TELEMETERING STANDARDS COORDINATION COMMITTEE

TSCC

SPONSORED BY

INTERNATIONAL FOUNDATION FOR TELEMETERING

Fall 2008 Meeting Minutes and Committee Reports

27 October 2008

Opening & Quorum Determination

- Meeting called to order at 0800
- Attendees:

Scott Brierley (m)
Lorin Klien(m)
Lee Eccles(m)
David Grebe(m)
Wayne Klein (a)
Shield Horan (m)
Michael Marcellin (a)
Greg Kazz (m)
Gerhard Mayer (m)
Gilles Freaud (a)
Steve Nicolo (m)
Jim Yates(m)
Duane Wheton (*)
Bill Rymer (IFT Rep)

Legend:
(m) Member
(a) Alternate
(*) Invited Guest/past member

A quorum of members was present.

Meeting Minutes 1/3

Reviewed and approved agenda
Reviewed agenda
Reviewed the following reports:

- Chairman
- Secretary Treasurer

Motion made & approved to accept minutes of last meeting without revision.

After reviewing the Committee's financial status and some discussion, it was agreed to ask the IFT for the customary $1000 funding.

Committee Reports:
Nominating Committee, RF, Networks, Data Multiplex, Transducers, Coding/Data Compression, Recorder/Reproduce

Received a briefing on CCSDS link security protocols by Gregg Kazz

Meeting Minutes 2/3

Nominating Committee Motions and Action Items:
Motion made & carried : To Accept Mark Bender from the Aerospace Corp as a TSCC member. He will be in the Class of 2014.

Motion made & carried : To accept Lorin Klein as a TSCC member and move Tim Chalfont to be his alternate.

ACTION ITEM : Marj will need to reflect these two changes on the web site

ACTION ITEM : Nominating Committee to contact Fil Macias about his future involvement plans. This to be closed out at spring meeting.

Motion made & carried : Dr. Sheila Horan re-elected to 5-year membership

Motion made & carried : Dr. Horan moves to TSCC Chair

Motion made & carried : Steve Nicolo becomes TSCC Vice Chair

Motion made & carried : David Grebe remains as Secretary-Treasurer

ACTION ITEM : The Nominating Committee should consider Chuck Weaver's offer to participate as a member

Meeting Minutes 3/3

Recorder/Reproducer Committee:

ACTION ITEM : Lorin requests that the website be updated to show Mark Buckly as Alternate Chair

Next meeting:

It was agreed to combine the TSCC spring meeting again with the RCC meeting. This will be the Week of March 9th.

Having no other topics or business brought forward, adjourned at 1045.

TELEMETERING STANDARDS COORDINATION COMMITTEE

TSCC

SPONSORED BY

INTERNATIONAL FOUNDATION FOR TELEMETERING

Chairman's Report

27 October 2008

Significant Activity (2008)

- 2 meetings of the TSCC were held
  - (Spring) March 4th/5th in Somerton, AZ - Joint TSCC/RCC/TG meeting.
  - (Fall) October 27nd in San Diego in conjunction with ITC

Significant Activity (2008)

- Revamp of TSCC website with special focus on updates to subcommittee memberships and applicable standards
  - Updates complete
    - Networking & Protocols
    - Recorder Reproduce
    - Data Multiplex
  - Still in process
    - Coding & Data Compression
    - Radio Frequency
    - Transducers

Significant Activity (2008)

- Standards reviewed over the last 12 months include:
  - CCSCS – Various – link layer security
  - IEEE1451
  - IRIG-106-09
    - XML TMATS schema, and more display schema, chapters 6, 7, 9 & 10 changes
  - IRIG-118
  - ECMA holographic storage standards

Significant Activity (2008)

- Best telemetry standards paper award at ITC 2008 (Considerations for deploying IEEE-1588v2 in DAS and Telemetry Systems - Newton, Grim, Moodie)
- Added no new members
- No further loss of members
- Attend 2008 ETC & ETSC meetings in Munich
- Agree to sponsor a special session at ITC 2008
- Utilize new template for reporting activities

Current TSCC Focus Areas

- New telemetry networking standards
- Membership recruiting
- Web improvements
- Best paper and special sessions for ITC

Treasurer's Report
for the Period 10/16/07 thru 10/24/08

- INCOME
  - Funding Received, IFT $1,000.00
- EXPENDITURES
  - Award Plaques $1,350.10
  - NMSU Foundation for Russell Jedlicka Memorial Scholarship $ 250.00
- Net Increase (Decrease) in Cash ($600.00)
- Beginning Cash Balance $2,579.86
- Ending Cash Balance $1,979.76

TELEMETERING STANDARDS COORDINATION COMMITTEE

TSCC

SPONSORED BY

INTERNATIONAL FOUNDATION FOR TELEMETERING

Nominating Subcommittee

Status Report

27 October 2008

Membership

- Scott Brierley
  - Lee Eccles

Sub-Committee Focus

- **The nominating subcommittee shall propose TSCC members and officers for approval by the membership.**
- **Prospective TSCC members and officers can be nominated by the TSCC membership or by a nominating subcommittee.**
- **All nominations must be approved by a membership vote.**

TSCC Membership Rules

- Adequate representation shall always exist from the diverse groups constituting the telemetry community.
- Representatives of government and commercial entities shall each constitute a minimum of one-third of the regular TSCC Membership.
- The remaining one-third may include, but is not limited to those in commercial, governmental, and academic organizations.
- Membership by representatives of non-US entities shall not exceed 25% of the total regular membership.

TSCC Group Definitions

- Government entities are defined to include agencies of the United States government, foreign governments, and not-for-profit organizations under contract to them.
- Commercial entities are defined as manufacturers or vendors of equipment, software, or systems, for-profit companies that use telemetry equipment, and suppliers of telemetry-related services, such as consulting on a for-profit basis.

