Using FMECA to Support Maintainability and FRACA

Orson John
Reliability & Risk Assessment Engineer

10 Sept 2019
NASA GSFC SMA Directorate
MAMII Meeting, GSFC - Greenbelt, MD

Agenda

- FMECA Approach that Supports Maintainability/ FRACA
- ATLAS Enhanced Maintainability Case Study
- FRACA Study?
- Lessons Learned

FMECA Approach that Supports Maintainability/FRACA

- **Process**
  - Establish analysis criteria with design and systems engineering team
  - Engage full design (including Software) and systems team to flush out interface issues and proactively increase the failure tolerance.
  - Verify and iterate to with design, test, or maintainability changes.
- **Analysis**
  - Postulate all potential failure modes
  - Identify causes and impacts of each failure mode
  - Ascertain each failure mode's or cause's available prevention and/or mitigation strategies and detection capabilities
  - Identify gaps in mitigation strategies that need maintainability design adjudication.

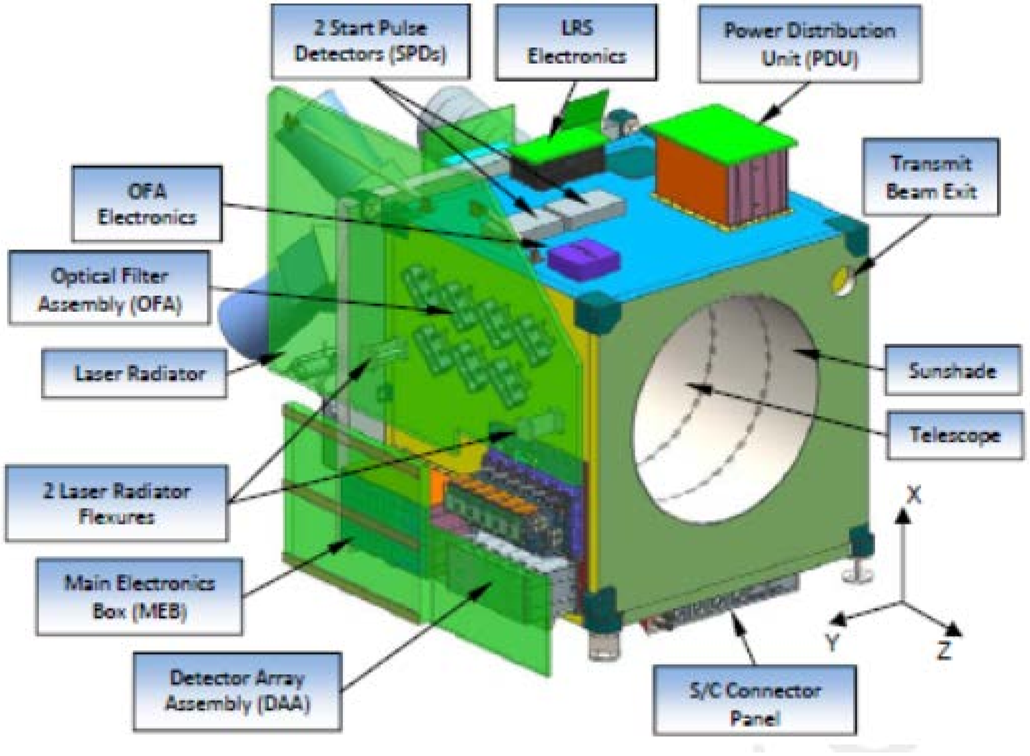
Failure Modes and Effects Analysis Worksheet															
Project: Mission													Analyst: GSFC/Name		
Subsystem:													Date: 11/04/11		
Ref. No.	Component Name	Component Function	Potential Failure Mode	Potential Cause of Failure	Occurrence Value	Potential Effects of Failure			Severity Value	Severity Category	Mitigating Factors (Detection/ Prevention)	D/P Value	RPN	Recommended Actions	Comments
						Local Effect	Subsystem Effect	Mission Effect							

