1 Twenty-two EPS MLTL Specifications

In our paper, we indicated that we elicited these twenty-two specifications according to the following patterns: operating range(OR), rate of change(RC), control sequence(CS), and physical model relationship(PMR). In this document, we identify the categorization of each specification we created along with giving a short description of how these specifications were elicited.

After the first thirty minutes, the 5V bus can be enabled. When it is enabled, it is implied that the bus is not overcurrenting and is supplying good power. (OR)

$$Atomic\ Propositions = \Big\{\phi \quad 5V\_Bus\_Current \leqslant 4A$$

$$G_{[360,M]}\{5V\_Bus\_Enabled \rightarrow (\phi \wedge 5V\_Power\_Good)\} \tag{1}$$

At all times, the 3.3V bus must be enabled as it directly powers the OBC. We also expect that this bus is not overcurrenting and is supplying good power. (OR)

$$Atomic\ Propositions = \Big\{\phi \quad 3.3V\_Bus\_Current \leqslant 4A$$

$$G_{[0,M]}\{\phi \wedge 3.3V\_Power\_Good \wedge 3.3V\_Bus\_Enabled\} \tag{2}$$

During the first thirty minutes after launch from the International Space Station (ISS), it is strictly required by the ISS that a CubeSat can only have its EPS and OBC subsystems powered on. During this time, all power buses (except for the 3.3 volt bus required for the OBC) and all enable signals must be in the off/disabled state. (CS)

$$\begin{aligned} G_{[0,360]}\{&\neg 5V\_Bus\_Enabled \wedge \neg LUP\_5V\_Bus\_Enabled \wedge \\ &\neg LUP\_3.3V\_Bus\_Enabled \wedge \neg ADCS\_Active \\ &\wedge \neg Payload\_Enabled \wedge \neg UHF\_Enabled \wedge \\ &\neg Boost\_Board\_Enabled\} \end{aligned} \tag{3}$$

At all times, the battery charge regulator(BCR) bus and raw battery bus should remain disabled. The CySat-I does not use these buses, and in order to save power, these buses should remain off. (CS)

$$G_{[0,M]}\{\neg BCR\_Bus\_Enabled \wedge \neg Battery\_Bus\_Enabled\} \tag{4}$$

The battery heaters have strict requirements of when they will turn off and on as defined in the EPS datasheet. These requirements are specified in equations 5-10. (PMR)

$$Atomic\ Propositions = \begin{cases} \phi & Battery\_Cell\_1\_Temp \leqslant 5^{\circ}C \\ \varphi & Battery\_Cell\_2\_Temp \leqslant 5^{\circ}C \\ \psi & Battery\_Cell\_3\_Temp \leqslant 5^{\circ}C \\ \sigma & Battery\_Cell\_4\_Temp \leqslant 5^{\circ}C \end{cases}$$

$$G_{[0,M]}\{(\phi \vee \varphi \vee \psi \vee \sigma) \rightarrow Heater\_1\_Enabled\} \tag{5}$$

$$Atomic\ Propositions = \begin{cases} \phi & Battery\_Cell\_1\_Temp \leqslant 1°C \\ \varphi & Battery\_Cell\_2\_Temp \leqslant 1°C \\ \psi & Battery\_Cell\_3\_Temp \leqslant 1°C \\ \sigma & Battery\_Cell\_4\_Temp \leqslant 1°C \end{cases}$$

$$G_{[0,M]}\{(\phi \vee \varphi \vee \psi \vee \sigma) \rightarrow Heater\_2\_Enabled\} \tag{6}$$

$$Atomic\ Propositions = \begin{cases} \phi & Battery\_Cell\_1\_Temp \leqslant -2°C \\ \varphi & Battery\_Cell\_2\_Temp \leqslant -2°C \\ \psi & Battery\_Cell\_3\_Temp \leqslant -2°C \\ \sigma & Battery\_Cell\_4\_Temp \leqslant -2°C \end{cases}$$

$$G_{[0,M]}\{(\phi \vee \varphi \vee \psi \vee \sigma) \rightarrow Heater\_3\_Enabled\} \tag{7}$$