TSCC Makeup

- The TSCC currently consists of
  - 2 academic organization members
  - 4 government entity members
  - 7 commercial entity members
- Members from commercial entities belong in two different groups:
  - Telemetry equipment suppliers
  - Telemetry equipment users

Two Open Membership Slots

- There are three open membership slots in the TSCC:
  - Previously had one open slot.
  - George Manz resigned and provided a second open slot.
  - Russ Jedlicka's slot is open.
- A minimum of one additional government member is required.
  - One-third minimum government representation required

TSCC Membership

- Academia
  - Sheila Horan, PhD
  - Gerhard Mayer
- Government
  - Tim Chalfant
  - Greg J. Kazz
  - Filiberto Macias
  - Dan Skelley
- Industry
  - Scott Brierley
  - Lee Eccles
  - David Grebe
  - John Kolb
  - Steve Nicolo
  - Michael Pizzutti
  - James A. Yates

New Membership

- Possible sources for new members:
  - SWRI (South West Research Institute)
    - SWRI would be a new category.
      - Crosses the lines between academia, industry, and government.
  - Aerospace Corporation
    - Aerospace corporation is defined in the bylaws as a government agency.
    - Aerospace corporation employee Mark Bender has expressed interest in becoming a full time member.

TSCC Chair

- TSCC Chair term expires after the 2008 Fall meeting
  - Officers shall serve for a two-year term of office.
  - The term of office shall begin at the start of the TSCC year in even calendar years.
  - Traditionally the Vice Chair succeeds to the Chair's position to fulfill a two-year term as Chair.
  - The Secretary-Treasurer may be re-elected

TSCC Membership Terms

- TSCC membership terms are for five years
  - Terms are staggered so that the terms of 20% (rounded to the nearest integer) of the regular membership end each year.
  - Members may be renominated for additional terms by the nominating subcommittee.
- Two membership slots expire this year.
  - The TSCC year begins immediately following the TSCC annual meeting, which is held in conjunction with the International Telemetering Conference.
- Not sure which membership slot belongs to Russell Jedlicka

TSCC Membership Terms

Year Term Expires				
2008	**2009**	**2010**	**2011**	**2012**
Filiberto Macias	**TBD**	**TBD**	Scott Brierley	Tim Chalfant
Sheila Horan, PhD	Lee Eccles	Michael Pizzutti	James A. Yates	David Grebe
TBD	Gerhard Mayer	Steve Nicolo	Dan Skelley	John Kolb
		Greg J. Kazz		

Second Nominating Committee Member Required

- The Nominating subcommittee shall consist of three members of the TSCC of any category.
- The membership shall consist of:
  - The immediate past Chair (or the most recent prior chair if the immediate past chair is unable to serve) who shall chair the subcommittee, and
  - Two Members at Large elected by the TSCC membership

Open Actions

- Three open membership slots
- Actions required:
  - New Chair
  - New Vice Chair
- Members that have terms expiring in 2008 need to be renominated at the fall TSCC meeting
- Need to verify membership terms are correct
- Need third nominating committee member

TELEMETERING STANDARDS COORDINATION COMMITTEE

TSCC

SPONSORED BY

INTERNATIONAL FOUNDATION FOR TELEMETERING

RF Subcommittee

Status Report

27 October 2008

Membership

- Scott Brierley
  - Mark Bender
  - Mark Dapore
  - Lloyd Lautzenhiser
  - Eugene Law
  - Warren Martin
  - Bill McNatt
  - Rich Siegal

Sub-Committee Focus

- RF subcommittee reviews standards dealing with the Radio Frequency (RF) telemetry link
- Current standards
  - **RCC IRIG-106**
  - **RCC IRIG-118**
  - **RCC RF Handbook**
  - **CCSDS-401**
  - **CCSDS-411**
  - **SGLS**
  - **STDN**
  - **1451.5**

Significant Activity

- No standards reviewed since the spring meeting

Open Actions

- Need to update TSCC Website for RF Subcommittee members
- Need contact information for Gene Law

TELEMETERING STANDARDS COORDINATION COMMITTEE

TSCC

SPONSORED BY

INTERNATIONAL FOUNDATION FOR TELEMETERING

Data Multiplex Subcommittee

Status Report

3 March 3 2008

Membership

- Steve Nicolo
  - Howard Eckstien
  - Alain Hackstaff
  - M. Pizzuti
  - Bill Rymer
  - Dave Sniffin
  - Erwin Straehley
  - Duane Weaton

Sub-Committee Focus

- Current standards
  - IRIG-106
    - Part 1: Telemetry Standards
      - Chapter 3: FM Data Standards
      - Chapter 4: PCM Data Standards
      - Chapter 8: Bus Data Formatting Standards
      - Chapter 9: TMATS
    - Part 2: Telemetry Networks
      - Chapter 4: Packet Telemetry Standards
  - RCC IRIG-118: Test Methods
  - RCC IRIG-119: Telemetry App's Handbook

Significant Activity

- RCC Completed and Released the following in IRIG-106-07
  - TG76 XML SCHEMA for TMATS
  - TG84 Standard for Data Display (XML SCHEMA)
- RCC Completed and Distributed Pink Sheets
  - Chapter 9 Changes
  - Message Data Attributes New
  - DDML 3.1 Changes
  - Appendix O Changes
  - Derived Parameter English New

Significant Activity (continued)

- Joint RCC/TSCC Meeting March 2008
- Reviewed Pink Sheets
  - Chapter 9 Changes: The entire Chapter 9 including most of the changes
  - Message Data Attributes New: A new TMATS group, describing message formats
  - DDML 3.1 Changes: Proposed changes to the data display standard
  - Appendix O Changes: Includes an additional floating point format
  - Derived Parameter English New: A new appendix, describing the format for derived parameters

