Peregrine Payload Networking

November 12th, 2019

This document is a brief on upcoming changes to the Astrobotic Peregrine IDD (Rev. G). It is intended only as a reference to payloads, to inform and update your design process. **This document does not replace or supersede the IDD Rev. F and is subject to change.**

Payload Networking Concept of Operations

The goal of the network described here is to provide a communication channel between payloads and their respective PMCC's. The communication channel is comprised of three primary segments, payload to lander (wired or WLAN), lander to DSN/AMCC (earth to/from space RF link), and the AMCC to PMCC (ground segment). Together these three segments link payloads to their respective control centers.

The lander to DSN/AMCC segment of the communication channel is unreliable because of the nature of deep space RF communication. DSN estimates that between $1/10^3$ and $1/10^4$ CCSDS packets will be dropped or corrupted. If necessary, the PMCC will need to implement mechanisms to cope with the unreliability of the lander to DSN/AMCC segment such as packet counters, acknowledgements and re-send requests, etc. Additionally, payloads should expect latencies between the payload and PMCC to be between 4 to 40 seconds.

The primary data unit of the payload network connection is not defined by a single packet or datagram. Instead, Astrobotic has defined clearly structured message formats for Payload Data and Commands described in the later sections of this document. Each message consists of header information which may be modified, added or removed by Astrobotic, however, the encapsulated payload data and commands are delivered without modification by Astrobotic.

This architecture provides transparency to the Payload Data and Commands. The exception to this process is the inspection of the "Command Hazard ID" on the header of a Command packet. Details of this exception will be provided later on this document.

Figure 1 illustrates the downlink chain, elements of which are described in detail in the following sections.

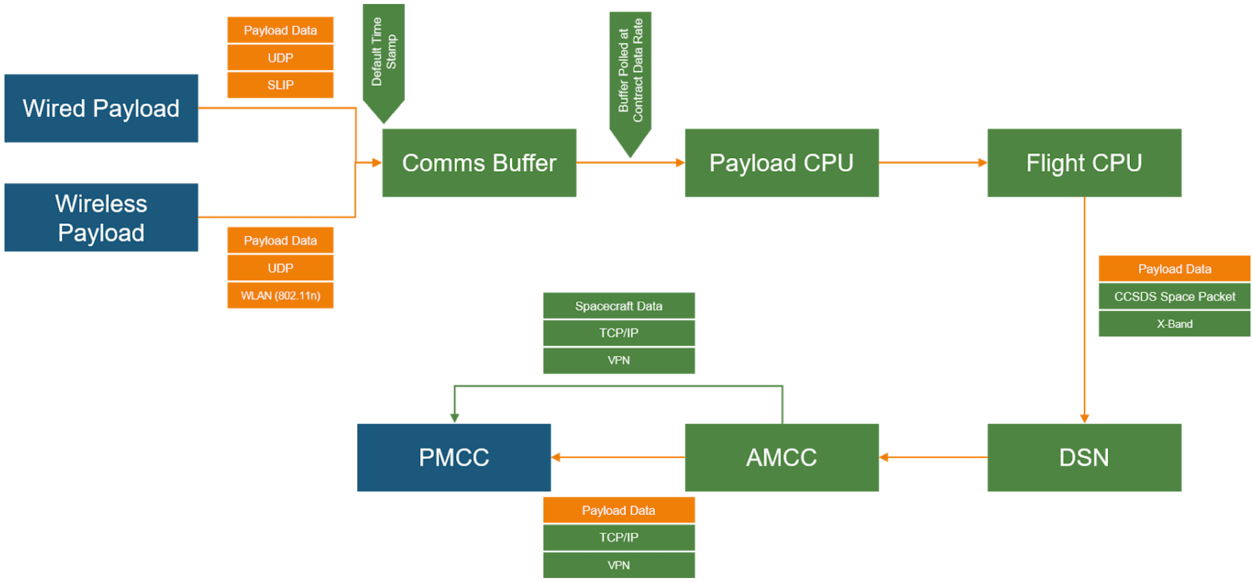

Figure 1: Illustration of the Astrobotic Payload Telemetry Architecture

Payload

Payloads are responsible for determining what telemetry is necessary for operation and monitoring. Payloads may communicate with the lander using one of two wired data interfaces, Serial RS-422 or Spacewire. Deployable payloads may connect to the lander using 802.11n WLAN for wireless communication.

