy electrons, positrons and other subatomic particles [21]. The energy of cosmic rays

are measured in units of megaelectronvolt (MeV) or gigaelectronvolt (GeV)[1]. Most cosmic rays range in energy between 100 MeV and 10 GeV [21].

During a solar flare, radiation can increase substantially over a short period of time and create more high energy radiation particles. This is shown in Figure 3.1 where the effect is documented by NASA's Cassini Spacecraft. It is important to note that space radiation varies with time, and therefore its effect on electronics is not constant.
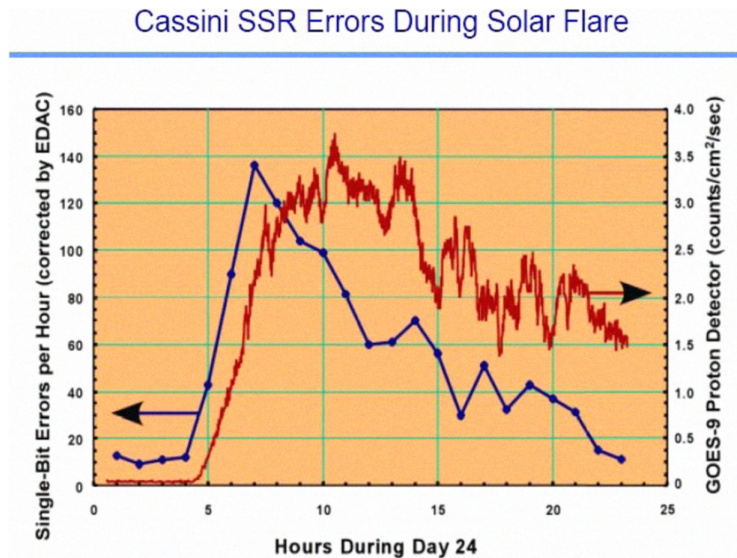
Figure 3.1: Data error rate during a solar flare as captured by the spacecraft Cassini [2]

When radiation reaches Earth, it will be affected by Earth's electromagnetic field which traps the particles, accelerating them and forming belts of radiation. These belts endanger satellites and sensitive components must be adequately shielded if they orbit for a significant amount of time in these radiation belts. The belts are called Van Allen radiation belts and as Figure 3.2 shows, Earth has two encircling it.

The belts vary in altitude from 3000 km to 20 000 km [22], higher than most LEOs, but due to its asymmetric nature, a region in the Atlantic, near Argentina and Brazil, has relatively high concentrations of electrons. This is known as the South Atlantic Anomaly (SAA) and is for a LEO satellite's electronics, a large source of single event effects [2]. Figure 3.3 shows where this high concentration of electrons occur. Further more, the belts are close to non-existing near Earth's magnetic poles, causing a harsher radiation environment for satellites in polar orbit.

The particles are mainly protons and electrons which are trapped within the belts by the Earth's magnetic field. The inner belt consists of highly energetic protons,

---

[1]One electron volt is the energy gained when an electron is accelerated through a potential difference of 1 volt [21]
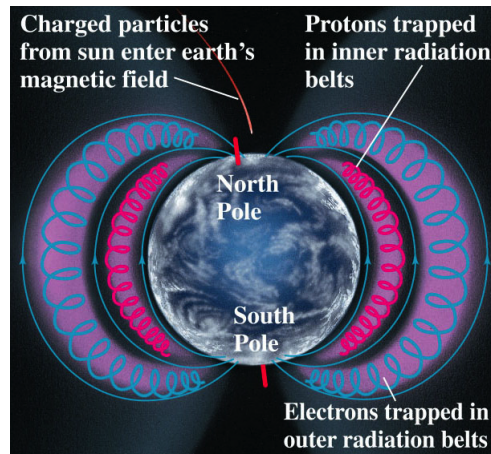
Figure 3.2: Van Allen belts [3]
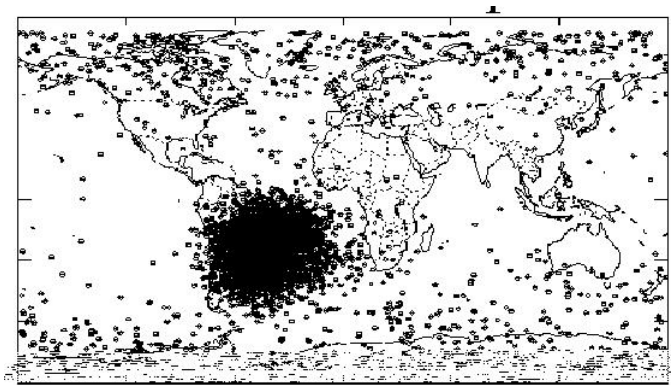
Figure 3.3: Single event effects in the South Atlantic Anomaly [4]

with energy exceeding 30 MeV. The outer belt contains charged particles of both atmospheric and solar origin. The protons in the outer belt have much lower energy levels and the most energetic particles of the outer belt are electrons. These electrons can reach several hundred MeV [22].

There are several radiation effects on electronics in space, of which total ionizing dose (TID) and single event effects (SEE) are of the most common.

3.2.1   Total Ionizing Dose - TID

Total ionizing dose (TID) is the accumulation of ionizing dose deposition over time. This occurs mainly as an effect of protons and electrons, and the ionization creates charges or electron-hole pairs in oxides. This could lead to circuit parameter changes and over time make the circuit ceases to function [5]. Figure 3.4 shows trapped positive charges inside the gate oxide. TID is difficult to mitigate since it occurs both in powered and unpowered states and accumulates over time [23]. TID can be handled through careful parts selection and shielding [24]. NASA sets the

worst case dose rates for a LEO to 1-10 krad(Si) per year [20], and typical total dose failure levels of microprocessors at 15-70 krad(Si) [25]. A krad(Si) is a commonly used unit for measuring total ionizing dose where Si refers to the material silicon. In reference to the SI unit of gray, 1 krad(Si) equals 10 miligray [23]. Seen in context with the NUTS mission's short lifetime of only 3 months, this would indicate that TID is not to become an issue for the satellite's microcontrollers. Therefore further mitigation of TID will not be considered in this thesis.
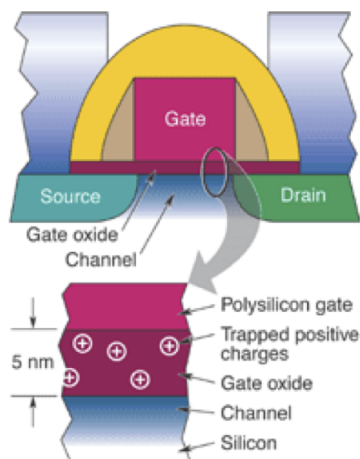
Figure 3.4: Trapped positive charges inside a transistor [5]

3.2.2 Single Event Effect - SEE

Cosmic radiation can cause spontaneous SEE by releasing energy when penetrating a component. This energy will cause a charge at a node and lead to a short current pulse as shown in Figure 3.5. SEE is divided into the following subcategories.
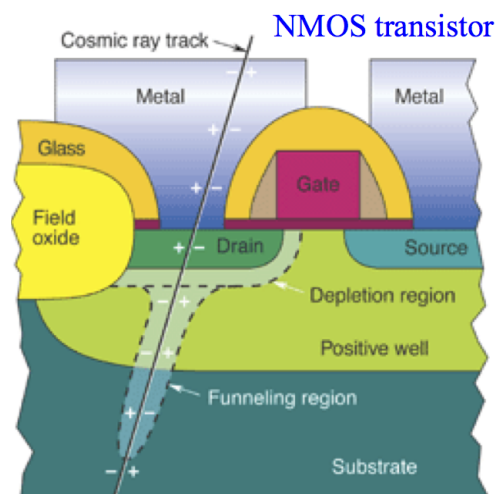
Figure 3.5: Particle producing an ionization track [5]

Single Event Upset

An SEU is caused by an internal charge deposition, which causes a bit-flip in a memory element or a change of state in a logic circuit. This could cause both non-destructive effects and destructive effects. Non-destructive effects could be corruption of information stored in a memory element or change a logic element's state. This can be resolved by refreshing the elements with the correct value. A destructive effect could be microprocessor program corruption, e.g. a calculation error, freezing or wrong command execution [5]. In Ødegaard's thesis [17], it has been stated that in a 128kB of RAM, as many as 10 bit-flips may accumulate per day in orbit.

Single Event Transient

An SET is a single transient current or a voltage spike. This spike can propagate through logic gates and produce system failures. If this spike is captured by a storage element, the SET may become an SEU [5].

Single Event Latchup

An SEL causes a permanent bit-flip and prevents it from exiting the logic state. The circuit must be powered down in order to correct the condition [23]. For Commercial Off-The-Shelf (COTS) electronics, an article from Journal of Modern Physics [26] reports a recovery time, i.e. the time a device must be unpowered, between 50 and 300 ms, while an article presented at the 11th AIAA/USU Conference on Small Satellites [27] reports recovery times from 45 μs to 2.5 ms. SELs happen due to of unintentional current flow between components on an integrated circuit [5]. This is a result of parasitic NPN-PNP transistors in the CMOS structures, which may cause both high and low current flow conditions. A high and low current condition can be discriminated between by having an accurate estimate of a module's power consumption when performing a predetermined task [24]. If not handled in time, SELs may cause irreparable damage [23]. Testing carried out at Lawrence Livermore National Laboratory [24], determined a rate of SELs for a commercial R3000 microprocessor in a worst-case LEO space environment such as a solar flare or passing through the SAA. With 2.54 mm of aluminium shielding, the microcontroller would experience SELs every few days, based on which the study [24] concluded mitigation of SELs was necessary. Note that NUTS carries little to no shielding, and may hence suffer from increased rates of SELs.

Single Event Burnout

An SEB is the most critical form of SEE. If the current from an SEL is not limited in a timely manner, it may cause the device to overheat and burn up. This effect is

permanent and irreversible [5]. SEBs can only be prevented by careful component selection [24] and by reducing SELs.

In this thesis only SELs and SEUs are considered since reducing and mitigating these also will resolve issues regarding the other single single event effects.

3.3 Mitigating Space Radiation Effects

There are several ways of reducing the effects of radiation. One may choose an orbit with a lower level of radiation, but this is not always a viable option. Adding shielding to reduce the radiation dose is also been proving to work, but this increases the total weight. However, increased shielding may lead to worse secondary particles when very high energy radiation interacts with materials with a high number of protons in their nucleus [2]. The use of radiation hardened components also increases radiation robustness, but such components are often expensive and not readily available. Furthermore, the use of radiation hardened components defeats the purpose of a low cost, student-built satellite where cheap commercial components are the backbone of the design. A cost effective solution is a system-level error correction architecture which requires very little special hardware and can be modified if the system needs different functionality in a later stage.

3.3.1 Redundancy

In order to have a fault tolerant system, the designer must expect that something will fail and yet be able achieve an operational system. This is in contrast to fault avoidance, where the designer aims at reducing the amount of faults that occur, e.g. by adding shielding or using radiation hardened components [23]. All techniques for achieving fault tolerance rely on extra elements introduced into the system to detect and recover from faults. There are two types of redundancy; hardware and software redundancy. Hardware redundancy is further divided into static and dynamic redundancy [28]. Static redundancy is redundant components inside a system or subsystem to hide effects of faults, while dynamic redundancy is to activate an unpowered spare when an original component fails [23].

Triple Modular Redundancy - TMR

An example of static redundancy is triple modular redundancy (TMR) which consists of three identical modules and a majority voter between them. If one of the modules differ from the others, the disagreeing member is masked out. In order to mask faults from more than one module, n modular redundancy (NMR) must be used where n denotes the number of modules[28]. TMR is commonly used to handled radiation impacts in electronics used in space [2]. TMR yields a system

with a higher fault-coverage and higher reliability, but with adding more hardware there is a higher risk of multiple failures over time, leading to a shorter time of life [23]. For a CubeSat application this may be acceptable due to often short mission lifetimes. TMR can operate through a failure in one of the modules, while a self-checking pair with dual redundancy only yields a fail-safe [23]. Another issue with a TMR system is the injection of the voter as a single point of failure, which may be acceptable since the voter circuit often is much less complicated than the systems which generate the inputs to the voter and hence is less prone to failure [29]. In order to further increase the reliability of the system, the voter can be implemented with radiation hardened components and/or be replicated. By replicating the voter to each part where its output is used, a malfunctioning voter will not cripple the entire system, but only affect the part to which it is connected. This comes at the cost of more hardware and consumed real estate [23].

Functional Redundancy

Redundancy with a higher form of granularity is functional redundancy and it is often used in space applications. Instead of replicating a module to mask failures, a similar module exists which can inherit the functionality of the malfunctioning module and support further operations, either at full or degraded performance. This is similar to the systems used on Skylab in 1973 [23] where each computer first ran a self-check and if it believed itself to be healthy and the other computer to be malfunctioning, the partner would be reset.

3.3.2   Watchdogs

A watchdog is an electronic circuit or a software program that detects and initiates corrective actions to a hardware or a program error. A watchdog must initiate two action; first it must set the output the system to a safe state as to prevent unwanted consequences. After setting the output to a safe state is must restore to a normal operating mode. This could be as simple as to restart the system or it may involve a sequence of actions [6].

A watchdog can respond to faults more quickly than an external operator, making it invaluable in cases where an operator would be too slow, or unavailable, to react to a fault condition [6].

For an external hardware watchdog, a controller, often an MCU, can reset the timer by toggling an input pin (WDI) to the watchdog within a known time-out period. This is known as tapping and during normal operation the controller regularly taps this pin to indicate that the program is functioning as expected. If a fault occurs and prevents the controller from tapping the timer, the watchdog will time out and initiate an action to recover the system [30]. In the case where the watchdog causes power to be removed, the amount of time before power is

brought back on is known as a power-on-reset (POR) delay. Figure 3.6 shows a basic digital watchdog timer.

Several MCUs contain an internal watchdog timer (WDT) which performs a reset of the MCU if not tapped within the time-out period. The time-out period can be *windowed*, meaning if it is tapped too slow or too fast, it will issue a reset regardless [30]. Software is responsible for tapping the watchdog and can in some implementations adjust its time-out period or disable it altogether. A watchdog design can combine software, hardware and internal watchdogs to create a more reliable system. The external hardware watchdog can be tapped conditionally based on results from the software watchdog's system health checks, while the internal watchdog can be tapped unconditionally to recover from e.g. code corruption [30].
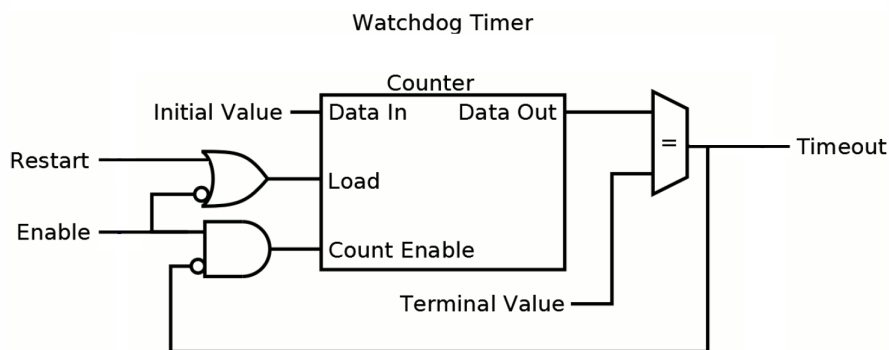
Figure 3.6: Basic digital watchdog timer [6]

3.3.3 Radiation Hardened Components

Figure 3.7 shows a comparison of commercial off-the-shelf (COTS), radiation-enhanced and radiation-hardened components. It is clear that the commercial components does not have a minimum requirement for radiation tolerance, leading to variations between manufactures, processes and applications. It also shows that radiation hardened components are design towards tolerating a much higher total ionizing dose (TID) than commercial ICs, but may still suffer from SELs and SEUs [7]. Furthermore, radiation hardened components are often difficult to source since they may be covered by strict military and export regulations, and processes used to hardened ICs are often kept as company secrets. In a design where commercial components are used, such as the NUTS project, the variations related to COTSs necessitates a design aimed at being as fault tolerant as possible. CubeSats are often design without radiation hardened components due to costs and the missions' short lifetimes.

	TID	SEL	SEU
Commercial ICs	3-30 krads (Si)	1 - 120 MeV	1 - 120 MeV
Radiation-Enhanced ICs	Customized to Orbit (100 krads (Si) Target)	Customized to Orbit (Up to 120 MeV)	Customized to Orbit (Up to 120 MeV)
Radiation-Hardened ICs	100 krads (Si) Minimum	Up to 120 MeV	Up to 120 MeV

Figure 3.7: Radiation hardness requirements [7]

3.4 Vacuum Considerations

All electronics generate a certain amount of heat which must be dissipated through one or several of the three different ways possible; by conduction, convection and/or radiation. In the vacuum environment of space, heat dissipation through convection is close to none, and with radiation being highly ineffective, maintaining good heat transfer by conduction is critical [31]. Also, with box-packaged components, a vacuum environment may effect their performance and thermal vacuum testing is necessary in order to ensure correct functionality [31]. Telemetry from California Polytechnic State University's CP3 CubeSat shows external temperature fluctuations between -40°C to +40°C in LEO [32]. The temperature extremes may vary based on orbit parameters, and internal temperatures may be higher than external due to power dissipation in electronics and charging of batteries.

3.5 Solar Cells

Solar panels, which is an array of solar cells, harvest energy from sunlight and convert it into electricity. Generation of electricity is possible because of the photovoltaic effect [33]. The photovoltaic effect is the creation of an voltage in a closed loop and begins when two dissimilar materials in close contact produce an electric voltage when struck by light [34]. Light striking crystals such as silicon or germanium, where electrons usually are not free to move from atom to atom, provides the energy needed to free some electrons from their bound condition [34]. Free electrons cross the junction between the two dissimilar crystals more easily in one direction than in the other, giving one side of the junction a negative charge and hence a negative voltage with respect to the opposite side. The photovoltaic effect will continue to provide voltage and current as long as light strikes the two materials [34].

3.6 Battery Charging

Battery theory is a large field, but a short presentation of charging characteristics related to NUTS will presented here.

The manufactures publish the nominal rating for a given set of discharge conditions and is given by the rate of discharge, temperature and minimum cell voltage. The minimum cell voltage is the lowest voltage to which a battery should be discharged. Discharging below this value can reduce or even destroy the battery's capacity [35]. The rate of discharge refers to the amount of current a battery can sustain for one hour while remaining within a specified voltage range.

When current is drawn from a fully charged battery, the voltage decreases gradually from nominal voltage to the discharged voltage. When the discharge curve for a typical battery is plotted, the cell voltage remains relatively flat until the discharge voltage is reached. When the discharge voltage is reached the battery capacity is exhausted [35]. Figure 3.8 illustrates such as curve. The same principle applies when charging the battery.
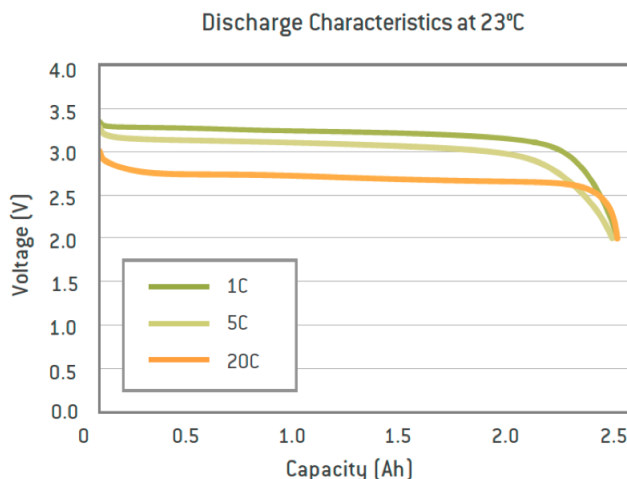
Figure 3.8: Battery discharge curve [8]

3.7 Beta Angle

The beta angle is the angle between the Sun vector and the orbital plane of any Earth-orbiting object [9]. Figure 3.9 illustrates how the Sun vector projects onto Earth and shows the Earth's axis and Equator. The beta angle determines how long an object in LEO, e.g. a satellite, can be exposed to direct sunlight and varies from $+90°$ to $-90°$. The direction the satellite revolves around the body it orbits, determines whether the beta angle sign is positive or negative [36].

With a high beta angle the satellite is exposed to the Sun more often. With a beta angle of $+/-90°$ the satellite spends no time in eclipse. With a low beta angle the eclipse time becomes longer and with a beta angle of $0°$ the satellite will have the longest possible eclipse time [9]. Figures 3.10 and 3.11 shows satellite positions at different beta angles in relation the Sun vector. This thesis applies a worst case situation of a $0°$ beta angle for solar charging estimates.
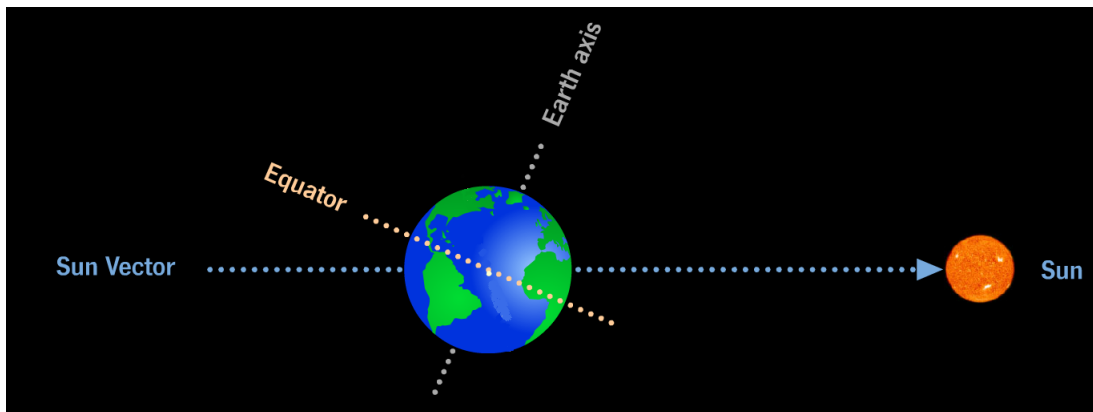
Figure 3.9: Illustration of the Sun vector [9]
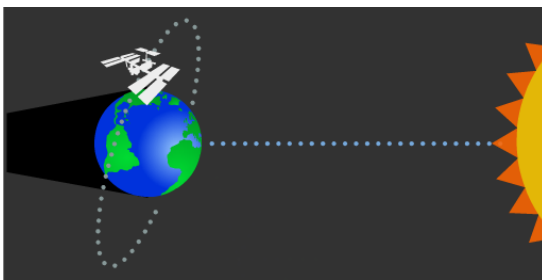
Figure 3.10: High beta angle [9]
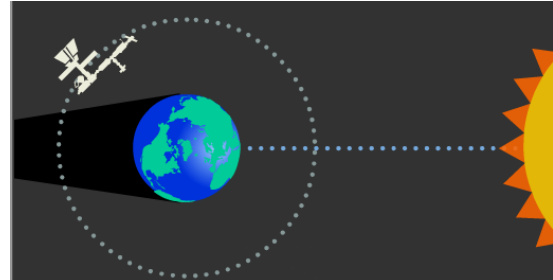
Figure 3.11: Low beta angle [9]

Chapter 4

System Overview

This chapter presents NUTS' system overview. The two main systems are the two master modules, On-Board Computer (OBC) and Radio module. Some of the different integrated circuits (ICs) performing important, dedicated tasks, are also presented.

Appendix A shows the initial block diagram of the system. A new and more detailed block diagram is presented in this chapter.

4.1   On-Board Computer - OBC

The OBC consists of an Atmel Microcontroller Unit (MCU), Ferroelectric RAM, NAND flash and various headers.

The Atmel AT32UC3A3 MCU is a complete System-on-Chip MCU based on a RISC architecture. It can run at frequencies up to 84 MHz, has a high-performance 32-bit microprocessor core, 256 kB programmable flash and 2x32 kB SRAM. It is designed for cost-sensitive embedded applications, with emphasis on low power consumption, high code density and high performance. The MCU has an absolute maximum current consumption of 100 mA, but consumes only 30.4 mA running in active mode at 42 MHz[37].

It also contains an internal watchdog circuit which, when enabled, must be tapped within a time-out window in order to avoid a soft reset. A reset caused by this watchdog will let its software know a reset has occurred as well as what the source for the reset was [37]. This is in contrast to a hard reset, i.e. removal of power. If an internal soft reset does not recover the system, an external hardware system will toggle power to the MCU if not tapped within its time-out period.