Open Actions

- New Work Tasks
  - Ongoing effort to keep TMATS IRIG 106 Chapter 9 and XML Scheme Current
  - TMATS Handbook
  - Review Pink Sheets

TELEMETERING STANDARDS COORDINATION COMMITTEE

TSCC

SPONSORED BY

INTERNATIONAL FOUNDATION FOR TELEMETERING

Coding and Data Compression

27 October 27 2008

Town & Country Hotel

San Diego, California

Membership

- Sheila Horan, Chair - NMSU
  - Michael Marcellin, Alternate - Univ. of Arizona; marcellin@ece.arizona.edu
  - Chuck Creusere – NMSU; ccreuser@nmsu.edu
  - Stephen Horan – NMSU; sthoran@nmsu.edu
  - Aaron Kiely – JPL; Aaron.B.Kiely@jpl.nasa.gov
  - Matt Klimesh – JPL; Matthew.A.Klimesh@jpl.nasa.gov
  - M. MacMedan – emeritus; macmedan@ieee.org

Membership - Continued

- George Nelson - Delta Information System; gcnelson2@netzero.net
- Jimmie Perkins – Raytheon; jwperkins@raytheon.com
- Khalid Sayood - Univ. of Nebraska – Lincoln; ksayood@sensin.unl.edu
- Pen-Shu Yeh - NASA – Goddard; pen-shu.yeh-1@nasa.gov
- Gary Thom - Delta Information System; gthom@delta-info.com
- Steve Nicolo - GDP Space Systems snicolo@gdpspace.com

Subcommittee Focus

- Data Compression and Coding
- Current Standards – Updates

Significant Activity

- National Geospatial Intelligence Agency (NGA) has developed the Motion Imagery Standardization Profile (MISP) for standardizing motion imagery compression for Intelligence, Surveillance, and Reconnaissance (ISR) applications.
- See: http://www.gwg.nga.mil/misb/index.html

- This profile attempts to get the community to adopt common compressed and uncompressed video formats in order to enhance interoperability and utility of acquired video sequences.
- The MISP initially directed the use of MPEG-2 for video compression but has now migrated that recommendation to the more efficient H.264 (MPEG-4 Part 10) algorithm.
- They also allow JPEG 2000 for very large format video.
- In addition to the video, the profiles specify the inclusion of metadata with the video.
- Metadata provides information such as source, location, optics, etc., related to the video.
- This is all multiplexed into a common transport (MPEG-2 transport stream) for real-time distribution.

Significant Activity

CCSDS

- Joint SEA/SLS Link Security BoF making good progress, and security authentication and encryption books are on their way out for review
- Cryptographic Service for CCSDS data Links and Concept of Operation. Cryptographic Service for CCSDS data links are two current CCSDS experimental specifications that describe a data encapsulation method for space missions that need to apply security protections to the contents of transfer frames used by Space Data Link protocols over a space link. These are Orange books.
- http://www.ccsds.org/

Significant Activity

- CCSDS Multispectral and Hyperspectral Data Compression working group – Aaron Kiely
- Agreed on work group priorities for standardization: lossless multi and hyperspectral, lossy multispectral, lossy hyperspectral
- Reviewed compression performance results (lossless and lossy) on test data sets from candidate algorithms from NASA JPL, CSA, CNES, ESA
- Reviewed selection criteria and requirements for proposed lossless compressors (JPL, ESA)
- Identified further work needed to provide a more thorough comparison between the two proposed lossless compressors (error containment, complexity), and consider using the existing CCSDS lossless entropy coder in the JPL proposed compressor
- Presentation on compression techniques under research at
- University of Wisconsin (NOAA)

Significant Activity

CCSDS Multispectral and Hyperspectral Data Compression working group

- Time Line:
  - Select lossless compression algorithm for standardization - Spring 2009
  - Lossless White Book - Fall 2009
  - Lossless Red Book - Spring 2010
  - Lossless Reference software & compliance data sets - Spring 2010
  - Lossless Blue Book - Fall 2010
  - Lossless Green Book - Fall 2010

Significant Activity

CCSDS Coding & Synchronization

- The WG resolves to request approval for starting the process to issue LDPCC Pink Sheets on the TM Channel Coding Book and eventually to include supporting material in a Green Book.
- The WG resolves to request approval for starting “Standard Track” processes for SCCC and DVB-S2 once the holding conditions are successfully accomplished and eventually to include supporting material in Green Book(s).

Significant Activity

CCSDS C&S: Coding & Synchronization

- Request CESG/CMC to approve TM Channel Coding book Pink Sheets for introduction of LDPC codes
- SLS-LEC: Long Erasure Codes (‘tornado codes’) BOF -

  Goal: Creation of a new working group for application of long erasure-correction codes.

Open Actions

- Complete information table for website.

TELEMETERING STANDARDS COORDINATION COMMITTEE

TSCC

SPONSORED BY

INTERNATIONAL FOUNDATION FOR TELEMETERING

RECORDER / REPRODUCER COMMITTEE

27 October 2008

Town & Country Hotel

San Diego, California

Membership

- Lorin Klein (AAC, Eglin AFB, FL, USA), Chairman
- Mark Buckley (JDA Associates, Concord, CA, USA) Alternate Chairman
  - Balázs Bagó (Heim Systems GmbH, Bergisch Gladbach, Germany)
  - Bob Baggerman (Georgia Tech Research Institute, Atlanta, GA, USA)
  - Tim Chalfant (AFFTC, Edwards AFB, CA, USA)
  - Tim Gatton (Wyle Laboratories, California, Maryland, USA)
  - Mike Lockhard (EMC Corp, Irvine, California, USA)
  - Barbara Wood (QinetiQ Boscombe Down, Salisbury, Wiltshire, UK)