The lines of responsibility for payload data are drawn at the Serial or Wireless links between payloads and the lander. Each party is responsible for the transceiver/receiver pair on the payload and lander respectively. Astrobotic is responsible for all wired communications harness up to the standard electrical connector interface.

Payload Communications Buffer

The payload communications buffer is the first part of element Astrobotic's provided downlink path. The buffer is designed to allow the spacecraft to communicate with payloads at different data-rates than the allocated downlink to earth would otherwise allow.

The communications buffer shall not be used as data storage, and Astrobotic does not guarantee the delivery of data stored in the data buffer. If payloads wish to store data for deferred transmission that data storage shall be incorporated into the payload design.

Payload data will be time stamped upon entering the buffer. Each payload communications buffer is then polled by the payload CPU at the allocated data rates, in a First In, First Out (FIFO) order.

When the lander loses downlink to earth (LOS) the communications buffer is erased and all payload data is ignored until the downlink resumes (AOS). This enables payloads to communicate with low latency to earth. During transit the lander will be in AOS for 4 hours followed by 4 hours of LOS. On the surface the lander will be in AOS for 7 hours followed by 1 hour of LOS while the lander establishes connection with a new ground station.

Payload CPU

The payload CPU is responsible for communication with all payloads and the default time stamping of payload data. The payload CPU polls the data buffer for each payload in a FIFO order, and passes the packets to the flight CPU for transmission to the ground.

Flight CPU

The flight CPU encapsulates payload data, and the Astrobotic time stamp, into a CCSDS packet which is transmitted to the ground.

Deep Space Network (DSN)

Astrobotic handles all interfaces with the DSN. The RF link will be entirely transparent to payloads with the exception of any dropped or corrupted packets.

Astrobotic Mission Control Center (AMCC)

The AMCC is the ground interface for the DSN and Payload Mission Control Centers, payload telemetry is received and removed from the CCSDS packet. The packets, now in the payload telemetry message format described in figure 4, are then transmitted to a network socket in a secure, payload specific, Virtual Private Network (VPN) over an internet connection (TCP/IP).

Payload data is logged as it enters the AMCC, ensuring that no data is lost in the event that a PMCC loses connection to the AMCC.

The AMCC is also responsible for processing and assembling a separate stream of ephemeral lander telemetry and information, which will be published for use by payload teams.

Payload Mission Control Center (PMCC)

The PMCC is the payload customer's responsibility and is comprised of the hardware and software used to operate payloads from the earth.

The line of responsibility between the Astrobotic and Payload customer systems is the TCP/IP payload telemetry stream created by Astrobotic. All payload data processing and commanding is to be handled by the PMCC.

Payload Messages

The goal of the Peregrine payload networking scheme is to allow payload telemetry and commands to be a black box to any Astrobotic systems. Astrobotic does not modify any payload telemetry or commands, however, certain framing for payload messages is required, added or modified by Astrobotic systems to facilitate the safe and effective operation of payloads.

Payload Command Messages

Payload customers will connect to the Astrobotic AMCC from their PMCC using a TCP connection through a Astrobotic provided VPN. The PMCC should structure their commands as follows when sending them through the VPN link to the Astrobotic AMCC.

Figure 2: Command Message Format as it is Transmitted to the AMCC

Message Size (2 bytes, big endian): a field that indicates the size in bytes of the following message minus one (Command Hazard ID + Payload Command -1). This field is used by the Astrobotic AMCC to determine message boundaries when reading from the TCP connection from the payload PMCC over VPN.

