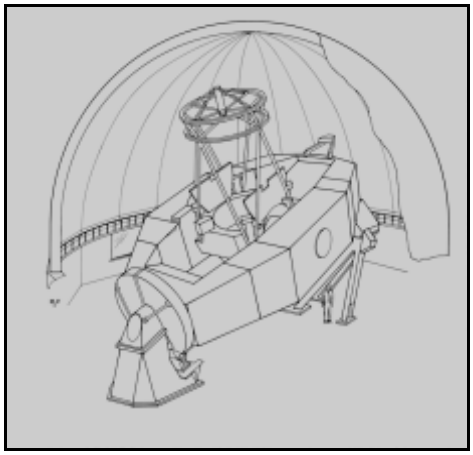
REV	DESCRIPTION	DATE	BY
-	Initial Release	4/4/08	EAW

T3-3004
Safety Board Hardware Description Document (HDD)
Revision: -



T3-3004 Rev -

University of Hawaii
Institute for Astronomy

FILENAME: T3-3004_Safety_Board_HDD.doc

LAST SAVE: 6/26/2008 4:14 PM

TABLE OF CONTENTS

TABLE OF FIGURES & REPORT TABLES

T3-3004 Rev -

1 HDD Overview

This hardware description document (HDD) explains the functions and the input and output signals of the Safety Board. The Safety Board revision at the time of this document creation was Rev C.

Also included is a section on known issues, severity of the issues, and how they may be resolved. Critical issues have been fixed. However, if another layout is ever done, there may be better ways to fix the issue in a new layout vs. the simple "green wire" modifications. For known issues that weren't severe and were not fixed, they are documented for future layout.

2 Safety Board Overview

The Safety Board has two main purposes:

1) To detect faults or inputs and disable the telescope.
   This protects personnel and the telescope. Hence, the name "Safety Board".

2) Contains an analog velocity circuit for TCS3 which ultimately provides the amplifier command.

3 Input and Output Signals

3.1 Connector P1 – Main Signal Inputs

Pin	Signal Name	I/O	Type	Level	Description
1	East Drive+	IN	Analog	+/- 25V	East tachometer. Negative terminal is reference. Scale factor is
2	East Drive-	IN		Differential	approximately 8.764 mV/(arcsec/s). 2000arcsec/s = ~17.5V.
3	AGND	-	GND	GND	
4	West Drive-	IN	Analog	+/- 25V	West tachometer. Negative terminal is reference. Scale factor is
5	West Driv+	IN		Differential	approximately 8.764 mV/(arcsec/s). 2000arcsec/s = ~17.5V.
6	AGND	-	GND	GND	
7	South Drive+	IN	Analog	+/- 25V	South tachometer. Negative terminal is reference. Scale factor
8	South Drive-	IN		Differential	is approximately 8.764 mV/(arcsec/s). 2000arcsec/s = ~17.5V.
9	AGND	-	GND	GND	
10	North Drive+	IN	Analog	+/- 25V	North tachometer. Negative terminal is reference. Scale factor
11	North Drive-	IN		Differential	is approximately 8.764 mV/(arcsec/s). 2000arcsec/s = ~17.5V.
12	AGND	-	GND	GND	
13	East Vel In	IN	Analog	0 - 10V	East motor PMAC velocity DAC output.
14	West Vel In	IN	Analog	0 - 10V	West motor PMAC velocity DAC output.
15	South Vel In	IN	Analog	0 - 10V	South motor PMAC velocity DAC output.
16	North Vel In	IN	Analog	0 - 10V	North motor PMAC velocity DAC output.
17	HA Vel Feedback	OUT	Analog	0 – 5V	Average of East and West tachometers. 596.83 arcscec/V
18	Dec Vel Feedback	OUT	Analog	0 – 5V	Average of North and South tachometers. 596.83 arcscec/V
19	Mtr Cntr Err	IN	Digital	0 – 5V	Driven by PC Parallel port. Not used. Set to 0V.
20	TCS Lockout	IN	Digital	0 – 5V	Driven by PC Parallel port. Not used. Set to 0V.
21	Brake En In	IN	Digital	0 – 5V	Driven by PC Parallel port. 0V=brake, 5V= brake disabled
22	Watchdog In	IN	Digital	0 – 5V	Driven by PC Parallel port. 5V=watchdog pulse
23	Reset	IN	Digital	0 – 5V	Driven by PC Parallel port. 0V=reset, 5V=not in reset mode
24	West Current	IN	Analog	0 – 10V	From NC307 amp. Scale factor is 11.66A/V.
25	East Current	IN	Analog	0 – 10V	From NC307 amp. Scale factor is 11.66A/V.
26	North Current	IN	Analog	0 – 10V	From NC307 amp. Scale factor is 11.66A/V.
27	South Current	IN	Analog	0 – 10V	From NC307 amp. Scale factor is 11.66A/V.
28	Dome1 Current	IN	Analog	0 – 10V	From NC307 amp. Scale factor is 11.66A/V.
29	Dome2 Current	IN	Analog	0 – 10V	From NC307 amp. Scale factor is 11.66A/V.
30	Dome3 Current	IN	Analog	0 – 10V	From NC307 amp. Scale factor is 11.66A/V.
31	Horizon Stop	IN	Switch	GND or open	Switch, Dec Emergency Stop, GND=OK, open=stop
32	HA Stop W	IN	Switch	GND or open	Switch, HA W Stop, GND=OK, open=stop
33	HA Stop E	IN	Switch	GND or open	Switch, HA E Stop, GND=OK, open=stop