The more radiation resistant FRAM will hold mission critical data and firmware code, while the 2 GB NAND flash will be used as primary storage for images from the camera payload and system logs. Ferroelectric Random Access Memory

is a type of non-volatile memory which uses a ferroelectric layer instead of the classical dielectric layer found in many types of volatile DRAM architectures [38]. Compared to other types of non-volatile memories, FRAM has a faster write performance, lower power consumption and a greater maximum write-erase cycles at the cost of lower storage densities, storage capacity limitations and higher production cost [39]. What makes FRAM an interesting option for space applications is its high resistance to radiation, fast programming time, solid data retention over a large temperature range and a high endurance rating [40]. The aim is to use FRAM as the main storage for mission critical data and the microcontrollers' firmware. NUTS' FRAM chip holds 4 Mbit of storage, which equals 512 kB.

Figure 4.1 shows a possible block diagram of the OBC with all the systems, both software and hardware. Note that the external memories overview does not show the current memory configurations.

4.2 Radio Module

The Radio module has the same components as the OBC, in addition to the necessary radio components. Figure 4.2 shows a possible configuration of the Radio module. Note that the external memories overview does not show the current memory configurations. Both Figure 4.1 and 4.2 are made in collaboration with NUTS' software group. The Radio module consists of two different radio transceivers, one UHF at 437 MHz, and one VHF at 145 MHz. The VHF band is used by an OWL[1] radio which can be controlled by the OBC regardless of an operational Radio MCU, yielding an additional layer of communication redundancy.

NUTS system is design such that it is possible to utilize the Ferroelectric RAM (FRAM) if the NAND flash memory fails, and vice versa. If both of the non-volatile memories are damaged, operations may continue with volatile memories as long as power is maintained. The system is also designed such that if the OBC fails, its functions can be taken over by the Radio module.

4.2.1 Antenna Release Mechanism

From the CubeSat operational requirements in Section 2.1.2 all antennas must wait a minimum of 30 minutes after ejection from the Poly Pico-Satellite Orbital Deployer (P-POD) before deploying. The satellite will carry the antennas coiled up inside the satellite before and during launch. After ejection and the 30 minutes delay, the antennas will deploy. The release mechanism will consists of four resistance wires designed to melt nylon cords. The satellite will have four antennas, arranged in two pairs for the VHF and UHF. As of 2014, design of the release

---

[1]Design with emphasis on receiver sensitivity and called OWL due to owl's excellent hearing
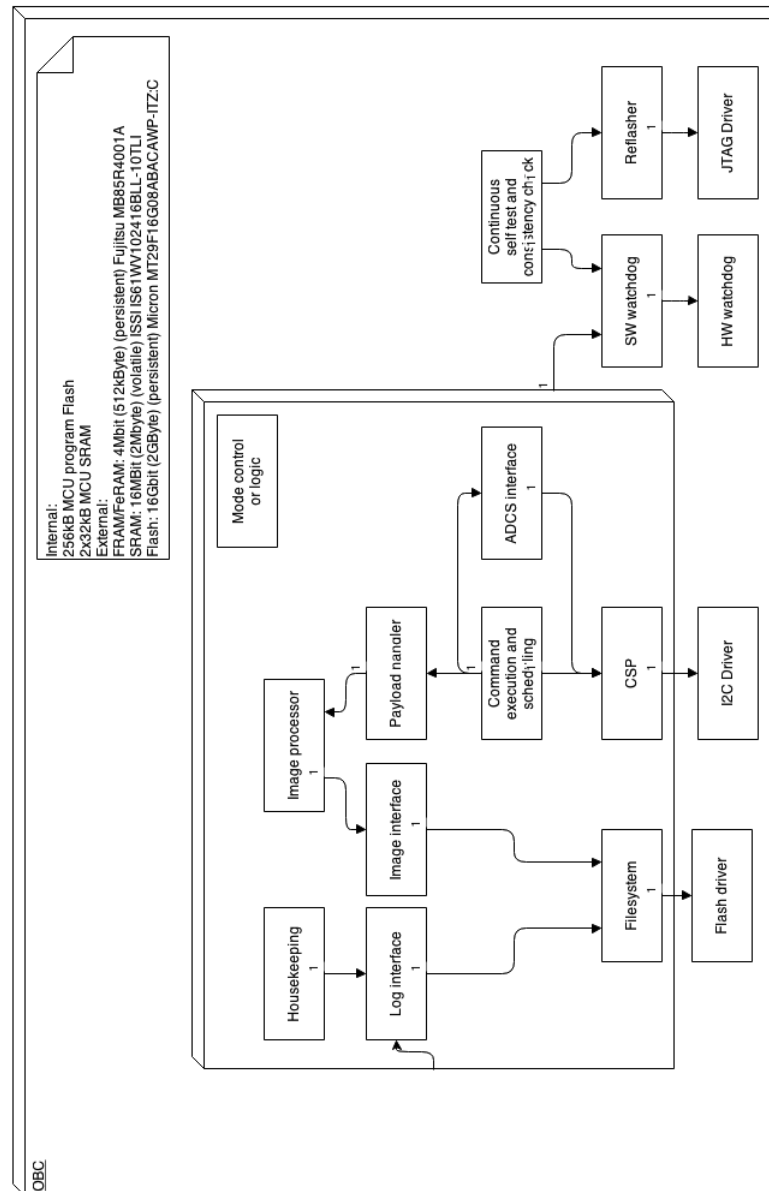
Figure 4.1: On-board computer module

mechanism is not finished, but initial tests shows a current consumption of approximately 350 mA per wire. Due to the importance of deploying the antennas, several consecutive burn-off attempts will be made after NUTS has reached orbit.

4.2.2 Beacon

The beacon signal can be regarded as the basic sign of life from the satellite while in orbit. This signal will be the first signal the ground station will receive and it indicates whether or not the satellite is operational. The beacon transmits at a given rate since it provides important tracking and identification. It has been
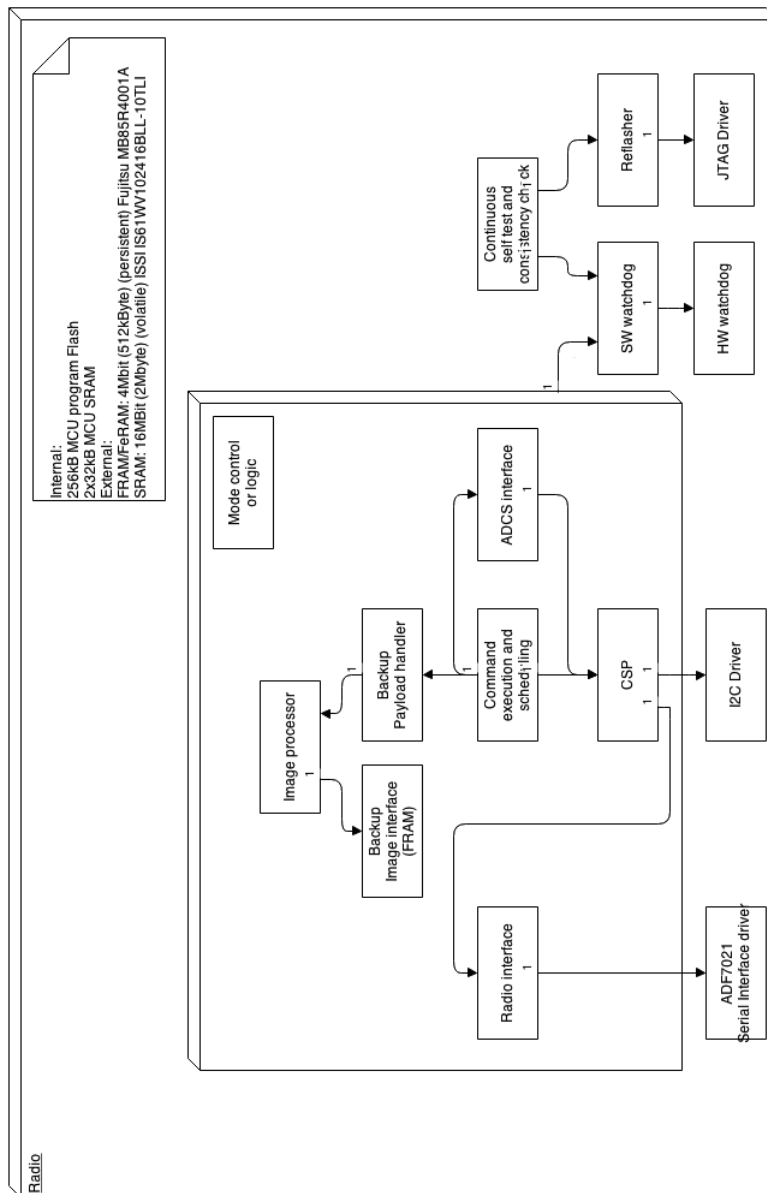
Figure 4.2: Radio module

decided by the project management that the beacon is never to be disabled due to the importance of maintaining radio contact with the satellite.

At the beginning of the mission it could be useful to transmit more often since this will help in determine if the satellite is operative after ejection from the P-POD. After the ground station receives the first beacon signal, the periodic rate could be decreased in order to save power.

4.3   Backplane

The backplane provides redundant power supply and current limitation to each module. This section will provide a brief overview of important structures already in place. In Appendix B a circuit diagram of the power distribution and control logic is shown. The hardware drawings are from Bruyn's thesis [11]. Figure 4.3 at the end of this chapter shows the existing design with the OBC and backplane connected together. The backplane features eight connectors enabling a total of two master modules and six submodules. The existing backplane implementation has a measured current consumption of 50 mA.

4.3.1   Power OR-ing - Linear Technologies LTC4413

LCT4413 is a power OR-ing chip capable of handling two independent power sources and switch between them if one fails. This enables continued operation even in the event of loss of one supply. The backplane receives two independent 3.3 V and two 5 V lines from four regulators on the EPS module, each connected to two power OR-ing chips for redundancy. The backplane distributes these four lines to each module, each with a separate power OR-ing chip. LTC4413 consists of two ideal diodes each capable of supplying up to 2.6 A between 2.5 V and 5.5 V [41].

4.3.2   Current Monitor - Texas Instruments INA219

The backplane and EPS have multiple current monitors from Texas Instrument. INA219 is a high-side current shunt and power monitor with an I^{2}C interface capable of providing instantaneous voltage and current flow measurements [42].

4.3.3   Current Limiter - Maxim Integrated MAX14523

MAX14523 current-limit switches features programmable current limitation to prevent damage to connected components due to faulty load conditions [10]. The current limiter has been implemented for two reasons: module power switching and over-current protection, and with a limit of 640 mA [11]. The current limit can be adjusted from 250 mA to 1.5 A to satisfy a preferred limit specific to the application. This will help mitigate high current single event latchups if the current limit is set correctly. A good estimate of each module's current consumption will help determine this level.

The MAX14523 features an ON pin which in the current design is connected to the two master modules, enabling them to turn off power to separate submodules by setting the connected line low. This is seen in Figure B.4 in Appendix B where the signal *PWR_ON1* is used to turn the chip on or off. Each module has a separate

signal and the suffix *1* indicates a signal connected to module 1. It also shows the *PWR_FLAG1* signal which goes low in an over-current situation. The signal is accessible by the OBC and Radio MCUs enabling them to perform necessary actions. It is important to note that a master can not turn itself off and can only be disabled by the other master.

4.4 Submodules

NUTS' submodules are Attitude Determination and Control System (ADCS), Electrical Power System (EPS) and the camera payload.

4.4.1 Attitude Determination and Control System - ADCS

ADCS orients the satellite in space using magnetic coils, performs de-tumbling and points the camera payload towards Earth. Work on the ADCS module is concurrently being performed at the Department of Engineering Cybernetics at NTNU and more information can be found in [43] and [44]. The ADCS consumes 500 mA if all coils to turn the satellite are active. This value is a preliminary calculation provided by NUTS member Øyvind Rein.

4.4.2 Electrical Power System - EPS

Electrical Power System (EPS) supplies the satellite with the correct and redundant voltages for the backplane, protects the batteries from overcharging and charges the batteries from the solar panels [18]. Power from the EPS is distributed to the backplane and submodules through the LTC4413 power OR-ing. NUTS will launch with a fully charged battery.

4.4.3 Camera Payload

The initial plan was to have an IR camera as a payload, but due to costs both financially and in engineering, the project decided to use an visual range camera instead. Based on a NTNU project report from the fall 2013 [45], a low power visual range camera will be implemented as a payload. The payload has an estimate current consumption of 164 mA.

4.5   Ground Station

A ground station for transmitting and receiving data to and from NUTS is located at Gløshaugen in Trondheim, Norway ($63°25'06.3"N10°23'58.2"E$). The station is capable of transmitting and receiving both UHF and VHF signals, and can track the satellite from when it rises above the horizon until it leaves the line of sight.

4.6   Evaluation of Existing Watchdog & Power Modules

In Bruyn's thesis [11], a watchdog has been implemented, but it only resets the state of the I^{2}C repeaters to a default on state and does not remove the power which is necessary for removing SELs. Only the master modules can remove power to the submodules and if one or both masters stop responding, the current watchdog will not recover the system. With the current design it is not possible to remove the supply voltage for the backplane logic, which again will inhibit on the system's capability of recovering from SELs. A new revision of the watchdog should aim at mitigating these issues. Hardware drawings of the existing watchdog are presented in Figure B.2 in Appendix B.

Another issue discussed in Bruyn's thesis is the dual use of an address line to tap the watchdog. The ADDR0 line is connected to the watchdog's input, but is also used elsewhere. This can be seen in Figure B.3 in Appendix B. The ADDR[2..0] lines are supposed to address the correct module by address match. Using the ADDR0 line to tap the watchdog could lead to toggling of an address signal and cause a mismatch when attempting to address a module. Also, if the ADDR0 line is held stable while addressing a module, the current watchdog could time-out and cause an unnecessary reset.
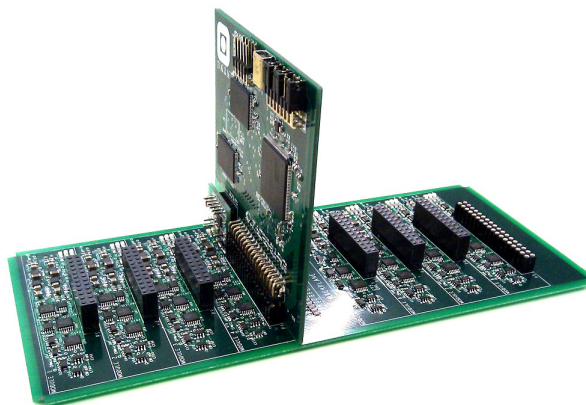
Figure 4.3: Existing prototype of on-board computer (OBC) and backplane

Chapter 5

Battery Charging & Discharging

This chapter presents estimated battery consumption and charging for different levels of beacon activity. Results achieved forms the basis for deciding when action must be taken in a low battery situation.

5.1 Battery Estimation

Since battery management is an integral part of keeping the satellite operational, a solid estimate is necessary as a foundation for a mission plan of high quality. Table 5.1 shows a rough initial estimate of the satellite's power consumption. The values have been measured, calculated or based on datasheet information.

Table 5.1: Estimated power consumption spring 2014

Component	Operating voltage [V]	Current draw [mA]	Watt [mW]	Method
Backplane	3.3	50	165	Measured
OBC MCU	3.3	100	330	Datasheet [37]
Radio MCU	3.3	100	330	Datasheet [37]
NAND Flash	3.3	30	99	Datasheet [46]
FRAM	3.3	20	66	Datasheet [47]
Power amplifier[1]	3.3	1000	3300	Measured
OWL Radio[2]	5.0	462	2310	Calculated
ADCS	3.3	500	1650	Calculated
Camera Payload	3.3	164	541.2	Calculated
TOTAL	-	**2426**	**8791.2**	

Note that the MCUs' power consumption is a maximum value from the datasheet, which in reality will be dependent on GIPO use and software execution. Values for the NAND flash and FRAM is per chip, and NUTS has two of each.

---

[1]Power amplifier's power consumption was measured by the radio group March 2014 during a test flight.

[2]Information provided by its designer. Power consumption is independent of input voltage. Datasheet sets the current draw to 140 mA at 16.5 V, giving 2310 mW.

The satellite carries a 4.4 Ah battery pack with a nominal voltage of 6.6 V, giving a capacity of 29.04 Wh. It has 18 solar cells divided into five solar panels, four at the sides and one at the top. The side panels have four solar cells and the top panel has two solar cells.

Power generated from the solar panels can be seen in Table 5.2. The worst case, best case and the average case are calculated based on Bruyn's thesis [11] and a report from Amund Gjersvik [48].

Table 5.2: Power from solar panels

Solar panels	
# of panels	18
One solar cell voltage [3]	2.409 V
One solar cell current [4]	502.9 mA
One solar cell power generation	1.211 W
One side	4.846 W
Top	2.423 W
Top + two sides	7.514 W
Two sides	5.091 W
One side & top	5.437 W
Average charging power	**5.062 W**

By normalizing the orbit time with respect to one hour, it is possible to find the relationship between charging time and time spent in eclipse as seen in Table 5.3.

Table 5.3: Orbit times at 600 km above the Earth's surface [11]

Per orbit	Minutes	%	Normalized [min]
Time in sun	61.1	63.32 %	38 - t_{sun}
Time in eclipse	35.4	36.68 %	22 - $t_{eclipse}$
Total	96.5	100 %	60 - t_{total}

By applying the average charging power from Table 5.2, a normalized charging power is given in Equation 5.1.

$$P_{norm} = P_{avg} \cdot \frac{t_{sun}}{t_{total}} = 5.062 \ W \cdot \frac{38}{60} = 3.205 \ W \tag{5.1}$$

Eclipse time per orbit is a maximum based on the worst case beta angle of 0° from Section 3.7. The beta angle can not be determined due to unknown launch parameters outside of the project's control. Best case charging is achieved at a

---

[3]Datasheet gives this value as *beginning of lifetime* and it decreases when the solar panel is exposed to radiation. After irradiation of $1 \cdot 10^{15}$ at 1 MeV, the voltage is expected to be 2.191 V as given in its datasheet [49]

[4]Also *beginning of liftime*. After irradiation of $1 \cdot 10^{15}$ at 1 MeV, the current is expected to decrease to 477.6 mA as given in its datasheet [49]

beta angle of $+/-90°$ where top and two sides are exposed to the Sun throughout the orbit, causing a charging power of 7.514 W.

5.1.1   Battery Fuel Gauge

Measuring the battery's net current flow is important in order to enable an estimate of remaining battery capacity. In the existing design this is done by the current monitors (INA219) on the electrical power system (EPS) which is unfortunate since a master must retrieve the information, which can accumulate an error over time if not retrieved often enough. The accumulated error will occur due to change in voltage while at the same capacity level due to temperature, impedance differences, and discharge current [50]. Accurate tracking of the battery capacity requires a dedicated system to monitor the current from the battery at all times. If the current is not measured continuously, the remaining capacity will be only a rough estimate. It is also problematic if a master module is tasked with continuously measuring current to accurately report battery capacity. An independent system should measure the current consumption and process the information so the master module may focus on other tasks. Battery fuel gauging is the process of collecting data such as current, voltage and temperature, and then use this data to calculate an accurate estimate of remaining battery capacity [50]. Integration of a fuel gauge is an issue that project management deems important towards a completed pre-flight test model and at their request, an example of a suitable candidate has been found.

A fuel gauge must be compatible with the LiFePO4 battery chemistry and the multi-cell battery configuration used for NUTS. It must also feature I^2C to interface the master modules and have a sufficient temperature range. Online vendor Farnell provides an option suitable for these requirements, Texas Instrument's BQ34Z100 [51]. BQ34Z100 has impedance tracking for 3 V to 65 V batteries, self-discharge and aging compensation. It has an operating temperature range of -40 to 85 °C. It can be interrogate by a host processor through commands returning estimated remaining battery capacity, full charge capacity and average current, and information is stored in non-volatile memory. It provides capacity predictions within 1 % accuracy over its operating conditions and has the possibility of tracking temperature with an negative temperature coefficient (NTC) thermistor. Implementing BQ34Z100 close to NUTS' battery pack will enable accurate battery management by the acting master and make taking continuously measurements with INA219 current monitor unnecessary.

5.2   Pass Time

Pass time is defined as the amount of time the satellite is visible from the ground station. The average pass time over the ground station is simulated with the

program System Tool Kit (STK) and is seen in Figure 5.1. The satellite does approximately 15 orbits during 24 hours, but the ground station will not cover all 15 passes since some will be out of sight. Table 5.4 shows the number of passes over Trondheim during a 24 hour window, with maximum, minimum and average pass times. In order to achieve the maximum duration, the ground station must track the satellite from horizon to horizon.
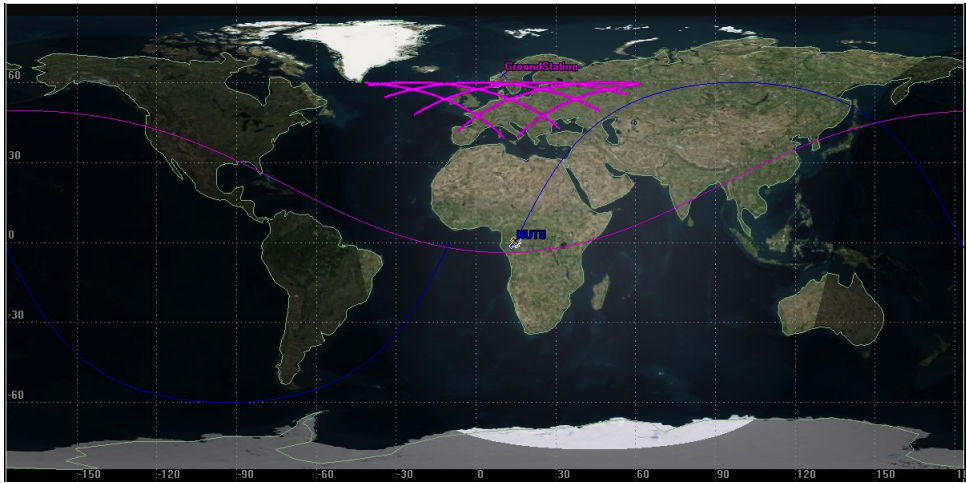
Figure 5.1: Ground station pass overs

Pass time is related to power consumption since radio communication will increase while in contact with the ground station. It also relates to the beacon transmission rate which must be high enough to guarantee received transmissions during a pass. This thesis applies a pass time estimate of 10 minutes. As of 2014, the launch details are not confirmed, making it impossible to know what type of orbit the satellite will operate in. STK has the possibility of setting the cone of the ground station which determines how the station sees the satellite. Since the ground station is able to track the satellite from horizon to horizon, the value has been set to 90°, giving a maximum tracking area tangential to the curve of the Earth. This is illustrated in Figure 5.2. The simulations result in an average pass time of 12 minutes, but due to uncertainties regarding the station's tracking capability, a 10 minute pass time for NUTS is a reasonable estimate.

Note from Table 5.4 that pass six is the last visible pass before an approximately 849.3 minute, or 14 hour, window until next visible pass.

5.3   Beacon Transmission Rate

In order to detect the satellite while in orbit, the satellite must transmit a beacon signal making it possible to identify and track the satellite. Transmitting a beacon signal unnecessary often consumes more power than needed, and in order to avoid draining the battery, the beacon transmission rate must be adjustable.
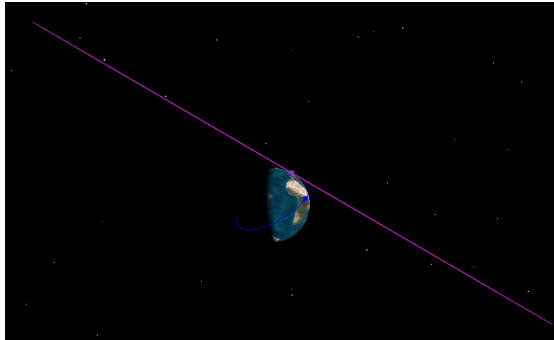
Figure 5.2: Ground station conic angle of 90°

Table 5.4: Pass times over Trondheim during 24 hours

Pass	Duration(min)	Time to next pass	
		Hour	Min
1	9.8309	1	27.60
2	12.5305	1	26.53
3	13.2478	1	26.42
4	13.2908	1	26.48
5	12.7696	1	27.22
6	10.6582	14	9.32
Minimum duration	**9.8309**	-	-
Maximum duration	**13.2908**	-	-
Average duration	**12.0546**	-	-
Total duration 24 h	**72.3275**	-	-

If the satellite has a low battery condition, the beacon transmission rate should be decreased to a minimum, with a minimum given as at least two detectable beacon transmissions in the 10 minute window over the ground station. The beacon transmission has a length of one minute, and in order to achieve maximum one detectable transmission, the beacon must transmit nine minutes apart as seen in Figure 5.3. To guaranteed two detectable transmissions in a 10 minute window, the beacon must transmit four minutes apart as seen in Figure 5.4.
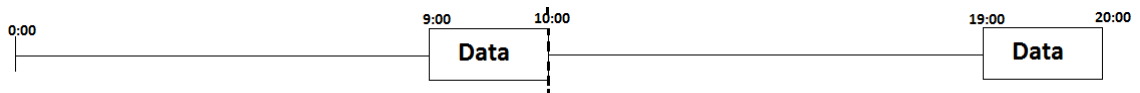
Figure 5.3: Beacon transmissions - one detectable transmission

5.3.1 Beacon Power Consumption

By defining three different levels for the beacon transmission rate, it is possible to present an estimate of the beacon's power consumption. The radio's power

amplifier (PA) is assumed to consume 1000 mA and each beacon transmission has a length of one minute. Based on the estimated pass time of 10 minutes and the minimum of two detectable transmissions, the lowest beacon rate is seen in Figure 5.4. The beacon transmits four minutes apart to provide a minimum of two detectable transmissions. A normal rate with four detectable transmissions enables easier tracking without consuming more power than necessary. Normal rate transmissions are seen in Figure 5.5, where the beacon transmits two minutes apart. A full rate is needed when contact between satellite and ground station has not yet been established. The beacon could transmit continuously, but at the cost of heat generation in the power amplifier and high power consumption. Transmitting 30 seconds apart as seen in Figure 5.6 reduces the power consumption and the load on the power amplifier, while enabling easier tracking.