Sub-Committee Focus

- Data Recorders, Ground and Airborne
- Standards in Place
  - IRIG 106-07 -- Range Commanders Council (RCC) Telemetry Standards
  - STANAG 4575 – North Atlantic Treaty Organization (NATO) Standard Agreement (STANAG) – NATO Advanced Data Storage Interface (NADSI)
  - ANSI ID-1 -- Recorded Instrumentation Digital Cassette Tape Format
  - MIL-STD-2179 – Helical Digital Recording Format For 19-MM Magnetic Tape Cassette Recorders/Recorders

Significant Activity

- RCC IRIG 106-09 is in final coordination with updates affecting recorders/reproducers to:
  - Chapter 10 (Solid State Recorders),
  - Chapter 9 (Telemetry Attributes Transfer Standard–TMATS), and
  - Chapter 6 (Digital Cassette Helical Scan Recorder/Reproducer, Multiplexer/Demultiplexer, Tape Cassette, and Recorder Control and Command Mnemonics Standards

Significant Activity (cont.)

- European Computer Manufacturers Association (ECMA) approved on May 2, 2007, published on June 11, 2007 two new standards for Holographic Information Storage -
  - ECMA-377 “Information Interchange on Holographic Versatile Disc (HVD) Recordable Cartridges – Capacity: 200 Gbytes per Cartridge” and
  - ECMA-378 “Information Interchange on Read-Only Memory Holographic Versatile Disc (HVD-ROM) – Capacity: 100 Gbytes per disk”.

  http://www.ecma-international.org/news/PressReleases/HVD-R%20Standards.htm

Open Actions

- RCC TG Addressing Ground TM Recorders
  - IRIG 106 Chapter 7 -- “Ground Based Digital Recording Standard (Solid State and Disk Systems)”
- Anyone still using tape?
  - RCC TG considering moving ID-1 and VLDS to the Appendix (not recommend for new purchases)

Open Actions

- RMM Security – TG-85
  - New RCC POC to STANAG
  - RCC Omnibus contract awarded
- Digital Recorder Programmers Handbook – TG-83
  - Document is in preparation for release by the RCC
- Update to IRIG 118 update on hold
  - IRIG 106 Ch 10 format validation techniques

TELEMETERING STANDARDS COORDINATION COMMITTEE

TSCC

SPONSORED BY

INTERNATIONAL FOUNDATION FOR TELEMETERING

"TSCC Fall 2008 ETSC Report"

27 October 27 2008

Town & Country Hotel

San Diego, California

Membership

- **Committee Chair**

  Gerhard Mayer , Gilles Freaud (A)
- **Subcommitee Chair**
  - **SC-1: RF Spectrum & Frequ. M´nt**

    Jean-Claude Ghnassia, Jean Isnard (A)
  - **SC-2: Data Acquisiton & Processing**

    Werner Lange, Christian Herbepin (A)
  - **SC-3: Data Recording & Storage**

    Steve Lyons , Balasz Bagó (A)

(A)...Alternate

Sub-Committee Focus

- SC-1:Spectrum availability & efficient use, data integrity in the transmission channel
- SC-2:Ensure time tagging in high-rate data streams
- SC-3:Info collection & dissemination on recording system and techniques

- Current important standards
  IEEE 1451,1588,802.xx;IRIG 106 Ch.10

Significant Activity

- ETSC meeting at the ETC 2008 in Munich, addressing time tagging (IEEE 1588), IRIG 106 update, standards followed on Australian test ranges et al.
- Harmonisation issues for additional spectrum now allocable globally and in ITU region 1 (AI 1.5 of the WRC 2007: Res. COM 4/2 and COM 4/7)
- Review and comments on IRIG 106-Ch.10

Open Actions

- "WRC Bands" Telemetry Issues:
  C-Band Systems&Standards, wave propagation, up front evaluation of tracking algorithms & systems
- Investigate potential of existing standards for wireless (e.g. intra-aircraft)RDAU-networking
  (IEEE 802.11n and UWB)
- Next ETSC- Meeting
  Venue: Centre de Congrès "Pierre Baudis", June 24 - 26, 2009, ETTC 2009 Toulouse, France

