

A photograph of the International Space Station (ISS) in orbit above Earth. The station's complex structure, including multiple solar panel arrays and modules, is clearly visible against the dark background of space. Below the station, the Earth's surface is shown with a mix of blue oceans, white clouds, and brownish-green landmasses. A thin blue line representing the atmosphere is visible at the bottom left. A horizontal black line is drawn across the middle of the image, passing through the station.

Fault Management in Human Spaceflight

Carlos Garcia-Galan, MOD/MPCV

Lee Morin, CB

FM Workshop, April 2012



Distributed Fault Management

Mission Control Center



Spacecraft

- Design Robustness
- Fault Protection



On-board Crew



EVA



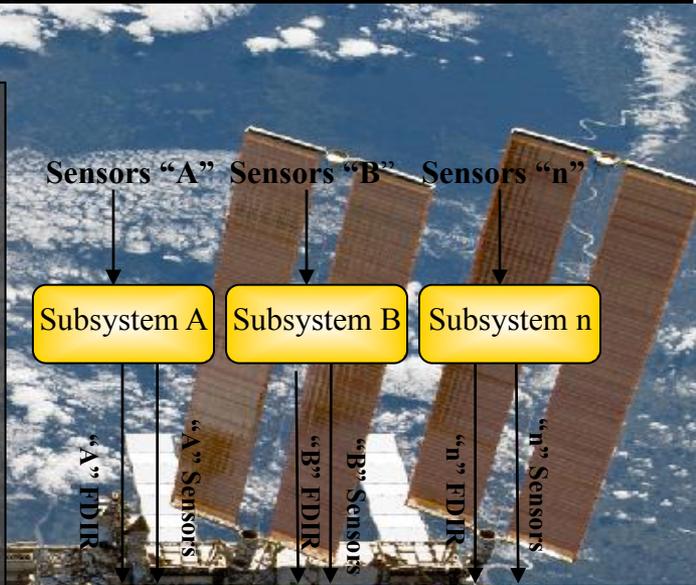


Mission Control Center

- **MOD flight controllers use system expertise gathered through training, interaction with the hardware, and significant real-time experience to develop nominal plans and procedures to achieve the goals established by the Agency and Programs**
 - That knowledge is an agency asset and is also critical to evaluating risk and making effective trades on which failures to develop contingency plans for, either due to the potential mission impact, likelihood, or cost in terms of time and resources
 - Detailed mission development, integration, and planning begins 1 yr before launch, coordinating with Program requirements, customers, and system experts/hardware
 - Validation of plans and procedures are done via testing with hardware and simulators/ mock-ups and are certified by MOD as part of the flight readiness process
- **Preparation:**
 - Flight controllers certified in real-time operations and their system for emergency safing and basic operations within 18 months. They are then able to operate on-console during quiescent ops, and become specialists with expertise for complex ops, with experience and follow-on training regarding their systems typically completed within another year
 - This process has been the focus of continuous improvement efforts to streamline and focus
 - Training of the crew for a mission by MOD using our expertise begins approx 9 months before launch

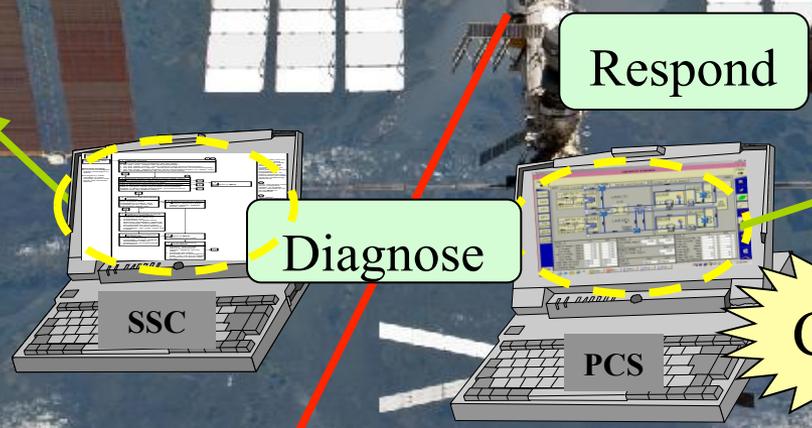
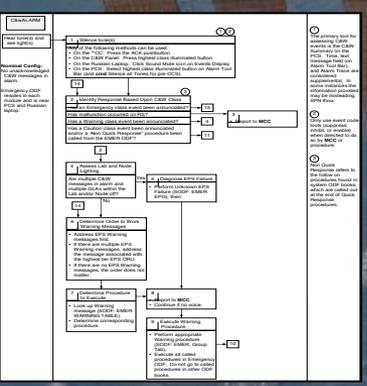
Fault Management on ISS

