Homogeneity of Frame Secondary Header/Insert Zone across CCSDS Link Protocols

Greg Kazz/Ed Greenberg
Jet Propulsion Laboratory,
California Institute of Technology
28 April 2010

Copyright 2010 California Institute of Technology. Government sponsorship acknowledged.

Agenda

1. What's New in proposed common definition and use of Insert Zone and Frame Secondary Header in CCSDS Link Layer Protocols
   - Brief overview of new frame formats and services

2. How these newly proposed protocol features can be implemented within Constellation to unify and simplify the production of all Telemetry and Command services between Mission Systems and Orion, et al.
   - Simplification achievable by using the new services
   - Detail description of how all the Constellation Program data formats can be accommodated by a single implementation approach

What's New in proposed Link Layer Protocols

- Link Layer Security
  - Provides Authenticated Encryption service*
    - Added and removed by the User
    - Transparent to the supporting link layer services

- Secondary Header Data Service
  - Provides a new pathway to support delay intolerant data
  - Dynamic Service to elastically support the various instantaneous data needs such as
    - Range Safety
    - Operational Voice

*In which the sender first encrypts the input frame data supplied by the user, then computes an authentication message digest over the resultant [uncoded] transfer frame.

Link Layer Security Methodology*

- Security Block Description
  - An integrated data block placed into the Insert Zone of the AOS frame containing the fields necessary to identify and accommodate the Authentication and/or the Encryption of the frame's data contents
  - Can be structured to provide identical security for all Virtual Channels (VC) or individually for each VC
  - Contains the following Fields:
    - A Security Protocol Identifier (SPI-identifies the current key and parameter usage)
    - An optional counter field (for use in the AES_GCM security process)
    - The ICV (initialization vector) to hold the created Authentication Tag
    - Optional Initialization and Pad fields (not used in AES_GCM process)

*Note: This Methodology is defined in the Draft CCSDS Orange book *Cryptographic Service for CCSDS Data Links*

Proposal for Harmonizing Insert Zone/FSH fields in TM/AOS/TC frames

- This presentation describes the proposed format changes to:
  - **TM** Space Data Link Protocol, CCSDS 132.0-B
  - **AOS** Space Data Link Protocol, CCSDS 732.0-B
  - **TC** Space Data Link Protocol, CCSDS 232.0-B

FSH and Insert Zone in Current Blue Books*

- Optional fields for carrying additional data in **TM** and **AOS** Transfer Frames:
  - **TM** frames have FSH for a Virtual Channel or for a Master Channel
  - **AOS** frames have Insert Zone for a Physical Channel
  - Lengths of the FSH and Insert Zone are fixed, usually for a mission phase
    - as a result, the length of the Frame Data Field is fixed within a Virtual Channel

*Published Blue Books, September 2003 (TM) and July 2006 (AOS)