Cryptographic Security
for CCSDS Protocols

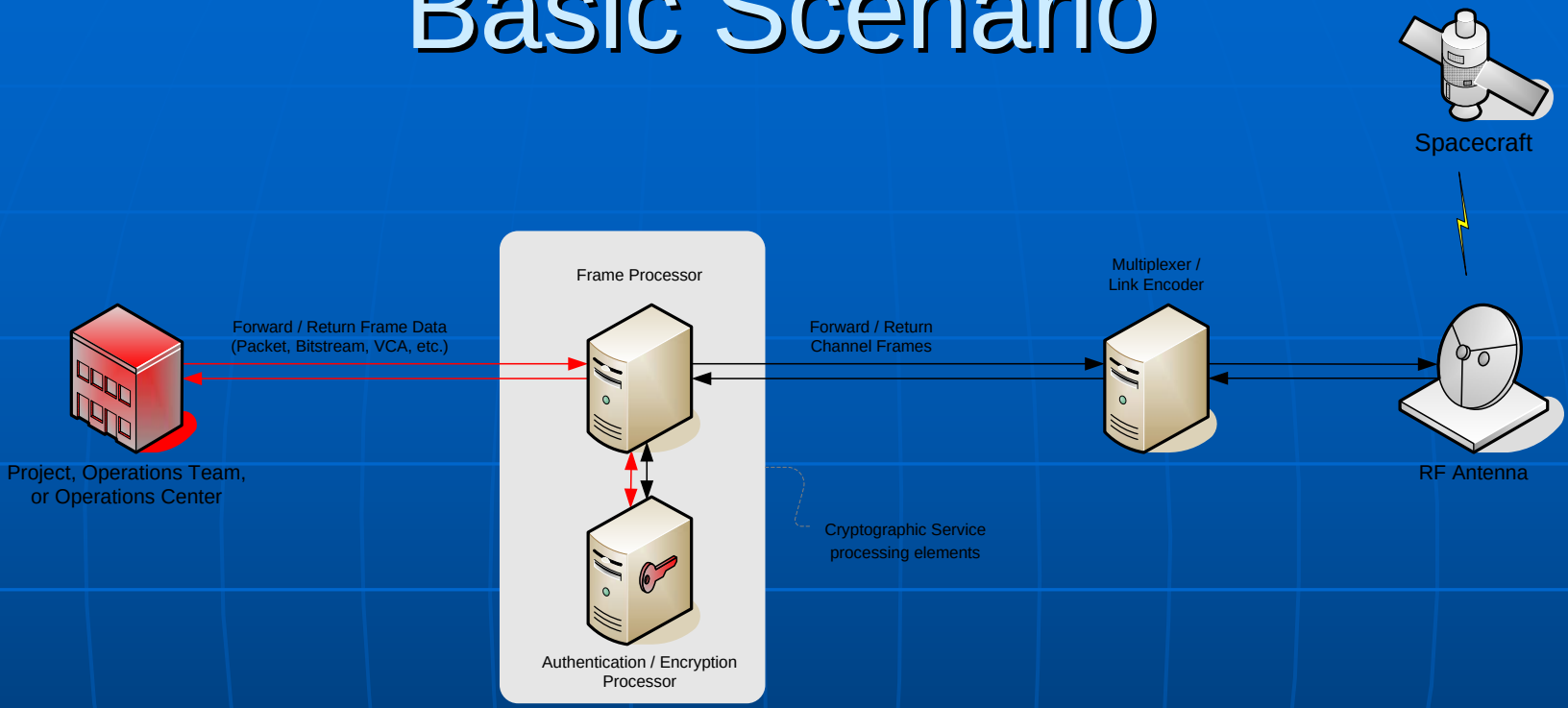
NASA CCSDS Link Security Team:

Craig Biggerstaff	**Lockheed Martin/JSC**
Edward Greenberg	**JPL**
Greg Kazz	**JPL**
Michael Pajevski	**JPL**
Howard Weiss	**Sparta/JPL**
Clayton Sigman	**GSFC**

Objectives

- Objectives:
  - Sound cryptography
    - Provide for authenticity and integrity of the security header and the ciphertext
    - Provide protection against replay attacks
  - Algorithm independence
    - Header format should not change, even if future discoveries of cryptographic weaknesses necessitates replacing one algorithm with another
  - Compatibility with AOS, TM, and TC
    - Comply with current CCSDS Formats
      - Only change spare bits where necessary to indicate the existence of Secondary Headers
    - Flexibility to encrypt and/or authenticate one or several VC IDs
    - Flexibility to encrypt and/or authenticate one or several TC MAP IDs
  - Compatibility with CCSDS Space Link Extensions (SLE) Services
    - Support provision of SLE forward and return services
    - Conform to current frame structuring rules for compatibility with current ground station provided services
    - Allow for encryption / authentication to be done by the operations center or at the ground station, as appropriate
  - Efficiency
    - Avoid resending any information that can be deduced from the transfer frame itself
    - Maintain state through the use of a Security Association (SA)
    - Provide ability to create SAs for carrying out both encryption and authentication operations
  - Simplicity
    - Avoid creating a complicated session negotiation protocol
- Not Objectives:
  - Protection against traffic flow analysis
    - SC ID and VC ID are transmitted in the clear
  - Creation and/or specification of a cryptographic key management protocol

Basic Scenario



Red: Indicates that data needs to be secured

Black: Indicates that data is secured for transmission or otherwise needs no protection

Concept of Operation: Security Association

- Define a CCSDS Security Header for use at the data link layer
  - Modeled after TM Frame Secondary Header
  - Provides a reference to a Security Association (see below)
  - Contains all the managed fields necessary for the receiver's frame processor to extract user data according to the options defined in the Security Association
- Define a Security Association for each communications session to be secured
  - A Security Association defines a simplex (i.e., one-way), stateful cryptographic session for providing one or more of the following:
    - Authentication
    - Encryption
    - Authenticated Encryption
    - Encryption with Validation
    - Replay protection
  - A Security Association may be associated with one or more Virtual Channels
    - This allows for individual SAs for different VCs sharing a physical channel
    - This allows for sharing of SAs by different VCs sharing a physical channel
    - If SAs are pre-loaded, the allocation of SAs (or sets of SAs) must be agreed-to by all users of the physical channel so that SA conflicts will not occur

Concept of Operation: Processing Options

- Authentication
  - Provides data integrity
  - Provides data authenticity (confirms the identity of the sender)
  - Typically a keyed HMAC (Hashed Message Authentication Code)
- Encryption
  - Provides data confidentiality
  - May be either a block or a stream cipher
- Authenticated Encryption
  - If Authenticated Encryption is selected for an SA:
    - The sender MUST encrypt the frame data before computing the authentication hash.
    - The receiver MUST verify the authentication hash before decrypting the frame data.
  - May specify either two algorithms with two keys, or one algorithm / one key if an “Authenticated Encryption with Associated Data” (AEAD) mode of operation is used (Galois/Counter mode, for example)

Concept of Operation: Processing Options (cont.)