34	HA Emerg W	IN	Switch	GND or open	Switch, HA W Emergency Stop, GND=OK, open=stop
35	HA Emerg E	IN	Switch	GND or open	Switch, HA E Emergency Stop, GND=OK, open=stop
36	Dec Stop N	IN	Switch	GND or open	Switch, Dec N Stop, GND=OK, open=stop
37	Dec Stop S	IN	Switch	GND or open	Switch, Dec S Stop, GND=OK, open=stop
38	Dec Emerg N	IN	Switch	GND or open	Switch, Dec N Emergency Stop, GND=OK, open=stop
39	Dec Emerg S	IN	Switch	GND or open	Switch, Dec S Emergency Stop, GND=OK, open=stop
40	Emerg Stop	IN	Switch	5V or open	Switch, Emergency Stop. Open=STOP, 5V=do not stop
41	TOP Dome Cntl	IN	Switch	5V or open	Switch, Dome under Software Control, open=Disable,
42	TOP Tel Enable	IN	Switch	5V or open	Switch, Telescope Enable, open=Disable, 5V=Enable
43	TOP Lm Overrride	IN	Switch	5V or open	Switch, Limit Override, open=Override Inactive, 5V=Override
44	HP Stop	IN	Switch	GND or open	Switch, Hand Paddle Stop button, GND=OK, Open=STOP
45	Spare In 1	IN	Switch	N/A	Not used, pulled up to VCC via 1kΩ
46	Spare In 2	IN	Switch	N/A	Not used, pulled up to VCC via 1kΩ
47	Spare In 3	IN	Switch	N/A	Not used, pulled up to VCC via 1kΩ
48	Spare In 4	IN	Switch	N/A	Not used, pulled up to VCC via 1kΩ
49	Spare In 5	IN	Switch	N/A	Not used, pulled up to VCC via 1kΩ
50	Spare In 6	IN	Switch	N/A	Not used, pulled up to VCC via 1kΩ

Table 1 Connector P1 – Main Signal Inputs

3.2 Connector P2 – Main Signal Outputs

Pin	Signal Name	I/O	Type	Level	Description
1	24V	IN	Power	24V	Power for relay output side.
2	Brake Enable Relay	OUT	Analog	Open or 24V	Relay output for brake. Open=enable, 24V=disable
3	East Tach Out	OUT	Analog	0 - 5.5 V	Buffered, filter East tachometer. ~1.845 mV/(arcsec/s)
4	Tel Amp	OUT	Analog	NA – relay	Relay connection for NC307 amplifier enable. When relays activated
5	Tel Amp Return	OUT		output	on Safety Board, closed contacts enable amplifiers.
6	Dome Amp	OUT	Analog	NA – relay	Relay connection for NC307 amplifier enable. When relays activated
7	Dome Amp Return	OUT		output	on Safety Board, closed contacts enable amplifiers.
8	West Tach Out	OUT	Analog	0 - 5.5 V	Buffered, filter West tachometer. ~1.845 mV/(arcsec/s)
9	South Tach Out	OUT	Analog	0 -5.5 V	Buffered, filter South tachometer. ~1.845 mV/(arcsec/s)
10	East Vel Out	OUT	Analog		East amplifier command voltage. 10.5A/V
11	AGND	-	GND	GND	
12	West Vel Out	OUT	Analog		West amplifier command voltage. 10.5A/V
13	AGND	-	GND	GND	
14	South Vel Out	OUT	Analog		South amplifier command voltage. 10.5A/V
15	AGND	-	GND	GND	
16	North Vel Out	OUT	Analog	-	North amplifier command voltage. 10.5A/V
17	AGND	-	GND	GND	
18	HA OS Latch	OUT	Digital	0 – 5V	HA overspeed fault latched. 0=no fault, 5V=fault.
19	Dec OS Latch	OUT	Digital	0 – 5V	HA overspeed fault latched. 0=no fault, 5V=fault.
20	West OC Latch	OUT	Digital	0 – 5V	West motor overcurrent fault latched. 0=no fault, 5V=fault.
21	East OC Latch	OUT	Digital	0 – 5V	East motor overcurrent fault latched. 0=no fault, 5V=fault.
22	North OC Latch	OUT	Digital	0 – 5V	North motor overcurrent fault latched. 0=no fault, 5V=fault.
23	South OC Latch	OUT	Digital	0 – 5V	South motor overcurrent fault latched. 0=no fault, 5V=fault.
24	Dome1 OC Latch	OUT	Digital	0 – 5V	Dome motor1 overcurrent fault latched. 0=no fault, 5V=fault.
25	Dome2 OC Latch	OUT	Digital	0 – 5V	Dome motor2 overcurrent fault latched. 0=no fault, 5V=fault.
26	Dome3 OC Latch	OUT	Digital	0 – 5V	Dome motor3 overcurrent fault latched. 0=no fault, 5V=fault.
27	Emerg Stop Latch	OUT	Digital	0 – 5V	Emergency Stop latched. 0=no fault, 5V=fault.
28	HP Stop Latch	OUT	Digital	0 – 5V	Hand Paddle Stop latched. 0=no fault, 5V=fault.
29	Mtr Cntr Err Latch	OUT	Digital	0 – 5V	Not used
30	TCS Lockout Latch	OUT	Digital	0 – 5V	Not used
31	HA Stop W Latch	OUT	Digital	0 – 5V	West travel stop 0=no fault, 5V=fault.
32	HA Stop E Latch	OUT	Digital	0 – 5V	East travel stop. 0V=no fault, 5V=fault
33	HA Emerg W Latch	OUT	Digital	0 – 5V	West travel emergency stop. 0V=no fault, 5V=fault
34	HA Emerg E Latch	OUT	Digital	0 – 5V	East travel emergency stop. 0V=no fault, 5V=fault
35	Dec Stop N Latch	OUT	Digital	0 – 5V	North travel stop 0=no fault, 5V=fault.
36	Dec Stop S Latch	OUT	Digital	0 – 5V	South travel stop 0=no fault, 5V=fault.
37	Dec Emerg N Latch	OUT	Digital	0 – 5V	North travel emergency stop. 0V=no fault, 5V=fault
38	Dec Emerg S Latch	OUT	Digital	0 – 5V	South travel emergency stop. 0V=no fault, 5V=fault

