Solar Probe Plus

A NASA Mission to Touch the Sun

Integrated Science Investigation of the Sun
Energetic Particles

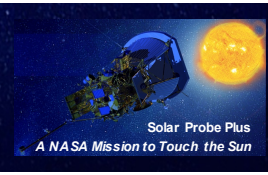
EPI-Lo Autonomy Review

24 June 2015

John Hayes

EPI-Lo Software Engineering (JHU/APL)

Overview

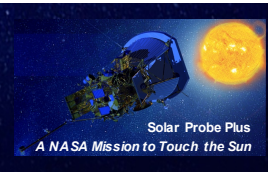


- Start-up: boot vs. application
- Stored command sequence (macros)
- Operations, per orbit
- Instrument safety

Start-Up

- Boot
  - Time and status from spacecraft includes startup mode: selects manual vs. autonomous operation
  - If autonomous operation is selected, EPI-Lo boot software will automatically try to boot a series of three programs from non-volatile memory (MRAM)
  - If autonomous operation is not selected, EPI-Lo boot software will wait for commands
- Application
  - If autonomous operation is selected, EPI-Lo application software will automatically:
    - Load macros from non-volatile memory
    - Run the start-up macro
  - If autonomous operation is not selected, EPI-Lo application software will wait for commands

Macros



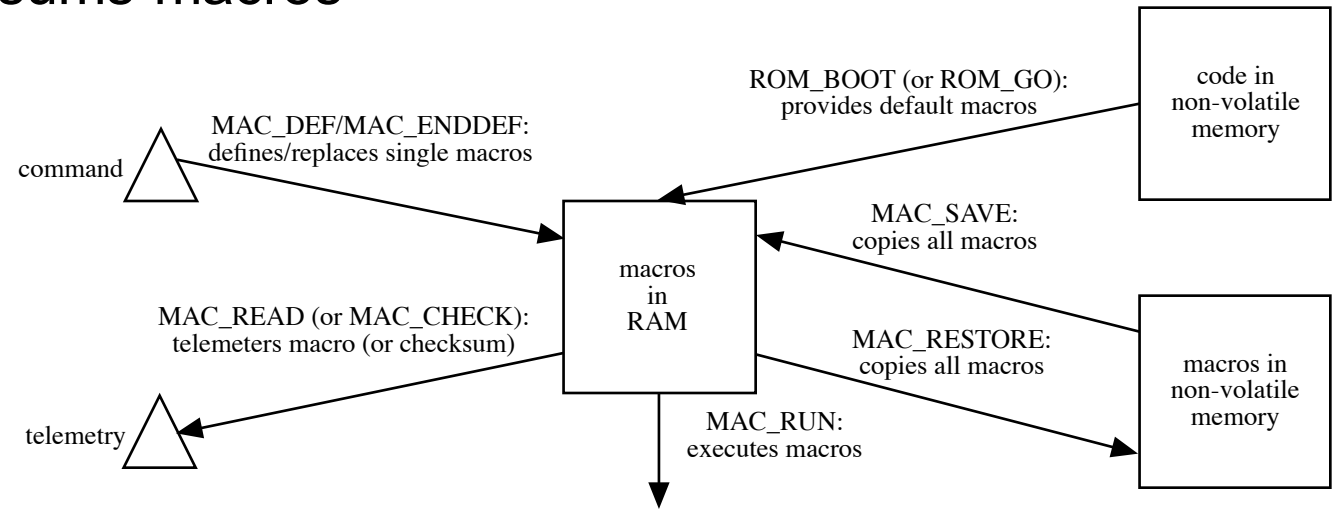
- Macros are stored sequences of commands
- 256 different macros can be defined
- 64 Kbyte of RAM is available for macro storage
- Macros can nest 16 deep; up to 64 macros can execute concurrently
- Real-time uplink commands take precedence over macro commands
- Commands from a macro are echoed; the echo includes a flag indicating that the command is from a macro