- Encryption with Validation
  - If Encryption with Validation is selected for an SA:
    - The sender MUST compute the message digest before encrypting the frame data.
    - The receiver MUST decrypt the frame data before verifying the message digest.
  - Provides data confidentiality
  - Provides a [possibly unkeyed] message integrity digest, encrypted along with the frame data
    - *Not a checksum or CRC* – a cryptographic hash algorithm must be used to avoid a bit-wise correspondence from input data to output hash
  - This SA option expects some truncation of the message digest.
    - If unkeyed, message digest does *not* provide authentication of the sender.
    - If keyed, message digest provides "weak" authentication of the sender (called "weak" here due to effects of truncation).
    - If "strong" authentication is mandatory and/or hash truncation is not possible, Authenticated Encryption should be chosen instead. Authenticated Encryption has been proven secure mathematically. Encryption with Validation has not been evaluated in this manner.
  - Enables the use of replay protection
  - Protects against bit-flipping ciphertext attacks
    - Believed to permit further truncation of the message digest (hash) than would be secure if the hash were transmitted unencrypted
    - Because the attacker has access only to ciphertext and encrypted hash, it is computationally difficult for an attacker to modify ciphertext so that decrypted plaintext still matches decrypted hash (cf. "second preimage resistance")
  - Should be considered for emergency or very-low-rate links.
    - Attempts to provide integrity and "weak" authentication with maximum transmission efficiency
    - Less computation-efficient for the receiver; each frame must be decrypted in order to verify the ICV.

Concept of Operation: Processing Options (cont.)

- Replay protection
  - Provides a sequence number to prevent the retransmission of previously recorded data (e.g., forward link commands)
    - Requires that Authentication or Validation be selected for the SA
  - Requires both sender and receiver to manage an internal sequence number as part of the Security Association
    - The Sequence Number MUST increment by one with each frame processed.
    - Internal sequence number MUST be an unsigned integer at least 32 bits long
    - Rollover of the internal sequence number indicates that the SA MUST expire immediately to avoid compromise due to reuse of initialization vector/key pairs
  - A Sequence Number Window (value ± current Sequence Number) is set when an SA is created
    - A data unit MUST be rejected if its Sequence Number is outside the defined window
    - Sequence Number Window setting should account for predicted delays and gaps in RF transmission
  - Transmitted length is a managed SA parameter
    - The whole length of the internal sequence number does not need to be transmitted over the air
  - If an SA is to be used with more than one Virtual Channel, the Sequence Number must be transmitted as part of the Security Header.
    - The transmitted sequence number is contained in the Security Header, and its length is managed as part of the Security Association.
  - If an SA is to be used with only one Virtual Channel, the least-significant bits of the Sequence Number may be transmitted in the Virtual Channel Frame Count field of the primary header.
    - To ensure synchronization, both the internal sequence number and the Virtual Channel Frame Count field MUST be reset in the first frame of this Virtual Channel in which the SPI is changed.

Concept of Operation: Security Association Database

- Security Association (SA) Database
  - Each sender and receiver must implement an internal SA Database for maintaining the state of each communications session
  - Two-way communications requires one SA Database for the sending channel and another SA Database for the receiving channel
    - 7-bit SPI allows for up to 127 SAs across the entire physical channel
  - Security Associations may be pre-loaded into the Database or created as needed
    - SAs are not used until marked as “active” in the Database
    - New SAs may be created even while other existing SAs are still active
    - Over-the-air negotiation of SA parameters, if implemented, is an (undefined) application-layer function.
- Security Parameter Index (SPI)
  - The SPI is used to reference Security Associations in the SA Database

Concept of Operation: Security Association Database

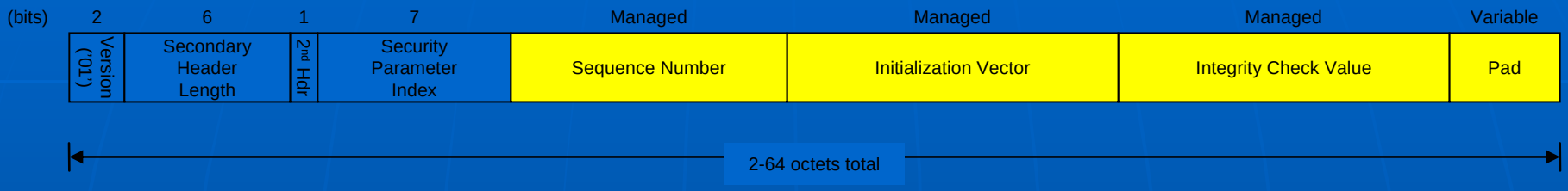
- Security Association (SA)
  - Every SA MUST include:
    - Security Parameter Index (SPI)
    - Context: a data structure identifying the MC IDs, GVC IDs, or GMAP IDs with which this SA is used
    - Active binary flag: indicates whether this SA is currently in use
    - Security Association maximum lifetime (expiration timeout)
    - Security Association maximum throughput (byte counter)
  - If Authentication is selected, the SA MUST include:
    - Authentication algorithm and mode of operation
    - Authentication key or key index
    - Transmitted length of Integrity Check Value (ICV)
  - If Encryption is selected, the SA MUST include:
    - Encryption algorithm and mode of operation
    - Encryption key or key index
    - Transmitted length of Initialization Vector (IV)
  - If Replay Protection is selected, the SA MUST include:
    - Anti-replay Sequence Number (internal length MUST be at least 32 bits)
    - Anti-replay Sequence Number window
    - Transmitted length of Sequence Number
      - NOTE 1: If the transmitted length is set to zero, the Virtual Channel Frame Count field of the primary header is used as the transmitted portion of the Sequence Number.
      - NOTE 2: the Sequence Number MUST be transmitted in the Security Header if the SA Context includes more than one Virtual Channel (because each VC's Frame Count in the primary header is incremented separately).