This field is removed by the AMCC before transmitting the Payload Command to the spacecraft, and payload.

Command Hazard ID (2 bytes, big endian): contains an unsigned integer that corresponds to the hazard level of the command in the "User Data" field. These numbers will be assigned to individual commands once each customer's command list/dictionary is reviewed by Astrobotic. As commands to individual payloads may be in different user-defined formats, Astrobotic has no insight into the actual contents of the command being sent. Thus, this field is used to electronically determine whether a command is hazardous for the current flight phase before uplinking to Peregrine.

This field is removed by the AMCC before transmitting the Payload Command to the spacecraft, and payload.

Payload Command (<=978 bytes): this field contains the command for the payload that the PMCC wishes to transmit to their payload. This field must be <=978 bytes in length. Commands greater than this length are discouraged but if necessary, may be split among multiple command messages. Customers should keep in mind that although the TCP link between the customer's PMCC and the Astrobotic AMCC is reliable and error-free per TCP specifications, the space-to-ground RF link is not, and frames may be occasionally dropped. Thus, customers shall implement mechanisms to cope with the unreliability of the DSN to/ from AMCC's RF Link, such as packet counters, acknowledgements and re-send requests. This will be especially important if customer payload commands are larger than the 978 byte message limit and must be split between messages. Due to the limited spacecraft uplink capability, payloads with large frequent commands may be throttled by the AMCC.

Message Size and Command Hazard ID fields should be in **big endian** byte order. The Payload Command field may be in whatever byte order the payload customer prefers, as the user data will be delivered as-is to the payload. The AMCC and Spacecraft treat the payload command field transparent manner.

Both wired (RS-422/Spacewire) payloads and wireless (802.11n) payloads will receive their payload command messages over a UDP connection from the lander. The UDP datagrams will contain the payload command field only, as the other fields (message size and Command Hazzard ID) will have already been stripped off. Note that commands are packaged by Astrobotic into standard CCSDS "Space Packets" for the RF link segment, however, the CCSDS packet header will be removed prior to forwarding the command user data on to the payload.

Addressing of payload commands is handled entirely by Astrobotic. Commands are flagged as being received from a specific PMCC on the ground and delivered to the appropriate payload.

Figure 3 illustrates the payload commanding architecture.