Macros - Definition and Control Flow

- Macros are “learned” by the instrument
  - EPILO_MAC_DEF starts a macro definition; any command uplinked with its “macro” arg set will be appended to the macro
  - EPILO_MAC_ENDDEF ends the definition
  - While a macro is being compiled, any real-time command, i.e., one without a set “macro” arg will be executed.
  - There is no need for macro compiler or macro memory management by ground software
- Macro control flow commands:
  - EPILO_MAC_DELAY and EPILO_MAC_PAUSE delay by a give number of seconds or until a given time, respectively
  - EPILO_MAC_NEST and EPILO_MAC_RUN nest a macro and starts a concurrently executing macro, respectively
  - EPILO_MAC_LOOP_BEGIN and EPILO_MAC_LOOP_END delimit a definite loop
  - EPILO_MAC_HALT kills a running macro

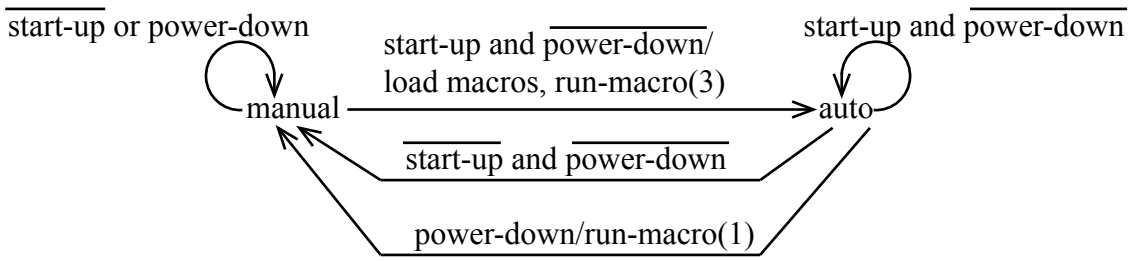
Macros - Dataflow

- Macros execute from RAM
- Macros can be saved in non-volatile memory (MRAM)
  - EPILO_MAC_SAVE saves and EPILO_MAC_RESTORE restores
  - These are done en masse, i.e. all macros are saved/restored
- Default macros can be pre-compiled in the flight software
  - Usually provides default responses involving instrument safety
  - Can be redefined or overridden by EPILO_MAC_RESTORE
- EPILO_MAC_READ dumps macros and EPILO_MAC_CHECK checksums macros



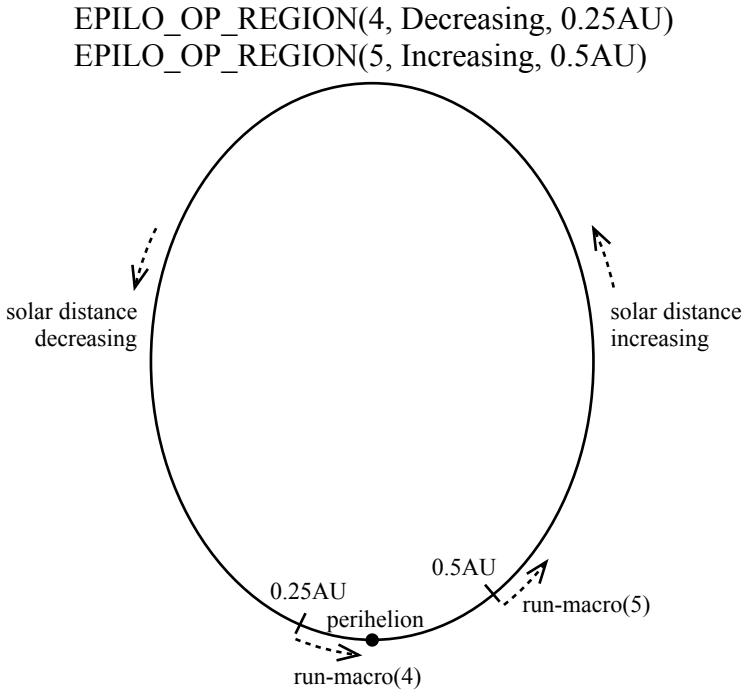
Operations

- Time and status from spacecraft includes
  - Startup Mode: selects manual vs. autonomous operation
  - Solar Distance:
    - Current distance to the sun (km)
    - Inbound vs. outbound flag
    - Validity flag
  - Power down warning flag
- If autonomous operation is selected, EPI-Lo software will:
  - Automatically load macros from MRAM
  - Run startup macro; this ramps up HVs, etc.
  - Monitor solar distance against a set of commandable thresholds
    - Different threshold crossings trigger different macros to run
    - Macros configure science collection, e.g. integration times, etc.