Low Rate

Equation 5.2 calculates the energy consumed when transmitting for one minute. The power amplifier (PA) operates at 3.3 V.

$$E_{1\ min} = \frac{1}{60}h \cdot 1000\ mA \cdot 3.3V = 55\ mWh \tag{5.2}$$

At low rate, the beacon transmits for one minute, four minutes apart, as seen in Figure 5.4.
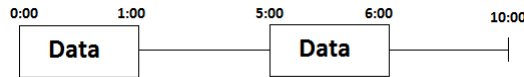
Figure 5.4: Beacon transmissions - low rate

The energy consumption for low rate is given in Equation 5.3, where the number of transmissions per hour is multiplied with the power amplifier's energy consumption.

$$E_{@low} = \frac{60}{5} \cdot 55\ mWh = 660\ mWh \tag{5.3}$$

The beacon's energy consumption for the low rate is 660 mWh. The power consumption becomes 660 mW.

Normal Rate

At normal rate, the beacon has the same transmission length of one minute as before and the energy estimate in Equation 5.2 is valid for this rate as well. The beacon rate is increased to transmit two minutes apart, as seen in Figure 5.5.

The energy consumption is given in Equation 5.4, yielding an instantaneous power consumption of 1100 mW, 66.67 % higher than low rate.

$$E_{@normal} = \frac{60}{3} \cdot 55 \ mWh = 1100 \ mWh \tag{5.4}$$
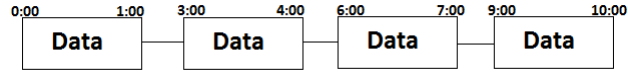
Figure 5.5: Beacon transmissions - normal rate

Full Rate

At full rate, the beacon transmits 30 seconds apart as shown in Figure 5.6. Energy consumption is given in Equation 5.5.

$$E_{@full} = \frac{60}{1.5} \cdot 55 \ mWh = 2200 \ mWh \tag{5.5}$$

The average instantaneous power consumption becomes 2200 mW, 233.33 % higher than low rate and 100 % higher than normal rate.
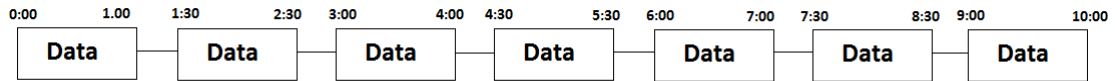
Figure 5.6: Beacon transmissions - full rate

5.4   Initial Mode

After the satellite is released from the P-POD and the antennas are deployed, the beacon transmits at full rate enabling easier detection. The antenna release mechanism consists of four resistance wires which melt thin nylon cords when current is pushed through. The wires have a current consumption of about 350 mA each and it is assumed a maximum of five re-deployment attempts. Based on data from HinCube [5], the time it will take to burn off the cords is close to 3 seconds, making the power draw 3.85 mW per attempt and 19.25 mW for five attempts with four wires. Detailed calculations can be found in Appendix D.1. Table 5.5 shows the total power consumption before contact with the ground station, and it is less than the normalized charging power of 3.205 W. External memories are not

---

[5]HinCube was built at Narvik University College. It was launched in 2014, but radio contact was never made.

included since these will not be used until after contact is made, and a worst case consumption for the MCUs is used. Power consumption by the release mechanism is not included since it is not used continuously. Given the normalized charging power, the satellite can operate in this mode indefinitely. However, due to post-ejection spin, a worst case charging scenario is possible, where power harvested from the solar panels is only 1.534 W. This will drain the battery in close to 20 hours. After contact with the ground station, the beacon transmission rate is adjusted based on system modes presented in Chapter 6, allowing the attitude determination and control system (ADCS) to de-tumble the satellite.

Table 5.5: Initial mode's average instantaneous power consumption

Component	Operating voltage [V]	Current draw [mA]	Power consumption [mW]
Backplane	3.3	50	165
OBC MCU	3.3	100	330
Radio MCU	3.3	100	330
Power amplifier[6]	-	-	2200
TOTAL	-	**914**	**3025**

---

[6]Beacon operates at its highest rate

Chapter 6

Mission Event Plan - Requirements

This chapter presents the requirements for the mission event plan. A thorough mission event plan is necessary to ensure optimal performance and the possibility of handling failures.

6.1 Different Modes

To efficiently respond to different events, the satellite should have defined modes, making the system capable of handling different fault conditions, low power levels and scheduled commands without the involvement of the ground station. Different modes must have dedicated tasks based on the type of events the satellite encounters. It is also important that commands from the ground station have the possibility of overriding a current mode in case of unforeseen events.

To execute decisions based on remaining battery capacity, NUTS operates with the following system modes:

- Critical mode - less than 25 % battery capacity

- Avoidance mode - between 25-50 % battery capacity

- Normal mode - between 50-100 % battery capacity

Remaining battery capacity will be reported by a battery fuel gauge implemented near NUTS' battery pack.

6.2   After Ejection from P-POD

The railing switches are depressed while in the P-POD and the satellite is therefore deactivated. After ejection from the P-POD, the switches will be released and the satellite will be activated. Following the CubeSat specification, the antennas must wait at least 30 minutes to deploy. As given by the project management, a first time start up should be executed in the following order:

1. Deploy antennas

2. Start beacon signal

3. Wait for acknowledgement from ground station

4. Reattempt antenna deployment if no acknowledgement from the ground station is received

5. De-tumble

It is important that the antennas deploy so that the ground station can receive the beacon signal indicating an operational satellite. Several attempts of deploying the antennas may be necessary if no acknowledgement is received from the ground station.

6.3   In Orbit

If the antennas deploy successfully, the satellite is to monitor its own health and execute received or stored commands. If the satellite encounters an issue, e.g. a low battery condition, it should perform appropriate actions. The satellite must continuously monitor submodules' current draw as this can be an indication of single event latchups (SELs).

6.3.1   Power Monitoring

Based on remaining battery capacity levels defined above, the satellite is allowed to operate in one of three system modes. A mission plan should result in the satellite being in normal system mode at all times, but loss of battery capacity necessitates reduction of power consumption by entering an avoidance mode. If the avoidance mode fails at increasing the battery level, a critical mode is initiated where submodules are turned off and radio activity decreased.

Avoiding damaging temperature levels is also important to maintain an operational satellite. For NUTS, a high temperature condition is treated as a critical system mode since reducing power consumption reduces heat generation. Decreasing radio activity reduces heat generated in the power amplifier and limiting submodules' current draw also reduces the load on the regulators.

6.3.2   Software Watchdog & Power Cycling

The software watchdog supervises other software tasks, taps the MCUs internal watchdog and interfaces external modules responsible for current sensing, temperature monitoring and battery monitoring. The internal watchdog can be tapped unconditionally at higher frequency than an external watchdog and will handle failures in task execution and code corruption caused by e.g., single event upsets (SEUs). For NUTS, a software watchdog should be implemented on the on-board computer (OBC) and Radio master modules and will be responsible for tapping an external watchdog. Based on results from health checks and external monitors, the software watchdog should initiate actions dependant on system state. If failures are detected, it must attempt to recover the system before turning off the affected submodules as a last resort.

A software watchdog must also enable the system to detect and respond to SEUs and SELs. An SEU, which commonly results in a bit flip, is not a permanent fault and refreshing the circuit will remove the error. An SEL is more critical since recovery is dependent on removal of power and increased current flow could ruin an IC if not handled in a timely manner. High current SELs can be detected through the current-limit switches, but low current SELs might only be possible to resolve by a periodic reset since these will be more difficult to detect. A thorough current consumption estimate for each submodule will help in detecting SELs, as software can compare actual to estimated values and thereby identify them. A periodic reset of submodules could be sufficient in maintaining an operational system, but situations could arise where a system wide reset is necessary. Before issuing a system wide reset, the software watchdog must, when possible, initiate a shutdown procedure in order to resume operations when power is brought back on.

Power Cycling

The satellite's hardware watchdog resets the system if it times out, and thereby clearing any SELs. If a watchdog time-out occurs in the current design, the state of the power modules and I^2C repeaters are simply reset to a default on-state, which is insufficient to recover from SELs. A period of time where power is disabled to the affected module is necessary for the system to recover. Supply voltages should be removed for a sufficient amount of time such that all voltages can reach a ground potential of 0 V relative to the satellite's ground plane. Rapidly resolving all SELs are important in order to minimize the risk of permanent damage.

Chapter 7

Mission Event Plan - Results

This chapter presents the mission event plans based on the requirements from Chapter 6.

7.1   After Ejection from P-POD

Section 6.2 describes the procedure of deploying the antennas. The CubeSat specification states that the antennas can not be deployed until 30 minutes after ejection from the P-POD and therefore it is necessary to use a 30 minute timer. An independent and redundant timer should provide a fail-safe if the first deployment attempt fails. Two deployments attempts will therefore be performed after ejection. One timer should be implemented on the on-board computer (OBC) and another on the Radio module. As described in Section 5.4, the power budget for an initial mode estimates a total of five re-deployment attempts as to give a margin to the estimated power consumption. The mission plan describing this initial mode can easily be expanded from two to five attempts if found necessary.

Figure 7.1 illustrates actions taken after ejection from the P-POD. A large concern and a single point of failure are the railing deployment switches. If both switches are broken or stuck, the satellite will not power up. If one or both switches are released, power will be provided and the satellite activated. After the antennas have deployed, the beacon signal is to transmit at the highest rate which makes it easier to find and track the satellite.

At this point there may be an uncertainty as to whether or not the antennas have deployed. If the antennas have not been deployed and the beacon is transmitting, it could generate reflection, which is less than ideal for the system. However, through discussion with project management, the need for establishing connection with the ground station outweighs the risk of such reflections.

When the satellite has received an acknowledgement from the ground station, the satellite should set a byte or a larger memory portion in order to avoid an attempt

to re-deploy the antennas at a later stage due to a restart or power cycling. This could be by reserving a page in the more radiation resistant FRAM. If the satellite looses power or temporarily fails, it will know that the antennas are deployed when the system is restored. This will prevent the satellite from waiting for a new acknowledgement from the ground station.

If an acknowledgement has not been received, the satellite will attempt to re-deploy its antennas. A valid command from the ground station will exit the satellite from *After ejection from P-POD* mode. Receiving a valid command is also a criteria for a mission success. As described in Section 5.2, a worst case interval from last visible pass to the next, is approximately 14 hours. For normalized average charging power, NUTS should be capable of sustaining this mode indefinitely, but only for 20 hours if worst case charging power is used.

7.2 In Orbit

Figure 7.2 shows the default state of the satellite when the radio flag has been set. When a command from the ground station is received, it is verified in order to prevent execution of invalid commands. If the system does not succeed to execute the command and has re-attempted it a certain amount of times, it should write a log entry describing the failure. A log entry is also filed after successfully executing the command.

7.2.1 Power Monitoring Mode

The power monitoring mode in Figure 7.3 shows the proposed plan for energy conservation.

This mode constantly monitors NUTS' remaining battery capacity through the battery fuel gauge described in Section 5.1.1. When the battery falls below 50 % of remaining capacity, NUTS enters the avoidance mode defined in Section 6.1. The beacon transmission rate is reduced and submodules' current consumption are measured. Submodules consuming more current than expected, are ask to reduce their consumption and are turned off if they are unsuccessful in doing so. If the satellite is not charging, critical mode will be initiated as shown in Figure 7.4.

In critical mode the beacon transmission rate is set its lowest rate and all submodules are disabled. The Radio and OBC MCUs should reduce software tasks and limit usage of external memories. The system checks the battery's state of charge and if is not charging it could be due to being in eclipse. If in eclipse, the satellite must wait an estimated maximum of 35 minutes as described in Section 5.1. If it is not in eclipse, the solar panels may not be at an optimal angle or one of the sides can be broken. The satellite will try to adjust its position so that a different solar panel is exposed. A possible issue is a live-lock condition where it is not

charging while exposed to the Sun and tries to adjust attitude using the attitude determination and control system (ADCS). This is the most critical of the possible battery situations and can indicate a complete failure of either solar panels, charging mechanisms or sensors responsible for determining charging conditions or Sun exposure. Damaged solar panels and broken chargers on the electrical power system (EPS) are not recoverable by the system, and false readings from sensors must be minimized by careful design and testing. If the ground station believes that the sensors are providing false data, a way of overriding system modes must be implemented.

7.2.2 Payload Verification

Figure 7.5 shows the proposed plan for the payload verification. The payload only has to be verified when a command to activate it is received, and it should otherwise be powered down. A functionality check of the payload module should be performed first and a possible failure written to the log. The payload module will then be restarted along with the verification procedure. If the module fails a given number of times, an module error is written to the log. If the payload check completes successfully, the command will be executed and an entry will be filed in the log describing the command as successful.

7.2.3 Software Watchdog

Figure 7.6 shows a proposal for the software watchdog. It taps its own internal watchdog to prevent a reset and performs health checks of all submodules. It will also be responsible for checking for single event effects (SEEs), verifying other software tasks and tap the external hardware watchdog. Figure 7.7 illustrates how the submodules are checked by sending a control sequence in order to receive an acknowledge. If the same sequences is received in return, the module is operational. If the communication acknowledge or sequence is missing or incorrect, the module is restarted. In order to prevent to live-lock, a loop limitation is introduced.

Check for SEEs can be seen in Figure 7.8 and attempts to discover any SEEs present in the satellite. It first checks for any single event upsets (SEUs) and performs a refresh of the module if any are detected. Checking for single event latchups (SELs) requires to read the current consumption for all submodules, which can be done from the INA219 current monitor. If an abnormal consumption is register, power to the module is toggled, and it is written to log. If no abnormal consumption is detected, the check is completed. For the software watchdog to tap the external hardware watchdog, all components controlled by the hardware watchdog must be verified. The software watchdog should not tap the hardware watchdog if a component fails and the system can not resolve the issue by refreshing or resetting the component. This conditional tapping will cause a power toggling when software watchdog's attempts are unsuccessful in resolving the issue.
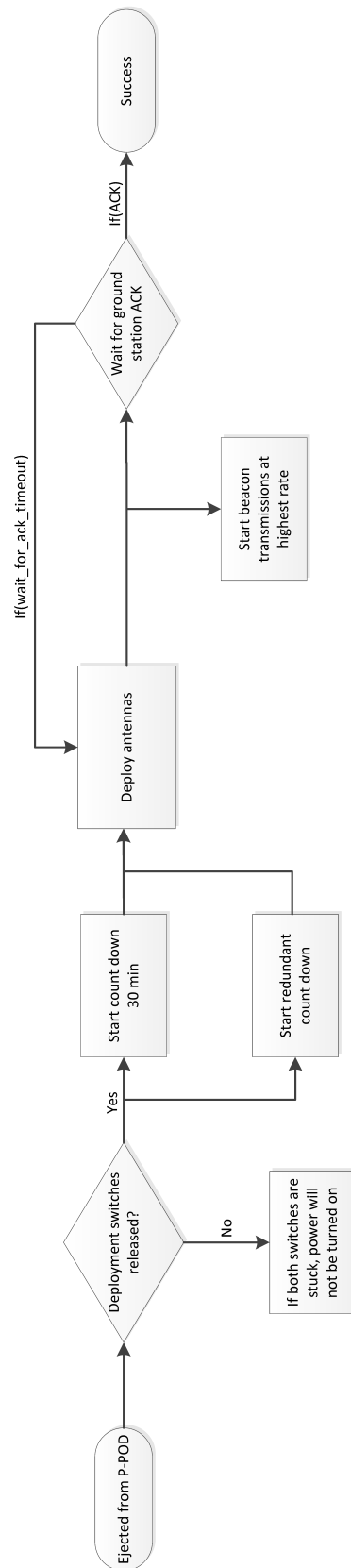
Figure 7.1: Mission Event Plan - After ejection from P-POD
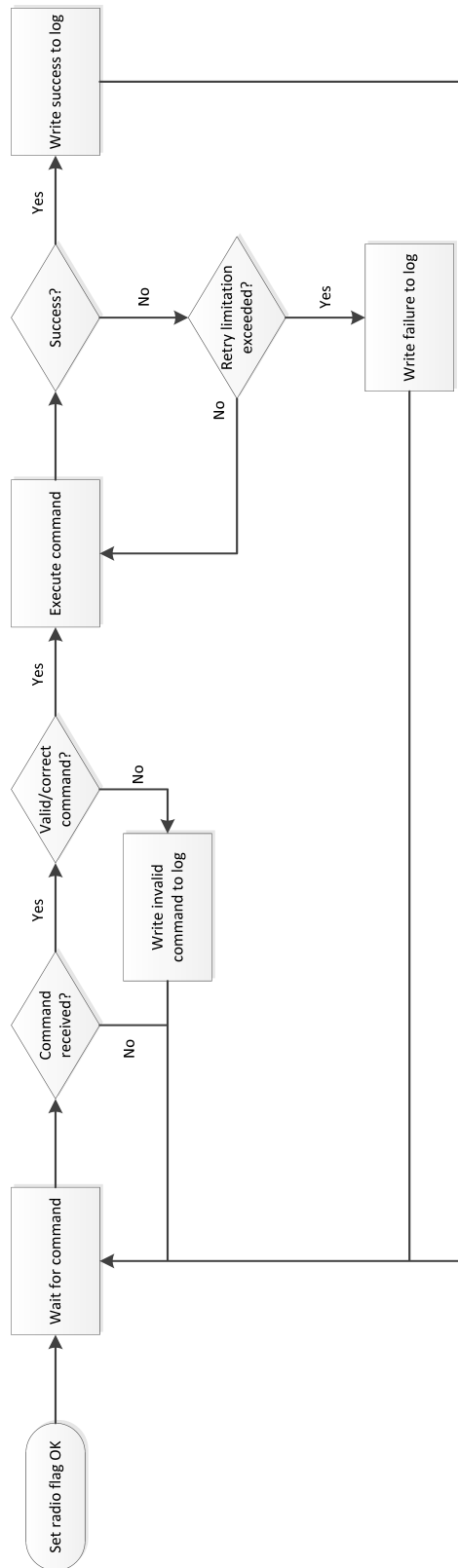
Figure 7.2: Mission Event Plan - Radio success
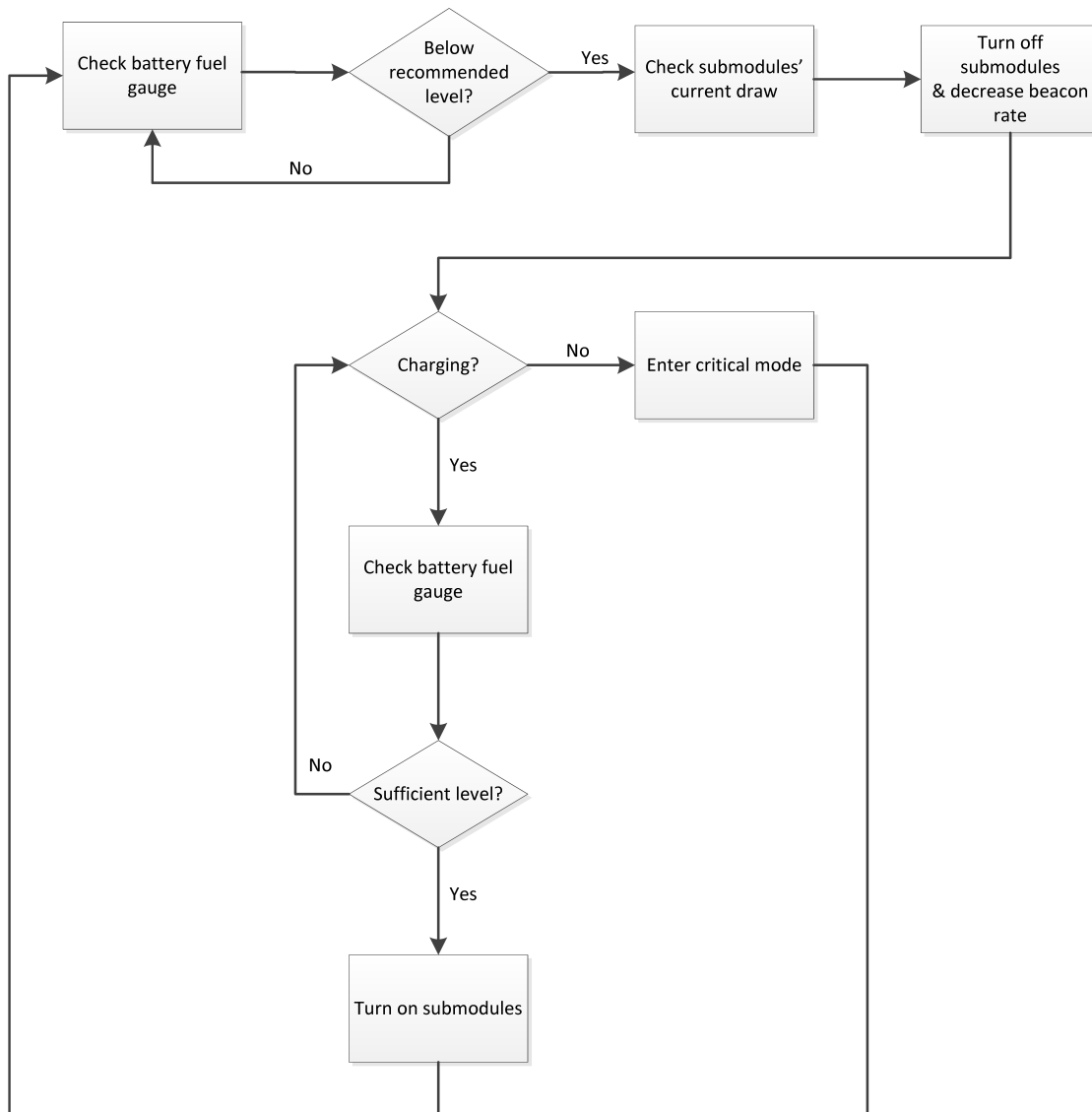
Figure 7.3: Mission Event Plan - Power monitoring mode
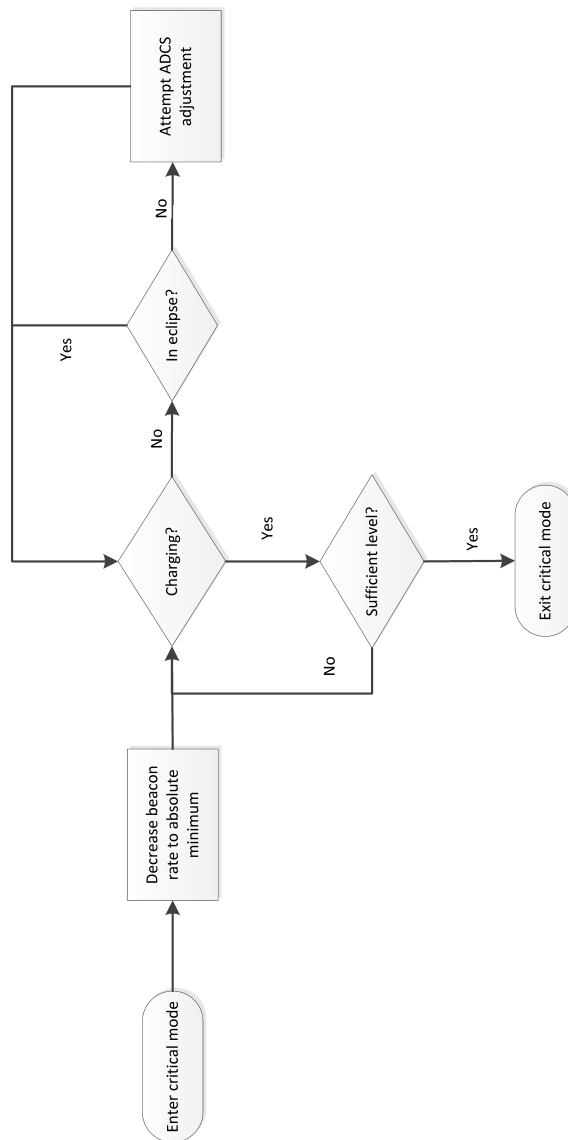
Figure 7.4: Mission Event Plan - Critical mode
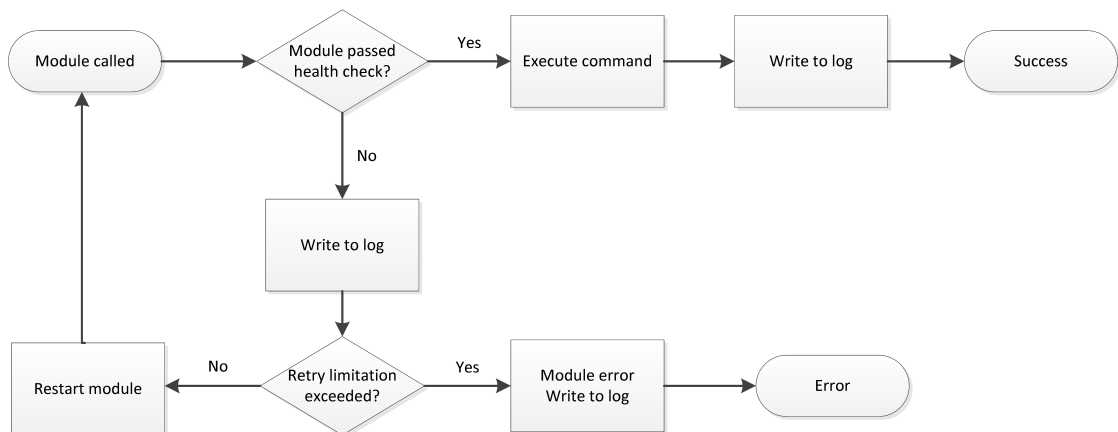
Figure 7.5: Mission Event Plan - Payload verification
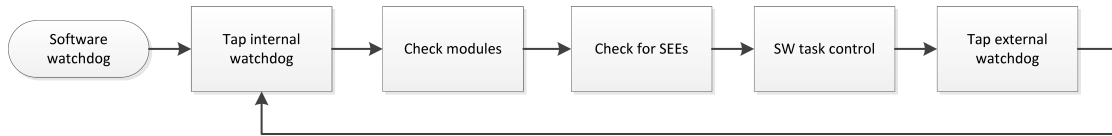
Figure 7.6: Mission Event Plan - Software watchdog
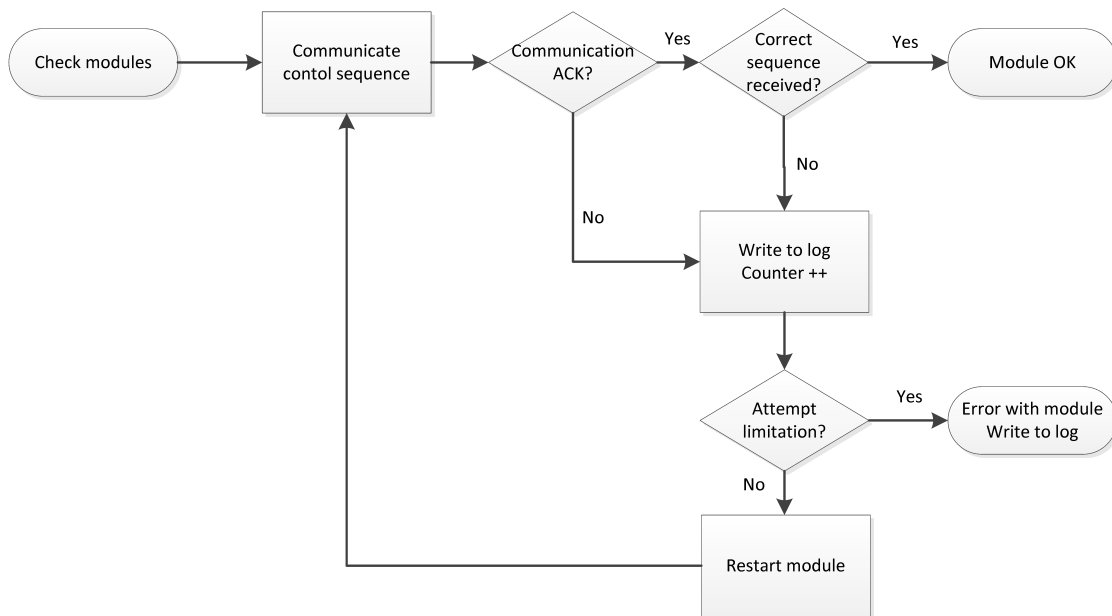
Figure 7.7: Mission Event Plan - Check submodules
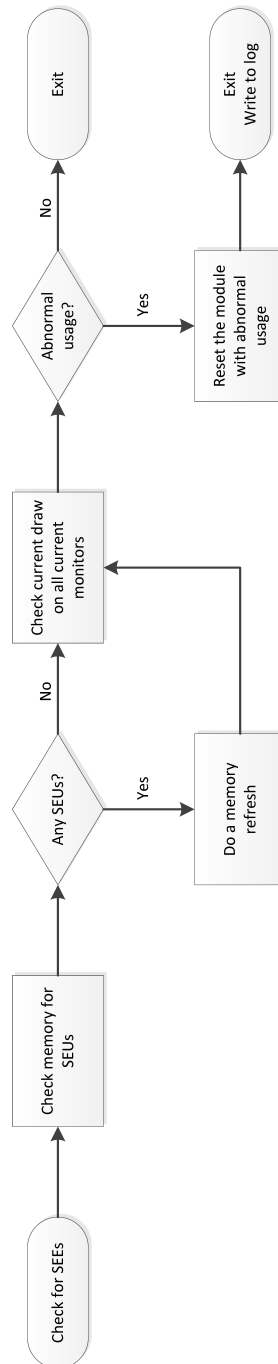
Figure 7.8: Mission Event Plan - Check for SEEs

