Appendix A. SCR Models and Analyses: DCIU Fault Protection

List of Tables:

Table A-1. DCIU Specification Editor
Table A-2. DCIU Type Dictionary
Table A-3. DCIU Mode Class Dictionary
Table A-4. DCIU Constant Dictionary
Table A-5. DCIU Variable Dictionary
Table A-6. DCIU Specification Assertion Dictionary
Table A-7. DCIU Condition Table for term_OVERPRESSURE_IN_PLENUM_TANK
Table A-8. DCIU Condition Table for term_UNDERPRESSURE_IN_PLENUM_TANK
Table A-9. DCIU Condition Table for con_CLOSE_LV3
Table A-10. DCIU Condition Table for con_CLOSE_LV4
Table A-11. DCIU Condition Table for con_OPEN_LV5
Table A-12. DCIU Condition Table for con_REGULATOR_1
Table A-13. DCIU Condition Table for con_REGULATOR_2
Table A-14. DCIU Mode Transition Table for smLatchValve3
Table A-15. DCIU Mode Transition Table for PressureMeasured
Table A-16. DCIU Dependency Graph Browser
Table A-17. DCIU Simulator - 1
Table A-18. DCIU Simulator - 2

Table A-1. DCIU Specification Editor

Table A-2. DCIU Type Dictionary

Name	Base Type	Units	Legal Values	Comment
Boolean	Enumerated		TRUE, FALSE	
Character				
Command	Enumerated	N/A	Issued, NotIssued	
Enumerated				
Float				
Integer				
ModeClass				
Plenum_Transducer	Enumerated	N/A	Main, Cathode	Ref: ND-310, FP
String				
Temperature	Float	degrees	[0,1000]	Ref: ND-310, FP. Range is stubbed.
Transducer_Pressure	Float	psia	[0,400]	Ref: ND-310, FP. Range is stubbed.

Table A-3. DCIU Mode Class Dictionary

Name	Modes	Initial Mode	Table?	Comment
PressureMeasured	On	On	Yes	Placeholder to use overpressure as a term.
smLatchValve3	sLV3Open, sLV3ClosedOK, sLV3LeakingOrFailed	sLV3ClosedOK	Yes	ND-310 inconsistent whether internal fault protection required only for LV5 or for LV3, LV4, and LV5 Note that the states of the LV being ClosedLeaking and the LV having failed are combined into one state since the FP can not distinguish these two states. LV3 open in thruster-firing mode (ND-310).
smLatchValve4	sLV4Open, sLV4ClosedOK, sLV4LeakingOrFailed	sLV4ClosedOK	Yes	ND-310 inconsistent whether internal fault protection required only for LV5 or for LV3, LV4, and LV5 Note that the states of the LV being ClosedLeaking and the LV having failed are combined into one state since the FP can not distinguish these two states.
smLatchValve5	sLV5Open,sLV5Closed	sLV5Closed	Yes	

Table A-4. DCIU Constant Dictionary

Name	Class	Type	Value	Comment
OVERPRESSURE_THRESHOLD	Constant	Transducer_Pressure	250.5	Initial value is a guess. ND-310 definesOverpressure as nominal + 0.5psi. Note that there is currently a very narrow(0.7 psi) gap between underpressure andoverpressure. Further analysis may beneeded to avoid excessive triggering offault protection.
UNDERPRESSURE_THRESHOLD	Constant	Transducer_Pressure	249.8	Initial value is a guess. ND-310 definesUnderpressure as nominal - 0.2 psi.