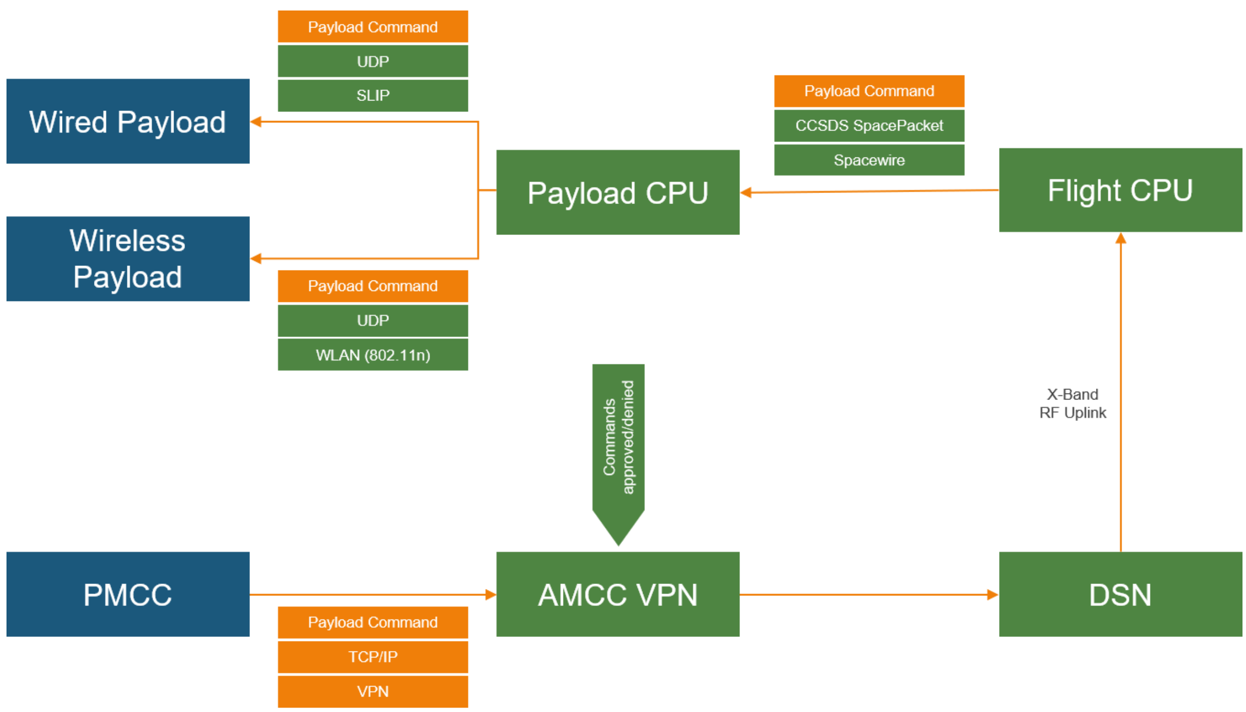

Figure 3: Illustration of the Astrobotic Payload Command Architecture

Time At the Tone Commands

The only command generated by the lander for payloads is for the "time at the tone" time synchronization service. This service is comprised of a 1 Pulse Per Second (PPS) signal, or tone, on a dedicated differential pair and an associated time synchronization command. This service is available to wired payloads using both RS-422 and Spacewire.

The service functions by sending a command with a timestamp to all payloads in advance of the tone, which is synchronized to the lander clock at the time of the 1 PPS tone. The command must include a 4 byte second, and 4 byte subsecond time stamp. Payloads must specify in the ICD if additional headers or encapsulation of this data is necessary for the command to be properly ingested by the payload.

Hazardous Commands

Hazardous commands are telecommands that, if executed in inappropriate circumstances, could threaten the mission, or other payloads. Upon receipt of the final payload command and telemetry lists, Astrobotic will work with the payload customer to assign each command a command hazard ID, which is used to populate the field of the same name. Astrobotic expects that any updates to the command and telemetry lists after these ID's have been assigned will be shared with Astrobotic for approval.

Hazardous commands include, but are not limited to:

- Any physical deployment activity of the payload from the Spacecraft;
- Any physical actuation activity of a payload and its subsystems while still attached to the Spacecraft;
- Any release or activity that produces, generates, or releases a mechanical, electrical, combustion, or chemical load and/or reaction from the payload; and
- Any release or activity that releases any solid, liquid, or gaseous matter from the payload.

When a payload is enabled to command, Astrobotic may enable only non-hazardous commands or all commands depending on the mission phase. Hazardous commands sent during a phase where those commands are not enabled will be flagged and not transmitted beyond the AMCC. Once the spacecraft enters a mission phase where the hazardous commands are considered safe, Astrobotic will enable their transmission and inform the Payload Customer.

Payload Telemetry Messages

Payloads should send their telemetry data in the form of UDP datagrams of <= 978 bytes each. Payload telemetry data will then be removed from these UDP datagrams and encapsulated into standard CCSDS "Space Packets" and downlinked to the Astrobotic AMCC. The AMCC will then strip off the space packet headers and deliver the payload telemetry messages to the customer PMCC in the following format. The "payload telemetry" field will contain the contents of the original UDP datagram as sent to Peregrine from the payload. Note that routing is handled by the Astrobotic system and the IP and UDP headers are not preserved. Only the data transmitted within those datagrams are delivered to the PMCC as "payload telemetry".