Chapter 8

Design

This chapter presents design proposals for the satellite's new hardware watchdog system. Two solutions are presented and one is chosen for implementation on an evaluation card.

8.1 Watchdog Requirements

As presented in Section 4.6, the existing watchdog circuit on the backplane is insufficient with regards to recovering from single event latchups (SELs) and single event upsets (SEUs). Code corruption in the MCUs as a result of SEUs may cause the processors to enter a stuck state and therefore be in need of a reset or power cycling. If this happens to both masters, there is currently no method for resolving such issues. This necessitates a revision of the design aimed at meeting new requirements.

A new watchdog must be able to restart both masters and provide the possibility of removing power to all submodules as a final attempt to recover from failure. It must also be as reliable and simple as possible. The existing backplane gives the masters the possibility of removing power to each submodule, as well as the other master module. However, it prevents a master of being able to turn itself off and therefore a system wide toggling of power is not possible if both masters are unresponsive. This can be solved by introducing a watchdog controlling a power switch, e.g. the already applied MAX14523 current-limit switch. The watchdog must not be able to turn itself off and not be a single point of failure. This is possible in two ways; either as a watchdog using triple modular redundancy (TMR) on the backplane or as two local watchdogs dedicated to each master module.

8.2 Backplane Watchdog Solution

Having a single watchdog on the backplane resolves two unresponsive masters while providing a redundant method of toggling power, but introduces a single point of failure. Section 3.3.1 presents TMR which mitigates the issue of a watchdog circuit as a single point of failure. By including three watchdogs and have their outputs voted on, a more reliable design is possible. Care must be taken in ensuring that a common property between the three watchdogs will not cause them to fail simultaneously. Such properties could be changes in functionality as a result of temperature fluctuations or radiation. A single signal TMR-voter often consists of a limited number of simple logic gates and Section 3.3.1 describes the issue of the voter as a possible single point of failure. Whether or not this is an acceptable risk must be determined based on a final degree of redundancy and reliability for the NUTS system.
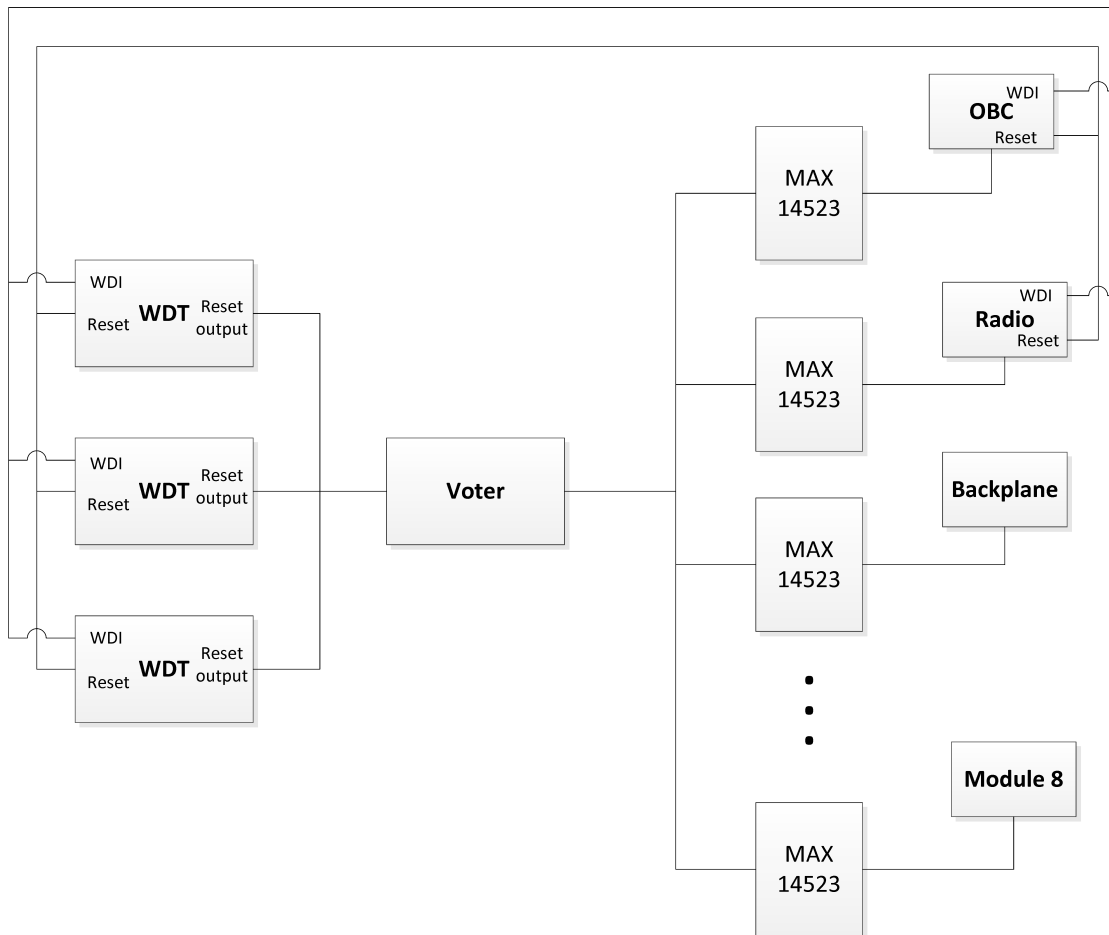
Figure 8.1: Backplane watchdog proposal

Figure 8.1 shows a proposal with the three watchdog timer (WDT) circuits connected to the MAX14523 current limit switches and interfaced by the on-board computer (OBC) and Radio masters. A line for tapping the watchdogs within a

defined time-out period and a manual reset line is included, along with the voter circuit and its output. Since a new watchdog on the backplane is to monitor both masters, there must also be possible for each master to tap each watchdog circuit. If both masters are unresponsive, this would enable the watchdog to issue a system wide reset. If only a single master was permitted to tap the watchdog circuits, a permanent fault in that master would cause a continuous reset condition. One unresponsive master is detected through a lack of communication response and the functional master can toggle power to its partner through the backplane.

8.2.1 Majority Voter Circuit

In order to determine the correct output of the TMR watchdog system, a majority voter must be implemented. The voter masks out a disagreeing member based on the majority of the watchdog circuits. If two or more watchdog circuits agree on a reset, the voter output should be low, in all other cases the output should be high. Table 8.1 shows the voter's truth table with the three outputs from the watchdogs as A, B and C.

Table 8.1: Voter circuit truth table

A	B	C	$\overline{Reset}$
0	0	0	0
1	0	0	0
0	1	0	0
1	1	0	1
0	0	1	0
1	0	1	1
0	1	1	1
1	1	1	1

The truth table leads to the boolean equation:

$$\overline{Reset} = \bar{A} \cdot B \cdot C + A \cdot \bar{B} \cdot C + A \cdot B \cdot \bar{C} + A \cdot B \cdot C \tag{8.1}$$

Table 8.2: Voter karnaugh diagram

Using the Karnaugh diagram in Table 8.2 and solving it for its minterms, a simplified boolean equation is found:

$$\overline{Reset} = A \cdot B + B \cdot C + A \cdot C \tag{8.2}$$

Based on the result in Equation 8.2, one observes that the voter consists of three 2-port AND gates and one 3-port OR gate.

8.3 Local Watchdog Solution

Implementing a separate watchdog on each master module circumvents the need for a watchdog on the backplane. Two local watchdogs cover the case of two unresponsive masters and combined with the existing mechanism of removing power to submodules, a system wide toggling of power is possible. With NUTS' capability of transferring control from the OBC to the Radio module, and vice versa, local watchdogs does not introduce a single point of failure if implemented correctly. By dividing the master modules into two power domains, it is possible to select which components that are affected by a watchdog time-out. Figure 8.2 illustrates this division where power to power domain B is provided through a watchdog controlled switch. Components within domain B are subjects to the watchdog, while components in power domain A are unaffected. It is required to place the watchdog in domain A as to prevent it from turning itself off. The backplane power domain consists of existing design.
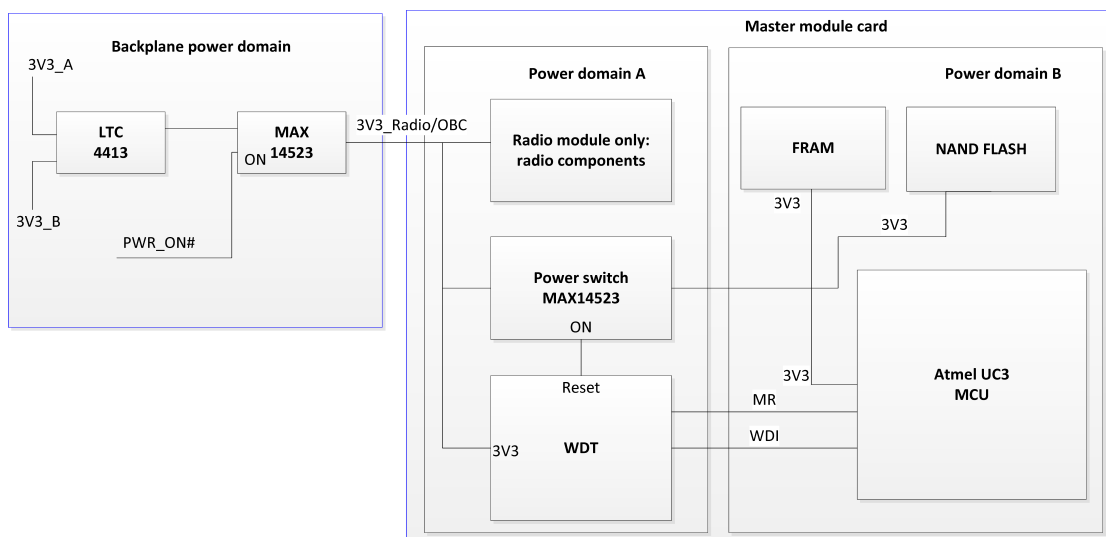
Figure 8.2: Local watchdog proposal

For the Radio module, components needed for radio transmissions are placed in domain A so to prevent a broken watchdog from permanently silencing the satellite. It is possible to place the module's MCU and memories in domain B due

to the functional redundancy between the Radio and OBC module. If one set of memories and MCU have failed, the other master can inherit its partner's tasks and functionality. However, this does not apply to radio components and these must therefore be kept in domain A. If radio components in domain A are in need of power toggling, it is possible for the OBC module to remove power to the entire Radio module through the backplane. This can also be done if the watchdog itself is in need of power toggling.

Complete redundancy for the OBC module is present in the Radio module and therefore all components on the OBC are placed in domain B. As before, the Radio module can toggle power to both domains of the OBC module, and thereby also toggle power to the watchdog, removing any SELs that may be present.

8.4   Watchdog Chip Selection

A new watchdog chip must be compatible with the existing 3.3 V supply, be operational over a large temperature range and have a long power-on-reset (POR) delay. A long POR delay is necessary to ensure that the system is powered off long enough in order to recover from SELs. A manual reset option is favourable in situations where a scheduled restart is necessary or in cases where one of the MCUs are stuck in a live-lock where the watchdog is being tapped when it actually should reset the system. The watchdog time-out period must also be long enough for the system to stabilize and the master modules to come back online such that a restart loop is avoided. Based on availability through the online vendors Digikey, Farnell and Mouser, three candidates fitting the requirements were found. Table 8.3, 8.4 and 8.5 presents an overview of the voltage supervisors with built-in watchdog timers from three different manufactures. All of the options operate with a 3.3 V supply.

Table 8.3: Maxim Integrated - MAX16058 [12]

Manufacturer	Maxim Integrated
Type	Voltage supervisor w/ watchdog
POR delay	16 ms to 24 s
Watchdog time-out period	16 ms to 300 s
Voltage threshold	Chip dependent
Operating temperature	-40C to +125C
Order designator	MAX16058ATA31+
Available	Yes
Manual reset input	Yes

The alternatives as presented all operate as both watchdog timers and voltage supervisors/brownout detectors (BOD), meaning that if their supply voltage falls below a certain voltage threshold, the circuit issues a reset. Based on information in Tables 8.3 through 8.5, the Maxim options stands out with a wide temperature range and substantially longer POR delay and watchdog time-out period than the

Table 8.4: Intersil - ISL88708 [13]

Manufacturer	Intersil
Type	Voltage supervisor w/ watchdog
POR delay	up to 2.4 s
Watchdog time-out period	1.6 s
Voltage threshold	3.09V
Operating temperature	-40C to +85C
Order designator	ISL88708IP83Z
Available	Yes
Manual reset input	Yes

Table 8.5: Texas Instruments - UCC2946 [14]

Manufacturer	Texas Instruments
Type	Voltage supervisor w/ watchdog
POR delay	up to 200 ms
Watchdog time-out period	up to 1.6 s
Voltage threshold	Adjustable
Operating temperature	-40C to +105C
Order designator	UCC2946TPWRQ1
Available	Yes
Manual reset input	No

competitors. The Texas Instruments option does not feature a manual reset, while Intersil has a rather high fixed voltage threshold and a more limited temperature range. Therefore, Maxim's MAX16058 is the chip of choice for the new watchdog. It will be ordered with the designator *MAX16058ATA31+* which, due to availability at vendors, has a 3.075 V voltage threshold. In the final implementation, a chip with a different voltage threshold could be used, but for testing purposes, the available 3.075 V is sufficient. The same watchdog circuit is used for both solutions.

8.4.1 Maxim Integrated - MAX16058

Figure 8.3 show the top view with corresponding pins of the MAX16058 chip. All following information is gathered from MAX16058's datasheet [12] unless otherwise noted. The device has an active low reset signal which asserts when one of the following conditions arise:

- At power-up when V_{CC} rise above the voltage threshold

- When the supply voltage V_{CC} falls below the voltage threshold

- When the manual reset pin is pulled low

- When the watchdog timer times out

The reset signal goes high an adjustable POR delay after all reset conditions are de-asserted.
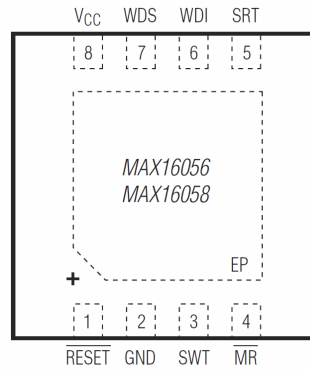
Figure 8.3: MAX16058 supervisory circuit

MAX16058's voltage threshold is chip dependent, and can be chosen between 1.575 V and 4.625 V in approximately 0.1 V increments. The threshold voltage has a 2.5 % accuracy over the entire temperature range, and Maxim Integrated recommends the threshold set higher than the minimum supply voltage of ICs connected to the chip [52].

The watchdog time-out period and POR delay are adjustable by using external capacitors. Capacitor value C_{SRT} for a POR delay t_{RP} is given by Equation 8.3

$$C_{SRT} = \frac{t_{RP}}{5.15 \cdot 10^6} \qquad (8.3)$$

The datasheet sets the minimum, typical and maximum t_{RP} for a 2.7 nF C_{SRT} as follows:

- Minimum: 10.50 ms

- Typical: 14.18 ms

- Maximum: 17.00 ms

The minimum value is 25.95 % lower than the typical value, while the maximum value is 19.88 % larger. No further information is given as to how, or if, the deviation is dependent on the capacitance of the C_{SRT} capacitor. Minimum, typical and maximum values must be seen in relation to the tolerance of the capacitor used such that the final deviation is manageable. E.g., a capacitor tolerance of 10 % will, as given by Equation 8.3, give a 10 % deviation of the t_{RP} delay.

A watchdog time-out period of t_{WD} requires the capacitor C_{SWT} as given by Equation 8.4

$$t_{WD} = Floor[\frac{C_{SWT} \cdot 5.15 \cdot 10^6}{6.4 \cdot 10^{-3}s}] \cdot 6.4 \cdot 10^{-3}s + 3.2 \cdot 10^{-3}s \qquad (8.4)$$

C_{SRT} and C_{SWT} are in farad, and t_{RP} and t_{WD} are in seconds. $Floor[]$ is used to take nearest lower integral value. All external capacitors must be low leakage ceramic capacitor with low temperature coefficient, such as X7R. Equation 8.4 sets

a typical value, but equations for minimum and maximum values are given in the datasheet, and are as follows:

$$t_{WD\_min} = Floor[\frac{C_{SWT} \cdot 4.16 \cdot 10^6}{9.5 \cdot 10^{-3}s}] \cdot 3.5 \cdot 10^{-3}s + 1.6 \cdot 10^{-3}s \qquad (8.5)$$

$$t_{WD\_max} = Floor[\frac{C_{SWT} \cdot 6.58 \cdot 10^6}{6.4 \cdot 10^{-3}s}] \cdot 6.4 \cdot 10^{-3}s + 3.2 \cdot 10^{-3}s \qquad (8.6)$$

Minimum and maximum time-out periods will be evaluated for the chosen C_{SWT}, and implementation should aim at keeping the time-out period for the three watchdogs as similar as possible. It is more difficult to evaluate the effect of capacitor tolerances for the time-out period than for the POR-delay. This is due to the $Floor[]$ function which has a large influence on the calculation than the capacitor tolerance. The minimum and maximum values of both time-out period and POR delay are valid for the entire temperature range of -40°C to +125°C, but would for a fixed temperature of 25°C be closer to their typical values. However, as the satellite is at risk of experiencing temperature fluctuation, worst case conditions should be considered when implementing the final design. Both the time-out period and the POR delay should be measured over a given temperature range.

The function of the different pins can be seen in Table 8.6.

Table 8.6: MAX16058 Pin functions

Pin	Function
$\overline{RESET}$	Open-drain active low reset output
GND	Ground
SWT	Watchdog time-out input. Connect C_{SWT} between this pin and GND in order to adjust the watchdog time-out period. Capacitance must be between 2275pF and 0.54μF to ensure valid operation
$\overline{MR}$	Active low manual reset input
SRT	POR delay input. Connect C_{SRT} between this pin and GND in order to adjust the POR delay period. Capacitance must be between 39pF and 4.7μF
WDI	Watchdog input. A high to low transition within the watchdog's time-out period prevents a reset and clears the timer. The timer also clears when $\overline{RESET}$ is asserted
WDS	Watchdog select input. Connect to GND for normal time-out mode or to V_{CC} for multiplying the time-out period t_{WD} by a factor of 128
V_{CC}	3.3V supply voltage

For this implementation, the WDS pin is connected to V_{CC} for a longer time-out period and the results from Equations 8.4, 8.5 and 8.6 must therefore be multiplied by 128.