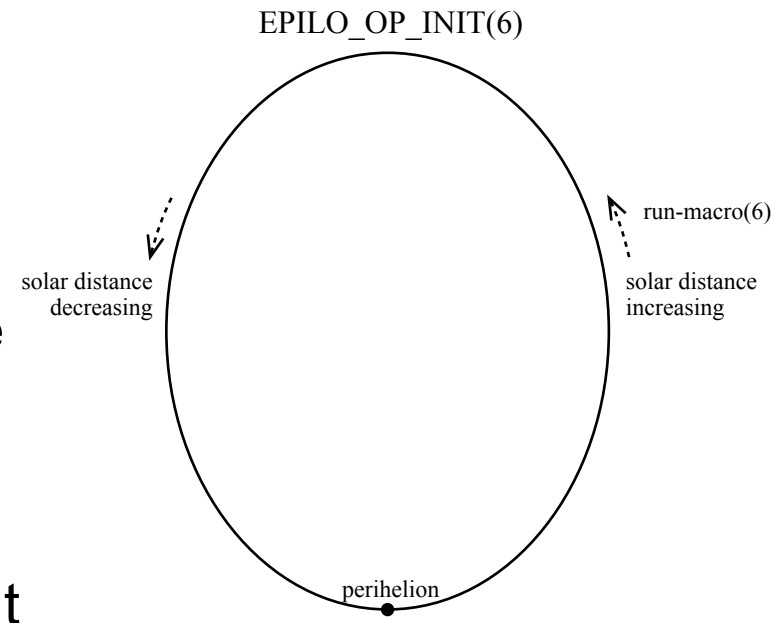
Operations - Regions Definition

- EPILO_OP_REGION command defines a region within the orbit
  - Arguments specify start of region; region extends to start of next region
  - Argument also specifies macro to run when region is entered
  - Up to 25 regions can be defined
- EPILO_OP_READ command dumps the definition of all regions



Operations - Regions Initialization

- EPILO_OP_INIT command initializations regions
  - Deletes all region definitions
  - Argument specifies macro to run
- Region definitions can be saved in non-volatile memory (MRAM)
  - Regions definition commands can be executed from macros, macros can be saved in MRAM, and therefore region definitions can be saved
  - Region definitions for a “generic” orbit could be available in the default macros



Instrument Safety - Alarms and Monitors

- Alarm packet is generated in response to a software problem or to a monitored value going out of limits
- Monitors watch analog voltages, currents, and temperatures
  - If a monitored value is out-of-limits just once, a transient alarm is reported
  - If a monitored value is consecutively out-of-limits twice, a persistent alarm is reported and the software may take corrective action
  - If a monitored value is consecutively out-of-limits more than twice, either corrective action is taken again, the shutdown macro is run, or nothing is done, depending on the thing being monitored
- Commands:
  - EPILO_MON_CNTRL enables or disables corrective action

Instrument Safety - Monitoring Algorithm

- High response (low response is similar):

```
high once:
      issue transient high alarm

high twice:
      issue persistent high alarm
      if enabled (via EPILO_MON_CNTRL command)
            execute high response macro for this alarm

high more than twice:
      case of monitor class
            current/voltage:
                  if enabled (via EPILO_MON_CNTRL command)
                        run shutdown macro
            temperature:
                  nop
            count rate:
                  if enabled (via EPILO_MON_CNTRL command)
                        re-execute high response macro
```

Instrument Safety - HV Over-Current

- Hardware monitors MCP HV current
  - EPILO_MCP_CUR_LIMIT command sets current limit
  - EPILO_MCP_CUR_ENB command enables/disables monitor
  - Analog circuitry compares current against limit, generates “trip” on over-current
  - FPGA monitors trip; if seen:
    - Generates MCP HV shutdown
    - Indicates “fault” to software
  - HV cannot be turned back on until current is within limits and monitor is disabled
- Software monitors fault indicator; if seen:
  - Issue alarm packet
  - Zeros control DAC
  - Runs response macro
- Independent current limits, monitors, and macros, per quadrant