Table A-5. DCIU Variable Dictionary

Name	Class	Type	Initial Value	Accuracy	Table?	Comment
con_CLOSE_LV3	Controlled	Command	NotIssued		Yes	
con_CLOSE_LV4	Controlled	Command	NotIssued		Yes	
con_OPEN_LV5	Controlled	Command	NotIssued		Yes	
con_REGULATOR_1	Controlled	Command	NotIssued		Yes	
con_REGULATOR_2	Controlled	Command	NotIssued		Yes	
mon_CATHODE_PLENUM_USED	Monitored	Boolean	False		No	If false, Main Plenum Tank used.
mon_LV3_CLOSE_ISSUED	Monitored	Boolean	False		No	
mon_LV4_CLOSE_ISSUED	Monitored	Boolean	False		No	
mon_LV5_OPEN_ISSUED	Monitored	Boolean	False		No	
mon_MAIN_PLENUM_USED	Monitored	Boolean	True		No	If false, Cathode Plenum Tank used.
mon_PRESSURE_TRANSDUCER_PA1	Monitored	Transducer_Pressure	250.0		No	In Main plenum transducer set
mon_PRESSURE_TRANSDUCER_PA2	Monitored	Transducer_Pressure	250.0		No	In Main plenum transducer set
mon_PRESSURE_TRANSDUCER_PA3	Monitored	Transducer_Pressure	250.0		No	In Main plenum transducer set
mon_PRESSURE_TRANSDUCER_PA4	Monitored	Transducer_Pressure	250.0		No	In Cathode plenum transducer set
mon_PRESSURE_TRANSDUCER_PA5	Monitored	Transducer_Pressure	250.0		No	In Cathode plenum transducer set
mon_PRESSURE_TRANSDUCER_PA6	Monitored	Transducer_Pressure	250.0		No	In Cathode plenum transducer set
term_OVERPRESSURE_	Term	Boolean	False		Yes	ND-310 requires

IN_PLENUM_TANK						detection & response to this fault within the XFS
term_UNDERPRESSURE_IN_PLENUM_TANK	Term	Boolean	False		Yes	ND-310 requires detection & response to this fault within the XFS

Table A-6. DCIU Specification Assertion Dictionary

Name	D/E?	Expression	Comment
aSafe1	E	con_CLOSE_LV3 = Issued OR NOT term_OVERPRESSURE_IN_PLENUM_TANK	Asserts that fault protection only issues a command to close Latch Valve 3 when an overpressure condition does exist.
aSafe2	E	con_CLOSE_LV4 = Issued OR NOTterm_UNDERPRESSURE_IN_PLENUM_TANK	Asserts that fault protection only issues a command to close Latch Valve 4 when an underpressure condition does exist.

Table A-7. DCIU Condition Table for term_OVERPRESSURE_IN_PLENUM_TANK

Name		Mode Class
term_OVERPRESSURE_IN_PLENUM_TANK		PressureMeasured
Modes	**Conditions**	
On	((mon_PRESSURE_TRANSDUCER_PA1 + mon_PRESSURE_TRANSDUCER_PA2 + mon_PRESSURE_TRANSDUCER_PA3) /3 > OVERPRESSURE_THRESHOLD AND mon_MAIN_PLENUM_USED) OR((mon_PRESSURE_TRANSDUCER_PA4 + mon_PRESSURE_TRANSDUCER_PA5 + mon_PRESSURE_TRANSDUCER_PA6) /3 > OVERPRESSURE_THRESHOLD AND mon_CATHODE_PLENUM_USED)	NOT (((mon_PRESSURE_TRANSDUCER_PA1 + mon_PRESSURE_TRANSDUCER_PA2 + mon_PRESSURE_TRANSDUCER_PA3) /3 > OVERPRESSURE_THRESHOLD AND mon_MAIN_PLENUM_USED) OR((mon_PRESSURE_TRANSDUCER_PA4 + mon_PRESSURE_TRANSDUCER_PA5 + mon_PRESSURE_TRANSDUCER_PA6) /3 > OVERPRESSURE_THRESHOLD AND mon_CATHODE_PLENUM_USED))
term_OVERPRESSURE_IN_PLENUM_TANK =	True	False
Description		
Voting logic for transducers not specified here.		