8.4.2   Watchdog Evaluation Card

Before a new hardware watchdog is implemented into the system, the design suggestion is created as a separate evaluation card. This facilitates simpler testing and interfacing with the MCUs without the need for a work-around on the current backplane. The TMR solution is the more complicated of the two presented solutions, and is therefore implemented on the evaluation card. Testing of the simpler solution is still possible since they use the same watchdog circuit and have similar operations.

To interface the two master modules, the card includes headers for the watchdog input and manual reset lines, as well as connectors for the supply voltages. In addition to the triplicated watchdog system and the voter, the card includes some legacy design from the current NUTS backplane in order to enable more realistic testing. The power OR-ing controller, LTC4413 gives the possibility of disabling one of the two power supplies in order to simulate a misbehaving regulator on the electrical power system (EPS). The card also uses the same adjustable current limit switch, MAX14523 with a limit of 630 mA as on the existing backplane. Figure 8.4 shows the top view of the current limit switch along with its corresponding pins.
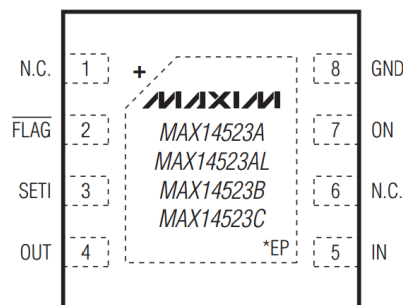
Figure 8.4: MAX14523 current limit switch [10]

The pins of interest are $\overline{FLAG}$, OUT and ON. OUT is the current limited output, while $\overline{FLAG}$ is active low when an over-current or thermal shut down condition arise [10]. A low signal on the ON pin turns the switch off, and hence removes power to all modules that are connected to the OUT pin. In the current backplane design, each module has two MAX14523 switches, one for 3.3 V and one for 5 V. The ON pin is used to enable the masters to turn off each submodule as well as the other master module. In order to keep late stage changes to the backplane to a minimum, a possible connection for the watchdog system's output is on the MAX14523's ON-pin. By doing so, two unresponsive masters or a manual reset

signal causes the watchdog to issue a reset, which turns the MAX14523 switches off, removing all power for a period of time given by Equation 8.3.

The logic gates constituting the majority voter are the same as the gates used on the current backplane. Evaluation card's hardware drawings can be seen in Appendix G along with its corresponding bill of materials in Appendix G.2.

For the TMR solution, the new watchdog system must be capable of being tapped by both masters. This leads to an issue since each watchdog circuit only has one WDI pin for tapping. Having both masters directly drive MAX16058's WDI pin is not possible. With two asynchronous tapping signals, a condition where one master pulls the line high while the other pulls it low, may occur. This leads to an undefined level on the WDI pin, and correct functionality can not be guaranteed. The issue is illustrated in Figure 8.5.
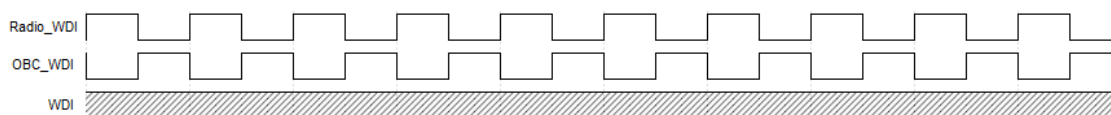
Figure 8.5: Undefined watchdog input signal

A form of buffer or driver is necessary so a high to low transition on the WDI pin is guaranteed to occur before the watchdogs time out. By having the WDI pin connected to the two masters' WDI lines through an XOR-gate, a change on one of two lines should cause a transition at the XOR-gate's output. This solution causes new issues if the XOR-gate is driven by two signals at the same frequency. Table 8.7 shows an XOR-gate's truth table and gives a clue to these issues. If input A and B where to change to a common or inverted value simultaneously, the gate's output would remain unchanged and not tap the watchdogs. Even though this might be a rare condition, its effect could cause problems for the entire system.

Table 8.7: XOR-gate truth table

A	B	F
0	0	0
0	1	1
1	0	1
1	1	0

By having the XOR-gate driven by two signal at different toggling frequencies, e.g. input A changes four times faster than input B, one is able to ensure that the XOR-gate's output changes as its inputs does. By selecting the toggling frequencies based on the watchdogs' time-out period, a high to low transition is guaranteed to occur before an unnecessary reset occurs. Figure 8.6 illustrates different toggling frequencies and a corresponding output. From the headers on the evaluation card, the inputs going to the watchdogs are pulled high with resistors in order to avoid floating inputs to the chips.
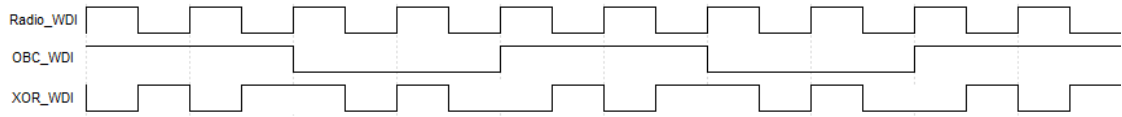
Figure 8.6: XOR-gate timing diagram

The issue of having two masters driving one pin is also evident for the watchdogs'
manual reset inputs. This signal is active low and does not need to be toggled
within a certain interval. By including a 2-port AND gate with its input lines
pull up by resistors, a low signal from one or two of the masters causes the gate's
output to go low, leading to a manual reset. The new triplicated watchdog system
with voter and logic gates can be seen in Figure 8.7.
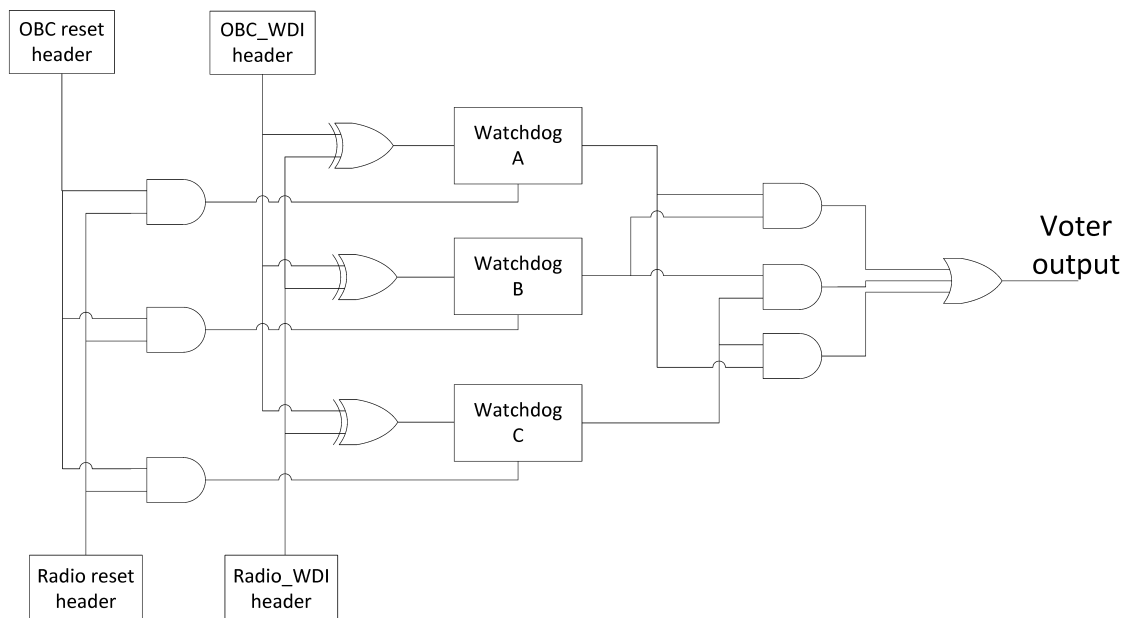
Figure 8.7: Triple modular redundancy watchdog system as implemented on the
evaluation card

Chapter 9

Testing & Results

This chapter presents testing and results of the watchdog evaluation card. The evaluation card was manufactured at the ELPRO lab at NTNU.

9.1 Hardware Watchdog Verification & Test

The watchdog evaluation card was implemented with a power-on-reset (POR) delay of 1.6995 s by choosing a C_{SRT} of 330 nF as given by Equation 8.3. The C_{SWT} capacitors were set to 3.3 nF. Based on Equation 8.4, a 3.3 nF capacitor should yield a typical time-out period of 2.048 s. The time-out period and POR delay were chosen such to enable an oscilloscope to capture an entire sequence of events from, e.g. the inputs ceased to toggle until the watchdogs timed out.

Feedback is given through two LEDs; LED0 indicates connected supply power and LED1 is connected to MAX14523's output indicating whether or not power is turned off when a reset, time-out or brownout occurs.

The finished evaluation card can be seen in Figure 9.1. The test setup is seen in Appendix F along with an overview of the test equipment.

9.1.1 Tests

The tests chosen for the evaluation card are presented in Table 9.1 along with defined success criteria. The test setup included two Atmel UC3-A3 Xplained cards which feature the same microcontoller as used by NUTS. These will act as the two master modules. For all tests, the microcontrollers ran a simple task toggling a GPIO-pin at a frequency of 5 Hz for card A and 1.25 Hz for card B. The 5 Hz signal would cause a high to low transition on the watchdogs' input (WDI) each 0.2 s and the 1.25 Hz signal each 0.8 s, both being well within the time-out period of 2.048 s. The frequencies were chosen such that one or more high to
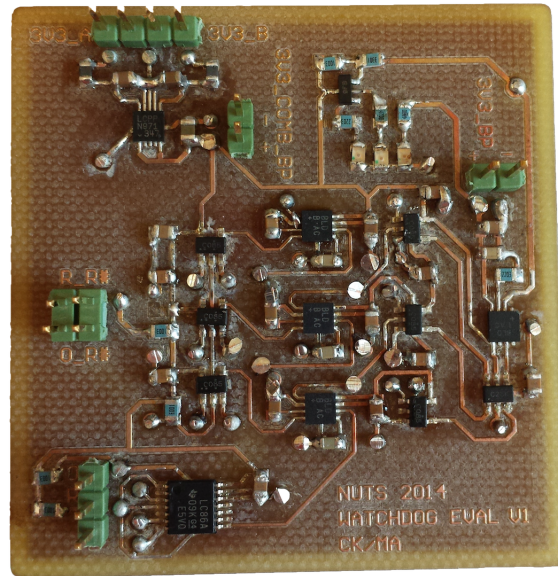
Figure 9.1: Watchdog evaluation card

low transitions were to happen before the time-out period. For a shorter time-out period, higher frequencies would have been applied to the WDI inputs. The GPIO-pins were connected to the evaluation card through on-board headers, while the manual reset lines were pulled to ground using a jumper when needed. Signals of interest were measured with an oscilloscope, which also provided screenshots and cursor measurements. The tests were carried out at room temperature.

Table 9.1: Evaluation card tests and success criteria

Test	Method	Success criteria
Power up	Connect 3.3 V from power supply	Status LED0 on, measured 3.3 V, LED1 on after POR delay
XOR-gate toggling	Lines driving WDI at two different frequencies	Several high to low transitions at gate's output
XOR-gate toggling	Driving both WDI lines with the same signal	No change at gate's output
Manual reset	High to low transition on manual reset line	LED1 off immediately
Manual reset	Low to high transition on manual reset line	LED1 on after POR delay
Toggling of both WDI lines	Both WDI lines connected and toggling	Time-out event does not occur. LED1 remains on
Toggling of single WDI line	One WDI line disconnected	Time-out event does not occur. LED1 remains on
Watchdog time-out	Cease WDI toggling from both microcontrollers	After time-out period: LED1 off. After restart delay: LED1 on
Voter circuit	Disable one watchdog	Output of voter remains high
Voter circuit	Disable two watchdog	Output of voter goes low
Power OR-ing	Remove one of two power supplies	Continued operation - LED0 remains on
Brownout detection	Gradually lower supply voltage	LED1 off

9.1.2   Results

During manufacturing the LTC4413 power OR-ing chip was rotated 180° which prevented testing of its functionality, but due to extra headers it was possible to power the rest of the card without affecting the other tests. A summary of the test results are given in Table 9.2.

Appendix G presents additional results not presented in this section.

Table 9.2: Evaluation card test results

Test	Result	Figure	Comments
Power up	Success	Figure 9.2	Supply voltages measured to be 3.3 V
XOR-gate toggling	Success	Figure 9.3	Correct behaviour for tapping the watchdogs
XOR-gate toggling	Success	Figure 9.4	Incorrect behaviour for tapping the watchdogs
Manual reset	Success	Figure 9.5	Measured POR delay of 1.66 s
Toggling of both WDI lines	Success	Figure 9.6	-
Toggling of single WDI line	Success	Figure 9.7	-
Watchdog time-out	Success	Figure 9.8	Measured time-out period of 2.59 s to 2.96 s
Voter circuit	Success	Figure 9.10	One disabled watchdog
Voter circuit	Success	Figure 9.11	Two disabled watchdogs
Power OR-ing	Fail	-	LTC4413 power OR-ing misplaced
Brownout detection	Success	-	Threshold voltage at 3.08 V

Power-up

The first test preformed was a power-up test and the result can be seen in Figure 9.2 where the 3.3 V supply voltage is seen (above - CH1) along with the output of the voter (below - CH2). The voter output rises high after a POR delay of 1.66 s, 2.32 % lower than calculated value of 1.6995. The output will remain high until either a manual reset occurs or the watchdogs time out.

XOR-gate Toggling

Section 8.4.2 presents several issues as to how to tap the watchdogs. Attempting to drive the watchdogs' WDI inputs with two directly connected lines causes undefined levels on the inputs. This is not sufficient for guaranteeing a high to low transition on the watchdogs' WDI inputs within their time-out period. The implemented solution was to include XOR-gates as drivers for the WDI inputs. Figure 9.3 shows an XOR-gate's inputs (above & middle - CH1 & CH2) and output (below - CH3). Driving the inputs at two different frequencies will cause several high to low transitions required for tapping the watchdogs within their time-out period, as well as avoiding undefined levels at their inputs. The optimal tapping frequencies can be determined based on the design's final time-out period.

An issue which could arise if the tapping frequencies are identical, or close to identical, is the lack of a valid change at an XOR-gate's output. This is illustrated
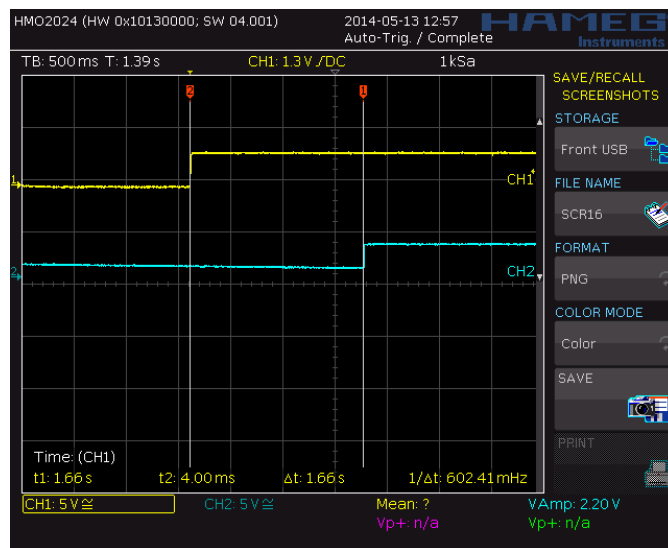
Figure 9.2: Power-up test - Supply voltage (CH1) & output of voter (CH2)
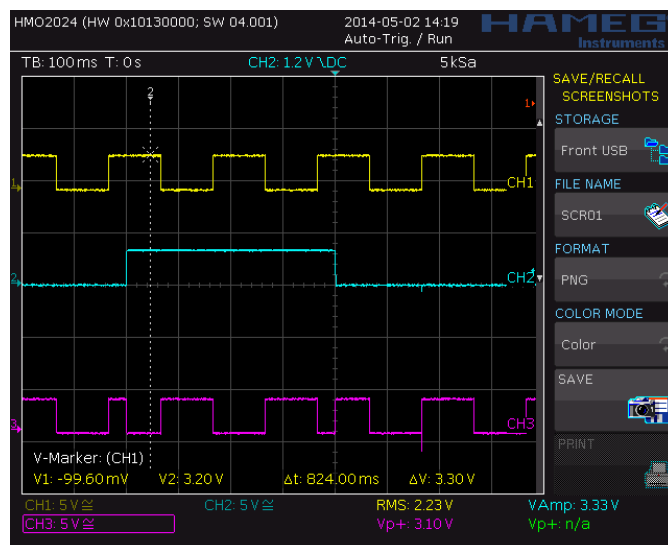
Figure 9.3: WDI input signals at 5 Hz (CH1) and 1.25 Hz (CH2) driving an XOR-gate with output (CH3)

in Figure 9.4 where the same signal is used to drive both inputs (above & middle - CH1 & CH2) causing no transitions at the output (below - CH3). Evidently, this will not tap the watchdogs and thereby cause a reset. Another scenario where the XOR-gates are removed is presented in Appendix G.1.

Manual Reset

A measured POR delay of 1.7 s can be seen in Figure 9.5. Pulling the manual reset line to ground caused an immediate high to low transition on the voter output. The release of the manual reset line (below - CH2) is followed by a low to high
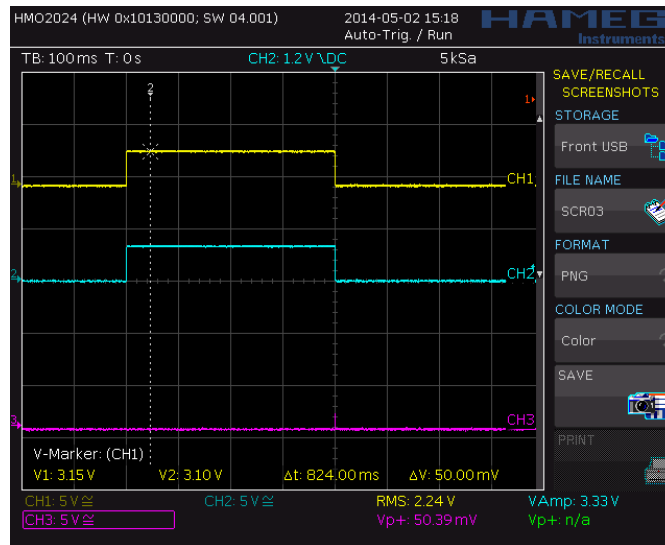
Figure 9.4: Synchronous WDI input signals (CH1 & CH2) and output of XOR-gate (CH3)

transition on the voter output (above - CH1) after a 1.7 s delay. The voter output will be held low as long as the manual reset line is low.
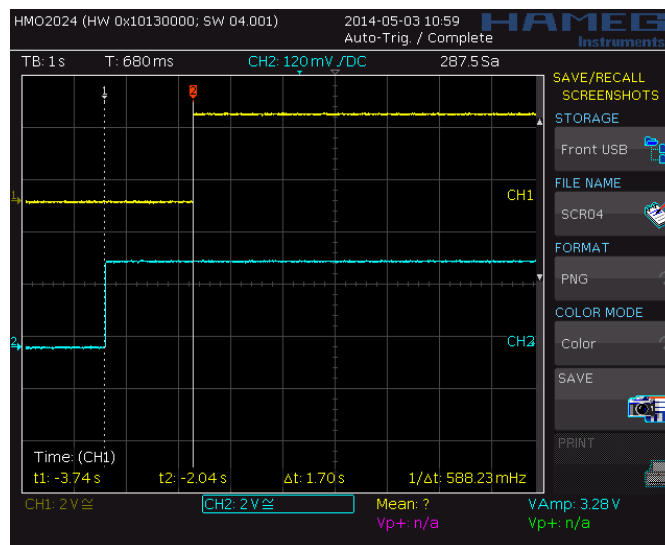
Figure 9.5: POR delay from release of manual reset line (CH2) to voter output transition (CH1)

WDI Line Toggling

Figure 9.6 shows the ideal situation where both masters toggle their respective WDI lines and prevent a time-out from occurring. This is the expected condition when both masters are operating as intended.
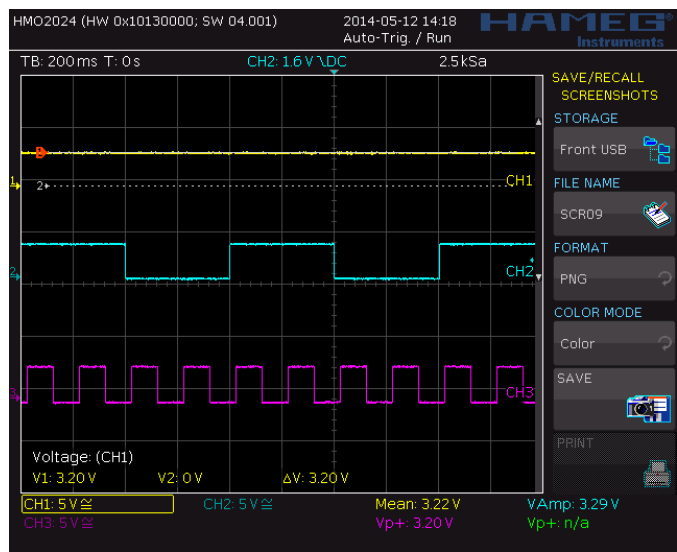
Figure 9.6: Output of voter (CH1) remains high as both WDI inputs are being toggled (CH2 & CH3)

When one master becomes unresponsive and ceases to toggle its WDI line, the situation becomes as shown in Figure 9.7. The voter output remains high (above - CH1) even though the 1.25 Hz WDI toggling line (middle - CH2) is disabled and only the faster 5 Hz WDI line (below - CH3) remains active. Note that CH2 remains high as a result of the implemented pull-up resistors.
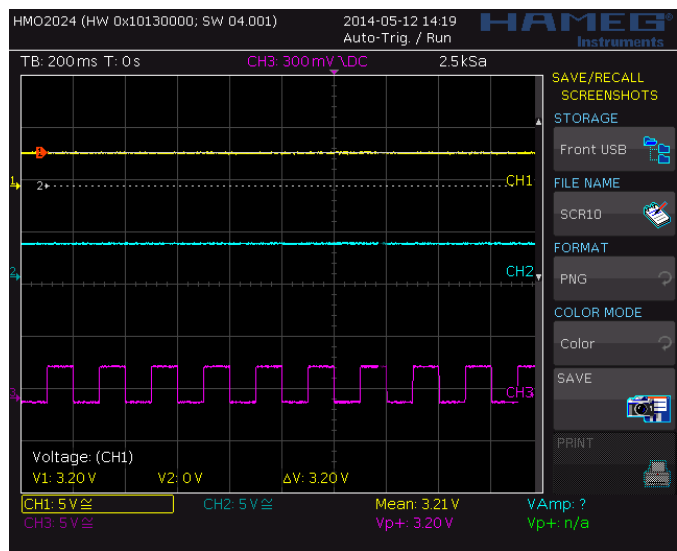
Figure 9.7: Output of voter (CH1) remains high as one WDI input is disabled (CH2) and the other toggles (CH3)

If the last functioning master becomes unresponsive and ceases to toggle its WDI line, the watchdog system will issue a reset after the time-out period as shown in Figure 9.8. After the last high to low transition of the 5 Hz WDI line (below - CH3), the voter output (above - CH1) goes low after a period of approximately

2.64 s, 28.9 % higher than typical time-out period. A time-out period of 2.96 s, 44.5 % higher than typical, is shown in Figure 9.9 where the 5 Hz WDI line is disabled and the slower 1.25 Hz ceases to toggle. The different time-out periods as measured at the voter output is due to chip specific differences in each watchdog's time-out period. Measurements seen in Appendix G.1 shows differences in time-out periods of 2.58 s and 3.28 s, respectively 25.98 % and 60.16 % higher than the typical value of 2.048 s.
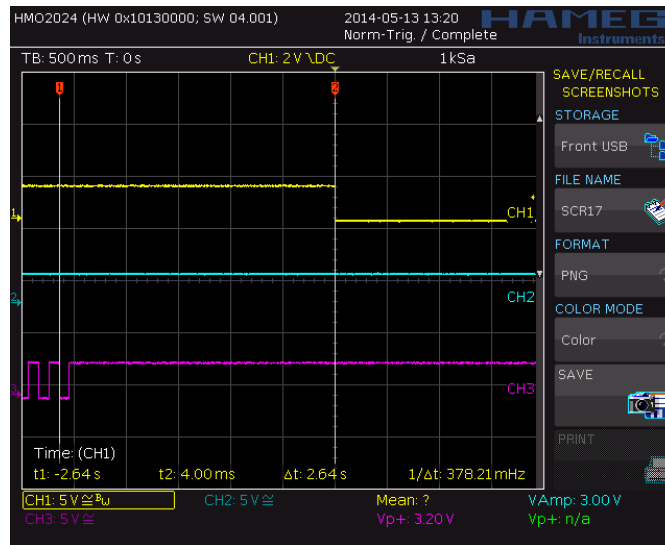
Figure 9.8: Watchdog time-out with voter output transitions low (CH1) as toggling ceases on last active WDI input (CH3) with one WDI input disabled (CH2)
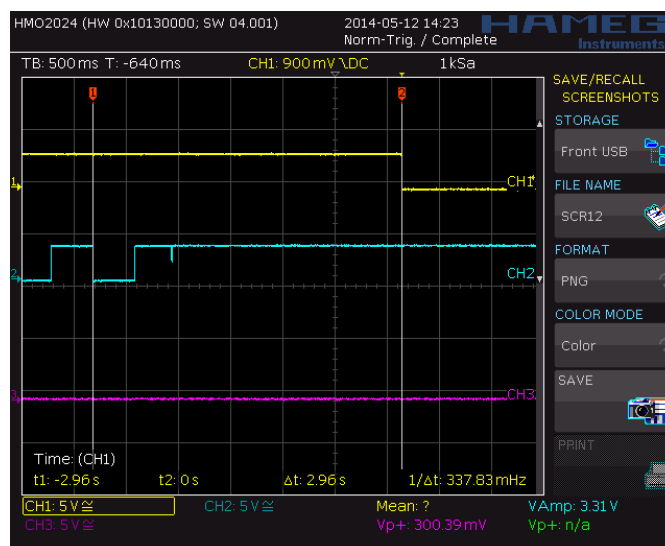
Figure 9.9: Watchdog time-out after slow WDI line cease to toggle - Voter output (CH1), WDI input lines (CH2 & CH3)

Voter

Correct functionality of the voter was ensured by removing the supply voltage from one of the three watchdogs. The three reset outputs of the watchdogs can be seen in the three signals from the top (CH1, CH2 & CH3) along with the output of the voter (bottom CH4) in Figure 9.10. The disabled watchdog's output is at 0 V and shows no transition as seen in CH2 (second from the top). Note the delay of 44 ms from the watchdog's first transition (above - CH1) until the transition of the third watchdog and the voter output. As with the first POR delay measured, this is 2.32 % lower than the calculated value. This may be due to chip differences or capacitance differences between the three watchdogs. The capacitors used to adjust the delays have a 10 % tolerance which along with the deviations described in Section 8.4.1, may account for uneven delays.
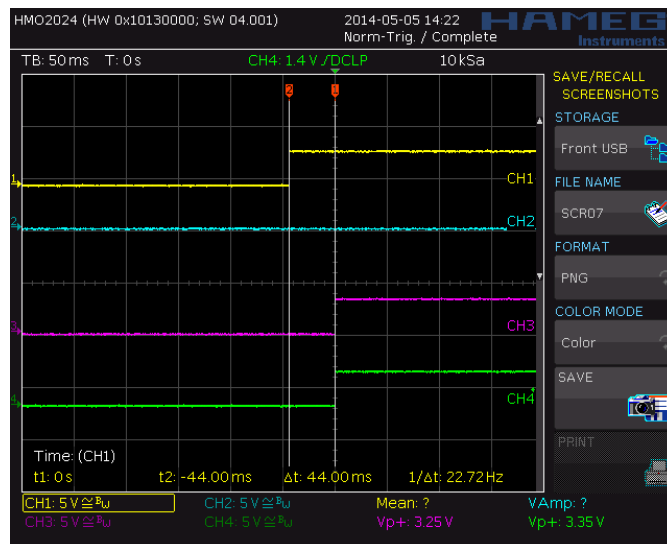
Figure 9.10: Voter output (CH4) and watchdogs' $\overline{RESET}$ output (CH1, CH2 & CH3). One watchdog disabled (CH2)

By removing the supply voltage from two of three watchdogs, the voter output was to remain low at all times. This is shown in Figure 9.11 with signals as described for Figure 9.10. The only active watchdog is seen at the top of the figure (CH1).

