FAULT MANAGEMENT FOR THE

WISE-HEADACHE INSTRUMENT (WHI)

# Introduction

Your spacecraft will fly the latest instrument from WISE[[1]](#footnote-1) Inc.: the much anticipated high-energy advanced detector with the actuator/capacitor/heater ensemble (HEAD-ACHE). Your team represents the fault-management, autonomy, and flight software engineers for the mission. You have been assigned the task of analyzing potential faults associated with the instrument, designing an autonomy system to keep the system safe, and implementing that autonomy system in flight software. Your engineering work will be evaluated in the context of a mission simulation that will attempt to make 6 observations with the instrument in a series of operational/environmental conditions.

# Learning goals

* Demonstrate the ability to reason about the possible real-world challenges associated with operating a science instrument in space.
* Become familiar with the types of monitoring autonomy and automation available in space systems to maintain the health of a spacecraft.
* Prototype in a flight-like environment autonomy to protect a reference science instrument.

# General Instrument Information

The WISE HEADACHE is a complex assembly consisting of the following physical components:

|  |  |
| --- | --- |
| Component | Description |
| Single-Board Computer | This is the computer that controls the instrument. |
| Active Thermal System | The HEADACHE uses an active thermal system to keep the instrument within prime operating temperatures. This system includes a heater to raise internal temperatures and a louver to lower internal temperatures. |
| Power System | HEADACHE is an active sensor and expends a large amount of energy to operate. As such, a secondary power system is included with the sensor. This power system comprises a redundant set of capacitors which are charged and used to power the instrument. HEADACHE cannot operate from spacecraft power alone. |
| Sensor Assembly | The HEADACHE sensing assembly is, itself, fairly mature and will not need additional autonomy. |

# States and Transition Sequences

## Instrument States

The instrument exists in one of four states at any given time, as identified in Table 1. These states are used to determine the capabilities of the instrument at a particular point in time. Flight software must consider the current state of the instrument before attempting to command it, otherwise instrument damage (or destruction) could occur.

Table – Instrument States

|  |  |
| --- | --- |
| State | Description |
| OFF | HEADACHE SBC and Power System are both powered down. Capacitors are at 0% charge. In this state, all reported telemetry other than the indicator that the instrument if off should be considered invalid. |
| POWERED | HEADACHE has powered on its SBC and power system. Capacitors are charging. |
| OBSERVING | HEADACHE is in the process of making an observation (recording data). Capacitors are discharging. |
| ERROR | HEADACHE has encountered an error and the error code is as reported in telemetry. The state of the instrument may be unknown and could place the instrument in a condition where it is damaged or destroyed. |

## Instrument State Machine

The transitions amongst states made by the instrument are illustrated in Figure 1. In this figure, circles represent instrument state (from Table 1) and arrows represent sequences of events that transition the instrument from being in one state or another. State transitions are not bidirectional.

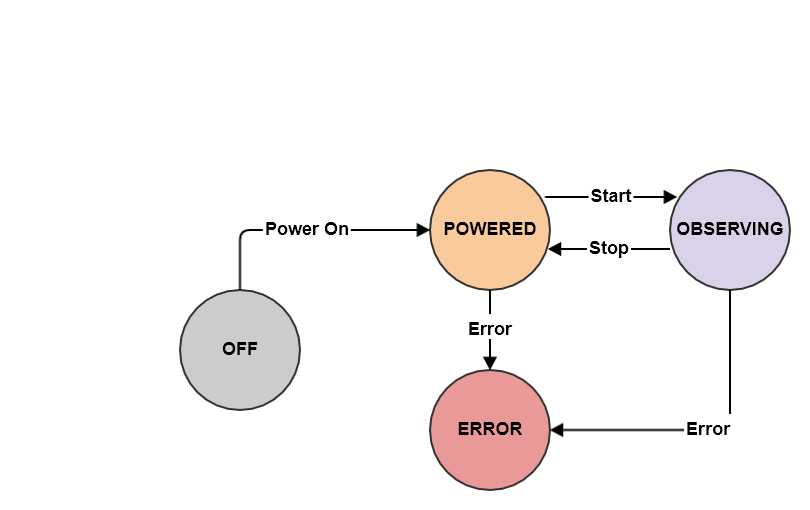


Figure - WHE State Diagram

## Transition Sequences

The instrument defines 6 transition sequences: PowerOn, Start, Stop, and Error.

|  |  |
| --- | --- |
| Transition | Description |
| PowerOn | Applies power to the instrument SBC which also starts the process of charging the instrument capacitors. The SBC takes 5 seconds to boot the SBC, after which the instrument transitions to the POWERED state. |
| Start | Begins an observation by opening the instrument door and starting the observation. Transitions to the OBSERVING state. |
| Stop | Ends an observation by stopping recording and closing the instrument door. Transitions to the READY state. |
| Error | On any cause of error, creates an error event and transitions to the ERROR state. |

# Manufacturer Caveats

WISE Inc. notes the following caveats when using the HEADACHE instrument.