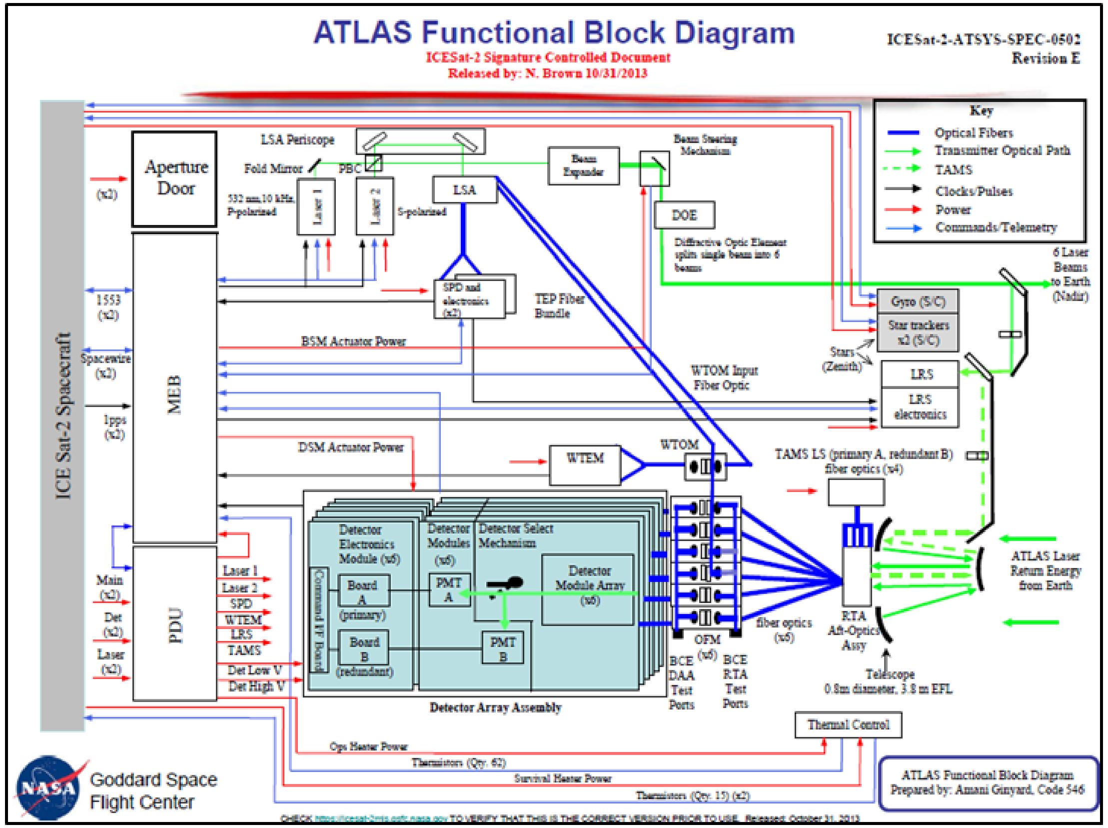
FMECA Example

Ref. No.	Component Name	Component Function	Potential Failure Mode	Potential Cause of Failure	Occurrence Value	Potential Effects of Failure			Severity Value	Severity Category	Mitigating Factors (Detection/Prevention)	D/P Value	RPN
						Local Effect	Subsystem Effect	Mission Effect					
MEB-6	Ultra-Stable Oscillators (USO)	Provides clock signal	USO frequency change/drift	No autonomous switching Thermal control (internal) loss	1	Degraded performance parameter	Inaccurate synchronization between systems using USO	Degraded Science	3	2R	Detection: USO drift identified in science data Mitigation: switch to redundant USO Prevention: High Quality Parts and Design, and workmanship with robust testing,	3	9