- H&S driven from individual subsystem-level health mgmt data, not vehicle-level health state
- C&W data only one “piece of the puzzle” to determine the nature of the failure, and system propagation
- H&S data does not directly provide failure response information, or system impact severity
- Each C&W message has associated procedures for crew or ground execution. Diagnosis within procedures



Caution & Warning Summary

STAT	CL	ACK	SYS	Message Text	Time of Event	C&W Toolbar
#Alarm	C		EPS	RPDM LAR616_A Loss of Conn-LAB	22Jun00/10:18:58	Time Newest
#Alarm	C		GDH	Primary DC NDM Detect Loss of Conn NDD1 2 NDM-PMA1	22Jun00/10:18:50	Filter On
#Alarm	C		TCS	Thermal Safing MTL Complete Load Shed Started	22Jun00/10:15:45	ALL EWC
#Alarm	H		TCS	ISIDS Vehicle Power Retru Action	22Jun00/10:15:39	Advisories
#Alarm	C		TCS	Thermal Safing LTL Complete Load Shed Started	22Jun00/10:15:36	Off
#Alarm	H		TCS	Thermal Safing Complete MTL Load Shed Timer Started	22Jun00/10:10:34	Robotics
#Alarm	H		TCS	Thermal Safing Complete LTL Load Shed Timer Started	22Jun00/10:10:34	Off
#Alarm	C		TCS	Thermal Safing LTL Partial Load Shed Started	22Jun00/10:05:20	Alarm Trace
#Alarm	C		GDH	Backup BND MDM Fail-LAB	22Jun00/10:01:45	Master On
#Nom	H		MCS	Auto Survival Mode Transition In Progress	22Jun00/10:00:18	Master Off
#Alarm	H		TCS	Lab ISIDS Mode Unknown-LAB	22Jun00/10:00:18	Event Code
#Alarm	H		TCS	Thermal Safing Partial MTL Load Shed Timer Started	22Jun00/10:00:18	Tools
#Alarm	H		TCS	Thermal Safing Partial LTL Load Shed Timer Started	22Jun00/10:00:18	Enable
#Alarm	C		GDH	Backup PMDU MDM Fail-LAB	22Jun00/09:59:53	Suppress
#Alarm	C		GDH	Primary PMDU MDM Detected Local Bus EPS Node 2 23 Fail-LAB	22Jun00/09:59:48	Inhibit
#Alarm	C		GDH	Primary PMDU MDM Detected Local Bus EPS DPM 23 Fail-LAB	22Jun00/09:59:48	Get Status
#Nom	C		GDH	Primary PMDU MDM Detected Ancillary Data Error-LAB	22Jun00/09:59:48	Log Tools
#Alarm	C		TCS	Lab MTL PPA Pump Failure-LAB	22Jun00/09:58:06	Log Menu
#Alarm	C		TCS	Lab MTL PPA Pump In Press Low-LAB	22Jun00/09:58:02	
#Alarm	C		TCS	Lab Rack LAB1B Overtemp-LAB	22Jun00/09:57:58	
#Alarm	C		GDH	Backup INT MDM Fail-LAB	22Jun00/09:57:05	
#Alarm	C		GDH	Primary Int MDM Detected Static Frame Count for Lab 3 MEM-LAB	22Jun00/09:57:05	
#Alarm	C		GDH	Primary Int MDM Detected Static Frame Count for Node 1-2 NDM-LAB	22Jun00/09:57:05	
#Alarm	C		GDH	Primary Int MDM Detected Static Frame Count for Lab 2 NDM-LAB	22Jun00/09:57:05	
#Alarm	C		EPS	RPDM LAR2B A Loss of Conn-LAB	22Jun00/09:57:05	
#Alarm	C		EPS	RPDM LAR2B A Loss of Conn-Node 1	22Jun00/09:57:05	
#Alarm	C		EPS	RPDM N13B A Loss of Conn-Node 1	22Jun00/09:57:05	
#Alarm	C		EPS	RPDM N13B B Loss of Conn-Node 1	22Jun00/09:57:05	
#Alarm	C		EPS	RPDM LAR2B B Loss of Conn-LAB	22Jun00/09:57:05	
#Alarm	C		EPS	RPDM LAR2B B Loss of Conn-Node 1	22Jun00/09:57:05	
#Alarm	C		EPS	Lab MTL PPA Pump In Press Low-LAB	22Jun00/09:57:05	
#Alarm	C		EPS	RPDM LAR2B E Loss of Conn-LAB	22Jun00/09:57:05	
#Alarm	C		EPS	Lab MTL PPA Pump In Press Sensor Failure and NIA Inhibited-LAB	22Jun00/09:57:05	
#Alarm	C		EPS	RPDM LAR2B F Loss of Conn-LAB	22Jun00/09:57:05	
#Alarm	C		EPS	RPDM LAR2B F Loss of Conn-Node 1	22Jun00/09:57:05	