Instrument Safety - Miscellany

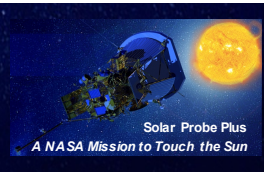
- Communications from spacecraft are monitored
  - If no communications are received within a timeout, the safing macro (macro 2) is run
  - EPILO_SAF_TIMEOUT command sets the timeout (s)
- Watchdog timer monitors software health
  - Timeout is ~4 seconds
  - Managed by application software from lowest priority process
  - Boot software starts on reset
    - If watchdog reset, a memory dump is started
    - If autonomous operation is selected, the dump is allowed to complete before restarting application software
- Various “last-ditch” commands are available to macros
  - EPILO_SAF_OFF requests power off
  - EPILO_SAF_CYCLE requests power cycle
  - EPILO_SAF_RESET forces a watchdog reset

Status

- Software implemented and tested
- Changes since peer review (Nov. 3, 2014)
  - Added command and telemetry to support operation regions dump
  - Added delay in boot software to allow watchdog reset memory dump to complete before autonomously re-booting


ISIS
Solar Probe Plus
Energetic Particles

Appendix


Solar Probe Plus
A NASA Mission to Touch the Sun

Monitored Data

- High temperatures cause shutdown
- Power supply problems cause emergency shutdown
- +13V current too high triggers HV shutdown

Source	Class	Alarm Ids Low / High		Macro Ids Low / High	
A1 SSD temperature	N	128	192		1
A2 SSD temperature	N	129	193		1
B1 SSD temperature	N	130	194		1
B2 SSD temperature	N	131	195		1
C1 SSD temperature	N	132	196		1
C2 SSD temperature	N	133	197		1
D1 SSD temperature	N	134	198		1
D2 SSD temperature	N	135	199		1
A Anode temperature	N	136	200		1
B Anode temperature	N	137	201		1
C Anode temperature	N	138	202		1
D Anode temperature	N	139	203		1
Event board temperature 1	N	140	204		1
Event board temperature 2	N	141	205		1
+1.5V current	S	142	206		10
+3.3V current	S	143	207		10
+5V current	S	144	208		10
+13V current	S	145	209		8
LVPS temperature	N	146	210		1
Primary current	S	147	211		10

Monitored Data (Cont.)

- +13V voltage too low, or common HV voltage too high triggers HV shutdown
- SSD voltage or power too high triggers SSD shutdown
- Current or voltage too high on individual HVs cause shutdown on just that HV

SSD BV power 2	N	148	212		9
+3.5V voltage	S	149	213	10	10
+13V voltage	S	150	214	8	10
+5V voltage	S	151	215	10	10
+3.3V voltage	S	152	216	10	10
+1.5V voltage	S	153	217	10	10
SSD BV power 1	N	154	218		9
SSD BV voltage	N	155	219		9
Common HV voltage	N	156	220		8
A HV voltage	N	157	221		4
B HV voltage	N	158	222		5
C HV voltage	N	159	223		6
D HV voltage	N	160	224		7
A HV current	N	161	225		4
B HV current	N	162	226		5
C HV current	N	163	227		6
D HV current	N	164	228		7

Default Macros

- Only macros used by instrument safety autonomy have defaults
- Safing stops science and ramps down HV and BV
- Shutdown runs safing, waits, then requests power off
- Emergency shutdown requests power off, then runs safing
- Separate ramp down of each HV

ID	Action	Commands
0	No action	EPILO_CMD_NULL
1	Shutdown	EPILO_MAC_NEST 2 EPILO_MAC_DELAY TBD EPILO_SAF_OFF
2	Safing	TBD
3	Startup	TBD
4	MCP HV A off	EPILO_HV_MCP_LEVEL 0 A
5	MCP HV B off	EPILO_HV_MCP_LEVEL 0 B
6	MCP HV C off	EPILO_HV_MCP_LEVEL 0 C
7	MCP HV D off	EPILO_HV_MCP_LEVEL 0 D
8	MCP HV off	EPILO_MAC_NEST 4 EPILO_MAC_NEST 5 EPILO_MAC_NEST 6 EPILO_MAC_NEST 7 EPILO_COM_HV_LEVEL 0
9	SSD bias voltage off	EPILO_BV_LEVEL 0
10	Emergency off	EPILO_SAF_OFF EPILO_MAC_NEST 2
11 - 20	*Reserved for instrument safety*	
21 - 45	*Reserved for autonomous operations*	
46 – 255	*Reserved for other operations*	