ATLAS Maintainability Enhancement Case Study

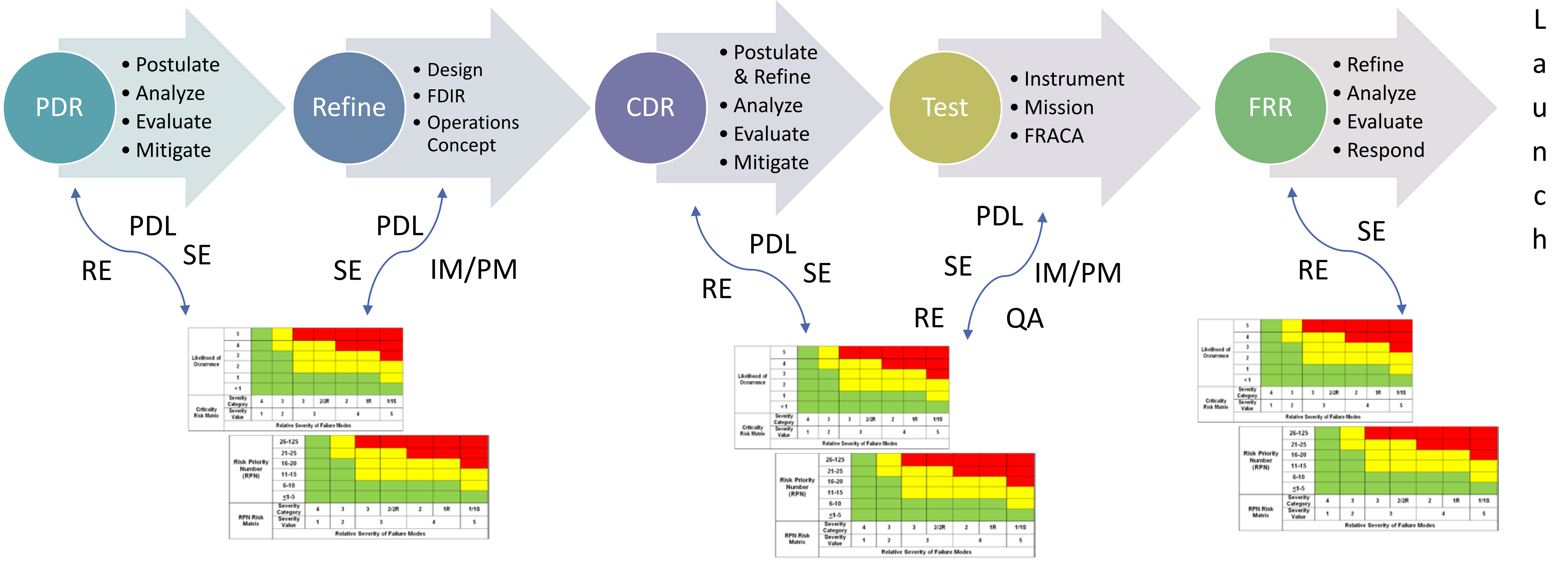
Advanced Topographic Laser Altimeter System (ATLAS)





FMECA Process

Iteration, Engagement, and Mitigation at each stage ensures Maintainability



ATLAS Results Summary

- S/C Autonomous ATLAS Safing Actions added to ensure the Instrument would be maintained for future Operations:
  - 9 Over Temperature Monitors
  - 8 Over current Monitors
  - ATLAS under no-communication conditions

- Reliability Impacting Design Refinements (8 Critical Items removed/13 added):
  - Ability to ignore/disable BSM sensor input in BSM control loop means the Loss of a BSM Sensor(s) can be mitigated given the MCE operates the BSM without the sensor soft-stop.
  - DSM Optical Sensors can be removed from control loop by command to avoid faulty sensors from preventing unnecessary detector switch and loss of science.
  - DSM elimination of Mirror 2 removes SPF from PMT bank switching.
  - FSW accommodation/error handling of missing spots.
  - Wavelength not expected to drift (based on testing) therefore WTEM is no longer mission critical