39	Horizon Stop Latch	OUT	Digital	0 – 5V	Horizon stop. 0V=no fault, 5V=fault
40	Watchdog Timer Latch	OUT	Digital	0 – 5V	No watchdog timer latched. 0=no fault, 5V=timer fault.
41	Spare Latch Out 1		Digital	0 – 5V	Not used
42	Spare Latch Out 2	OUT	Digital	0 – 5V	Not used
43	Spare Latch Out 3	OUT	Digital	0 – 5V	Not used
44	Spare Latch Out 4	OUT	Digital	0 – 5V	Not used
45	Spare Latch Out 5	OUT	Digital	0 – 5V	Not used
46	Spare Latch Out 6	OUT	Digital	0 – 5V	Not used
47	North Tach Out	OUT	Digital	0 - 5.5 V	Buffered, filter South tachometer. ~1.845 mV/(arcsec/s)
48	TOP Dome Cntl Handpaddle	OUT	Digital	0 – 5V	Dome Control switch. 0V=not handpaddle 5V=handpaddle control
49	TOP TCS Enable	OUT	Digital	0 – 5V	TO Panel TCS LED. 0V=OFF, 5V=ON
50	TOP Brake Enable Out	OUT	Digital	0 – 5V	TO Panel Brake LED. 0V=OFF, 5V=ON

Table 2 Connector P2 – Main Signal Outputs

3.3 Connector P3 - Power

Pin	Signal Name	I/O	Type	Level	Description
1	VCC	IN	Power	+5V	+5V Digital Power
2	DGND	-	GND	GND	Return for digital power.
3	+15V	IN	Power	+15V	+15V for op-amps, comparators, etc.
4	AGND	-	GND	GND	Return for analog power.
5	-15V	IN	Power	-15V	-15V for op-amps, comparators, etc.

Table 3 Connector P3 - Power

3.3 Connector P4 – Spare Differential Line Receiver

This connector consists of the inputs and outputs of a DS26LS32AC differential line receiver.

Pin	Signal Name	I/O	Type	Level	Description
1	OUT A	OUT	Digital	0 – 5V	Spare output.
2	IN A+	IN	Differential	-7 to +7V	Spare input.
3	OUT B	OUT	Digital	0 – 5V	Spare output.
4	IN A-	IN	Differential	-7 to +7V	Spare input.
5	OUT C	OUT	Digital	0 – 5V	Spare output.
6	IN B+	IN	Differential	-7 to +7V	Spare input.
7	OUT D	OUT	Digital	0 – 5V	Spare output.
8	IN B-	IN	Differential	-7 to +7V	Spare input.
9	NC	-	-	-	
10	IN C+	IN	Differential	-7 to +7V	Spare input.
11	NC	-	-	-	
12	IN C-	IN	Differential		Spare input.
13	VCC	OUT	Power	+5V	Output power, +5V.
14	IN D+	IN	Differential	-7 to +7V	Spare input.
15	DNGD	-	GND	GND	
16	IN D-	IN	Differential	-7 to +7V	Spare input.