Concept of Operation: Security Association Database

- Frames out of context should be discarded
  - -- where a security header is expected for this context but the received frame does not have it
  - -- where a security header is not expected for this context but the received frame has it
  - -- where the received frame has a security header, but with the wrong context

Concept of Operation: Security Header

Security Header



Version: '01' = Security Header
New Secondary Header version is in addition to existing definition -- does not replace it
(Revision of existing Blue Book CCSDS 135.0-B-3, "Space Link Identifiers", §7.4)

Secondary Header Length: 2-64 octets total

2nd Header Follows: '1' if another Secondary Header follows this one (next header may be encrypted)
Flag permits nesting of Secondary Headers
Facilitates additional extraction by receiver after security processing

Security Parameter Index (SPI): Index used to identify a Security Association (SA).
Allows for up to 127 possible SAs per physical channel. (The value 0 is reserved.)

Sequence Number: Optional; fixed-length for the duration of the SA
Anti-replay sequence number

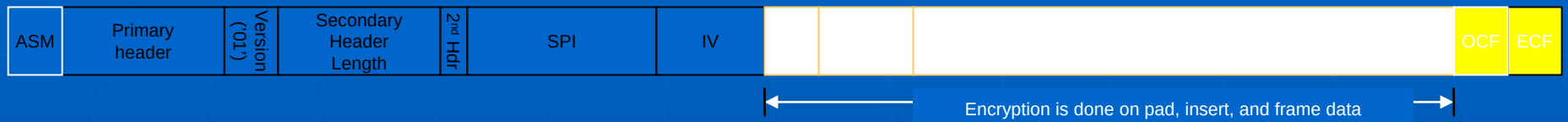
Initialization Vector (IV): Optional; fixed-length for the duration of the SA (up to the algorithm's block size)
Algorithm-dependent data that some modes of encryption require as an additional initial input

Integrity Check Value (ICV): Optional; fixed-length for the duration of the SA
Algorithm-dependent integrity hash or Message Authentication Code (MAC)
ICV is computed over entire transfer frame minus ECF, if any

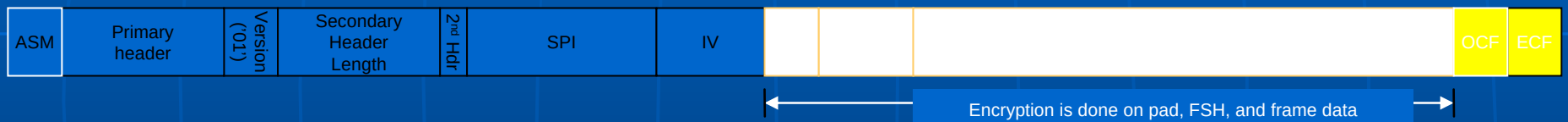
Pad: Optional; variable-length (up to the algorithm's block size)
Algorithm-dependent fill data that certain modes of encryption require

Frame Processing: Encryption alone

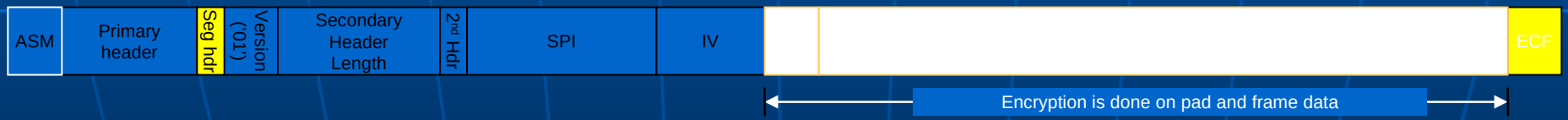
AOS



TM



TC



LEGEND:

White = required
Yellow = optional
Black = encrypted

Frame Processing: Authentication alone

LEGEND:

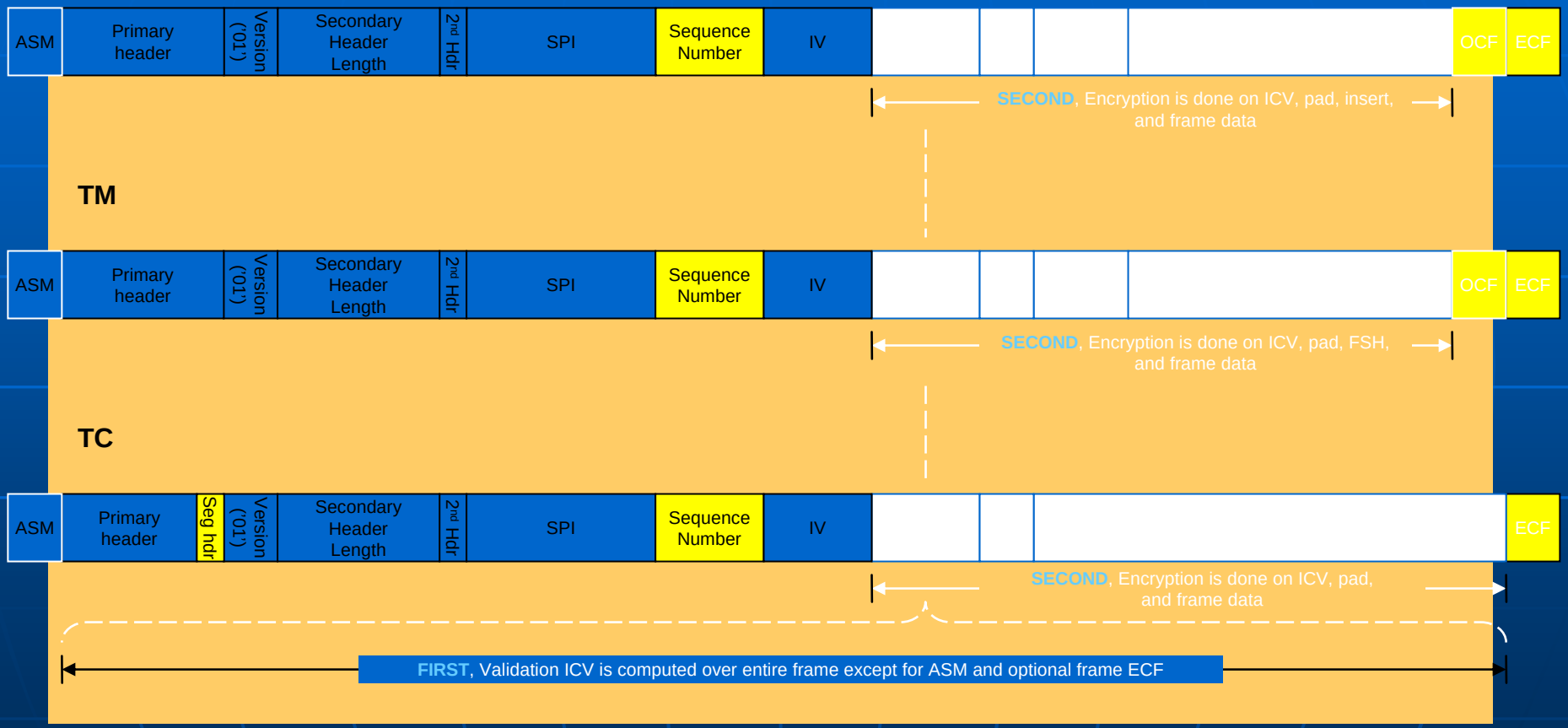
White = required
Yellow = optional
Black = encrypted