$$Atomic\ Propositions = \begin{cases} \phi & Battery\_Cell\_1\_Temp > 8°C \\ \varphi & Battery\_Cell\_2\_Temp > 8°C \\ \psi & Battery\_Cell\_3\_Temp > 8°C \\ \sigma & Battery\_Cell\_4\_Temp > 8°C \end{cases}$$

$$G_{[0,M]}\{(\phi \wedge \varphi \wedge \psi \wedge \sigma) \rightarrow \neg Heater\_1\_Enabled\} \tag{8}$$

$$Atomic\ Propositions = \begin{cases} \phi & Battery\_Cell\_1\_Temp > 4°C \\ \varphi & Battery\_Cell\_2\_Temp > 4°C \\ \psi & Battery\_Cell\_3\_Temp > 4°C \\ \sigma & Battery\_Cell\_4\_Temp > 4°C \end{cases}$$

$$G_{[0,M]}\{(\phi \wedge \varphi \wedge \psi \wedge \sigma) \rightarrow \neg Heater\_2\_Enabled\} \tag{9}$$

$$Atomic\ Propositions = \begin{cases} \phi & Battery\_Cell\_1\_Temp > 1°C \\ \varphi & Battery\_Cell\_2\_Temp > 1°C \\ \psi & Battery\_Cell\_3\_Temp > 1°C \\ \sigma & Battery\_Cell\_4\_Temp > 1°C \end{cases}$$

$$G_{[0,M]}\{(\phi \wedge \varphi \wedge \psi \wedge \sigma) \rightarrow \neg Heater\_3\_Enabled\} \tag{10}$$

We should not see a large jump in the change in temperature. If we see a large jump, this is most likely due to a bad read value from the EPS. (RC)

$$Atomic\ Propositions = \begin{cases} \phi & |Battery\_Cell\_1\_Temp - Battery\_Cell\_1\_Temp_{i-1}| < 1°C \\ \varphi & |Battery\_Cell\_2\_Temp - Battery\_Cell\_2\_Temp_{i-1}| < 1°C \\ \psi & |Battery\_Cell\_3\_Temp - Battery\_Cell\_3\_Temp_{i-1}| < 1°C \\ \sigma & |Battery\_Cell\_4\_Temp - Battery\_Cell\_4\_Temp_{i-1}| < 1°C \end{cases}$$

$$G_{[0,M]}\{\phi \wedge \varphi \wedge \psi \wedge \sigma\} \tag{11}$$

We would expect the number of times the EPS to be under voltage to remain constant. If we see other behavior occur, then the EPS has experienced a new under voltage fault. (RC)

$$G_{[0,M]}\{Num\_Under\_Voltage_i == Num\_Under\_Voltage_{i-1}\} \tag{12}$$

We would expect the number of times the EPS to incur a short circuit to remain constant. If we see other behavior occur, then the EPS has experienced a new short circuit fault. (RC)

$$G_{[0,M]}\{Num\_Short\_Circuit_i == Num\_Short\_Circuit_{i-1}\} \tag{13}$$

We would expect the number of times the EPS to be over temperature to remain constant. If we see other behavior occur, then the EPS has experienced a new over temperature fault. (RC)

$$G_{[0,M]}\{Num\_Over\_Temp_i == Num\_Over\_Temp_{i-1}\} \tag{14}$$

The ADCS requires the boost board, LUP 3.3V bus, and the LUP 5V bus in order to power up all of its components. If any of these are not enabled properly, the ADCS cannot preform its main function. (PMR)

$$G_{[360,M]}\{ADCS\_Active \rightarrow (Boost\_Board\_Enabled \wedge LUP\_3.3V\_Bus\_Enabled \wedge LUP\_5V\_Bus\_Enabled\} \tag{15}$$