Table 4 Connector P4 – Spare Differential Line Receiver

3.4 Connector JP1 – JTAG

Pin	Signal Name	I/O	Type	Level	Description
1	DGND	-	GND	GND	
2	VCC	OUT	Power	+5V	+5V used for JTAG connector power out.
3	DGND	-	GND	GND	
4	TMS	IN	Digital	0 – 3.3V	JTAG Test Mode Select
5	DGND	-	GND	GND	
6	TCK	IN	Digital	0 – 3.3V	JTAG Test Clock
7	DGND	-	GND	GND	
8	TDO	OUT	Digital	0 – 3.3V	JTAG Test Data Out
9	DGND	-	GND	GND	

T3-3004 Rev -

10	TDI	IN	Digital	0 – 3.3V	JTAG Test Data In
11	DGND	-	GND	GND	
12	NC	-	-	-	
13	DGND	-	GND	GND	
14	NC	-	-	-	

Table 5 Connector JP1 – JTAG

4 Analog Velocity Compensation Circuit

The analog velocity circuit can best be described with a very simple block diagram. This diagram does not show any filtering or any frequency dependent characteristics. The DEC axis is shown as an example. There is no adjustment for this circuitry.

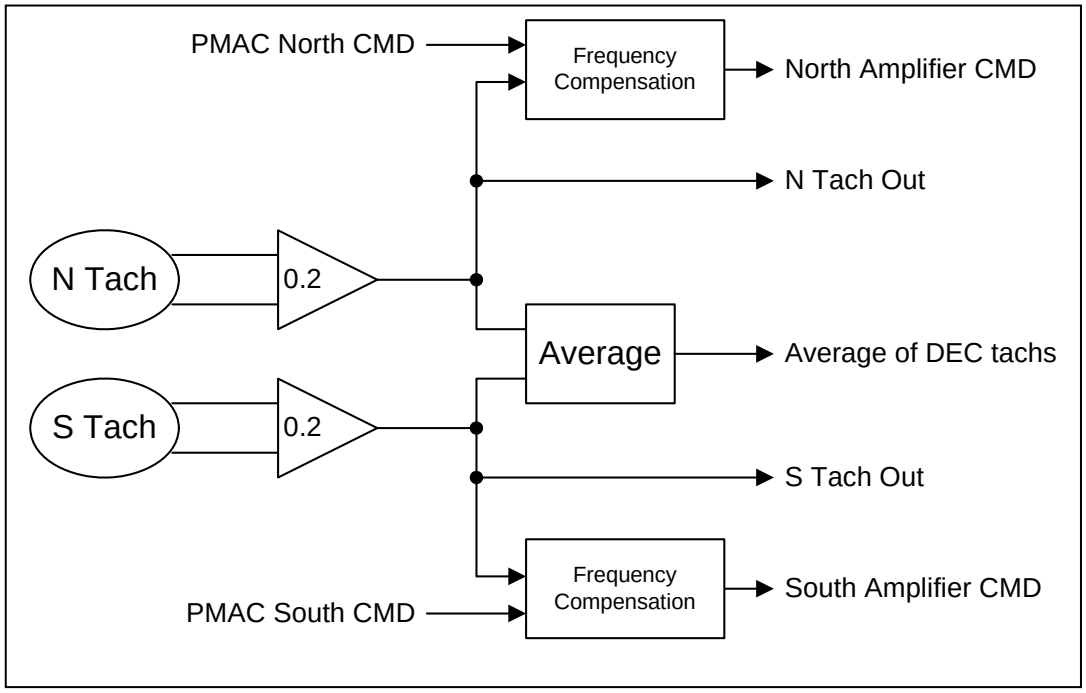


Figure 1 Simplified analog velocity circuitry block diagram

Essentially the velocity circuitry does 3 main things

1) Buffers and divides each tachometer input

2) Averages the tachometers together for one value to be used by the PMAC servo

3) Adds some frequency dependent compensation to the velocity command from the PMAC

5 Fault Detection & Control Inputs

The Safety Board detects various faults and accepts multiple control signals. These faults and control signals are used as inputs to logic programmed into a CPLD. The combination of those signals and faults determines the state of the four output signals.

T3-3004 Rev -

Signal Name	Connector	Pin	Description
Dome Enable	NA	On Board	Sinks current for (enables) Dome Amp Relay. 0V=ON, 5V=OFF
TOP TCS Enable	P2	49	Powers TO Panel Brake LED. 0V=OFF, 5V=ON
Tel Enable	NA	On Board	Sinks current for (enables) Brake Enable and Telescope Amp Relays. 0V=disable brakes, enable tel amp, 5V=enable brakes, disable tel amp
TOP Brake Enable Out	P2	50	Powers TO Panel Brake LED. 0V=OFF, 5V=ON

Table 6 CPLD output signals

The logic programmed into the CPLD can be seen in a schematic form in "T3-2071-Safety_CPLD_Logic.pdf". This schematic is shown below, but may be difficult to read.