ISS FM Example

- **Failure of ISS External Thermal Coolant System (ETCS) Loop A Pump Module – provides half of the ISS systems cooling, resulted in immediate loss of 50% of ISS capability**
 - **Immediate assessment and response (critical to prevent hardware loss):**
 - **13 hours of ground commanding to powerdown and reconfigure systems required to achieve a safe state that optimized capability**
 - **This set of contingency procedures had been developed by MOD and maintained/updated as ISS configuration changed through assembly [*preparation*]**
 - **ISS crew – trained by MOD for skills required in contingency ops (installation of jumpers, rack reconfigurations) [*expertise*]**
 - **Crew and ground ops choreography trained before launch to allow teams to be able to communicate crisply and effectively and function as a cohesive unit in critical time response situations [*experience*]**
 - **Recovery action: MOD team integrated with engineering support and Program management to perform 3 spacewalks and recover full system capability within 17 days of initial failure**
 - **Initial contingency EVA procedures developed by MOD several years in advance and taken to a state where a real-time team could then develop final procedures based on the actual configuration of the vehicle associated with the specific pump failure [*risk assessment and upfront preparation/investment*]**
 - **Plans and procedures required adjustments for robotics support, ammonia line hazards, tool configurations, and system repowering sequences using MOD experts and mission systems (NBL, MCC, ISS simulator) [*assets, integration skills, and expertise*]**
 - **Real-time quick responsiveness required well trained flight controllers and expertise to rapidly respond to additional contingencies during the EVA (ammonia quick disconnect failures, EMU suit sensor failures, connector and bolt issues, worksite and tool adjustments) [*experience*]**



Health & Status On-board Orbiter

1	2	3	4	5
123456789012345678901234567890123456789012345678901				
XXXX/XXX/079	SM STS SUNN 2	XX X	000/HH:MM:SS	000/HH:MM:SS
CRYO TK 3	2	3	4	MANF1 MANF2
H2 PRESS XXXX	XXXX	XXXX	XXXX	OM1 OM2
O2 PRESS XXXX	XXXX	XXXX	XXXX	OM3 OM4
HTR T1	OM1	OM1	OM1	DF2
T2	OM2	OM2	DF3	DF3
APU	1	2	3	HYD 1 2 3
TEMP COT	DA1	DA2	DA3	PRESS DA2
P/O EGT	DA2	DA3	DA1	RTRV 1
OIL IN	DA1	DA2	DA3	P
OUT	DA2	DA3	DA1	QTY
SPEED	N	DA1	DA2	DA3
FUEL QTY	XXXX	XXXX	XXXX	H2O QTY
PMP LK	P	OM3	OM3	BYP VLV
OIL OUT	P	DA1	DA2	DA3
AV BAY	1	2	3	H2O PUMP P
TEMP	DF2	DF3	DF1	FREON FLOW
FAN SP	X.XXX	X.XXX	X.XXX	EVAP OUT T

P
A
S
S

```

08017 /099 FAULT 5 000/00:11:50
BFS 000/00:00:00
CRT FAULT C/W GPC TIME
SM0 THERM FRN 1 2 000/00:11:05
SM1 FC STACK T 1 2 000/00:10:16
SM2 FREON FLOW 1 2 000/00:09:10
SM1 FC PUMP 1 2 000/00:09:08
SM2 AV BAY FAN 000/00:09:08
SM0 TARGET ERR RTLS 000/00:07:05
SM0 THERM PRFLT 000/00:05:49
SM0 SSME FAIL CLR L 000/00:05:26
SM0 SSME FAIL CLR L 000/00:05:25
SM0 MPS HE P CLR L 000/00:03:30
SM0 MPS HE P CLR L 000/00:03:29
SM1 CABIN FAN M 000/00:02:11
SM1 CABIN FAN M 000/00:02:10
SM0 MPS HE P CLR L 000/00:02:10
SM0 I/O ERROR PCM 000/00:00:00
SM2 AV BAY FAULT FAN 5 00:09:06(04)
SM2 AV BAY FAULT SUMM
  