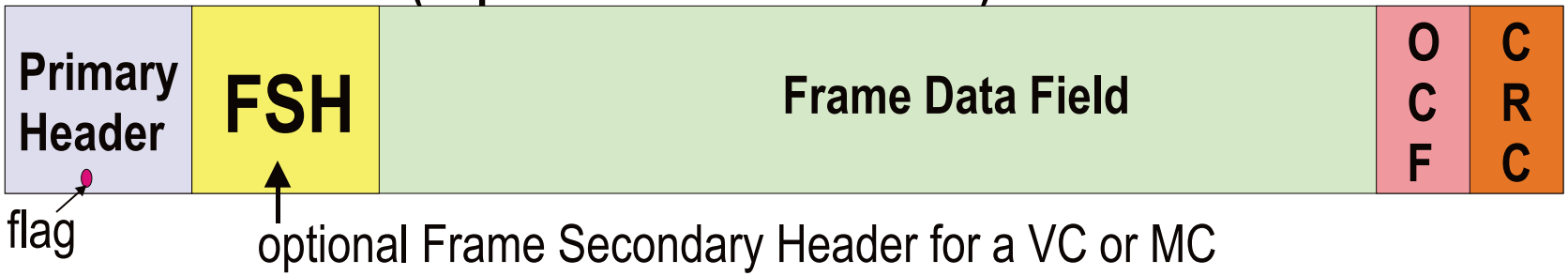
FSH and Insert Zone in CCSDS Blue Books

- ***definitions:***
  - *Master Channel (MC): all the frames with the same Spacecraft ID on the same Physical Channel*
  - *Virtual Channels (VCs) allow multiple users to share a Master Channel*
  - TM and AOS frames are *fixed length and operate over a synchronous data link*
  - TC frames are *variable length and operate over an asynchronous data link*
  - *FSH is signaled (by flag in TM primary frame header) and has internal length field, giving maximum length of 64 octets*
  - *Insert Zone is a managed field that allows for the insertion of periodic data within a Physical Channel*

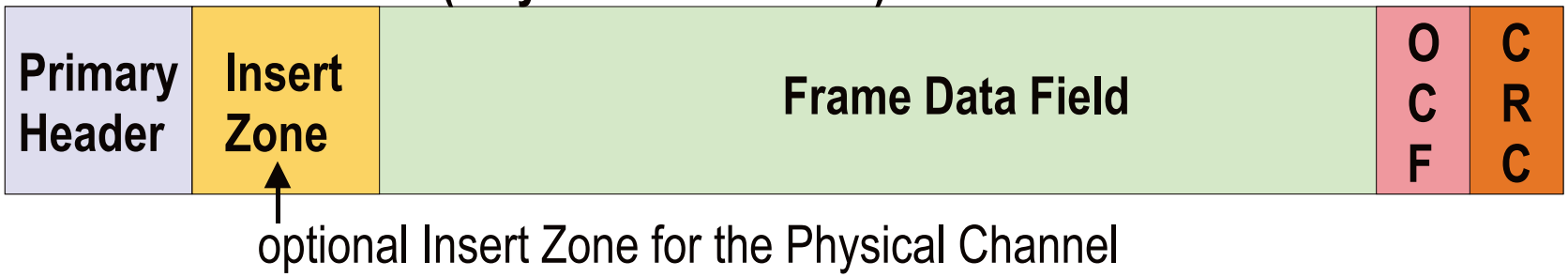
Proposed Changes to TM/AOS Space Link Protocols

- TM and AOS frames to have **Frame Secondary Header per Virtual Channel**
- TM and AOS frames to have **Insert Zone for a Master Channel**
- Introduce option to **vary the length of the FSH within a Virtual Channel**
  - Also intended for **multiple users** of the FSH service for the Virtual Channel

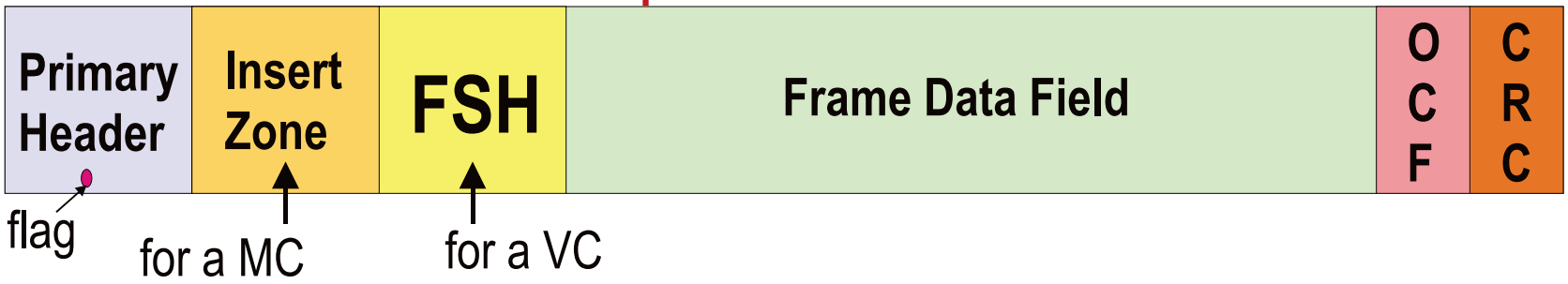
TM Transfer Frame (September 2003 Blue Book)