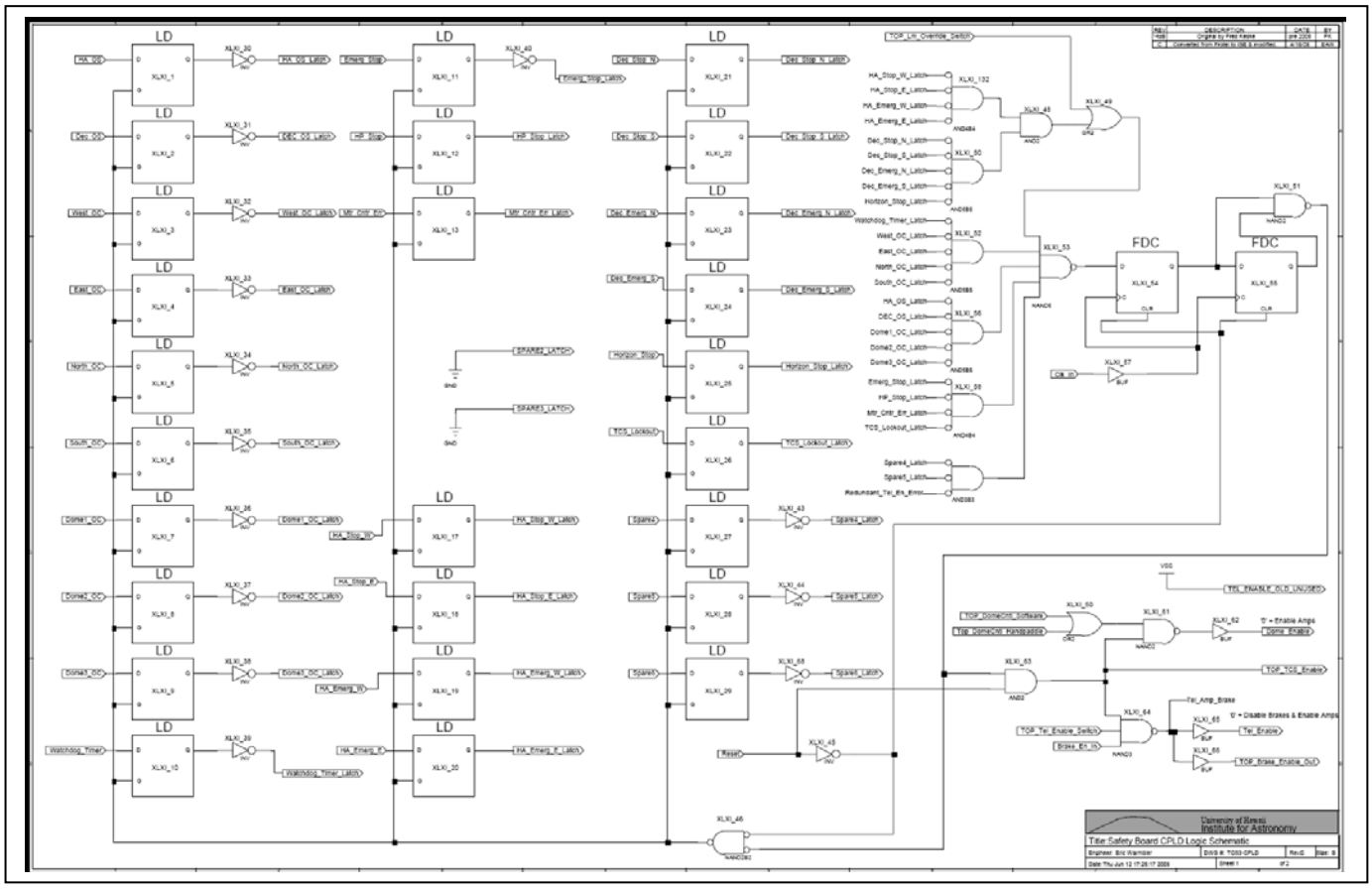


Figure 2 Completer CPLD logic schematic

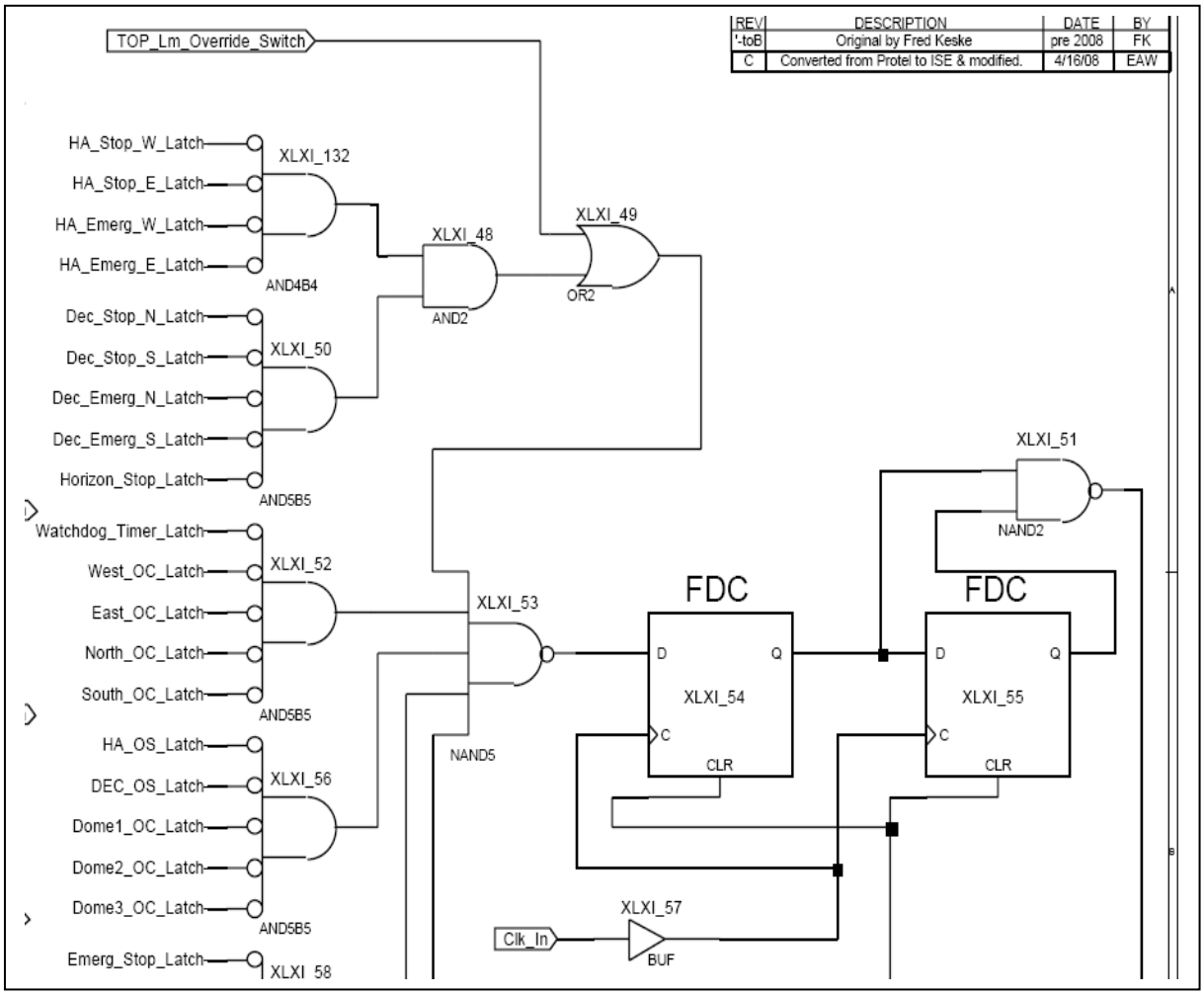


Figure 3 Zoom in of override faults and clock circuitry

From the zoomed in portion of the logic in Figure 3, it can be seen that ten faults can be overridden using TOP Limit Override and they consist of the HA and DEC axis stops, the Horizon Stop, and spare1. Notice XLXI_54 and XLXI_55. These D flip-flops load D into Q on