```

O ₂ PRESS	H ₂ PRESS	FUEL CELL REAC	FUEL CELL STACK TEMP	FUEL CELL PUMP
CABIN ATM (R)	O ₂ HEATER TEMP	MAIN BUS UNDERVOLT (R)	AC VOLTAGE	AC OVERLOAD
FREON LOOP	AV BAY/ CABIN AIR	IMU	FWD RCS (R)	RCS JET
H ₂ O LOOP	RG/ACCEL (R)	AIR DATA	LEFT RCS (R)	RIGHT RCS (R)
PAYLOAD WARNING (R)	GPC	FCS SATURATION (R)	OMS KIT (R)	OMS TVC (R)
PAYLOAD CAUTION	PRIMARY C/W	FCS CHANNEL	MPS (R)	
BACKUP C/W ALARM (R)	APU TEMP	APU OVERSPEED	APU UNDERSPEED	HYD PRESS

- Annunciator Matrix and On-board Fault Summary data based on individual conditions or pre-defined “hard-coded” rules
- Failures that impact multiple components result in the generation of many seemingly unrelated messages that the crew needs to isolate
- Generated alerts are often not indicative of the real failure. E.g. ‘EPS bus ‘undervolt’ failure generated ‘Fuel cell Ph low’



EFT-1 FM Capability Strategy/Groundrules

On-board

- **All planned mission events will be automatic**
- **FDIR should align to planned Orion 2 FDIR** to the extent that HW is in place for OFT-1
 - Defer FDIR for which there is no OFT-1 HW
 - *Defer all FDIR that does not have associated responses (e.g. system reconfiguration)*
 - Defer FDIR intended for crew situational awareness (e.g., C&W)
- **FDIR must provide 1FT for mission completion (CM recovery) for credible failure modes as determined by FMEA and System Analysis**
 - *Where high value and practical to accommodate, FDIR should allow ground to command back to original string – Via approved contingency commands only*
 - *Fault recovery capability may be allocated to the flight control team for cases where FDIR would be complex and scenario is considered low risk by the FM team (e.g., long time available to respond). Ground commands needed for these cases would be verified*
- **Uplink commands will be verified for a subset of priority events** associated with FCT Fault Response requirements
 - Additional command /manual control capability will be provided for all individual items, but use of these commands will be restricted to “last resort” type scenarios and therefore will have minimal verification
 - *Classified commands into 4 categories: CAT 1-3 meet (small set) meet verification criteria above, and CAT 4 require Program authorization prior to uplink.*

Flight Control Team (FCT)

- Will monitor automatic events for proper operation
- Manually command/alter events if determined to be needed
- Monitor health of systems as backup to FDIR
- Monitor FDIR response to ensure proper response to first failure
- Manually command events or individual components (verified capability) where 1-failure cases are allocated to the ground
- Manually command events or individual components for multi-failure cases
- **Flight Telemetry Maps built to follow the following priorities:**
 1. Support In-flight Commanding
 2. Support Anomaly Resolution
 3. Support Gathering of Primary FTO data
 4. Support Gathering of Secondary FTO data

April, 2012



Enhancing Fault Management in the Cockpit

- Cockpit Avionics Upgrade (CAU)
 - Color Coded Messages
 - Revised error message text
 - Describes error in greater detail
- Enhanced Caution & Warning (ECW)
 - Root Cause Analysis
 - Parent-child relationships
 - Message grouping



ECW Scripting Tool

- Developed in Visual Basic
 - Build and save scripts to display C&W Messages
 - Assign Parent Child Relationships
 - Adjust message display timing
 - Depict CRT messages as they would appear in
 - Legacy Shuttle Display
 - CAU Display
 - ECW Display
 - Playback Controls to interact with script

April, 2012



ECW Scripting Tool (Continued)

Messages Spreadsheet: C:\Users\phenry\Desktop\ECW\ECW010100\ECW Messages 010a.csv

