PURPOSE(S) OF MEETING:

- Review EPI-Lo FSW autonomy CONOPS and macro
- Review S/C autonomy and interface with EPI-Lo for consistency in ICD interpretation & assumptions

PARTICIPANTS:

- In Person:
  - Scott Cooper, JHU-APL
  - Kris Fretz, JHU-APL, Spacecraft
  - John Hayes, JHU-APL, EPI-Lo FSW
  - Adrian Hill, JHU-APL, Spacecraft Autonomy (stopped in to answer some questions)
  - Matt Hill, JHU-APL, EPI-Lo Science
  - Ronnie Killough, SwRI, ISIS Software SE
  - Dave McComas, NASA-GSFC, External Reviewer (Not Dave McComas the SwRI PI)
  - Chuck Schlemm, JHU-APL, EPI-Lo Event Board
  - Helmut Seifert, JHU-APL, EPI-Lo PM
  - Scott Weidner, SwRI, ISIS PM
- Via WebEx:
  - A. Cat, Independent Consultant, Reviewer/Meower
  - Nigel Angold, Angold Consulting, ISIS Deputy SE
  - John Dickinson, SwRI, ISIS SE
  - Jason Legere, UNH, SOC
  - Jon Niehof, UNH, SOC

LIST OF MATERIALS DISTRIBUTED

- EpiLo_AutonomyRvw_Agenda_WebEx_Objectives.pptx
- ISIS_EPI-Lo_Sensor_Overview_for_autonomy_review_hill_00.pptx
- ISIS_SCAutonomy_150623.pptx
- EPI-Lo-Autonomy.pptx

MEETING NOTES

1. Introductions/Objectives – Ronnie Killough/SwRI

Review resulted from autonomy-related concerns from Steve Jaskulek and Ronnie Killough at EPI-Lo FSW CDR in November 2014.

Steve Jaskulek could not make this review so John Hayes kindly distributed his slides to Steve (and Ronnie) in advance and received Steve's feedback already (and also some from Ronnie).

A. Cat joined via WebEx and loudly asserted that "Meow, Meow, Meow, Meow, Meow." No one knew what he meant by that so we muted him.

Special thanks to Alex Dupont for bringing some home-baked sweets! Eat your heart out, WebExers.

2. EPI-Lo System Overview – Matt Hill/JHU-APL

Q: Does the Instrument have to protect itself against sun exposure?

A: No –the S/C ensures that the shield stays between the observatory and the sun at all times. This is one of the key requirements on the S/C.

3. Spacecraft Autonomy & Instrument Interface – Kris Fretz/JHU-APL

Autonomy Rules

Autonomy rules are any combination of telemetry and simple arithmetic/compares. Rules have a persistence parameter & limit on how many times they can fire. Rules fire macros. Multiple rules can fire the same macro (i.e. may have same response to multiple rules). S/C macros have a priority scheme (e.g. keeping S/C out of the sun is the top priority).

The autonomy requirements are already signed off - but the Instrument limits associated with these are captured in an engineering limits spec that is signed off late in I&T so tha they can continue to update those as things are learned during I&T, without changing baselined requirements/design documents.

S/C Modes and Processor Rotation

They are running 3 processors in parallel during critical operations (and two other times) so that if there is a fault they can immediately "rotate" to another processor. When possible, the S/C gives 60 second notice before shutting them down to allow time to ramp HV down.

Q: Does the S/C tell the instruments that the S/C is moving between these Operational Modes?

A: The specific mode isn't given – rather there are bits that indicate a processor rotation, solar distance, and if a power-off is pending, among other things.

The S/C does not continue time tagged commands when Op State has been downgraded. However, EPI-Lo doesn't use these currently, so once the macro file has been sent to EPI-Lo, dropping down to lower Op mode in which time tagged commands are suspended doesn't affect EPI-Lo.

The S/C checks the ITF sequence counter and declares a fault/resets the Instrument if stale.

Q: Do the logic and persistence rules correctly handle these scenarios:

a) EPI-Lo WDT timeout period + EPI-Lo reboot period vs. ITF sequence drop-out rule persistence value?
b) ITF may or may not stop temporarily but skips some sequence numbers?
c) ITF flow stops, then resumes and doesn't skip sequence numbers?
d) ITF flow stops, then resumes with ITF sequence number reset to zero/one?