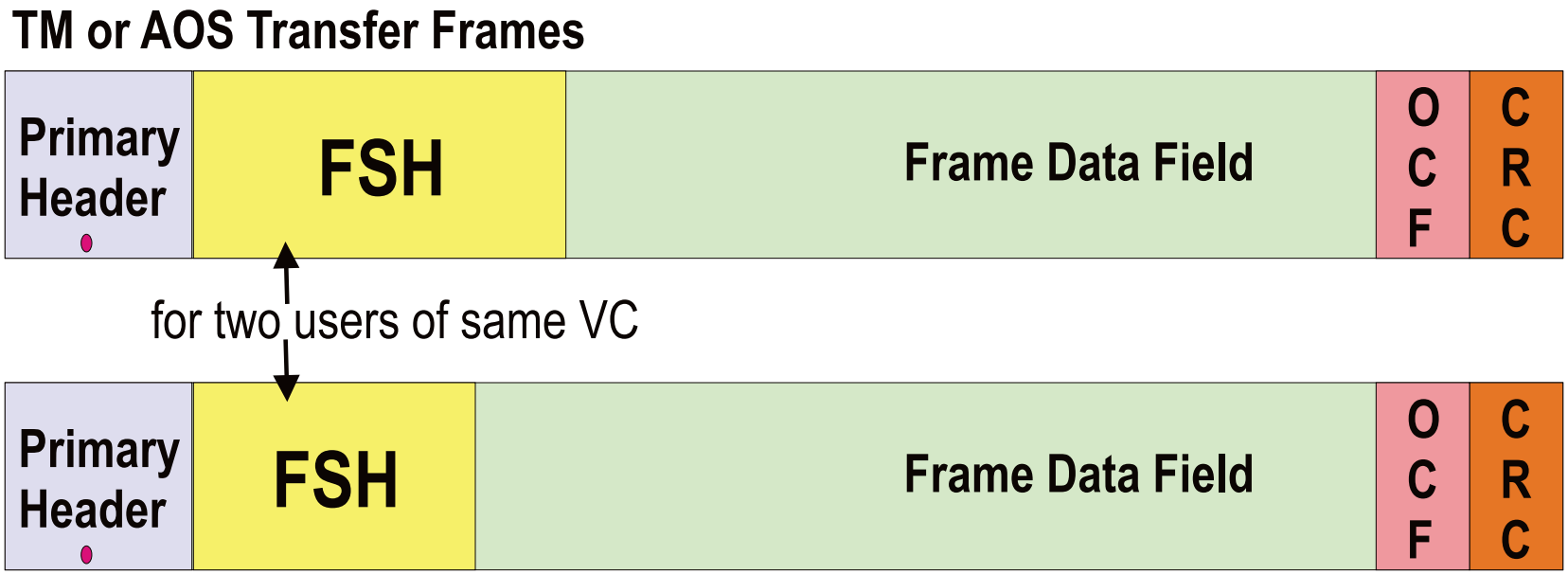
AOS Transfer Frame (July 2006 Blue Book)