Table A-8. DCIU Condition Table for term_UNDERPRESSURE_IN_PLENUM_TANK

Name		Mode Class
term_UNDERPRESSURE_IN_PLENUM_TANK		PressureMeasured
Modes	**Conditions**	
On	((mon_PRESSURE_TRANSDUCER_PA1 + mon_PRESSURE_TRANSDUCER_PA2 + mon_PRESSURE_TRANSDUCER_PA3) /3 < UNDERPRESSURE_THRESHOLD AND mon_MAIN_PLENUM_USED) OR((mon_PRESSURE_TRANSDUCER_PA4 + mon_PRESSURE_TRANSDUCER_PA5 + mon_PRESSURE_TRANSDUCER_PA6) /3 < UNDERPRESSURE_THRESHOLD AND mon_CATHODE_PLENUM_USED)	NOT(((mon_PRESSURE_TRANSDUCER_PA1 + mon_PRESSURE_TRANSDUCER_PA2 + mon_PRESSURE_TRANSDUCER_PA3) /3 < UNDERPRESSURE_THRESHOLD AND mon_MAIN_PLENUM_USED) OR((mon_PRESSURE_TRANSDUCER_PA4 + mon_PRESSURE_TRANSDUCER_PA5 + mon_PRESSURE_TRANSDUCER_PA6) /3 < UNDERPRESSURE_THRESHOLD AND mon_CATHODE_PLENUM_USED))
term_UNDERPRESSURE_IN_PLENUM_TANK =	True	False

Table A-9. DCIU Condition Table for con_CLOSE_LV3

Name		Mode Class
con_CLOSE_LV3		smLatchValve3
Modes	**Conditions**	
sLV3LeakingOrFailed	term_OVERPRESSURE_IN_PLENUM_TANK	NOT term_OVERPRESSURE_IN_PLENUM_TANK
sLV3Open,sLV3ClosedOK	term_OVERPRESSURE_IN_PLENUM_TANK	NOT term_OVERPRESSURE_IN_PLENUM_TANK
con_CLOSE_LV3 =	Issued	NotIssued
Description		
Confirm accuracy of this with domain specialist: specs allow Overpressure to cause command to close LatchValve to be issued without determination that LV is leaking or failed.		

Table A-10. DCIU Condition Table for con_CLOSE_LV4

Name		Mode Class
con_CLOSE_LV4		smLatchValve4
Modes	**Conditions**	
sLV4LeakingOrFailed	term_UNDERPRESSURE_IN_PLENUM_TANK	NOT term_UNDERPRESSURE_IN_PLENUM_TANK
sLV4Open,sLV4ClosedOK	term_UNDERPRESSURE_IN_PLENUM_TANK	NOT term_UNDERPRESSURE_IN_PLENUM_TANK
con_CLOSE_LV4 =	Issued	NotIssued

Table A-11. DCIU Condition Table for con_OPEN_LV5

Name		Mode Class
con_OPEN_LV5		smLatchValve5
Modes	**Conditions**	
sLV5Closed	term_UNDERPRESSURE_IN_PLENUM_TANK OR term_OVERPRESSURE_IN_PLENUM_TANK	NOT term_UNDERPRESSURE_IN_PLENUM_TANK AND NOT term_OVERPRESSURE_IN_PLENUM_TANK
sLV5Open	term_UNDERPRESSURE_IN_PLENUM_TANK OR term_OVERPRESSURE_IN_PLENUM_TANK	NOT term_UNDERPRESSURE_IN_PLENUM_TANK AND NOT term_OVERPRESSURE_IN_PLENUM_TANK
con_OPEN_LV5 =	Issued	NotIssued

Table A-12. DCIU Condition Table for con_REGULATOR_1

Name		Mode Class
con_REGULATOR_1		smLatchValve4
Modes	**Conditions**	
sLV4LeakingOrFailed	term_UNDERPRESSURE_IN_PLENUM_TANK	NOT term_UNDERPRESSURE_IN_PLENUM_TANK
sLV4ClosedOK, sLV4Open	term_UNDERPRESSURE_IN_PLENUM_TANK	NOT term_UNDERPRESSURE_IN_PLENUM_TANK
con_REGULATOR_1 =	Issued	NotIssued