A: Adrian joined us later and clarified that the persistence is set for twice the boot time. I noted that they need to account for WDT+boot time. Currently the S/C persistence is something like 20 seconds. The EPI-Lo WDT is 5 seconds + < 1 second boot time so this should be OK. Adrian also said they only look for a change in the sequence #, so seq # resets or skips aren't a problem.

If an instrument was shut off for certain reasons, the S/C will try once to power instruments back on at 0.25AU for a "second chance" to collect science near perihelion. This is done just to try and maximize science.

Q: Should the S/C do these second-chance power-ons in advance of the 0.25AU threshold to give the instruments time to warm up, boot, ramp up HVs, and get read to start the science that normally begins at 0.25AU?

A: These "second chance" power-ons are normally controlled by timed command sequences, and so this can be setup to occur prior to the 0.25AU. So, the concern would only be applicable if there was a fault/processor rotation causing the timed commands to be suspended. EPI-Lo said this was acceptable, so no action.

Q: Can there be some jitter or backward motion in time, solar distance, inbound/outbound flags as a result of a processor rotation?

A: All the processors use a common time sync so there should be no issue for time. The solar distance/flags are not conveyed to the other processors—that is independently calculated, but all processor should be using the same ephemeris so it should be the same, but some "jitter" could be possible. John Hayes said some jitter on this is OK with EPI-Lo if it were to occur since "the last macro wins".

As a result, no AI was taken for this review re: EPI-Lo.

However after the review as I reviewed the notes, I thought it would be good for the S/C to review this with the other instruments as well to make sure an unlikely-but-possible jitter on the solar distance/inbound-outbound flags won't cause them any issue either. This can be combined with the other action item regarding the autonomy/manual bit and what is/isn't conveyed to the rollover processor.

Heater Control

Q: How does the S/C test all this heater control logic – is there a simulator?

A: They don't have a simulator to test it – likely they will have to wait until the Instrument is delivered to test the logic.

Q: Do the instrument teams get a S/C simulator?

A: The Instrument teams do have a S/C emulator on GSEOS that emulates the S/C interfaces to the instrument.

Q: How will all this autonomy (rules and macro responses) get tested to make sure they don't have unexpected interactions/behaviors/conflicts? The rules can seem simple but you almost need a Monte Carlo-type simulation to see if the rules work as intended in various scenarios.

A: There are several levels of testing of this: (1) test individual rules and macros, (2) testing of the integrated set on the test bed, (3) anything that can be tested on the integrated S/C will be tested there, and 4) there is dedicated fault management testing that will be done.

Q: Do you have the capability to run all the autonomy rules without actually running the macros?

A: Can disable the macros and run the rules, but can't run the macros with command echo but not execute the commands.

Instrument Interface

Q: I didn't see anything in the presentation about what is sent to the Instrument in terms of signals/messages (e.g. inbound/outbound, distance to sun?)

A: The General ICD has the autonomy rules and a table (4.6) with the bits that are sent. John said he will cover what EPI-Lo expects in his presentation so the Kris can see if there are any disconnects.

4. EPI-Lo Autonomy – John Hayes/JHU-APL

Macro Capability

Macros can delay an amount of time or for a specific MET (i.e. ATS) – so they are both RTS and ATS.

Manual vs. Autonomous Operations

Discussions on how/when the autonomy bit gets set. Since the EPI-Lo FSW monitors it continually, and moves out of autonomy mode at any time if the bit changes, even if it started up in autonomous mode, the concern is that this bit has to be correct all of the time. For example, does this bit stay the same across a processor rotation?

Adrian joined the meeting and said he believed the default is manual mode and that the current setting is not conveyed to the rotation processor.

This approach would result in lost science in the event of a rollover. Could solve this operationally by always commanding the current and hot-spare processor, but this doesn't help with the cold spare processor.

Determined that this will have to be handled internal to EPI-Lo, by just having the default be autonomous instead of manual, and having EPI-Lo manage this internally by use of ground safing plugs (which already exist) and by manipulating the macro contents so that autonomous mode can be like manual mode if you aren't wanting to do the full autonomy.

So, in this scheme, S/C would ALWAYS send the autonomy bit, unless there was a need to load new EPI-Lo FSW in which case would set the manual bit and reboot (so the Bootstrap would stay in bootloader mode).

AI/Kris - Add notes to the S/C-to-EPI-Lo ICD re: decisions we made today on how the autonomy/manual bit will be used by EPI-Lo.