The UHF requires the LUP 3.3V bus as input in order to properly operate. Therefore, if the UHF is enabled, then it is implied that the LUP 3.3V bus is also enabled. (PMR)

$$G_{[360,M]}\{UHF\_Enabled \rightarrow LUP\_3.3V\_Bus\_Enabled\} \tag{16}$$

The boost board takes the 5 volts supplied by the EPS bus and amplifies it to 7.4 volts for the ADCS. If the boost board is enabled, then it is implied that the 5 volt bus is also enabled. (PMR)

$$G_{[360,M]}\{Boost\_Booard\_Enabled \rightarrow 5V\_Bus\_Enabled\} \tag{17}$$

The payload requires the 5V bus as input in order to properly operate. Therefore, if the payload is enabled, then it is implied that the 5V bus is also enabled. (PMR)

$$G_{[360,M]}\{Payload\_Enabled \rightarrow 5V\_Bus\_Enabled\} \tag{18}$$

Based on the current battery capacity, we are either in low power mode, or we are not in low power mode. This is defined in the concept of operations manual. (CS)

$$Atomic\ Propositions = \begin{cases} \phi & Battery\_Capacity \geqslant 8Wh \\ \varphi & Battery\_Capacity \leqslant 3Wh \end{cases}$$

$$G_{[0,M]}\{(\varphi \rightarrow Low\_Power\_Mode)\} \tag{19}$$

$$G_{[0,M]}\{(\phi \rightarrow \neg Low\_Power\_Mode)\} \tag{20}$$

As defined in the concept of operations manual, when we are in low power mode, the payload, ADCS, and boost board must be inactive. (CS)

$$G_{[360,M]}\{Low\_Power\_Mode \rightarrow (\neg Payload\_Enabled \wedge \neg ADCS\_Active \wedge \neg Boost\_Board\_Enabled)\} \tag{21}$$

The OBC communicates with the EPS over an I2C bus interface. We create a variable called I2C_Errors that will increment whenever the HAL I2C driver on the OBC indicates a I2C error. We will monitor this value within R2U2. If more than one error occurs within a time step, we reset the I2C bus in hopes to mitigate the problem. (RC)

$$G_{[0,M]}\{Num\_I2C\_Errors_i == Num\_I2C\_Errors_{i-1}\} \tag{22}$$

2 EPS Signals

Table 1 contains a list of the EPS signals that were inputted into R2U2. The signal number corresponds to how these signals were identified within our implementation of R2U2.

Table 1. Output Signals from the EPS

Signal	Description	Signal No.	Units
5V_Bus_Current	5V Bus Current	s0	A
5V_Power_Good	5V Power has a good status flag	s1	Boolean
5V_Bus_Enabled	5V Bus Enabled Flag	s2	Boolean
LUP_5V_Bus_Enabled	LUP 5V Bus Enabled Flag	s3	Boolean
3.3V_Bus_Current	3.3V Bus Current	s4	A
3.3V_Power_Good	3.3V Power has a good status flag	s5	Boolean
3.3V_Bus_Enabled	3.3V Bus Enabled Flag	s6	Boolean
LUP_3.3V_Bus_Enabled	LUP 3.3V Bus Enabled Flag	s7	Boolean
BCR_Bus_Enabled	BCR Output Bus Enabled Flag	s8	Boolean
Battery_Bus_Enabled	Raw Battery Output Enabled Flag	s9	Boolean
Battery_Temp_1	Battery Cell 1's temperature	s10	Celsius
Battery_Temp_2	Battery Cell 2's temperature	s11	Celsius
Battery_Temp_3	Battery Cell 3's temperature	s12	Celsius
Battery_Temp_4	Battery Cell 4's temperature	s13	Celsius
Heater_Enabled_1	Heater 1 Enabled Flag	s14	Boolean
Heater_Enabled_2	Heater 2 Enabled Flag	s15	Boolean
Heater_Enabled_3	Heater 3 Enabled Flag	s16	Boolean
Num_Under_Voltage	Number of times under voltage	s17	Integer
Num_Short_Circuit	Number of times a short circuit was observed	s18	Integer
Num_Over_Temp	Number of times over temperature	s19	Integer
ADCS_Active	ADCS is active	s20	Boolean
Payload_Enabled	Payload Enabled Flag	s21	Boolean
UHF_Enabled	UHF Enabled Flag	s22	Boolean
Boost_Board_Enabled	Boost Board Enabled Flag	s23	Boolean
Battery_Capacity	Current capacity of battery pack	s24	Wh
Low_Power_Mode	Satellite is currently in low power mode	s25	Boolean
I2C_Errors	The number of I2C errors	s26	Integer