TM or AOS Transfer Frame Proposed Format



Proposed Format: Variable-length Frame Secondary Header within a VC

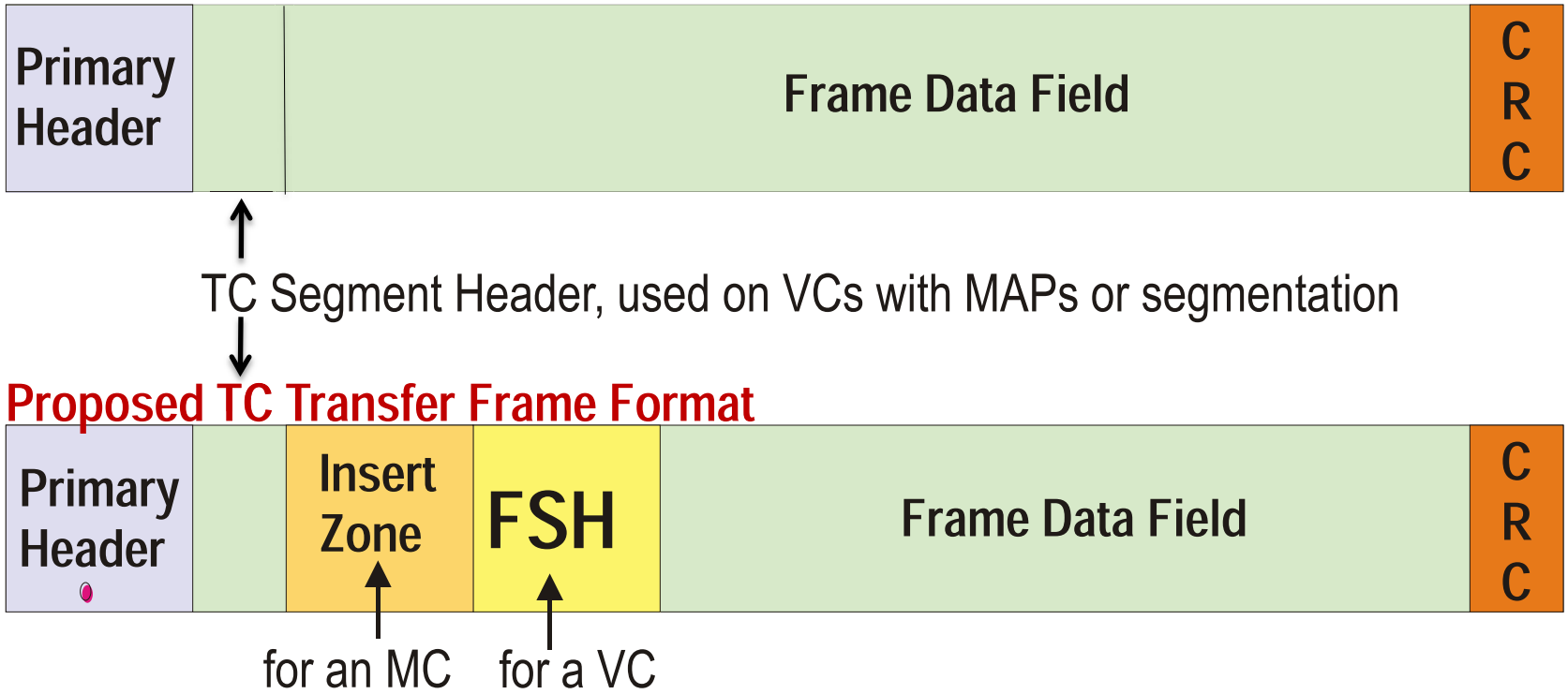


Note: We are proposing a variable length FSH to provide missions with a more flexible FSH data service for mission modes, using the FSH length field.

Proposed Changes to TC Space Link Protocol

- **TC** frames to have variable-length **Frame Secondary Header for a Virtual Channel**
- **TC** frames to have fixed-length **Insert Zone for a Master Channel**
- Current drafts for the *Cryptographic Service* show the Security Block FSH follows the TC Segment Header (which is inside the Frame Data Field)
- In **TC**, Insert Zone and FSH follow the TC Segment Header, which is now outside the Frame Data Field.

TC Transfer Frame (September 2003 Blue Book) Format



Why Constellation should consider using the proposed AOS protocol services

- The newly proposed AOS service provides capabilities that Constellation requires (i.e. link layer security)
- These services offer a capability that can unify and simplify the implementation of all AOS frames for both Telemetry and Command
- Offers a single method for including operation voice in all operational modes with minimum overhead
  - also provides an automated way for correlating dissimilar voice when delivered via different physical paths
- A single AOS Frame Construction technique is utilized

Attributes of FSH Data Service

- An optional data block whose inclusion in the frame is announced by a flag in the AOS primary header
- The use of the Secondary Header Data Service is applied on an individual VC basis
- The FSH is self-delimited (includes a length field) and self identifying (includes a type/identification field)
- The FSH will only appear within the frame when its service is required
- The size of the FSH can elastically adjust to the instantaneous need of the user of the VC

AOS Frame Organization for Constellation (CxP)