a low to high transition. It takes two clock cycles from when a fault appears ("1") on the input of XLXI_54 to change the output of XLXI_51. The output of XLXI_51 latches all fault inputs and is the final fault signal that puts the CPLD output signals into fault states. This means that a fault must be present longer than a clock cycle, minimum, or 133 ms (1/7.5Hz).

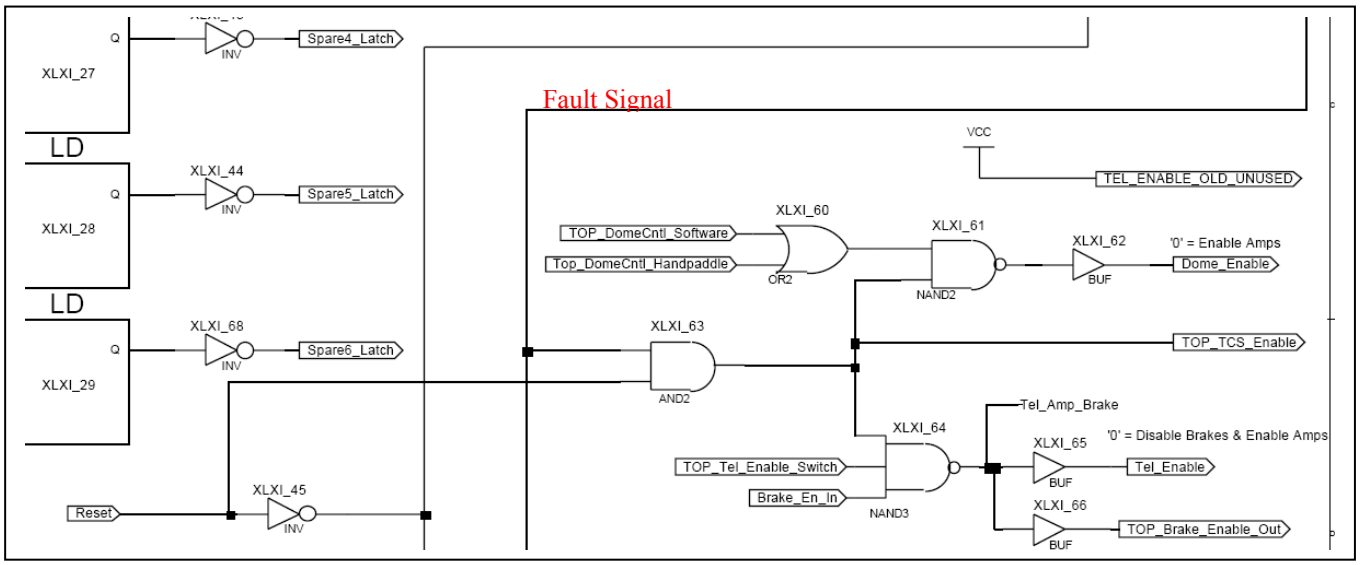


Figure 4 Zoom in of CPLD output signals.