ATLAS Safing for Maintainability Example

Failure Modes & Effects Analysis Worksheet

Project: ICESat-2 | **Analyst: Orson John (GSFC Code 322)**

Instrument Subsystem: Thermal Control System (TCS) | **Date: 12/20/13**

Ref. No.	Component Name	Component Function	Potential Failure Mode	Potential Cause of Failure	Occurrence Value	Potential Effects of Failure: Local Effect	Potential Effects of Failure: Subsystem Effect	Potential Effects of Failure: Mission Effect	Severity Value	Severity	Mitigating Factors (Detection/Prevention)	D/P Value	RPN	Recommended Actions	Comments
TCS-14	Laser Loop Heat Pipe (LHP) for Lasers	Radiates Heat from the Lasers	Loss of Laser LHP's Heat Transfer	Debonding Fluid loss (rupture) Operational Heater does not maintain fluid temperature (see TCS-27, TCS-28) Survival Heater Does not maintain fluid temperature when LHP is not in use (See TCS-31, TCS-32) LHP Evaporator fails to evaporate (see TCS-15)	***1	LHP looses conduction Loss of Heat Transfer Lasers continue to heat up, Electronics will stop functioning Change in laser wavelength (see Laser FMEA)	Degraded Performance of ATLAS Laser OR Run the Risk of *LASER Overtemp	Loss of science opportunities (loss of a major amount of critical science data) due to ATLAS over temperature (safing)	5	1	Detection: Thermal Hsk Telemetry, Thermistors Degraded Science Sensor No. TCS-34, Execution of ATLAS LASERSHED Mitigation: Spacecraft will safe the instrument AND Ground Investigation and Intervention Prevention: High Quality Testing and Design	3	15		*Laser Over-temp will execute "ATLAS LASERSHED (Laser Shutoff, Turn on LHP Shutdown Heater, Switches in S/C PDU and ATLAS PDU Turned OFF)" Per ICESat-2-ATSYS-SPEC-0947 ** Significant downtime even with duty cycling due to laser start up times (8-12hours) ***Occurrence Value based Probability of MMOD damage on LHP, Pf=0.0091 (Source: ATLAS Heat Pipe MMOD Prediction (TBR))
TCS-15	Laser Loop Heat Pipe (LHP) Evaporator	Radiates Heat from the Lasers	Laser LHP Evaporator fails to evaporate	Fluid loss (rupture) Operational Heater does not maintain fluid temperature (see TCS-27, TCS-28) Survival Heater Does not maintain fluid temperature when LHP is not in use (see TCS-31, TCS-32) Inefficient heat transfer of the Start up Heater (see TCS-23, TCS-24)	1	Evaporator fails to evaporate the fluid Loss of Heat Conduction Lasers continue to heat up, possible change in laser wavelength (see Laser FMEA)	Degraded Performance of ATLAS Laser OR Run the Risk of *LASER Overtemp Leading to loss Leading to Loss of LHP (see TCS-14)	Degraded Science leading to Temporary Loss of science opportunities (loss of a major amount of critical science data) due to ATLAS over temperature (safing) until thermally driven duty cycling can **possibly be performed with ground intervention	4	2	Detection: Thermal Hsk Telemetry, Thermistors Degraded Science Sensor No. TCS-34, Execution of ATLAS LASERSHED Mitigation: Spacecraft will safe the instrument AND Ground Investigation and Intervention Prevention: High Quality Testing and Design	3	12		*Laser Over-temp will execute "ATLAS LASERSHED (Laser Shutoff, Turn on LHP Shutdown Heater, Switches in S/C PDU and ATLAS PDU Turned OFF)" Per ICESat-2-ATSYS-SPEC-0947 ** Significant downtime even with duty cycling due to laser start up times (8-12hours)