ASM	Primary Header	Insert Zone (Security Data)	Secondary Header Data Unit	MPDU
		SPI-CTR-ICV	Header-Type-Data	Header- Packets
4 Bytes	6 Bytes	(1+X+8 Bytes)	[2+(Y) Bytes]	(2+Z Bytes)

1. **Primary Header**
   - Master Channel ID, VC ID, VC Counter, Secondary Header Flag
2. **Insert Zone** (Security Data Unit)
   - Managed field that is present in all VCs of a Master Channel
   - SPI (Security Key ID #), Counter LSBs (1 Fwd/3 Rtn), ICV(initialization vector)
3. **Secondary Header Data Unit** (carries delay intolerant data)
   - Unique to a VC and is announced by a flag and delimited by length
   - Header, followed by multiple self-identified data sets (header, size, data)
4. **MPDU** (Multiplexing Protocol Data Unit)
   - **Encapsulation Packets** (all CCSDS packet types allowed)

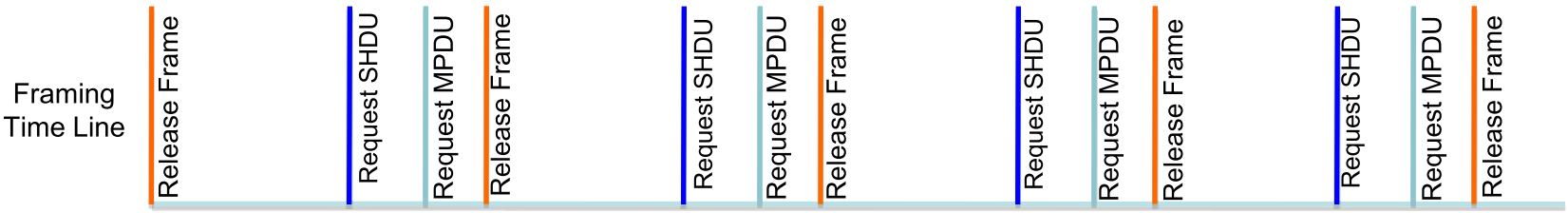
For CxP Operational, Dissimilar, Emergency Modes AOS Frame Formats all use the same Process

	Primary Header	Insert Zone	FSH	FSH-Data		MPDU Header	MPDU Data Field
CMD		**Security Parameters**		**Range Safety Commands**	**Voice**		**Encapsulation Packets**
	6 bytes	10 bytes	2 bytes	Optional & Variable		2 bytes	Variable

	Primary Header	Insert Zone	FSH	FSH-Data		MPDU Header	MPDU Data Field
TLM		**Security Parameters**		**Range Safety TLM DEM**	**Voice**		**Encapsulation Packets**
	6 bytes	8 bytes	2 bytes	Optional & Variable		2 bytes	Variable

- Security Block for CMD has 1 byte SPI, 1 byte Counter Field and 8 byte ICV
- Security Block for TLM is 1 byte SPI, 4 byte Counter Field and 4+ byte ICV
- FSH Service- supports Range Safety and Operational Voice
  - Header is 2 bytes: version, Header Type/Contents ID, length of header +data (10 bits)
  - Range Safety: contains pre-specified DEM/Command
    - Pre-defined size and included only when necessary
  - Voice data is aggregated from a variable number of 10 byte voice blocks
    - 1/2 chip may be required for 10.24 kbps rate
    - 1k frame @ 24 kbps number of voice blocks per frame varies between 4 and 5 (40 or 50 bytes)
    - This data is only included when necessary
- MPDU is standard CCSDS data field carrying CCSDS Packet types