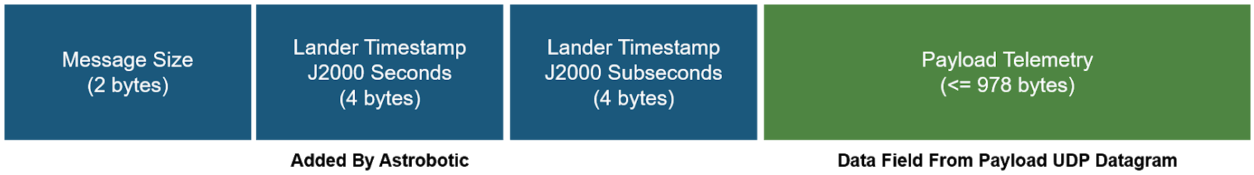

Figure 4: Telemetry Message Format as it is Delivered to the PMCC

Message Size (2 bytes, big endian): a field that indicates the size in bytes of the following message minus one (Lander Timestamp Seconds + Lander Timestamp Subseconds + Payload Telemetry -1). This field will be used by the customer PMCC to determine message boundaries when reading from the TCP connection from the Astrobotic AMCC over VPN.

This field is added to the message by the AMCC.

Lander Timestamp Seconds (4 bytes, big endian): indicates whole number of seconds since J2000 epoch as encoded by Peregrine at time of receipt. This time stamp will be added regardless of if payloads choose to add an internal payload timestamp within the payload telemetry field.

This field is added to the payload telemetry message by the Peregrine lander.

Lander Timestamp Subseconds (4 bytes, big endian): indicates fractional number of seconds since J2000 epoch as encoded by Peregrine at time of receipt. Together with the Lander Timestamp Seconds field, this field gives the full resolution time of receipt of the telemetry message at Peregrine's payload computer.

This field is added to the payload telemetry message by the Peregrine lander.

Payload Telemetry (<=978 bytes): this field may contain downlink/telemetry data in any format the payload customer wishes. This field must be <=978 bytes in length. Customers should keep in mind that although the TCP link between the customer's PMCC and the Astrobotic AMCC is reliable and error-free per TCP specifications, the space-to-ground-link is not, and frames may be occasionally dropped. Thus, customers shall, if necessary, implement mechanisms to cope with the unreliability of the DSN to/ from AMCC's RF Link, such as packet counters, acknowledgements and re-send requests, etc. This will be especially important if customer payload telemetry is larger than the 978 byte message limit and must be split between messages.

Message Size and Lander Timestamp fields should be in **big endian** byte order. The Payload Telemetry field may be in whatever byte order the payload customer prefers, as the user data will be delivered to the PMCC in the same byte order it was sent from the payload.

Network Configuration

Astrobotic supports both wired and wireless payload communications, wired payloads interface with the lander over Serial RS-422 and use the Serial Line Internet Protocol (SLIP) which is defined in RFC 1055 as an encapsulation of the Internet Protocol (IPv4) RFC 791, for use over serial interfaces. Payloads transmit and receive data from the lander using the User Datagram Protocol (UDP), an alternative transport layer protocol to TCP, which is defined in RFC 768.

Wireless payloads connect to the lander using standard 802.11.n WLAN and transmit data using UDP. Deployable payloads must also include a wired connection for communication during transit.

UDP connections should be considered peer to peer, where neither endpoint need be considered a master. This allows for transparent reestablishment of communications if either endpoint is restarted.

Wired Configuration

The Serial Line Internet Protocol is an encapsulation of the Internet Protocol designed to work over serial ports and router connections. SLIP is a relatively simple protocol which does not provide error detection and requires that an IP address be configured before the connection is established. SLIP was selected for its very low overhead and relative simplicity to implement.

Baud rates are negotiated between Astrobotic and the payload customer. The SLIP connection is configured as described in Table 1.

Table 1: SLIP Configuration Parameters Controlled by Astrobotic

Parameter	Value
Baud Rate	TBR (negotiated <= 115,200)
Flow Control	None
Carrier Detect	None
Authentication	None
Maximum Transmission Unit	2,012 bytes[1]

Note 1. SLIP implements an “ESC” byte for the “END” byte which means the Maximum Transmission Unit (MTU) at the data link (SLIP) layer must be double the MTU at the network (IP) layer. This doubling is to accommodate the case where a maximum size packet at the IP layer is comprised entirely of “END” characters.