Brownout Detector

The voltage supervisory function, or brownout detector, of the watchdogs was tested by slowly decreasing the evaluation card's supply voltage. Multimeter measurements showed a threshold voltage of 3.08 V, 0.16 % higher than the typical threshold of 3.075 V and well within the chip's 2.5 % accuracy. The reset signal will be active low for as long as the supply voltage is below the threshold and is guaranteed to be valid for supply voltages down to 1.1 V [12].
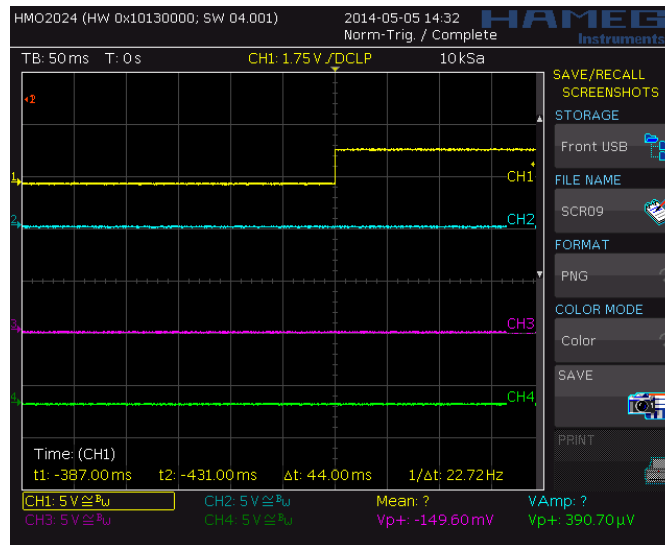
Figure 9.11: Voter output (CH4) and watchdogs' $\overline{RESET}$ output (CH1, CH2 & CH3). Two watchdogs disabled (CH2 & CH3)

Current Consumption

For integration into the backplane, the LEDs will be removed and the power OR-ing chip and current limit switch are already in place. This leaves three watchdog chips, three XOR-gates, six AND-gates and one OR-gate with current consumption as shown in Table 9.3. These values are based on maximum current consumption values from the ICs' datasheets.

Table 9.3: Current consumption - Watchdog evaluation card

Chip	#	μA	Total μA
MAX16058	3	0.415	1.245
2-input AND	6	200	1200
3-input OR	1	200	200
2-input QUAD XOR	1	20	20
Total	**11**	**-**	**1421.245**

9.2 Battery Management

Three system modes were defined in Section 6.1:

- Critical mode - less than 25% battery capacity

- Avoidance mode - between 25-50% battery capacity

- Normal mode - between 50-100% battery capacity

Conditions for the three modes must be given as a part of a battery management framework. The framework is divided into the three scenarios critical, avoidance and normal. It aims at keeping the satellite in normal mode at all times and in a situation where the solar panels deliver more power than what is consumed. A framework implementation assumes the use of a battery fuel gauge capable of providing remaining battery capacity.

Section 7.2.1 presents actions necessary to prevent the satellite from completely discharging its battery. Together with calculations from Chapter 5, it forms the basis for the battery management framework presented below.

9.2.1 Critical Mode

Critical mode is as described in the mission event planning Section 7.2.1 and Figure 7.4. In this mode the remaining battery capacity is 25% or less. No subsystems are allowed to be active and the beacon rate is set to minimum, meaning the satellite will transmit a beacon signal four minutes apart. At its minimum, the beacon consumes 660 mW and with only the on-board computer (OBC), backplane and Radio module active, the total power consumption becomes approximately 1.485 W. Use of external memories are not permitted. A value for the attitude determination and control system (ADCS) has not been included, since a final implementation is not in place. For readjusting the attitude as an attempt to increase charging power, the ADCS must be given a runtime high enough to sufficiently change attitude, but without draining the battery further. Section 5.1 calculates the normalized charging power to 3.205 W, which is 1.720 W higher than the consumption. Calculations found in Appendix E estimates that the satellite charges from a completely discharged battery to full capacity in approximately 17 hours, given a linear charging characteristic. From a battery at 25 % remaining capacity, a charge time of approximately 4 hours is necessary to reach 50 % capacity. The satellite will stay in this mode until the battery has reached 50 %, after which normal mode operations will commence.

9.2.2 Avoidance Mode

Avoidance mode attempts to reduce the power consumption of the modules before turning them off. This is to avoid entering critical mode prematurely which greatly

inhibits on the satellite's functionality. The battery is at 25-50% of full capacity and the beacon transmission rate is set to its minimum value. The power consumption for all modules are measured to determine if they consume more power than what is allowed. If a module is found to consume too much power, it is told to reduce its consumption or it will be restarted to reduce consumption caused by either rouge software or a single event latchup (SEL). If this does not cause a net charging state of the battery, critical mode will be initiated.

9.2.3   Normal Mode

Normal mode applies from 50-100% of remaining battery capacity. No power-saving restrictions apply for the submodules and periods of time where the satellite consumes more energy than it generates, are allowed. The beacon transmission rate is set to normal causing its power consumption to increase to 1.100 W, 66.67 % higher than its consumption in avoidance and critical mode. Normal mode's worst case power consumption is 4.442 W as calculated in Appendix E, 199.1 % higher than critical mode. The OWL radio is not included since its protocol and activity level has not yet been decided.

Example of Basis State

By assuming a certain runtime per hour for each module and a given beacon transmission rate, it is possible to estimate energy consumption for a basis state where the satellite should generate more energy than it consumes. Table 9.4 shows such an example. The typical current consumption of 30.4 mA from Section 4.1 is used for the OBC and Radio MCUs, which gives approximately a 100 mW power consumption. NAND flash and FRAM power consumptions are doubled compared to Table 5.1 in Section 5.1, since the memories are present both on the OBC and Radio module.

Table 9.4: Estimated basis state

Component	Power consumption [mW]	Runtime [h]	Energy consumption [mWh]
Backplane	165	1	165
OBC MCU	100	1	100
Radio MCU	100	1	100
NAND Flash	198	0.1	1.98
FRAM	132	0.1	1.32
Power amplifier[1]	3300	-	1100
TOTAL	-	-	1468.3

Only components and modules which are either always on or used often, are included. The attitude determination and control system (ADCS) can be granted a degree of autonomy as long as net charge is positive. Full use of the ADCS is an

---

[1]Beacon transmissions at normal rate

exception to the base state since it is only necessary to perform complete attitude adjustment when pointing the camera or as an attempt to change exposed solar panels. The OWL radio is also omitted since it is only active when transmitting telemetry or image data to the ground station. As an example, external FRAM and NAND flash memories are permitted to run 1 % of the time, since frequent logging and backup may be necessary. The example presented in Table 9.4 shows a energy consumption of approximately 1.468 Wh, 1.737 Wh lower than the normalized charging of 3.205 Wh. This margin can be increased by using the lowest beacon transmission rate. However, the example illustrates the need for careful battery management in order to avoid a basis state where net charging is negative, which over time will cause the satellite to abort normal mode operations and enter avoidance or critical mode.

A coding proposal for the presented battery management framework is presented in Appendix C.

Chapter 10

Discussion

This chapter presents the discussion related to the new watchdog system, battery management and mission event planning.

10.1 Hardware Watchdog

The evaluation card designed in Section 8.4.2 has been tested and found to operate as intended. For both solutions, the time-out period, power-on-reset (POR) delay and brownout detector (BOD) threshold voltage must be selected. For a backplane watchdog solution, also the watchdog input (WDI) toggling frequencies must be selected.

10.1.1 Brownout Detector Threshold Voltage

The voltage supervisory function of the MAX16058 is an added benefit of the chip since it is the watchdog timer that is its main function in this design. The Atmel MCUs have an internal BOD with a threshold of 2.7 V, 18 % lower than the 3.3 V supply. Maxim Integrated recommends having a threshold voltage higher than that of connected ICs. This sets the MAX16058's threshold higher than 2.7 V. Atmel recommends the threshold voltage of an external BOD to be set 5 - 15 % lower than the typical supply voltage of 3.3 V [53], which gives an interval of 2.805 V to 3.135 V. Adjusted for MAX16058's 2.5 % accuracy, the interval is 2.875 V to 3.057 V, of which Maxim Integrated offers two possibilities with a typical threshold voltage of 2.925 V and 3.000 V. The final choice may be based upon availability.

10.1.2 Power-On-Reset Delay

Section 3.2.2 presents the time necessary to clear a single event latchup (SEL) as between 4.7 μs and 300 ms. This is related to the length of the POR delay

which must be sufficient for all voltages to reach the ground potential of 0 V. Performed tests used an arbitrary POR delay of approximately 1.7 s and measurements showed actual delays within 2.32 % of the calculated value, which is well within the deviations as described in Section 8.4.1. A final decision of its length can not be made based solely on an evaluation card. Measurements of module voltages in the final pre-flight model must form the basis for determining the necessary length of the POR delay. Deviations caused by capacitor tolerances and temperature fluctuations must be taken into account for this final value.

10.1.3 Time-out Period

The time-out period is adjustable from 16 ms to 300 s, and a reasonable value must be selected for this design. The 3.3 nF C_{SWT} capacitor used on the evaluation card gave a typical time-out period of 2.048 s, while the measured period ranged from 2.58 s s to 3.28 s, respectively 25.98 % and 60.16 % higher than the typical value. The theoretical minimum value from Equation 8.5 is 0.65 s, with a maximum value of 7.98 s as given by Equation 8.6. Deviation from the typical value is 68.26 % lower for minimum and 289 % higher for maximum. Note that these are the absolute worst case values over the entire temperature range for the chip, -40°C to +125°C. It is especially the minimum value that must be controlled since a large shift could cause unintended resets.

A new hardware watchdog system is used as a last resort when the active master has exhausted all other options for recovering the system. Code corruption or failures in task execution will be handled by the MCUs' internal watchdog, and as for single event latchups (SELs) and single event upsets (SEUs) external to the MCUs, the software watchdog should mitigate these. This supports the argument for a long time-out period. A long period is also necessary to prevent a reset-loop as a result of a long stabilization time, which for the Atmel MCUs can be as much as 1.2 s [37], and a short period. It must also provide enough time for the system to attempt to recover itself and log its current condition before a system wide reset. Reduced overhead for the MCUs is also an argument for a long period. With a long period, the hardware watchdog may be tapped conditionally only after the system has passed certain health checks. This will prevent tapping the hardware watchdog without being certain that the submodules are functioning.

For the NUTS system, time-out periods as high as the maximum value of 300 s should be suitable to accommodate the functionality as described above. Considering the large deviations of both time-out periods and POR delays, thorough tests of the finished pre-flight test model and flight model must be conducted after the final values are selected. This includes thermal vacuum tests needed to ensure that variations between desired and actual periods and delays, also between each watchdog chip, is not likely to cause failures in orbit. Time-out periods and POR delays must be chosen such that the new watchdog system serves its purpose at each extreme of the expected temperature variations.

10.1.4 Watchdog Input Toggling Frequencies

For a backplane watchdog, the WDI toggling frequencies must also be determined. Frequencies with which the master modules are to toggle the hardware watchdog, must be based on the minimum time-out period as given by Equation 8.5. This is in order to avoid unintentional resets. The XOR-gate at the watchdog inputs must be driven by signals at two different frequencies in order to produce a valid high to low transition at its output within the time-out period. Each frequency must be high enough to tap the watchdog by itself if the other master ceases to toggle its WDI line. During testing the frequencies were separated by a factor of 4, which produced desirable results. The lowest frequency must have a shorter period than the watchdogs' time-out period, and using a $\frac{1}{3}$ or a $\frac{1}{4}$ of the time-out period gives some margin towards preventing a time-out. This results in the highest frequency having a period between a $\frac{1}{12}$ or a $\frac{1}{16}$ of the time-out period.

10.1.5 Manual Reset Option

Through testing and evaluation of the overall functionality of the watchdog system, it has been decided to remove the possibility of a manual reset. This is due to the possible issue of one of the masters continually pulling its reset line low, even after power cycling. This would keep the system in permanent reset and power will never be brought back on. This is not an issue when only using the time-out function, since a master misusing or disabling its WDI line will not effect the other master nor cause a continuous reset condition. The possibility of a remotely revoke reset is still present through the option of transmitting a command ordering the on-board computer (OBC) and Radio to cease toggling of the WDI lines. This causes the watchdogs to time out and would be a last resort in an attempt to recover from SELs which have not been resolved through power cycling of submodules. Overall, the risk of misusing the manual reset option has been deemed larger than its benefit, especially since the same functionality is redundantly present through the time-out function of the watchdogs. It also removes the single point of failure related to a stuck manual reset signal. Power cycling of one of the two masters is possible by removing power to the module through the backplane whenever a master fails a health check or fails to answer a communication attempt from its partner.

10.1.6 Backplane Watchdog Solution

For a backplane watchdog there are two major issues, namely how to best incorporate the design into the existing backplane and how to make it as reliable as possible. Incorporation concerns are from where the new ICs should receive supply voltages, where and how the voter output should be connected and how to combine it with existing hardware and signals.

Supply Voltage

As for providing power to the new ICs, there exists two options; use one of the two redundant 3.3 V supplies from the electrical power system's (EPS) regulators or from a LTC4413 power OR-ing chip on the backplane. If the ICs are powered directly from the EPS, the existing redundancy of two independent regulated voltages is left unused and a faulty regulator will leave the ICs unpowered. Powering the ICs after the power OR-ing will take advantage of the redundant power supply and the loss of one regulator will not inhibit on continued operation, making this a desirable approach. If this single LTC4413 chip fails, the watchdog system will be disabled as a whole and it will no longer be necessary to toggle the WDI lines to prevent a reset. By including a pull up resistor on the voter output, the reset signal is pulled high and the power to the rest of the satellite will remain on and be otherwise unaffected.

Since the new watchdog is based on triple modular redundancy (TMR), powering the triplicated ICs from three LTC4413s will further improve redundancy with each replica of the MAX16058 watchdog chip and its watchdog input (WDI) XOR-gates receiving supply voltage from a power OR-ing chip. Compared to the simpler solution described above, this will enable the watchdog system to operate as intended if one LTC4413 chip fails. Challenges which must be considered in the final pre-flight test model is the risk of short circuits and crossing lines when increasing the number of separate power lines on an already populated PCB, and hence the simpler solution with less routing of power lines may be desirable.

Incorporation into Existing Backplane

The new watchdog system has been design to provide an active low reset signal at its output whenever the watchdogs time out or the supply voltage drops below a certain threshold. For the system to be useful in the backplane, the ideal interconnection of the output and existing hardware must be found. The backplane already provides a mechanism for disabling power to separate submodules as seen in Appendix B and in Figure 10.1. E.g. in the case for *Module 8*, this is done by pulling the ON pin on the MAX14523 current-limit switch to ground using the *PWR_ON#* signal and thereby removing power at its output. Since the main goal of the new watchdog is to reset unresponsive masters and remove SELs, it is possible to connect its output to the current-limit switches located at each module connector. This will cause a global reset with a delayed start, a power-on-reset delay, cycling the power to both master modules. By connecting the watchdog's output to the backplane's own MAX14523 switch, the satellite now has the possibility of restarting the backplane logic as well, removing any SELs left unresolved by the old design, solving the issue described in Section 4.6.

Since both signals are active low, the simplest way of combining the watchdog's output with the existing *PWR_ON#* signal is through a 2-input AND-gate located

at each module's current-limit switch. This keeps the possibility of independently cycling power to the submodules while also enabling a global cycling of power. Figure 10.1 shows a possible way of implementing the design into the backplane.

Figure 10.1: Possible implementation for a backplane watchdog

Considerations for Increased Reliability

On the evaluation card, the three XOR-gates connected to the watchdogs' WDI inputs are all a part of a single IC consisting of four 2-input XOR-gates, where one is left unused. In the final implementation, it is recommended to use three XOR-gates, each on a separate IC, when interfacing the watchdogs. This will require more real estate on the backplane, but will prevent a failure in the IC from disabling the entire satellite. As a result, one XOR-gate and one watchdog circuit can fail or loose power without effecting the other watchdogs and the rest of the satellite.

10.1.7   Local Watchdog or Backplane Watchdog

By using TMR for a backplane watchdog system, the watchdog as a single point of failure in itself is resolved, but the necessary voter creates a new one. How far to extend the design towards optimal redundancy and reliability must be weighed against its usefulness to the project, time and resource constraints, as well as mission lifetime. A final degree of reliability and redundancy must be determined in order to avoid an unnecessary increase in complexity. It is natural to discuss if a

triple modular redundancy (TMR) watchdog system is necessary, or if it overcomplicates the design. NUTS' mission lifetime is of such a limited period (3 months) that the probability of a critical failure is reduced compared to longer missions. It is none the less desirable to have some form of mechanisms in place capable of resetting the system as a last resort upon a failure. It is given by the problem description that such a mechanism, if malfunctioning, is not to leave the satellite non-operational, which is where a backplane watchdog solution falls short. The voter remains a single point of failure unless it is duplicated to each place where its output is used. With four ICs in the voter, this rapidly increases components count and amount of signalling and power lines needed on the backplane, which again increases the total amount of possible failures. A local watchdog solution adds a MAX16058 chip and a power switch to each master module without changes to the backplane. A backplane watchdog solution required dedicated lines for manual reset and watchdog toggling, while local watchdogs only rely on connections on-board the module card. As a total, the backplane solution adds 11 ICs and has higher degree of complexity than the local watchdog solution. By avoiding logic gates in the voter and at the watchdogs' inputs, the local solution using only two MAX16058 chips, has a lower current consumption as seen in Table 9.3 in Section 9.1.2. Due to its simplicity and desirable functionality, the local watchdog solution is the preferred solution and is recommended for implementation in the pre-flight test model.

10.2 Battery Management

Section 5.1 presents estimates for charging power from the solar cells. An adjustable beacon transmission rate helps the satellite to maintain a healthy battery state and it is controlled by the system modes and ground station.

10.2.1 Power Estimation

Based on the defined beacon rates, it is unnecessary to use the beacon at full rate other than for the initial mode. The 100 % increase in power consumption compared to normal rate, will drain the battery quicker and reduce submodules' runtime. In a worst case situation, as much as 14 hours can separate two visible passes over the ground station. Estimates from Section 5.4 shows that for a worst case charging condition, the battery can drain in close to 20 hours. If contact is not established during the six visible passes, there is another 14 hours until next possible attempt. Therefore, a high beacon transmission rate can reduce the chance of establishing contact with the ground station, given that the battery can be discharged before the next visible pass occurs. Project management has to decide if this is an acceptable risk, or if the beacon should transmitting at low or normal rate in order to make the battery last longer, at the cost of fewer detectable transmissions. Applying the lowest transmission rate reduces initial mode's power

consumption by 49.1 % to 1.485 W, less than the worst case charging power of 1.535 W, meaning the satellite should be able to sustain this mode indefinitely. Regardless, the ground station should have the possibility of overriding any mode, both for beacon rates and system modes.

A final implementation of the battery management should result in a basis state where the satellite is fully operational, and where the net charge over a given time period is positive and large enough to keep the battery at more than 50 % capacity. An example of such a basis state is given in Table 9.4 in Section 9.2.3, where the net charging is large enough to grant a certain degree of autonomy to the submodules. If applying the lowest beacon rate is acceptable, power consumption by the power amplifier can be reduced by 40 % from its normal rate. More net charge that is available, the higher the degree of autonomy can be given to the attitude determination and control system (ADCS) and payload.

10.2.2   Discharge Considerations

In order ensure that the battery does not reach its depth of discharge (DoD), the battery must be monitored constantly. It is up to the battery management to avoid reaching the critical mode defined as 25 % or less remaining capacity. For this to be possible, accurate battery measurements are necessary, e.g. from a battery fuel gauge. The same applies to battery charging. If the battery overcharges it could destroy the battery pack and it is therefore important to stop charging when full capacity is reached. Section 5.1.1 presents a suitable battery fuel gauge which is capable of accurately reporting both remaining and full battery capacity. Project management must decide whether or not to implement a fuel gauge, but it is recommended that its functionality is in place for the pre-flight test model.

10.2.3   Solar Cells

Charging power for the solar cells have been calculated based on ideally values from its datasheet. The solar cells become less effective due to irradiation and random solar flares. A worst case reduction in efficiency is about 8.79 %, which causes a normalized charging power of 2.923 W instead of 3.205 W. If this reduction will take place during NUTS' mission life time is not possible to predict due to the random nature of irradiation and solar flares.

Estimates in this thesis applies an average case charging power per orbit based on a worst case beta angle of 0°. Charging power per orbit was adjusted to a normalized charging power based on ratio between time exposed to the Sun and in eclipse. This made it possible to compare power generation and consumption. In a best case scenario, the normalized charging will more than double to 7.514 W, since the satellite will be exposed to the Sun throughout its orbit.