Table A-13. DCIU Condition Table for con_REGULATOR_2

Name		Mode Class
con_REGULATOR_2		smLatchValve3
Modes	**Conditions**	
sLV3LeakingOrFailed	term_OVERPRESSURE_IN_PLENUM_TANK	NOT term_OVERPRESSURE_IN_PLENUM_TANK
sLV3ClosedOK,sLV3Open	term_OVERPRESSURE_IN_PLENUM_TANK	NOT term_OVERPRESSURE_IN_PLENUM_TANK
con_REGULATOR_2 =	Issued	NotIssued

Table A-14. DCIU Mode Transition Table for smLatchValve3

Source Mode	Events	Destination Mode
sLV3Open	Never	sLV3LeakingOrFailed
sLV3Open	@T(mon_LV3_CLOSE_ISSUED)	sLV3ClosedOK
sLV3ClosedOK	@T(term_OVERPRESSURE_IN_PLENUM_TANK)	sLV3LeakingOrFailed
sLV3ClosedOK	Never	sLV3Open
sLV3LeakingOrFailed	Never	sLV3Open
sLV3LeakingOrFailed	@F(term_OVERPRESSURE_IN_PLENUM_TANK)	sLV3ClosedOK

Table A-15. DCIU Mode Transition Table for PressureMeasured

Source Mode	Events	Destination Mode
On	@T(True)	On

Table A-16. DCIU Dependency Graph Browser

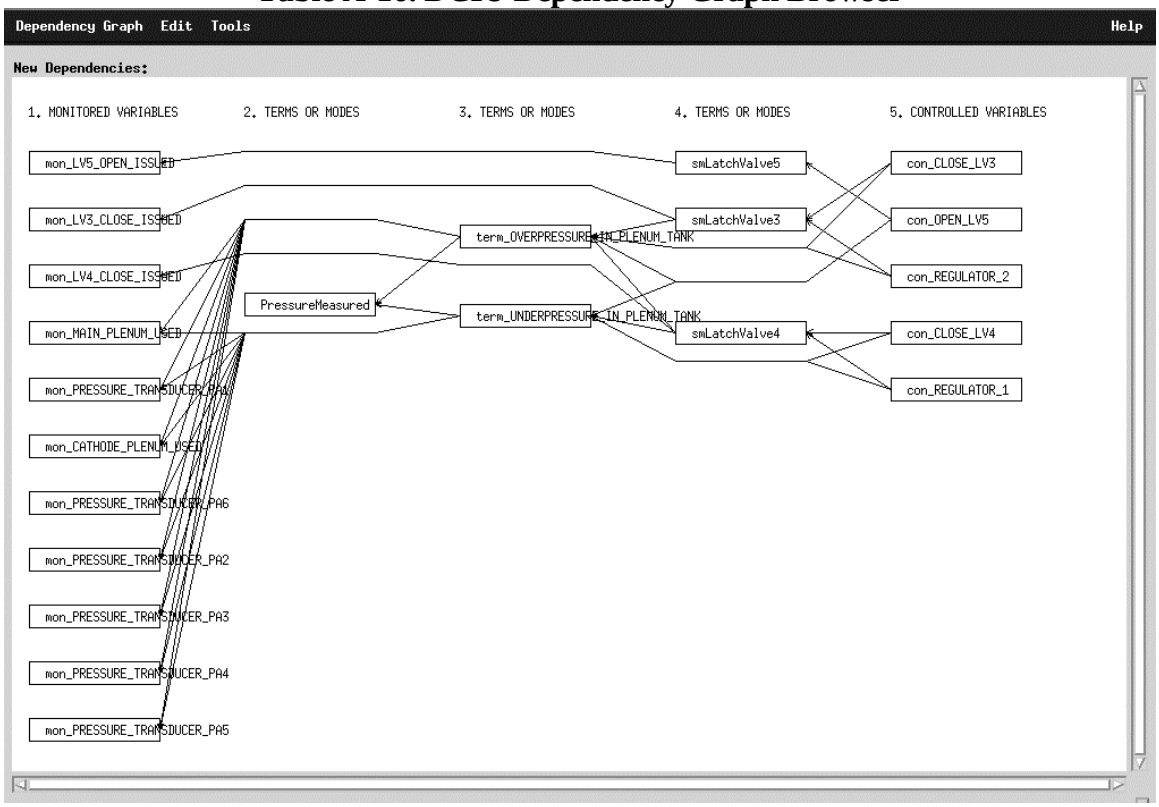

Table A-17. DCIU Simulator - 1
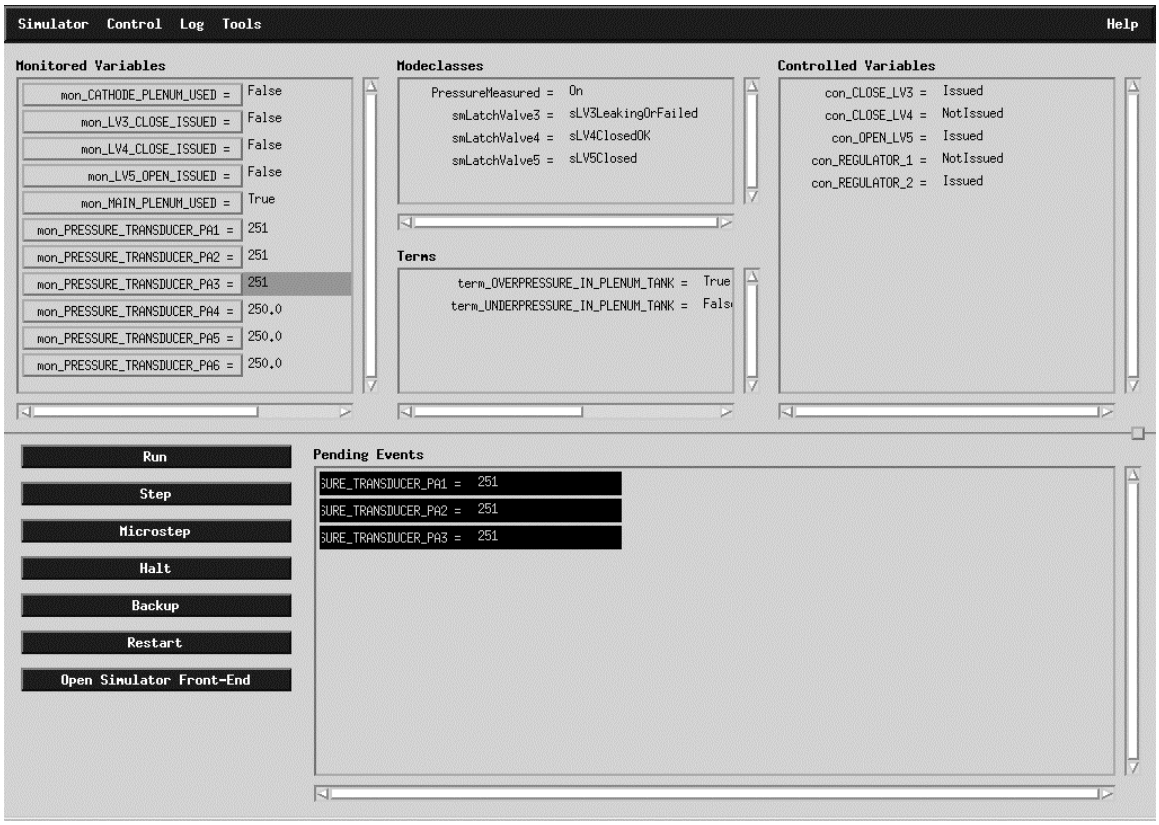
Table A-18. DCIU Simulator - 2