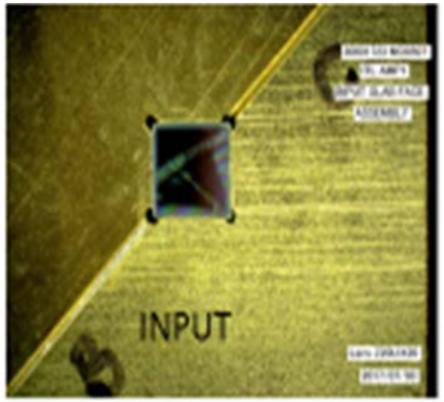
Result: Revised Safing Plan Examples

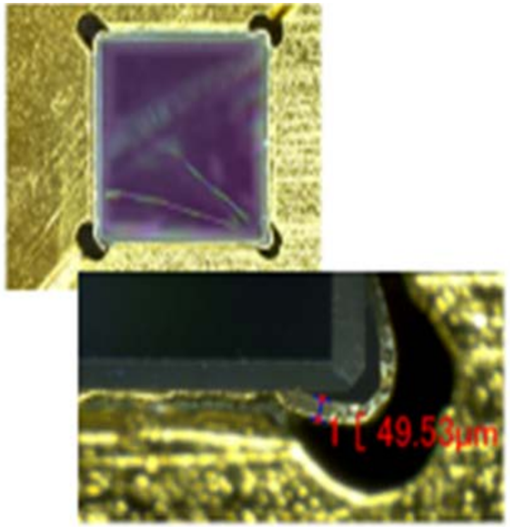
ID	Description	Condition	Collection	Sensor No.	Monitor	Action	Rationale
17	MIL-STD-1553 Remote Terminal Bus Errors (S/C side)	RT message errors > 8000 [TMON Sample Rate: Every 5s; Persistence of 12 samples]	S/C		S/C	ATLAS LOADSHED1 (Survival Heaters and LHP Shutdown Heater ON, all components OFF)	Communications has been lost to/from ATLAS for more than one minute. Nominal 1553 communications with ATLAS is approximately 6780 transactions in one minute. One minute was chosen since it is longer than the reboot time of the MEB RAD750. Thermal mass of ATLAS components will not result in extreme temperatures in only one minute. This will allow the MEB RAD750 watchdog timer to reset the MEB RAD750 once and reestablish communications without ATLAS being powered OFF.

ID	Description	Condition	Collection	Sensor No.	Monitor	Action	Rationale
23	Laser Still Overtemp	Laser1 I/F > 28C for over 5 minutes [Telemetry Generation Rate: 5Hz; TMON Sample Rate: Every 20s; Persistence of 15 samples]	S/C	SC-01	S/C	ATLASLASERSHED (Survival Heaters ON, LHP Shutdown Heater ON, lasers OFF) 1. Turn ON ATLAS Survival Heaters-A 1-4 (S/C Switches) 2. Turn ON ATLAS Survival Heaters-B 1-4 (S/C Switches) 3. Turn ON LHP Shutdown Heater-A (S/C Switch) 4. Turn ON LHP Shutdown Heater-B (S/C Switch) 5. Send command to ATLAS MEB to disable science data collection 6. Send command to ATLAS MEB to disable AMCS BSM control 7. Send to ATLAS PDU-A to turn OFF Laser-1 Switch 8. Send to ATLAS PDU-A to turn OFF Laser-2 Switch 9. Send to ATLAS PDU-B to turn OFF Laser-1 Switch 10. Send to ATLAS PDU-B to turn OFF Laser-2 Switch 11. Turn OFF Laser-A Service (S/C Switch) 12. Turn OFF Laser-B Service (S/C Switch) 13. Send command to ATLAS to disable TCS heater control including LHP control.	ID#5 is intended to be executed when the Laser has reached its operational hot temperature (25C) and has been commanded to goto Ready. The Laser has exceeded its operational hot temperature (25C) (Hot Qualification is 30C). Note that although this sensor is named “Laser1”, the Laser1, Laser2, and the LHP are tightly coupled together thermally. The monitoring of a second sensor for Laser2 is not necessary. Switches in S/C PDU and ATLAS PDU turned OFF to mitigate risk of switch stuck ON. Turn ON LHP shutdown heater to stop loop and avoid excessive cooling. Investigate from the ground. Stop science since the Laser is turned OFF.