AI/Kris - Add this topic to the instrument team discussions as this may be an issue with other instruments as well. General discussion should be what is and isn't passed and whether there are issues with any of the instruments in that regard [see also the item above with regard to possible jitter on the solar distance/inbound/outbound flags).

Science Operations – Regions and Macros

Slide 7 says macros are run at threshold crossings, but in fact the FSW has a state machine that determines if it is in a region and if the macro is running or not, and if not runs it.

Q: Could something like the following scenario occur?

a) In Region A and running macro A
b) FSW reboots
c) FSW discovers still in Region A and runs macro A
d) Turns out the S/C was just crossing into Region B
e) FSW runs macro B, but macro A is still running
f) Macro B runs and is very short
g) Macro A is a longer macro and continues to run and "undoes" some of what Macro B did

A: The macros are very short – run in microseconds, so this shouldn't be a concern.

Further discussion was that it might be possible during calibration for there to be a longer operation in a macro, so this would need to be handled operationally. John mentioned they could use manual mode in this case – but manual mode may not be used anymore per prior discussion.

AI/Matt/Chuck/John - review design/ops plans and make sure that there are no other side effects of this "decision" to effectively not use the manual bit other than for reloading FSW.

Telemetry and HV Monitoring

The limit monitors are hard-coded in terms of the once, twice, more than twice logic. The limits themselves are programmable, but not the once/twice thresholds.

However, the HV limit monitors are custom coded and don't use this scheme.

Q: Can you disable the HV limits? SScott W noted that on prior instruments have sometimes had to disable them during HV ramp-up to avoid spurious triggers.

A: Yes they can be disabled but don't expect to have to do so. If disabled, you do still get the telemetry values.

Q: Scott W asked about issue of getting a lot of protons that might trigger a monitor and knock your HV down but you don't want that to occur, or at least not permanently - how handle this?

Much discussion – Matt mentioned maybe running at a lower gain. Chuck said they may run MCPs

Lower, but Matt said they want some of the protons – just not all of them.

AI/Chuck: (a) does instrument safety need to monitor count rates for safety? (b) does the instrument need to "dip" MCP voltages for some time period before going back to full levels when there are "large" solar events that we want to ride through and try to keep operating while remaining safe?

Issues to consider:

- Adding this adds complexity, which FSW is hesitant to do if there is no clear need.
- However, if you think you might want it, would probably be better to add it now vs. after launch.
- Adding this logic would mean that you now have two 'sources' for HV control which is a concern.

5. Wrap-Up Discussions

Review Steve Jaskulek's comments for open issues:

Open items had to do with the S/C interface and were both addressed.

Review of review objectives:

The inter-instrument autonomy was not discussed. John and Kris said bits had been added to the ITF per Jaskulek's recommendation at FSW CDR, but that the CONOPS for how those bits will be used has not been fully fleshed out. Kris said a table was presented at a Payload Systems tcons that defined who cares about what bits.

Related issues from recent SWT:

A couple of issues arose at the recent SWT meeting at UNH having to do with EPI-Lo's ability to do fixed vs. variable rate collection and implementation of a scheme to consume unused bandwidth at the end of an

orbit period (when approaching 0.25 AU inbound) with high-rate data. Would these issues impact the EPI-Lo FSW autonomy desing? Matt said these issues were still being discussed within the EPI-Lo team.

ACTION ITEM WRAP-UP

AI #	Who	What	When
1	Kris Fretz	Add notes to the S/C-to-EPI Lo ICD to document the decisions made today regarding use of the manual/autonomy bit.	Capture now in draft while fresh; publish at next ICD release
2	Kris Fretz	Add topic of what is and is not carried over to the rollover processor to upcoming discussions with other instrument teams. Specifically including the autonomy bit issue, and that there could possibly be jitter on the solar distance/inbound-outbound flags during a processor rollover.	Next instrument meeting
3	Matt/Chuck/ John	Review design/plans/assumptions and make sure there are no “side effects” of the decision to essentially not use the manual bit except for FSW reloads.	ASAP
4	Chuck/Matt/ John	(a) does instrument safety need to monitor count rates for safety? (b) does the instrument need to “dip” MCP voltages for some time period before going back to full levels when there are “large” solar events that we want to ride through and try to keep operating while remaining safe?	Earlier is better due to FSW design impact