File

Script- C:\Users\phenry\Desktop\ECW\ECW010100\Session 1 Run1.spt

Playback Controls

ACK Log CAA Pause

Reset Sim On Script

Reset Sim 19:31:55

Reset IO Top

Message Info

CAU Message:

ECW Messages:

Delete Line<<<

Script Type

Old

CAU

LC

W

All

Parent Group

A

Parent

Child

New

Apply

SetEWCA & PASS-E

Apply

"X" means

PASS GPCs

ID	DPS	EWCA
Current Message		
RM DLMA PRL		
SM2 APU SPD HI 1		
SM2 APU SPD LO 1		
SM2 APU SPD HI 1		
APU 1 COOL DOWN		
SM2 APU SPD HI 2		
SM2 APU SPD LO 2		
SM2 APU SPD HI 2		
APU 2 COOL DOWN		
SM2 APU SPD HI 3		
SM2 APU SPD LO 3		
SM2 APU SPD HI 3		
APU 3 COOL DOWN		
SM2 HYD PRESS 1		
SM2 HYD PRESS 2		
SM2 HYD PRESS 3		
SM2 APU TEMP 1		
SM2 APU TEMP 2		
SM2 APU TEMP 3		
SM2 HYD QTY 1		
SM2 HYD QTY 2		
SM2 HYD QTY 3		
SM2 HYD RSVR T 1		
SM2 HYD RSVR T 2		
SM2 HYD RSVR T 3		
SM2 W/ B QTY 1		
SM2 W/ B QTY 2		
SM2 W/ B QTY 3		
SM2 HYD ACUM P 1		

Type_Search_Text

Find Previous Find Next

Find from Script

ECW:a:C: :AV Bay 1 Sig Cnдр Power Lost

OLD: :C:B:SM2 HYD QTY 1

CAU: :C:B:Hyd 1 Rsvr Qty

ECW:b:W: :Hyd 1 Rsvr Qty

192831

OLD: :C:B:SM1 FC PH 1

CAU: :C:B:FC 1 pH H1

ECW:a:C: :FC 1 pH H1

192834

OLD: :W:B:SM2 FREON FLOW 2

CAU: :W:B:Freon 2 Flow Lo

ECW:a:W: :Freon A Sig Cnдр Power Lost

193020

OLD: :W:B:SM2 APU SPD LO 2

CAU: :W:B:APU 2 Speed Lo

ECW:B:C: :APU 2 Speed Lo

193023

OLD: :W:B:SM2 HYD PRESS 2

CAU: :W:B:Hyd 2 Press B Lo

ECW:b:C: :Hyd 2 Press B Lo

193131

OLD: :C:B:RM FAIL IMU

CAU: :C:B:IMU Fail

ECW:c:C: :IMU Fail

193144

OLD: :C:B:BCE STRG 2 PASS

CAU: :C:B:Strg 2 BFS Byp

ECW:c:C: :Strg 2 BFS Byp

OLD: :C:B:BCE STRG 3 PASS

CAU: :C:B:Strg 3 BFS Byp

ECW:c:W: :14 V 2 V 3

ECW: :X: :RS Set Split

ECW:c:C: :Strg 3 BFS Byp

193146

OLD: :C:B:RM FAIL IMU

CAU: :C:B:IMU Fail

ECW:c:C: :IMU Fail

193211

Fault Log

RS Set Split 19:31:44

◆ 14 V 2 V 3 19:31:44

IMU Fail

Strg 3 BFS Byp

Strg 2 BFS Byp

IMU Fail

◆ APU 2 Speed Lo 19:30:20

Hyd 2 Press B Lo

■ Hyd 1 Rsvr Qty 19:28:29

◆ AC1 Multi \$ Short 19:28:28

Freon A Sig Cnдр Power Lost

FC 1 pH H1

AV Bay 1 Sig Cnдр Power Lost

H2O Lp 2 Fail

Cab Air Sig Cnдр Failed

ECW Engine Model

A = 30

B = 3

C = 30

D = 0

ACK Log CAA Pause Fast

Reset Sim 19:31:55 Reset to Top Instant

Auto Instantiation

ABCD

Low

High

Legacy CRT Messages - PASS & BFS Fault Summs

```

RM FAIL IMU 19:31:46
BCE STRG 3 PASS 19:31:44
BCE STRG 2 PASS 19:31:44
RM FAIL IMU 19:31:31
SM2 HYD PRESS 2 19:30:23
  