ATLAS FRACA Case Study

FMECA FRACA Support Example





Failure Modes & Effects Analysis Worksheet															
Project: ICESat-2									Analyst: Orson John (GSFC Code 322)						
Instrument Subsystem: Laser									Date: 12/20/13						
						Potential Effects of Failure									
Ref. No.	Component Name	Component Function	Potential Failure Mode	Potential Cause of Failure	Occurrence Value	Local Effect	Subsystem Effect	Mission Effect	Severity Value	Severity Category	Mitigating Factors (Detection/Prevention)	D/P Value	RPN	Recommended Actions	Comments
L-4	LASER A or B	Provide Laser Light for ATLAS instrument to work	Amplifier 1 degradation	See LGS/Fibertek FMECA Ref. No. L-4.1, 2,3,4,5,6,7,8,9,10,11,12,13,1,4,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98,99,100,101,102,103,104,105,106,107,108,109,110,111,112,113,114,115,116,117,118,119,120,121,122,123,124,125,126,127,128,129, 130,131,132,133,134,135,136,137,138,139,140,141,142,143,144,145,146,147,148,149,150,151, 152,153,154,155,156 Optical Coating degradation • Manufacturing Defect • Contamination • Laser Damage Threshold met Optic Crack • Launch Vibration Optic Misaligns • Improper installation • Launch Vibration • Bonding Degradation	2	Laser output degraded	Transmit optics will still operate but will be degraded based on the amount of laser output	Temporary Degraded Science until switched to redundant Laser	3	3	Detection: • science data received on the ground • internal laser power TLM doesn't match SPD power TLM LRS sees degraded laser pattern LRS Intensity TLM Incomplete packet counter increments Mitigation: Switch to redundant Laser Prevention: High Quality Testing and Design	3	18		
						Laser pulse frequency change	Cause missing laser pulses that the SPD tags and cause the DOE clocking stability to be out of								
						Laser pulse energy change	Transmit optics will still operate but the output will still be degraded based on the amount of laser output OR the transmit optics could degrade if more laser energy is sent through								
L-5	LASER A or B	Provide Laser Light for ATLAS instrument to work	Amplifier 1 Failure	See LGS/Fibertek FMECA Ref. No. L-5.1, 2,3,4,5,6,7,8,9,10,11,12,13,1,4,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98,99,100,101,102,103,104,105,106,107,108,109,110,111,112,113,114,115,116,117,118,119,120,121,122,123,124,125,126,127,128,129, 130,131,132,133,134,135,136,137,138,139,140,141,142,143,144,145,146 Optical Coating Failure • Manufacturing Defect • Contamination • Laser Damage Threshold met Optic Crack • Launch Vibration Optic Misaligns • Improper installation • Launch Vibration • Bonding Failure	2	Laser output Loss	Instrument will no longer operate (no light, no science)	Temporary Loss of Science until switched to redundant Laser	3	2R	Detection: • MEB science Algorithm reads "No SPD" • No science data received on the ground • SPD timing TLM sends all zeros • SPD Power TLM sends zeros and only sees noise • internal laser power TLM LRS sees no laser pattern (LRS Flags) Missed calculation / Incomplete packet counter increments Energy Monitor Sensor TLM (pressure and temperature) Mitigation: Switch to redundant Laser Prevention: High Quality Testing and Design	3	18		

- It was hypothesized during the Failure Review Board that cracks in the crystal could cause laser light to be deflected onto other sensitive components within the system. Per the ATLAS Laser FMECA the risk of damage to these components is extremely low since the reflected energy would be much less than the energy the system was designed for, will likely not be at the focal point of the system components, and would not propagate beyond the first reflection (Likelihood: non-credible)

Lessons Learned

- FMECAs need to always include Detection, Prevention, Mitigation and Cause analysis to enable system optimization.
- Designers are ready to make design/maintainability changes if they are engaged in the failure postulation process.
- The FMECA process is of highest value if it is supported by all system disciplines interactively.
- FMECA reports can not only be utilized in design to assess risk but they can be used to support test/operational failure investigations.
- FMECAs need to be kept up-to-date with all changes and lessons learned to be useful.
- Since FMECAs do only look at one failure mode at a time additional analyses (i.e., LLAs, FTAs, PRAs, etc.) should be performed as well so a full system risk, maintainability, and/or availability perspective is attainable.