Looking at Figure 4, a Reset state of "0" or a Fault Signal state of "0" will cause all of the CPLD's outputs to go into fault states. Fault states put all outputs to "1" except "TOP TCS Enable", which goes to "0".

If there is no fault or reset and if "TOP_DomeCntl_Software" or "Top_DomeCntl_Handpaddle" is a logic "1", then the "Dome Enable" signal will go low and activate a relay enabling the dome amplifiers.

If there is no fault or reset and if "TOP Tel Enable Switch" or "Brake En In" go to a logic "0", then "Tel Enable" will go to logic "1" and turn off the relay that enables the amplifier and will also turn off the relay that disables the brakes (brakes now ON). The "TOP_Brak_Enable_Out" will become a logic "1" and power the Brake LED on the TO panel.

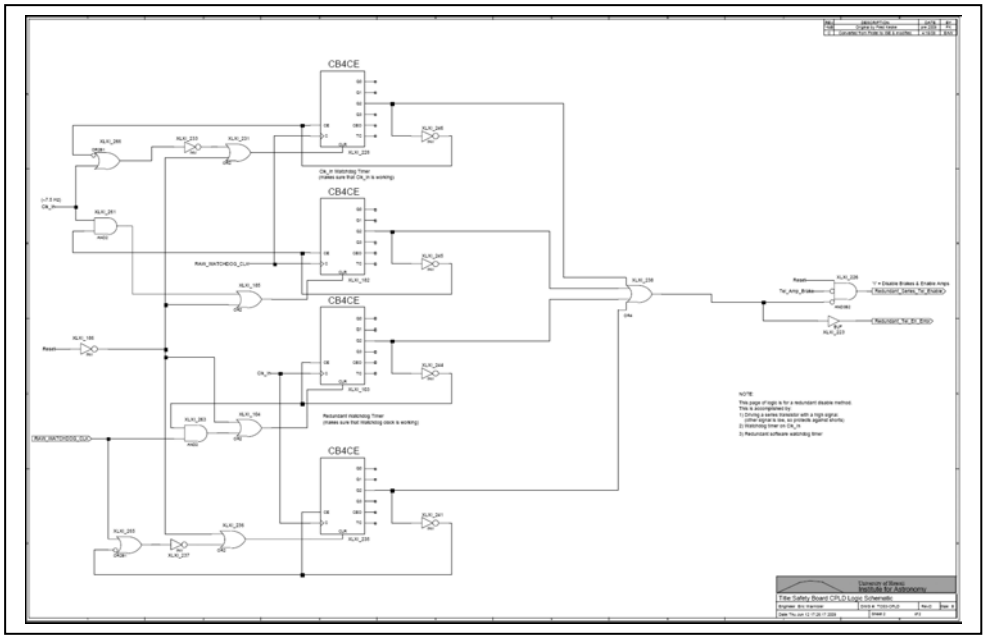


Figure 5 Redundant Tel_Enable Logic

The redundant Tel_Enable signal is controlled by 3 signals. The Reset and Tel_Amp_Brake signals are simply ANDed together. The last signal is the the ORing of two watchdog timers.

T3-3004 Rev -

There are two clock signals – Clk_In and RAW_WATCHDOG_CLK. The Clk_In is the local oscillator on the Safety Board and the RAW_WATCHDOG_CLK is the watchdog clock from the parallel port of the TCS3 PC. These two clocks are used to form two watchdog timers that essentially check each other. If either clock is removed, an error will occur. The final output signal is logic high, which is opposite of the active logic low signal on the main Tel_Enable signal. Having opposite logic enable signals reduces that chance of a fault state not disabling the telescope.

5.1 Adjustable, Analog Faults

There are overspeed and overcurrent faults that are adjustable via potentiometers. The table below lists the faults that are adjustable.

Fault Name	Type	Description
HA_Overspeed	Overspeed	HA Axis overspeed.
Dec_Overspeed	Overspeed	DEC Axis overspeed.
West_Overcurrent	Overcurrent	West motor overcurrent.
East_Overcurrent	Overcurrent	East motor overcurrent.
North_Overcurrent	Overcurrent	North motor overcurrent.
South_Overcurrent	Overcurrent	South motor overcurrent.
Dome1_Overcurrent	Overcurrent	Dome motor1 overcurrent.
Dome2_Overcurrent	Overcurrent	Dome motor2 overcurrent.
Dome3_Overcurrent	Overcurrent	Dome motor3 overcurrent.

Table 7 Adjustable analog faults

6 Miscellaneous Circuits

6.1 Relays

There are three relays. Two realys enable/disbale the amplifiers for the telescope and dome. The other relay enables/disables the telescope brakes.