## Power System Considerations

* The power system is directly connected to the spacecraft solar power and receives a constant energy feed whenever the instrument is powered. The capacitors cannot be “unplugged” so as to not charge.
* The instrument requires a large amount of power to operate and, therefore, must charge a local capacitor in order to take observations. The instrument cannot start an observation without enough charge to make an observation.
* The capacitors are not reliable. As such, there are two capacitors in the system. If one is not ready when it is time for an observation, the spare can be used, and vice versa.
* The capacitors are labelled A and B.
* Capacitor charge is measured in % of safe charge (0% - 100%). A capacitor may have a charge > 100% which means it is now charged beyond its safe limit. For each second that a capacitor has a charge > 100%, there is a ((charge-100)/2)% chance that the capacitor will explode and destroy the instrument. There is a ((charge-100))% chance that the capacitor will leak and damage the instrument. If a capacitor leaks or explodes, it can no longer be used.
* A special “discharge capacitor” command exists to prevent capacitor overcharge. It takes 3 seconds to start discharging. Once started, the capacitor cannot be used during the discharge cycle and the other capacitor charges at twice the rate. The capacitor discharges at a rate of 10% each second and continues until the capacitor reaches 0%.
* Capacitors continuously charge when not in use at a rate of 1% per second. If one capacitor is unavailable for some reason (broken, discharging, or leaking), the other charges at a rate of 2% per second during that time.
* If both capacitors are discharging at the same time, the instrument cannot handle the power into the system and has an 80% chance of being destroyed for each second that this condition persists.
* The capacitors heat when discharging. Each discharging capacitor adds 1 degree of heat for each second it is discharging.

## Thermal Considerations

* The instrument needs a strict thermal environment in order to take good observations and a slightly less thermal environment to stay safe. The internal temperature of the instrument must be between 10-20C to take usable observations. The safe operating environment for the instrument is 0-35C.
* For each degree outside of the safe operating temperature, the instrument has a 5% chance of being destroyed and a 20% chance of being damaged.
* A very reliable louver has been installed on the instrument, which can be commands “open” and “closed”. When closed, the louvers do not affect the internal temperature of the instrument. When opened, they reduce the internal temperature of the instrument by 5% each second.
* A very reliable heater has been installed on the instrument, which can be commanded “on” and “off”. When on, the heater increases the internal dissipation of the instrument by 10% each second.
* The impact of heaters and louvers start the second after they are applied.

## Observation Considerations

* An observation takes approximately 15 seconds to complete.
* An observation depletes the capacitor, losing 5% of total capacity for every second of observation.
* If the active capacitor goes below 5% charge during an observation, the instrument will be destroyed.
* When observing, the SBC temperature increases by 0.4 degree every second, in addition to any thermal contribution from capacitors.

# Instrument Commands

|  |  |  |
| --- | --- | --- |
| Command Op Code | Short Description | Value |
| WHE\_NOOP\_CC | Dummy command for testing | 0 |
| WHE\_CAP\_A\_ACTIVE\_CC | Sets Capacitor A as the active capacitor. | 1 |
| WHE\_CAP\_A\_DISCHARGE\_CC | Discharge Capacitor A. | 2 |
| WHE\_CAP\_B\_ACTIVE\_CC | Sets Capacitor B as the active capacitor. | 3 |
| WHE\_CAP\_B\_DISCHARGE\_CC | Discharge Capacitor B. | 4 |
| WHE\_OBS\_START\_CC | Start Observation | 5 |
| WHE\_OBS\_STOP\_CC | Stop Observation | 6 |
| WHE\_POWER\_SBC\_CC | Turn on SBC | 7 |
| WHE\_THERM\_HTR\_OFF\_CC | Turn off heater | 8 |
| WHE\_THERM\_HTR\_ON\_CC | Turn on heater | 9 |
| WHE\_THERM\_LOUVER\_CLOSE\_CC | Close louver | 10 |
| WHE\_THERM\_LOUVER\_OPEN\_CC | Open louver | 11 |
| WHE\_TLM\_RESET\_CNTS\_CC | Reset command counts. | 12 |

# Instrument Telemetry

The following data items are produced by the HEADACHE instrument.

|  |  |
| --- | --- |
| Description | Values |
| SBC State | OFF/POWERED/OBSERVING/ERROR |
| Instrument Damage | NONE/MINOR/MAJOR |
| Active Capacitor | CAP\_A / CAP\_B |
| Capacitor A State | CHARGING/LEAKING/DISCHARGING/BROKEN |
| Capacitor A Charge | # representing % of safe charge. |
| Capacitor B State | CHARGING/LEAKING/DISCHARGING/BROKEN |
| Capacitor B Charge | # representing % of safe charge. |
| Heater State | ON/OFF |
| Measured Temperature | # representing temp in degrees (as integer) |
| Louver State | OPEN/CLOSE |

# Project Artifacts

1. A fault tree of what could go wrong with the system
2. A listing of monitors and responses, in the template form.
3. Updated LC WDT and ADT tables
4. Project Presentation (20 minutes each)
5. Live demo

# Grading Breakdown

* Fault Tree: 20%
* Monitors/Responses Description: 20%
* CFS Implementation: 10%
* Project Presentation: 30%
* Project Demonstration: 20%
  + Proof of CFS life: 5%
  + Proof of commanding: 5%
  + Proof of telemetry downlink: 5%
  + Proof of complete run: 5%
  + Proof of observations: 1% \* # observations
  + Proof of no damage: -2%/damage counter
  + Proof of no destruction: -5% if destroyed.

# Code GitHub Account and Files

The code and documents needed for this assignment can be found at:

<https://github.com/NasaDtn/spacesystems>\_2018

1. **W**orst **I**nstrument **S**upplier **E**ver,Inc. [↑](#footnote-ref-1)