```

Fault Summ Message Behavior

```

14 V 2 V 3
APU 2 Speed Lo
Hyd 1 Rsvr Qty
AC1 Multi $ Short
RS Set Split
  
```



Fault Summ

3.2 Coast

Send To eProc-1

Ack 2

Send To eProc-2

- W EPS Load Sw Card 2 Fail
- W EPS Htr Cntl Card 3 Fail
- W EPS Intl Pwr Supply A Fail
- W EPS AC1 Multi \$ Short
- C EPS AV Bay 1 Sig Pwr Lost

COH-EPS	ECLS	CM Prod	GNC NAV



Fault Log

1
of 8

Send To
eProc-2

Send To
eProc-1

- CEPS Pwr Bus 2 Volt HI 214/18:37:57
- CEPS Batt 5 Temp HI 214/18:37:52
- WEPS Cab Air Cntl Pwr Lost 214/18:37:47
- WEPS Load Sw Card 2 Fail 214/18:37:42
- CEPS AV Bay 1 Sig Pwr Lost 214/18:37:37
- WEPS Htr Cntl Card 3 Fail 214/18:37:32
- WEPS Intl Pwr Supply A Fail 214/18:37:27
- WEPS AC1 Multi \$ Short 214/18:37:22

Ack
All

Scroll
Mode

Clear



Electronic Procedures

Electronic procedures are the heart of an effective spacecraft glass cockpit.

The image shows a spacecraft Electronic Procedures Display (EPD) interface. At the top, there are several physical buttons and a rotary knob labeled 'Brt'. The main display area is divided into sections. The top section shows a menu with 'Sys', 'EPS', 'EPS.SM', 'EPS.Ary', 'EPS.SMB', 'EPS.CM', and a page number '2'. Below this, the 'TOC:' (Table of Contents) section displays '3.14 AS1 FAULT' and 'Version 2.0.2 July 26, 2007'. A yellow oval highlights the 'Conf' (Configure) menu item, which is currently selected. The configuration menu lists several parameters, with 'Bus S1 Voltage - 0.0' highlighted in pink. Other parameters include 'AS1 Mode', 'AS1 Closed FETs', 'Batt S1 Mode', 'Batt S1 SOC', 'Isol S1-2', 'Feeder S1', and 'RPC S1 Load'. To the right of the configuration menu are buttons for 'Set Asst', 'Anot', and 'Go Scr1'. Below the configuration menu is a 'Skip' button. The bottom section of the display shows a power distribution diagram for 'AS1 Fault'. It includes a status bar with 'AS1 Fault', 'U 111/20:09:06', and 'EPS'. The diagram shows four power buses: S1, S2, S3, and S4. S1 is at 0.0 V and has a 'Trip' status. S2 is at 28.6 V. S3 and S4 are at 31.9 V. The diagram also shows power levels for AS1 (0.00 kW, Off), AS2 (1.13 kW, Auto), AS3 (0.91 kW, Auto), and AS4 (0.91 kW, Auto). A yellow arrow points from the 'Bus S1 Voltage - 0.0' in the configuration menu to the '0.0 V' in the power distribution diagram. A yellow text box on the right side of the display reads: 'Electronic Procedures, by directly interacting with system displays, cue operator actions. These cues greatly reduce workload and errors.'



ECW Prototyping

Legacy CRT Messages - PASS & BFS Fault Summs

```
RM FAIL IMU 19:29:24
BCE STRG 3 PASS 19:29:15
BCE STRG 2 PASS 19:29:15
RM FAIL IMU 19:29:10
SH2 HYD PRESS 2 19:29:05
```

Fault Summ Message Behavior

14 V 2 V 3
APU 2 Speed Lo
AC1 Multi \$ Short

RS Set Split

Fault Log

RS Set Split 19:29:15
◆ 14 V 2 V 3 19:29:15
Strg 3 BFS Byp
Strg 2 BFS Byp
IMU Fail
◆ APU 2 Speed Lo 19:28:50
Hyd 2 Press B Lo
Hyd 1 Rsvr Qty
◆ AC1 Multi \$ Short 19:28:28
Freon A Sig Cndr Power Lost
FC 1 pH Hi
AV Bay 1 Sig Cndr Power Lost
H2O Lp 2 Fail
Cab Air Sig Cndr Failed