6.2 Watchdog Timer

The watchdog timer receives a pulse from the TCS3 PC via a parallel port. It has a time delay of 600 ms. A high to low transition resets the timer. If another high to low transition does not occur within 600 ms, the watchdog timer with go to a logic low (reset) state.

6.3 CPLD Latch Clock

A 7.5 Hz clock is used as an input into the CPLD for the transparent latches contained in the CPLD logic.

7 Known Issues / Recommendations

7.1 Comparator Output Logic Level Mismatch

Severity: High
Status: Board Modified, Problem Fixed

Issue
The comparators had an output logic of -15V and +5V (through a pullup resistor). The reason that the logic level was -15V was because the comparators had to sense positive and negative values and therefore had +/-15V supplies. This was perfectly fine. However, the outputs of the comparators were directly connected to the CPLD. It required logic of 0 or +5V. The -15V on the CPLD forward biased the protection diodes on the CPLD pin inputs. This in turn put the comparators in a current limited state and caused the CPLD to dissipate the power of the diode drop multiplied by the current pulled through the comparator.

Fix
The CPLD can withstand -0.5V minimum, which is right below the forward diode drop. The easiest solution to implement on the existing boards was to create a -0.7 V "power supply". This supply was nothing more than a resistor and a diode clamp since a large amount of current was not necessary. With an actual supply of around -0.65V, and a drop of around 150mV for the comparator output, the input signal was very close to -0.5V. Since error signals are only present for a short time, this should not stress the CPLD. Changing the supply also required lowering the reference voltages from +/-1V to +/-0.44 V.

Relayout Suggestion
If relaying out the board, using -15V for the comparators with some type of level shifter buffer after the output would be preferable.

7.2 Faults Detected by TCS3 With No Latched Faults

Severity: Very Low, Informative
Status: No changes to Safety Board

Issue
The CPLD uses transparent latches that latch when the 7.5 Hz external clock transitions from high to low. A transparent latch allows the input to pass through to the output while the clock is high and latches the value on the input to the output when the clock goes high to low. Furthermore, the fault signal must remain for an entire clock cycle for the safety board to enter a fault state. If a fault condition occurs for a short period of time, less than 133ms (1/7.5Hz), the TCS3 OPTO22 modules which monitor all fault outputs will report a fault, but the Safety Board will not enter a fault state. This acts as a filter that will filter out small glitches. All fault inputs to the Safety Board will be slow, long term faults much greater than 133ms. So, if errors "blip" on the TCS3 control screen, this is why.

7.3 Overcurrent and Overspeed Comparators Trip Points Not Symmetrical

Severity: Medium
Status: Overspeed circuits modified, Overcurrent unmodified

Issue
The comparator circuits for the overspeed and overcurrent are not driven be low impedance drivers. Instead, they are driven by a resistor divider. Since the negative trip point is not high impedance, loading on the resistor divider occurs. This translates into unsymmetrical trip points, that is, the positive and negative magnitudes are not the same. For the overcurrent comparators, this is actually acceptable. The motors are only driven in one direction, so current only flows in one direction. Therefore, requiring a larger (or smaller) value in the opposite direction doesn't matter. It still trips on catastrophic (i.e. short) overcurrent conditions.

Fix
The Overspeed comparators need to be more symmetrical. The dividers were reduced in value from a total of 60kΩ to 2kΩ. This reduced the loading error and made the outputs more symmetrical, but not perfectly.

Relayout Suggestion
If relaying out the board, place a buffer such as an op-amp follower with a gain of one in between the voltage divider and the comparator circuit.

7.4 Relays

Severity: Medium
Status: Board modified, CPLD logic modified

Issue
The Brake Enable and Telescope Amplifier relays are driven by the same active low signal. If

T3-3004 Rev -

a short occurred on this signal, then the telescope would have no brakes and the amplifiers would be enabled. This is the normal condition when the servo is in operation. However, if the servo exits due to an error or if the Safety Board (which ultimately sends the command to the amplifier) has some fault which results in an unexpected command, then the telescope will not be under control.

Fix
An NPN transistor was added in series with the current active low output signal. The NPN transistor is driven with a logic high signal from the CPLD. Two signals with opposite logic greatly reduce the probability of a fault or failure occurring that does not disable the amplifiers and turn of the brakes. Furthermore, the new redundant signal is controlled by additional, unrelated input. In this case, watchdog timers monitoring the two clock signals were used.

Relayout Suggestion
If relaying out the board, two relays in series for the brake signal, each controlled by completely separate signal could be implemented. One step beyond that would be having one of the relays controlled by a pulse. This pulse could be of a fixed frequency, filtered, and then used with a diode and capacitor to create a charge pump.

7.5 Miscellaneous

Severity: Low
Status: No changes to Safety Board

Relayout Suggestion
If relaying out the board, there are some minor additions that may be preferable. They are not absolutely necessary, but may provide a more robust design.

1) Schmitt Triggers on switch inputs after the filter provide clean digital signals.

2) When driving off board signals from and CPLD or FPGA, a buffer may be good idea to protect the CPLD against shorts, and to provide the current to external loads such as LEDs.

3) Bias current canceling resistors on grounded op-amp terminals are desirable.