10.3   Mission Event Planing

Throughout this thesis, the mission event plans have evolved. Chapter 7 presents several possible mission event plans for NUTS. Through flowcharts and discussion, proposals aimed at increasing reliability by handling power conditions, payload verification and single event effects (SEEs) efficiently, are presented. The release of the deployment switches and the antenna deployment after ejection from the P-POD, are the most critical events NUTS encounter. Stuck deployment switches are an inherent risk of the P-POD solution of delivering CubeSats to orbit, which can not be mitigated by a mission event plan. Antenna deployment can not be guaranteed due to possible mechanism failures, but this risk can be reduced through multiple redeployment attempts. The NUTS project has evaluated different methods of detecting deployed antennas, but has not decided which, if any, methods to implement. A detection mechanism would prevent transmitting the beacon signal if the antennas have not been deployed, thereby preventing harmful reflection in the radio components. The current solution of multiple reattempts is the simplest solution, one that does not cause false indication of whether deployment was successful or not. Since radio communication is essential, the effect of possible reflections must be evaluated before launch.

10.3.1   Periodic Restarts

It is possible to plan for periodic restarts of the satellite in order to resolve single event effects (SEEs) which is not detected by the software watchdog. The on-board computer (OBC) can remove power to each submodule one after the other, while the Radio module can remove power to the OBC. Power should not be completely removed from the Radio module, since this will silence the satellite. If the MCU or memories on the Radio module are in need of periodic restarts, the Radio MCU can cease tapping its watchdog, which removes power for the predetermined power-on-reset (POR) delay.

10.3.2   Temperature Considerations

NUTS has so far not been through vacuum and thermal tests. This is necessary to ensure correct functionality of the proposed watchdog, as well as to avoid destroying the power amplifier and regulators on the electrical power system (EPS). To efficiently respond to high temperatures, the mission plan recommends treating this condition as a low battery condition, which initiates the critical system mode. By reducing radio activity to a minimum and reducing power consumption in the submodules, heat generated in the power amplifier and the EPS' regulators is reduced. It is recommended that temperature sensors are implemented in these strategic locations, including the battery pack. A fuel gauge with an negative temperature coefficient (NTC) thermistor will enable accurate tracking of the battery

pack's temperature.

Chapter 11

Conclusions

In this thesis, detailed mission event plans have been proposed and reviewed. The mission plans have been evaluated to minimize error and fault consequences, and to maximize the probability for a mission success. A detailed battery estimation has been presented along with defined levels for the beacon transmission rate. The beacon rate has been divided into three levels; low, normal and full. This aims at reducing power consumption, which together with a battery management framework, will help the NUTS project towards defining a final power budget for its flight model. Beacon transmissions at full rate consume 2200 mW, which are 100 % higher than normal rate and 233.33 % higher than low rate.

This thesis has shown the importance of maintaining a net charging state for the satellite, and the proposed beacon rates will help maintain this state. Being able to adjust the beacon transmission rate is shown to conserve energy and enable normal mode operations for a prolonged period of time. An avoidance mode is defined as an attempt to reach a net charging state without severely inhibiting on the satellite's operations. If a net charging state is not achieved in avoidance mode, NUTS enters a critical mode in order to recharge its battery.

An initial mode has been defined for when the satellite is ejected from the P-POD, and before contact with ground station has been established. The beacon is set to its highest rate so the ground station can detect the satellite more easily. With an average case charging scenario, NUTS consumes less energy than it generates, suggesting it can sustain initial mode indefinitely.

A method for removing lasting faults by toggling power has been designed and implemented. Two watchdog proposals have been suggested, a triple modular redundancy (TMR) watchdog on the backplane and a local watchdog on each master. The TMR watchdog solution was implemented on an evaluation card, and has been thoroughly tested and verified. Based on testing results and subsequent analysis, the most suitable solution for the NUTS project, is the local watchdog placed on each master module. Both solutions provide the possibility of toggling power to all subsystems, and have a global reset with a delayed start. Guidelines for

choosing the time-out period, power-on-reset (POR) delay and threshold voltage have been provided, and final values must be based on measurements on the pre-flight test model.

11.1 Further Work

The watchdog circuits must be routed and placed on the on-board computer (OBC) and Radio module and tested thoroughly. It is also necessary to verify if the power-on-reset (POR) delay is long enough for all voltages to reach ground before power is brought back on. This is needed to ensure that toggling of power is successful in removing any single event latchups (SELs).

The battery management framework must be finalized and a decision to implement a battery fuel gauge must be made. The satellite must undergo vacuum and thermal tests to measure how temperature and a lack of convection affects the systems. Results achieved will, together with reported battery capacity, form the basis on which the battery management framework regulates power consumption. Vacuum and thermal tests are also needed to determine changes in time-out period and POR delay for the watchdog chips.

When all components, modules and software tasks are in place, the estimated power consumption must be revised in order to be as accurate as possible. This forms the basis on which the mission event plans can maintain a net charging state for the satellite.

Bibliography

[1] California Polytechnic State University. CubeSat Design Specification Rev. 12. `http://browncubesat.org/wp-content/uploads/2013/01/Cubesat-Reqs.pdf`, 2009. Retrieved May, 2014.

[2] Kosta A. Varnavas Todd C. MacLeod, W. Herb Sims. Satellite Test of Radiation Impact on Ramtron 512K FRAM. <u>IEEE</u>, 2009.

[3] H.D. Young, R.A. Freedman, and F.W. Sears. <u>University Physics with Modern Physics vol 2</u>, pages 925–927. Pearson/Addison Wesley, 2003.

[4] European Space Agency. Radiation Effects. `http://www.esa.int/TEC/Space_Environment/SEMQ95T4LZE_0.html`, 2007. Retrieved May, 2014.

[5] Jan Kenneth Bekkeng. Lecture in Radiation Effects on Space Electronics. `http://www.uio.no/studier/emner/matnat/fys/FYS4220/h11/undervisningsmateriale/forelesninger-vhdl/Radiation%20effects%20on%20space%20electronics.pdf`, 2011. Retrieved May, 2014.

[6] Jim Lamberson. Single and Multistage Watchdog Timers. `http://www.sensoray.com/downloads/appnote_826_watchdog_1.0.0.pdf`, 2012. Retrieved May, 2014.

[7] Michael Dowd. How Rad Hard Do You Need? The Changing Approach To Space Parts Selection? `http://www.maxwell.com/products/microelectronics/docs/how_rad_hard.pdf`. Retrieved May, 2014.

[8] A123 Systems. Cylindrical Battery Pack Design, Validation and Assembly Guide. `http://assets.buya123batteries.com/images/a123/Battery_Pack_Design_Guide_Rev_07.pdf`, 2013. Retrieved May, 2014.

[9] NASA. Beta Angle. `http://spaceflight.nasa.gov/station/flash/start.swf`, 2014. Retrieved May, 2014.

[10] Maxim Integrated. MAX14523 datasheet. `http://datasheets.maximintegrated.com/en/ds/MAX14523A-MAX14523C.pdf`, 2011. Retrieved May, 2014.

[11] Dewald De Bruyn. Power Distribution and Conditioning for a Small Student Satellite. Master's thesis, NTNU, 2011.

[12] Maxim Integrated. MAX16056-MAX16059 datasheet. `http://datasheets.maximintegrated.com/en/ds/MAX16056-MAX16059.pdf`, 2013. Retrieved May, 2014.

[13] Intersil. ISL88708 datasheet. `http://www.intersil.com/content/dam/Intersil/documents/isl8/isl88705-706-707-708-716-813.pdf`, 2009. Retrieved May, 2014.

[14] Texas Instruments. UCC2946-Q1 datasheet. `http://www.ti.com/lit/ds/symlink/ucc2946-q1.pdf`, 2013. Retrieved May, 2014.

[15] David M. Pozar. Microwave and RF Design of Wireless Systems, pages 6–7. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2000.

[16] Andøya Rocket Range. The Norwegian Student Satellite Program, ANSAT. `http://www.rocketrange.no/?page_id=254`, 2014. Retrieved May, 2014.

[17] Kjell Arne Ødegaard. Error Detection and Correction for Low-Cost Nano Satellites. Master's thesis, NTNU, 2013.

[18] Lars Erik Jacobsen. Electrical Power Systems of the NTNU Test Satellite. Master's thesis, NTNU, 2012.

[19] Roger Birkeland. NUTS-1 Mission Statement. `http://nuts.cubesat.no/upload/2012/01/20/nuts-1_mission.pdf`, 2011. Retrieved May, 2014.

[20] Wil Harkins. Space Radiation Effects on Electronic Components in Low-Earth Orbit. NASA, 1999.

[21] R. A. Mewaldt. Cosmic Rays. `http://www.srl.caltech.edu/personnel/dick/cos_encyc.html`, 1996. Retrieved May, 2014.

[22] Encyclopædia Britannica Online. Van Allen Radiation Belts. `http://www.britannica.com/EBchecked/topic/622563/Van-Allen-radiation-belt`, 2014. Retrieved May, 2014.

[23] Douglas W. Caldwell. Minimalist Fault-Tolerance Techniques for Mitigating Single-Event Effects in Non-Radiation-Hardened Microcontrollers. University of California, Los Angeles, 1998.

[24] D. L. Shaeffer J. L. Kaschmitter and N. J. Colella. Operation of Commercial R3000 Processors in the Low Earth Orbit (LEO) Space Environment. IEEE, 1991. Lawrence Livermore National Laboratory.

[25] Jr. Dr. John F. Conley. Total Dose Effects - Space Radiation Effects on Microcontrollers. NASA, page 115, 2003.

[26] Lei Luo Qingkui Yu Pengwei Li, Xiaoyun Fu. A New Analyzing Method of Single Event Latch-Up Protection Circuit Based on Current Comparing and Its Performance Verification. Journal of Modern Physics, (5):387–393, 2014.

[27] J. Marshall H. Anthony R. Boss P. Layton, D. Czajkowski. Single Event Latch Up Protection of Integrated Circuits. (SSC97-I-l), 1997.

[28] Alan Burns and Andrew J Wellings. Real-Time Systems and Programming Languages, chapter 2. Pearson Education Limited, 2009.

[29] R. Kapitza D. Lohmann W. Schröder-Preikschat P. Ulbrich, M. Hoffmann. Eliminating Single Points of Failure in Software-Based Redundancy. IEEE, 2012.

[30] Greg Manyak. Fault Tolerant and Flexible CubeSat Software Architecture. Master's thesis, CalPoly, 2011.

[31] Mihail P. Petkov. The Effects of Space Environments on Electronic Components. NASA, 2003.

[32] Jonas Friedel and Sean McKibbon. Thermal Analysis of the CubeSat CP3 Satellite. http://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1054&context=aerosp, 2011. Retrieved May, 2014.

[33] Ingrid Melody and Florida Solar Energy Center. Photovoltaics: A Question and Answer Primer. 1985.

[34] Encyclopædia Britannica Online. Photovoltaic Effect. http://www.britannica.com/EBchecked/topic/458271/photovoltaic-effect, 2014. Retrieved May, 2014.

[35] LLC Gears Educational Systems. Battery Basics. http://www.gearseds.com/files/determining_battery_capacity3.pdf, 2009. Retrieved May, 2014.

[36] YoazE. Bar-Sever. A New Model for GPS Yaw Attitude. Journal of Geodesy, 70(11):714–723, 1996.

[37] Atmel Corporation. UC3A3 datasheet. http://www.atmel.com/Images/32072s.pdf, 2012. Retrieved May, 2014.

[38] W. Hartner I. Kasko M.J. Kastner-N. Nagel M. Moert C. Mazure T. Mikolajick, C. Dehm. FeRAM Technology for High Density Applications. http://www.sciencedirect.com/science/article/pii/S002627140100049X, 2001. Retrieved May, 2014.

[39] Fujitsu Semiconductor Limited. Ferroelectric RAM (FeRAM). http://www.fujitsu.com/emea/services/microelectronics/fram/. Retrieved May, 2014.

[40] Jagdish Patel Jeffrey Namkung. Reliability and Endurance of FRAM: A case study. NASA, 2002.

[41] Linear Technologies. LTC4413 - Dual 2.6A, 2.5V to 5.5V, Ideal Diodes. http://cds.linear.com/docs/en/datasheet/4413fc.pdf, 2004. Retrieved May, 2014.

[42] Texas Instrument. Zerø-Drift, Bi-Directional CURRENT/POWER MON-ITOR with I2C Interface. `http://www.ti.com/lit/ds/symlink/ina219.pdf`, 2008. Retrieved May, 2014.

[43] Toril Bye Rinnan. Power Distribution and Conditioning for a Small Student Satellite. Master's thesis, NTNU, 2012.

[44] Fredrik Sola Holberg. Design of Attitude Estimation and Control System for a Cube Satellite. Master's thesis, NTNU, 2012.

[45] Magnus Haglund Arnesen. Design & Test of Camera Module NUTS Project Report, 2013.

[46] Inc. Micron Technology. NAND Flash Memory. `http://media.digikey.com/pdf/Data%20Sheets/Micron%20Technology%20Inc%20PDFs/MT29FxG08xAA.pdf`, 2006. Retrieved May, 2014.

[47] Fujitsu Semiconductor. 4 M Bit MB85R4001A. `http://www.fujitsu.com/downloads/MICRO/fsa/pdf/products/memory/fram/MB85R4001A-DS501-00005-3v0-E.pdf`, 2013. Retrieved May, 2014.

[48] Amund Gjersvik. Testing of the NUTS Electrical Power System. `https://www.ntnu.no/wiki/download/attachments/61146014/Testing%20of%20the%20NUTS%20Electrical%20Power%20System2.docm?version=1&modificationDate=1377853948000&api=v2`, 2013. Retrieved May, 2014, available through log-in.

[49] AZUR SPACE Solar Power GmbH. 30% Triple Junction GaAs Solar Cell As-sembly Type: TJ Solar Cell Assembly 3G30A. `http://www.azurspace.com/images/pdfs/0003401-00-00_DB_3G30A.pdf`, 2012. Retrieved May, 2014.

[50] Texas Instrument. Choosing Between Battery Gas Gauges and Battery Moni-tors to Track Charge Availability in Handheld Devices. `http://www.ti.com/lit/an/slua358/slua358.pdf`, 2005. Retrieved May, 2014.

[51] Texas Instruments. bq34z100 datasheet. `http://www.ti.com/lit/ds/symlink/bq34z100.pdf`, 2012. Retrieved May, 2014.

[52] Maxim Integrated. Tutorial 589 - CPU Supervisors: Frequently Asked Ques-tions. `http://pdfserv.maximintegrated.com/en/an/AN589.pdf`, 2010. Re-trieved May, 2014.

[53] Atmel. AVR180: External Brown-out Protection. `http://www.atmel.com/Images/doc1051.pdf`, 2002. Retrieved May, 2014.
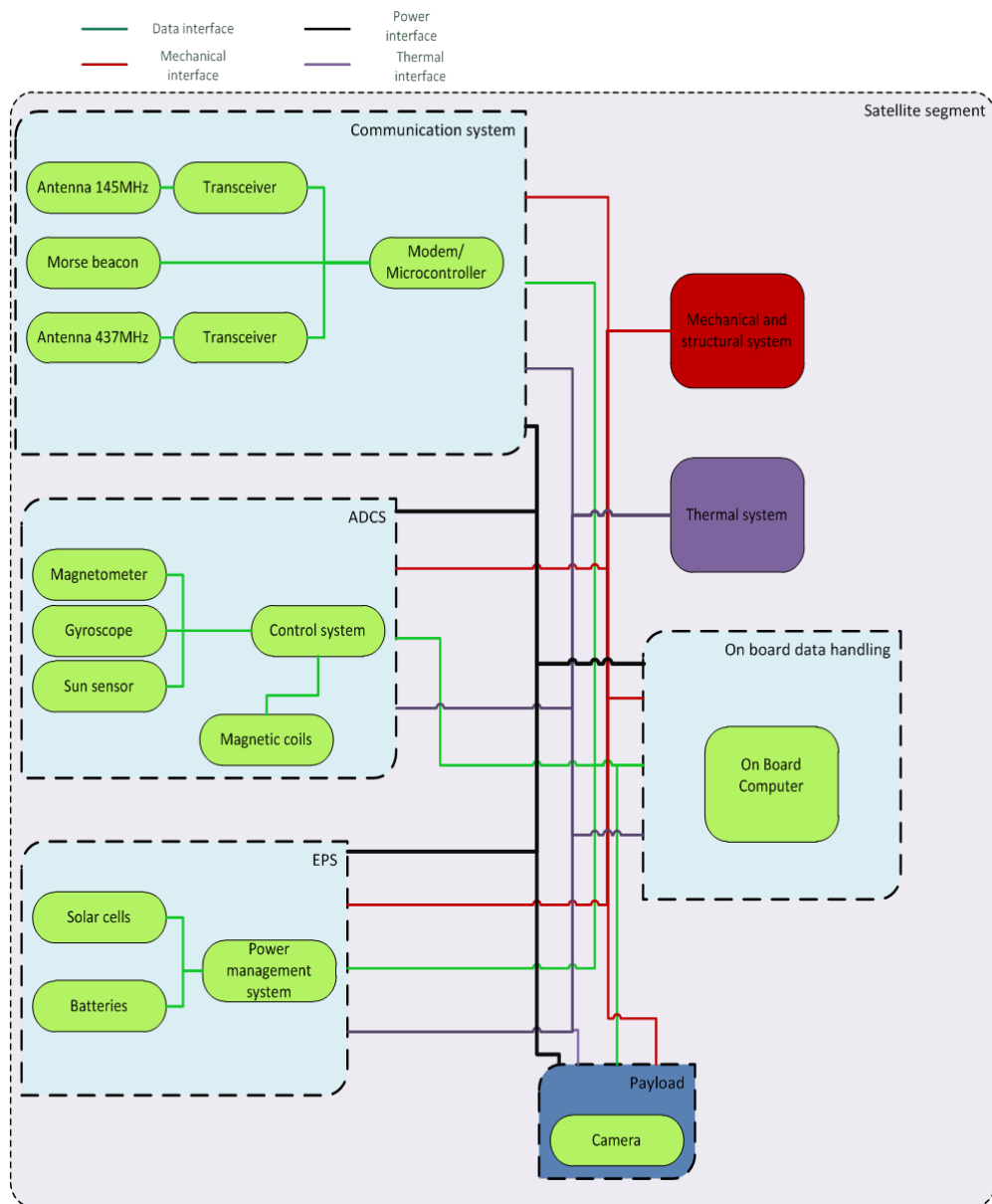
Appendix A

System Block Diagram

Figure A.1: The satellite's systems as proposed. Figure by: Emma Litzler

Appendix B

Existing Backplane Drawings

All following hardware drawings are created by Dewald de Bruyn and presents the existing hardware of NUTS' backplane. Figure B.1 shows the INA219 current monitoring circuit.
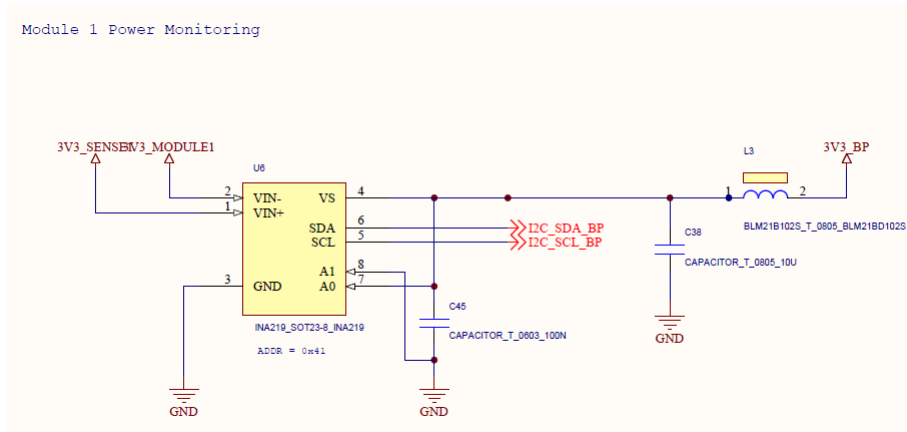

Figure B.1: Power monitoring module [11]

Figure B.2 shows the existing watchdog in the backplane. ADDR0 is used as watchdog input (WDI) to toggle the watchdog.
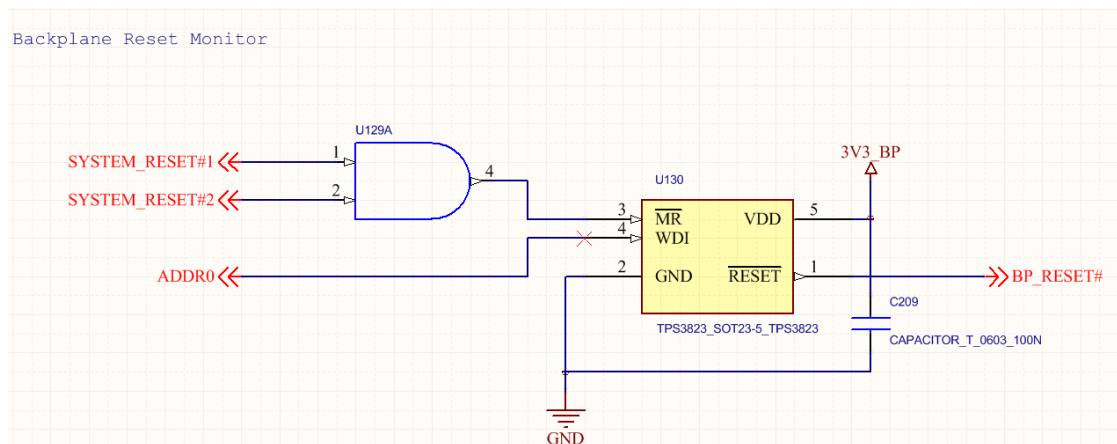

Figure B.2: Existing backplane watchdog [11]

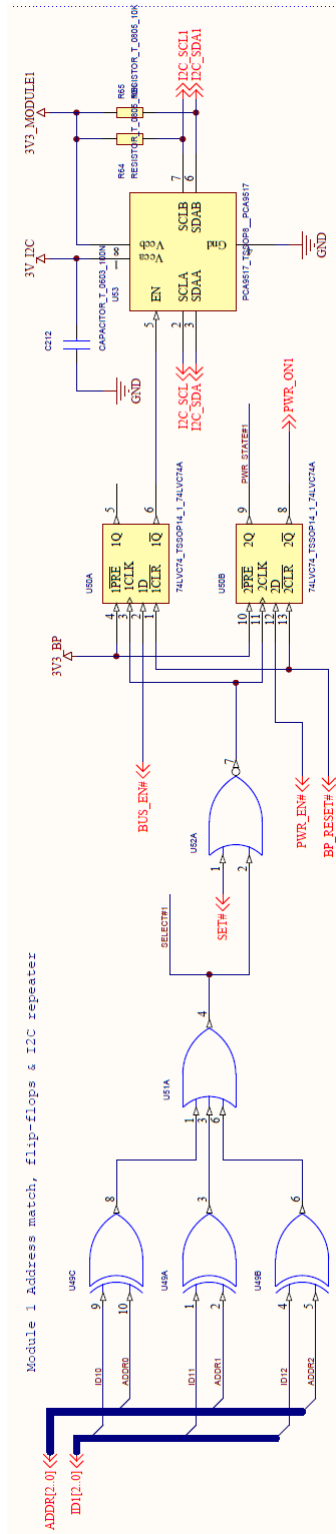Figure B.3 shows how to address the different modules on the backplane.

Figure B.3: Address match [11]

Figure B.4 shows how the power OR-ing LTC4413 is connected to the current limit
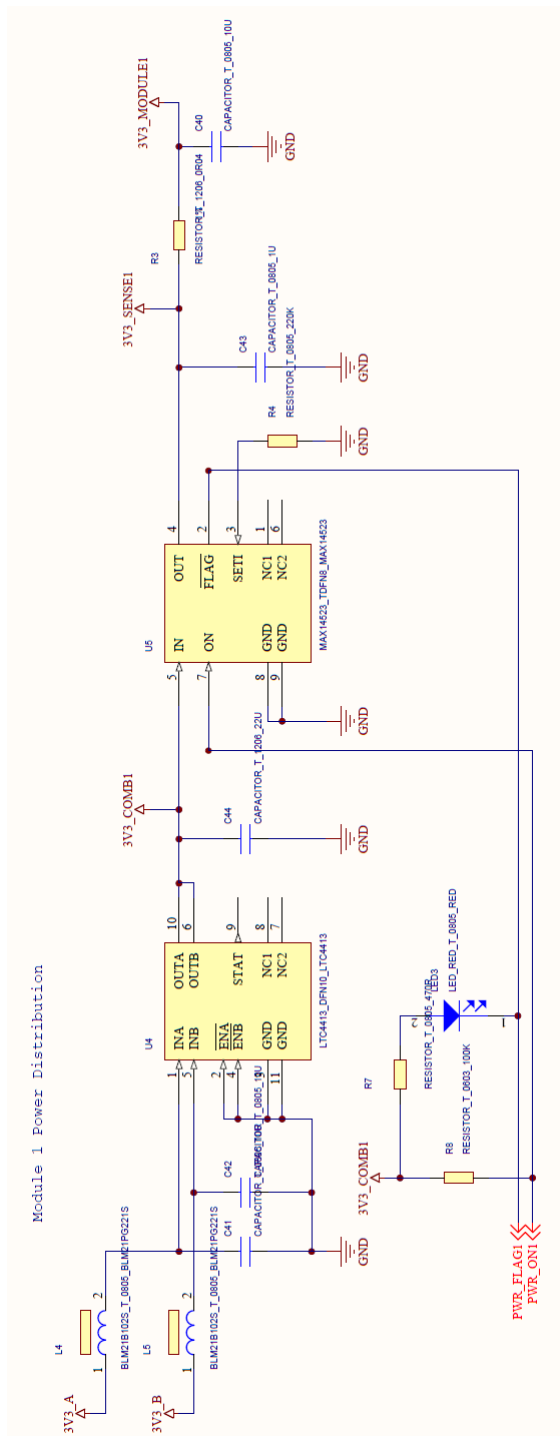
switch MAX 14523.