As SLIP is a link layer protocol, payloads must also implement an IPv4 stack. While it is possible to mimic IPv4 datagrams without the implementation of a full IP stack Astrobotic recommends the use of full IPv4 implementations to guarantee compatibility. Since each wired payload requires a unique network interface, and SLIP does not support the dynamic assignment of IP addresses, each payload will therefore be assigned an IPv4 address by the Astrobotic team.

The IPv4 configuration requirements are described in Table 2.

Table 2: IPv4 Configuration Parameters Controlled by Astrobotic

Parameter	Value
Maximum Transmission Unit	1,006 bytes
Source IPv4 Address	TBD (assigned by Astrobotic)
Destination IPv4 Address	TBD (assigned by Astrobotic)

The User Datagram Protocol is an alternative transport layer protocol to the Transmission Control Protocol (TCP). Port numbers need not be tightly controlled between payloads and may be negotiated between payload customers and Astrobotic.

The UDP configuration requirements are described in Table 3.

Table 3: UDP Configuration Parameters Controlled by Astrobotic

Parameter	Value
Source Port	TBR (negotiated)
Destination Port	TBR (negotiated)
UDP Checksum	Required

Interface Availability

Since the connection between between payloads and the lander, with the exception of deployable payloads, is permanent it is safe to assume that the Astrobotic SLIP interface will be configured and available whenever payloads are powered. However, the RF link between the lander and AMCC is intermittent and payload data received when the lander is in LOS will be ignored. For more details on the AOS/LOS timing see the payload networking concept of operations.

Wireless Configuration

Deployable payloads may communicate with the lander using the WLAN 802.11n standard.

The following parameters are used to configure the wireless network connection to payloads:

Table 4: WLAN 802.11n Network Configuration

Parameter	Value
Maximum Data Rate	600 Mbps[1]
RF Band	2.4 GHz
Channel Width	40 Mhz

Note 1. The bitrates and bandwidth listed are only for the WiFi link from the lander to the wireless payloads. The actual bitrate assigned per payload for transmissions to earth using the RF link is the one that has been agreed with each customer.

IP addresses for wireless payloads are statically assigned by Astrobotic. The IPv4 configuration requirements are described in Table 5.

Table 5: IPv4 Configuration Parameters Controlled by Astrobotic

Parameter	Value
Maximum Transmission Unit	1,006 bytes
Source IPv4 Address	TBD (assigned by Astrobotic)
Destination IPv4 Address	TBD (assigned by Astrobotic)

Wireless payloads use UDP datagrams to transmit telemetry and receive commands from the lander. Each wireless payload will be assigned a port number by Astrobotic, all payload data and commands will be sent through this port. The SNTP time synchronization service will utilize port 123 for all payloads. Note that UDP over wireless connections is not a reliable packet delivery service, therefore, wireless payloads should consider implementing loss tolerant systems or automatic resend requests for critical telemetry.

The UDP configuration requirements are described in Table 6.

Table 6: UDP Configuration Parameters Controlled by Astrobotic

Parameter	Value
Source Port	TBD (assigned by Astrobotic)
Destination Port	TBD (assigned by Astrobotic)
SNTP Port	123
UDP Checksum	Required

Bandwidth Estimation

Telemetry is polled from the payload communications buffer at the contracted data rate. Table 7 describes what overhead is counted against this bandwidth and what is not.

Table 7: Bandwidth Overhead

Overhead	Size (bytes/packet)	Transmitted
Payload telemetry	<978	Yes, created by payload
SLIP “esc”/”end” characters	2-1008	No, removed by lander.
IP header	≥20	No, removed by lander.
UDP header	8	No, removed by lander.
Lander timestamp	8	Yes, added by lander
CCSDS header	6	Yes, added by lander
Message size	2	No, added by AMCC