AOS Frame Construction



- **AOS Framing Process** (time driven)
  - Frames are constructed on a periodic basis
    - If no data is available no frame is created, an idle frame will be supplied by the Link Transmission Process
  - The initial frame construction reserves space where the Primary Header will be placed later
  - A few ms before the rate defined Frame Release instant a request is issued to the Secondary Header Data Unit (SHDU) Constructor requesting a Secondary Header Data Unit
  - A few ms later the SHDU, if one is available, is received and placed into the Frame
  - Then a request is issued to the MPDU Constructor (containing the size of the MPDU required)
  - A Primary Header is constructed and set in place (If a SHDU was received the FSH Flag Bit is set)
  - The MPDU Constructor returns an MPDU of the requested size that is then added to the frame
- **Frame Secondary Header Data Unit Constructor** (Range Safety-Voice)
  - When a request is received it builds the SHDU with the data it had received and passes it to the Framing Process
- **MPDU Constructor**
  - Buffers packets received via the designated port
  - Once receiving the allowable MPDU length in the data request, the MPDU is built and transferred to the Framing Process

Example Approach for Security

- The security block could be provided by a single crypto unit for every frame transmitted on a link.
  - The Security Block would be placed in the AOS Frame Insert Zone
- AES-GCM shall be used for command
  - An eight byte counter would be used but only a portion need be sent
    - For Command only a single byte need be transmitted within the Block
    - For Telemetry only four bytes need be transmitted within the Block
- The SDI will increment when the counter overflows providing automated key changes
- The minimum of eight bytes of ICV is required for authentication
  - Its need for telemetry is optional
- Command Counter could be up to 8 bytes in length

Secondary Header Data Unit Construction

- **Launch/Range Safety Data**
  - A defined DEM is created by the launch vehicle controllers and forwarded for inclusion in the Frame Secondary Header Data Unit.
- **Voice**
  - Receives and buffers 10 byte Voice Chips from the voice codec
  - Builds a Voice Group containing a Label and the received Voice Chips
    - Label contains a Master Chip Counter and a count of the number of chips included in this FSHDU
    - Master Chip Counter is a sequential count of chips transmitted prior to this frame (modulo 4096)
    - No Voice Group is created if less than 2 chips are available

Label		Voice Chips	FSHDU Fill
Chip Counter	# of Chips		
12 bits	4 bits	Variable (20-125 bytes)	

Note:
SHDU can include fill to eliminate the inclusion of an MPDU

- **Frame Secondary Header Data Unit**
  - The FSHDU Header contains the FSH version ID, the Type ID and Length of the FSHDU
    - Example Type ID 1) Voice only with label 2)- Voice with label and fixed Range Safety
    - 3) Selective Engineering DEMs with header
  - If a FSHDU is created it is passed to Frame Constructor

	Secondary Header			Range Safety DEM	Label		Voice Chips
Optional	Version	Type ID	Length		M Counter	# of Chips	10 bytes/Chip
	2 bits	3 bits	11 bits	Fixed if present	Optional		Optional

Frame Secondary Header Service

Version	Type	Length	Data
2 bits	3 bits	11 bits	Variable up to a maximum of 2046 bytes

- This service is dynamic, self identifying & self delimiting
- Type field identifies contents of FSH data field
  - Up to 8 content definitions can be identified
    - i.e. Voice only, Voice and Range Safety DEM, other
  - Data field can fill frame eliminating a MPDU when desired
    - For Launch: Range Safety and Operational Voice delivery
    - For Dissimilar service: Voice and/or Engineering data
  - Data field can be empty allowing the MPDU to fill the frame

Acronyms

- AES = Advanced Encryption Standard
- AOS = Advanced Orbiting Systems
- ASM = Attached Synchronization Marker
- CRC = Cyclic Redundancy Check
- DEM = Data Exchange Message
- FSH = Frame Secondary Header
- GCM = Galois Counter Mode
- ICV = Integrity Check Value
- MAP = Multiplexer Access Point
- MPDU = Multiplexing Protocol Data Unit
- OCF = Operational Control Field
- SPI = Security Parameter Index
- TC = Telecommand (Space Data Link Protocol)
- TM = Telemetry (Space Data Link Protocol)
- VC = Virtual Channel

Acknowledgements

- The work described in this paper was performed at the Jet Propulsion Laboratory, California Institute of Technology und a contract with the National Aeronautics and Space Administration.
- The authors thankfully acknowledge the collaboration of Marjorie de Lange Long of IB + MA deLandeLong Software + Consultancy in the description of the current TM, AOS, and TC CCSDS Space Data Link Protocols in this paper.