Figure B.4: Power distribution [11]

Appendix C

Battery Management Code Proposal

```
1  #include <asf.h>
2  #include "twim.h"
3
4
5  #define battery_minimum_value 5.8
6  #define battery_under_minimum_value 1
7  #define current_limit 100
8  #define current_limit_radio 200
9  #define solar_sensor_value 1
10
11
12
13 double read_voltages(void){
14     //Here the voltages at the battery are measured
15     //I2C communication
16 }
17
18 double read_net_current(void){
19     //I2C communication to the correct chip and get the current
20     //measure
21     twi_package_t packet;
22     uint8_t twi_data[2];
23     packet.chip =0x01; //! TWI chip address to communicate with.
24     packet.addr[1] = 0x11;//! TWI address/commands to issue to the
           other chip (node).
25     packet.addr_length = 0x01;//! Length of the TWI data address
           segment (1-3 bytes).
26     packet.buffer = (void*)twi_data;//! Where to find the data to be
           written.
27     packet.length = 0x01;//! How many bytes do we want to write.
28     uint8_t status = 0;
29     status = twi_master_read(&AVR32_TWIM0, &packet);
30
31     if(status == STATUS_OK){
32         uint16_t voltage = (twi_data[0] << 8) | twi_data[1];
33         double current = (double)voltage/4;
34         return current;
35         //Write current to log
```

```
36        }else{
37            //Error reading the current
38            //Write to log
39        }
40  }
41
42  int is_charging(void){
43        //Checks if the satellite is charging
44        if (read_net_current() > 0){
45            return 1;
46        }
47        return 0;
48  }
49
50  void log(double value){
51        //Generate timestamp
52        //Write the value into the memory
53  }
54
55  void submodule_off(int module){
56        //module 0 is ADCS
57        //module 1 is Payload(camera)
58  }
59
60  void submodule_on(int module){
61        //module 0 is ADCS
62        //module 1 is Payload(camera)
63  }
64
65  void all_submodules_off(void){
66        //Short cut if the battery is critical to turn
67        //of all submodules as quickly as possible
68  }
69
70  void all_submodules_on(void){
71        //Turn on all submodules
72  }
73
74  void beacon_rate(int value){
75        //Determine how often the beacon should transmitt
76        //3 is maximum, while 0 is off.
77  }
78
79  int in_eclipse(void){
80        //checks if the satellite is in eclipse
81        if (solar_sensor_value > 10){
82            return 0;
83        }
84        return 1;
85  }
86
87  double read_module_current(int module){
88        //module 0 is ADCS
89        //module 1 is Payload(camera)
```

```
90       //module 2 is radio
91   }
92
93
94   void powermanagement (void){
95       while(1){
96       //The function get_battery_status outputs a value from 0 to 2,
97       //were 2 is full/normal and 0 is critical
98           switch(get_battery_status()){
99               case 0:
100              //This is critical level
101              //Here everything need to be turned off immediately
102                  beacon_rate(1); //This sets the beacon rate to the lowest
                           rate
103                  all_submodules_off(); //NOT radio
104                  log(read_net_current());//Logs the net current
105                  if (!is_charging() && !in_eclipse()){
106                      //something is wrong
107                      //Try full system reset
108                  }
109                  while(is_charging() && battery_under_minimum_value){
110                      //We want to be in this loop until the battery have
                               reached
111                      //its minimum value (nominal 6.6V) to operate by
                               itself.
112                      if (battery_minimum_value >= 6.6){
113                          //Write to log
114                          all_submodules_on();
115                          beacon_rate(2);
116                          break;
117                      }
118                  }
119                  break;
120
121              case 1:
122              //This mode is avoidance critical, try to reduce current
                       draw on some
123              //modules before shutting down every module
124              //Check submodules current draw
125              beacon_rate(1); //Decrease the rate of the beacon to save
                       power
126              //read the module current to see if some modules using to
                       much power
127              double ADCS = read_module_current(0);
128              double payload = read_module_current(1);
129              double radio = read_module_current(2);
130
131              if (ADCS > current_limit){
132                  submodule_off(0);
133                  //wait a given time to turn on the module
134                  wait(100);
135                  submodule_on(0);
136              }
137              if (payload > current_limit){
```

```
138                submodule_off(1);
139                //wait a given time to turn on the module
140                wait(100);
141                submodule_on(1);
142            }
143            if (radio > current_limit_radio){
144                beacon_rate(1);//sets the beacon rate to low
145            }
146
147            if (!is_charging() && !in_eclipse()){
148                //something is wrong
149                //Try full system reset
150            }
151
152            while(is_charging() && battery_under_minimum_value){
153                //charge the batteries
154                if (battery_minimum_value >= 6.6){
155                    //Write to log
156                    beacon_rate(2);
157                    all_submodules_on();
158                    break;
159                }
160            }
161            break;
162
163            case 2:
164            //Normal
165                beacon_rate(2);//setting the beacon rate to normal
166                break;
167
168            default:
169                break;
170        }
171    }
172 }
```

Appendix D

Initial Mode Operation

D.1   Burn Off Mechanism

- Current consumption per wire: 350 mA
- Time to burn off nylon cord: 3 seconds
- Number of wires: 4

3 seconds as a fraction of hours:

$$3sec = \frac{3}{60 \cdot 60} = \frac{1}{1200}h \tag{D.1}$$

Energy used by four wires in 3 seconds:

$$E = 350mA \cdot \frac{1}{1200}h \cdot 4 \cdot 3.3V = 3.85mWh \tag{D.2}$$

Five attempts wires:

$$E_{tot} = 3.85mWh \cdot 5 = 19.25mWh \tag{D.3}$$

D.2   Power Calculations

- Battery capacity: 4.4 Ah
- Nominal voltage: 6.6 V
- Battery capacity, watts: 29.040 Wh $(4.4Ah \cdot 6.6V)$
- Average charging: 3.205 W
- Worst case charging: 1.534 W
- Estimated consumption: 3.025 W
- Average net power: 0.180 W

- Worst case net power: -1.482 W

Discharging time with worst case charging:

$$h = \frac{29.040Wh}{1.482W} = 19.6h \tag{D.4}$$

Appendix E

Battery Management Framework Calculations

E.1   Critical Mode

- Battery size: 29.040 Wh

- Average case normalized charging: 3.205 W

- Worst case consumption: 1.485 W

  – Beacon rate at low (660 mW), backplane (165 mW) and Radio & OBC MCUs active (660 mW combined)

- Net power: 1.720 W

Completely drained battery charging time to full battery:

$$h = \frac{29.040Wh}{1.720W} = 16.88h \tag{E.1}$$

25% battery capacity charging time to full capacity:

$$h = \frac{29.040Wh - 7.260Wh}{1.720W} = 12.66h \tag{E.2}$$

From 25% capacity to 50% capacity charging time:

$$h = \frac{14.520Wh - 7.260Wh}{1.720W} = 4.22h \tag{E.3}$$

E.2   Normal Mode

A worst case power consumption is when all components are active. The beacon transmits at its normal rate, causing a power amplifier's (PA) power consumption of 1.100 W. Due to NAND flash and FRAM being present on both master modules, their power consumption is doubled. OWL radio is not included since its protocol and activity level has not yet been decided.

- Maximum consumption: 4.446 W

$$P_{max} = PA + 2x(MCUs) + ADCS + 2x(FRAM) + 2x(NAND) + Backplane + Camera$$
$$(E.4)$$
$$P_{max} = 1100 + 660 + 1650 + 198 + 132 + 165 + 541 = 4446mW \qquad (E.5)$$

Appendix F

Test Equipment

- **Oscilloscope:** Rode & Schwarz Hameg HMO2024 Serial number: 015213802

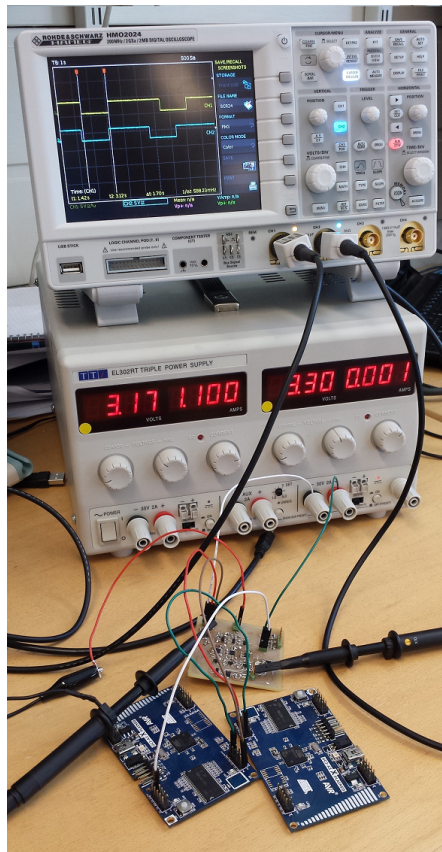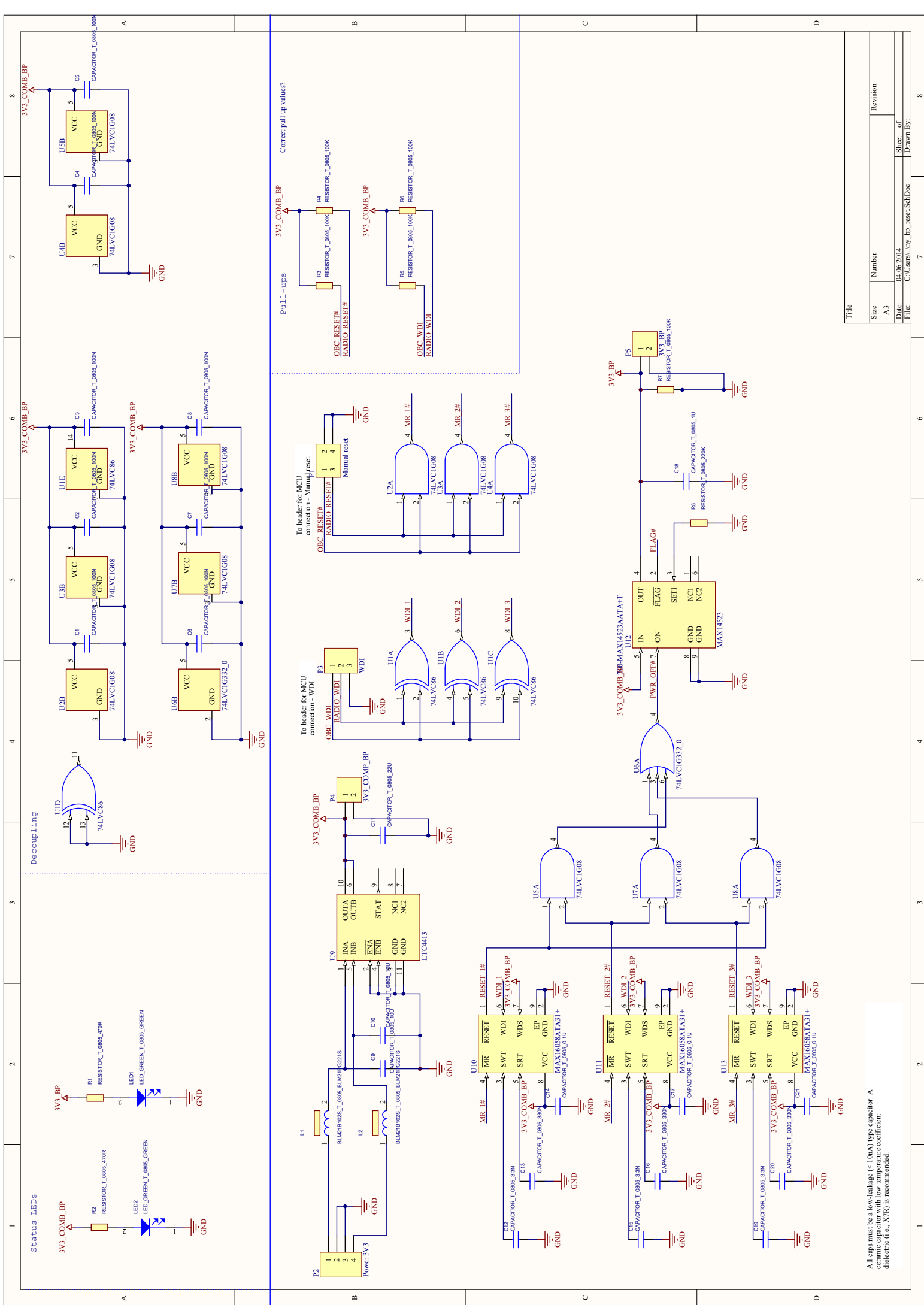- **Power supply:** TTi EL302RT Triple Power Supply Serial number: 350827

Figure F.1: Test setup showing power supply, oscilloscope, Atmel Xplained cards and evaluation card

Appendix G

Evaluation Card - Hardware Drawings

Figure G.1: Hardware drawings - TMR watchdog circuit

G.1   Additional TMR Watchdog Results

When attempting to drive the watchdogs' WDI inputs with two directly connected
lines at two different frequencies, the situation becomes as shown in Figure G.2.
The undefined levels of the two signals are as expected when driving one input
directly with two lines from two different sources. This is not sufficient for guaran-
teeing a high to low transition on the watchdogs' WDI inputs within their time-out
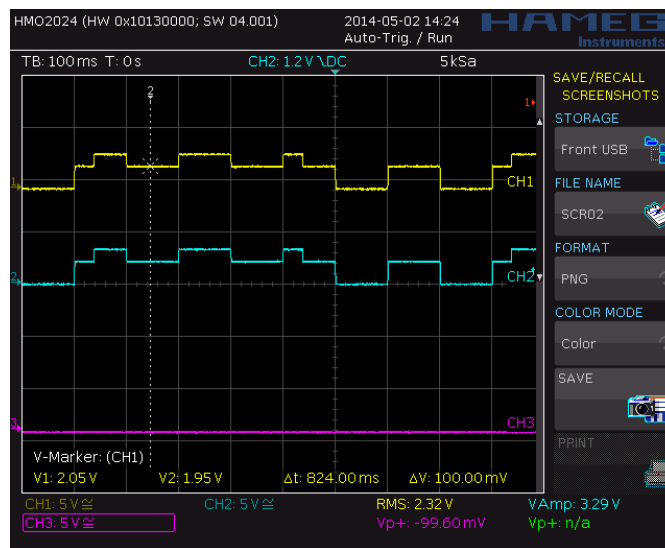period.

Figure G.2: Directly connecting two WDI lines together without an XOR-gate.
Lines toggling at different frequencies causing an undefined signal (CH1 & CH2),
disregard CH3

Propagation delay from a manual reset condition (CH2) to the voter output goes
low (CH1) was measured to 1.9 μs as seen in Figure G.3. This is the propagation
delay through three logic gates and one watchdog.

If both masters cease to toggle their WDI lines simultaneously, the watchdogs will
cause a reset as seen in Figure G.4.

The case where the 1.25 Hz WDI line remains active and the 5 Hz WDI line is
disabled can be seen in Figure G.5.

Measurements seen in Figure G.6 and G.7 shows time-out periods of 2.58 s and
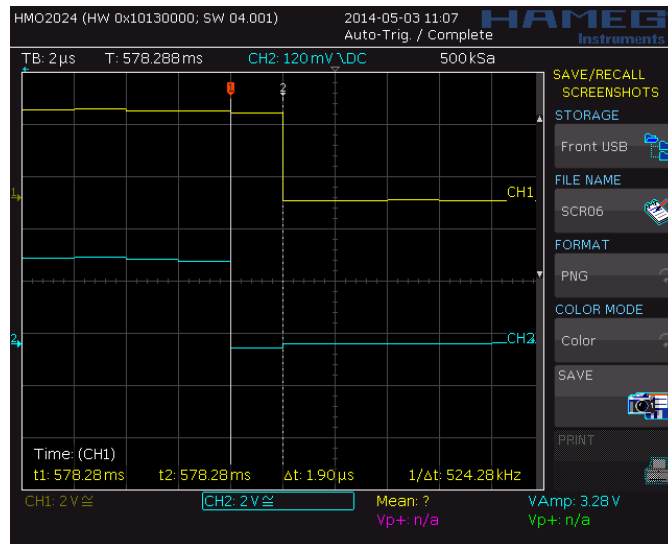3.28 s, respectively 25.98 % and 60.16 % higher than the typical value of 2.048 s.

Figure G.3: Propagation delay from manual reset transition (CH2) to voter output transition (CH1)
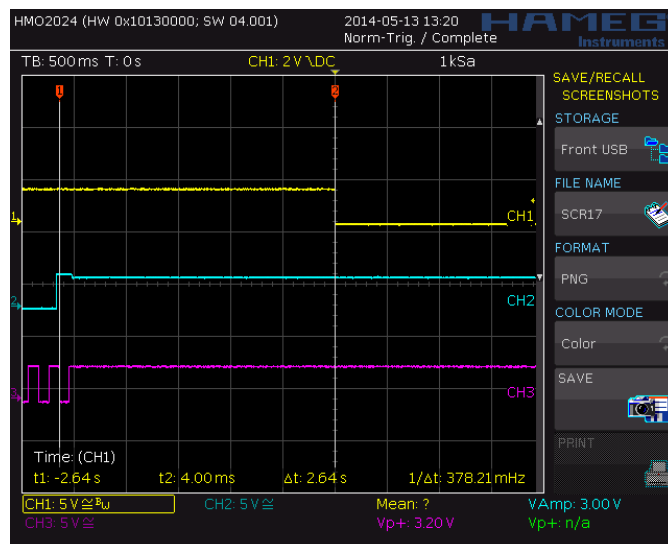

Figure G.4: Appendix - Watchdog time-out after both WDI lines cease to toggle - Voter output (CH1), WDI input lines (CH2 & CH3)
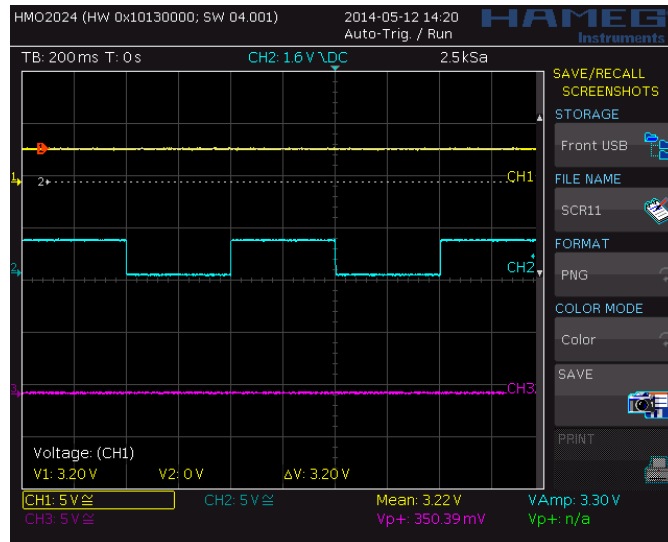
Figure G.5: Appendix - Voter output remains high with fast WDI line disabled - Voter output (CH1), WDI input lines (CH2 & CH3)
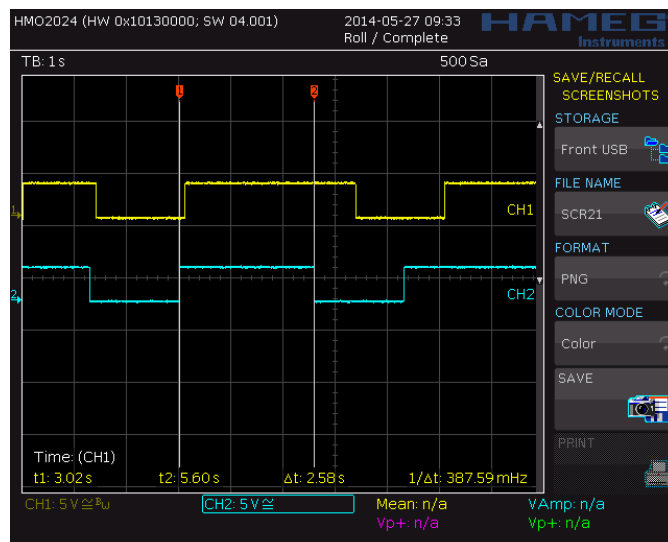

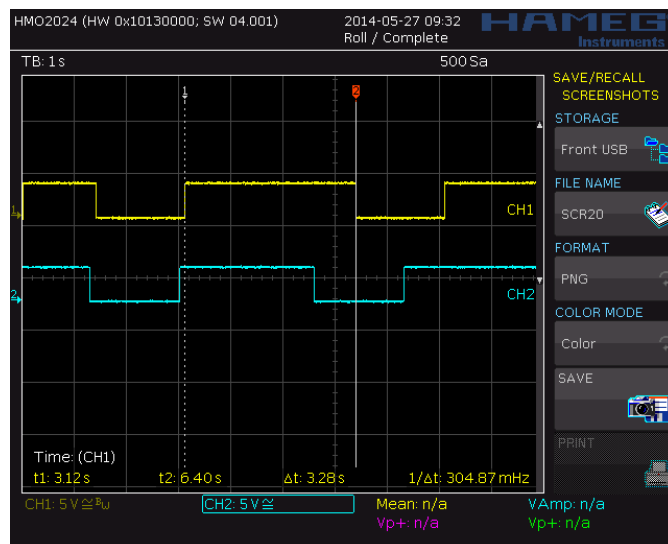Figure G.6: Appendix - Watchdog time-out period variations - chip specific

Figure G.7: Appendix - Watchdog time-out period variations - chip specific

G.2 Evaluation Card - Bill of Materials

Table G.1: Bill of materials

Footprint	Comment	Designator	Description	Quantity
T_0805	CAPACITOR_T_0805_100N	C1, C2, C3, C4, C5, C6, C7, C8	-	8
T_0805	CAPACITOR_T_0805_10U	C9, C10, C17	-	3
T_0805	CAPACITOR_T_0805_22U	C11	-	1
T_0805	CAPACITOR_T_0805_150N	C12, C15, C20	-	3
T_0805	CAPACITOR_T_0805_330N	C13, C16, C21	-	3
T_0805	CAPACITOR_T_0805_0.1U	C14, C18, C22	-	3
T_0805	CAPACITOR_T_0805_1U	C19	-	1
T_0805	BLM21B102S_T_0805_BLM21PG221S	L1, L2	-	2
T_0805	LED_GREEN_T_0805_GREEN	LED1, LED2	-	2
HDR2X2	Manual reset	P1	Header, 2-Pin, Dual row	1
HDR1X4	Power 3V3	P2	Header, 4-Pin	1
HDR1X3	WDI	P3	Header, 3-Pin	1
HDR1X2	3V3_COMP_BP	P4	Header, 2-Pin	1
HDR1X2	3V3_BP	P5	Header, 2-Pin	1
T_0805	RESISTOR_T_0805_470R	R1, R2	-	2
T_0805	RESISTOR_T_0805_100K	R3, R4, R5, R6, R7	-	5
T_0805	RESISTOR_T_0805_220K	R8	-	1
TSSOP14	74LVC86	U1	Quad 2-input EXCLUSIVE-OR gate	1
SOT23-5	74LVC1G08	U2, U3, U4, U5, U7, U8	Single 2-input AND gate	6
SOT23-6	74LVC1G332_0	U6	Single 3-input OR gate	1
DFN10	LTC4413	U9	Dual 2.6A, 2.5V to 5.5V, Ideal Diodes	1
T833+2	MAX16058ATA31+	U10, U11, U13	125nA Supervisory Circuit with Capacitor-Adjustable Reset and Watchdog Timeouts, open-drain reset, Watch-dog timer, 8-Pin TDFN, -40C to +125C, Pb-Free	3
TDFN8	MAX14523	U12	250mA to 1.5A, Adjustable Current-Limit Switches	1