Frame Processing: Authenticated Encryption

LEGEND:

White = required
Yellow = optional
Black = encrypted

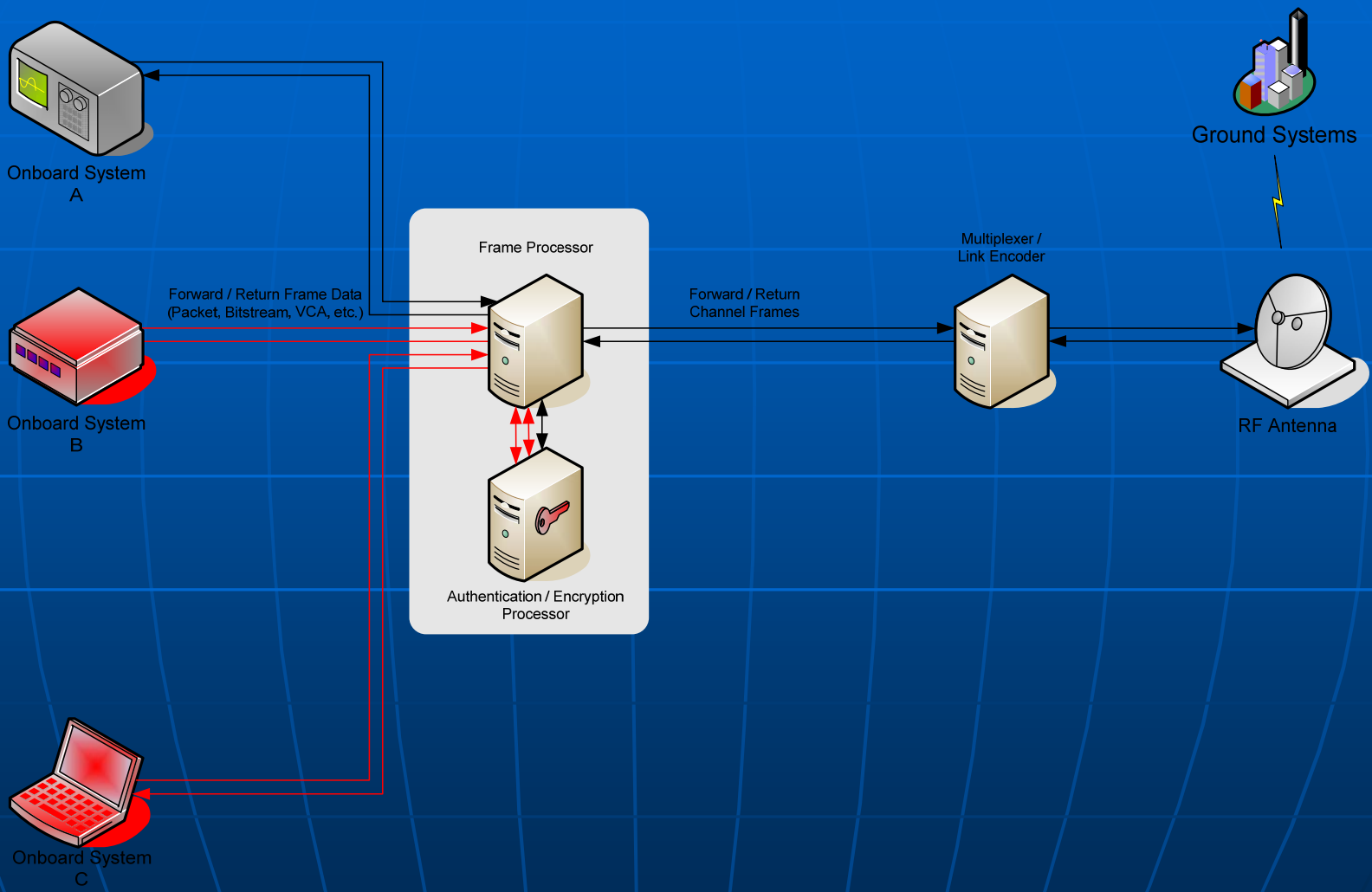
Frame Processing: Encryption with Validation



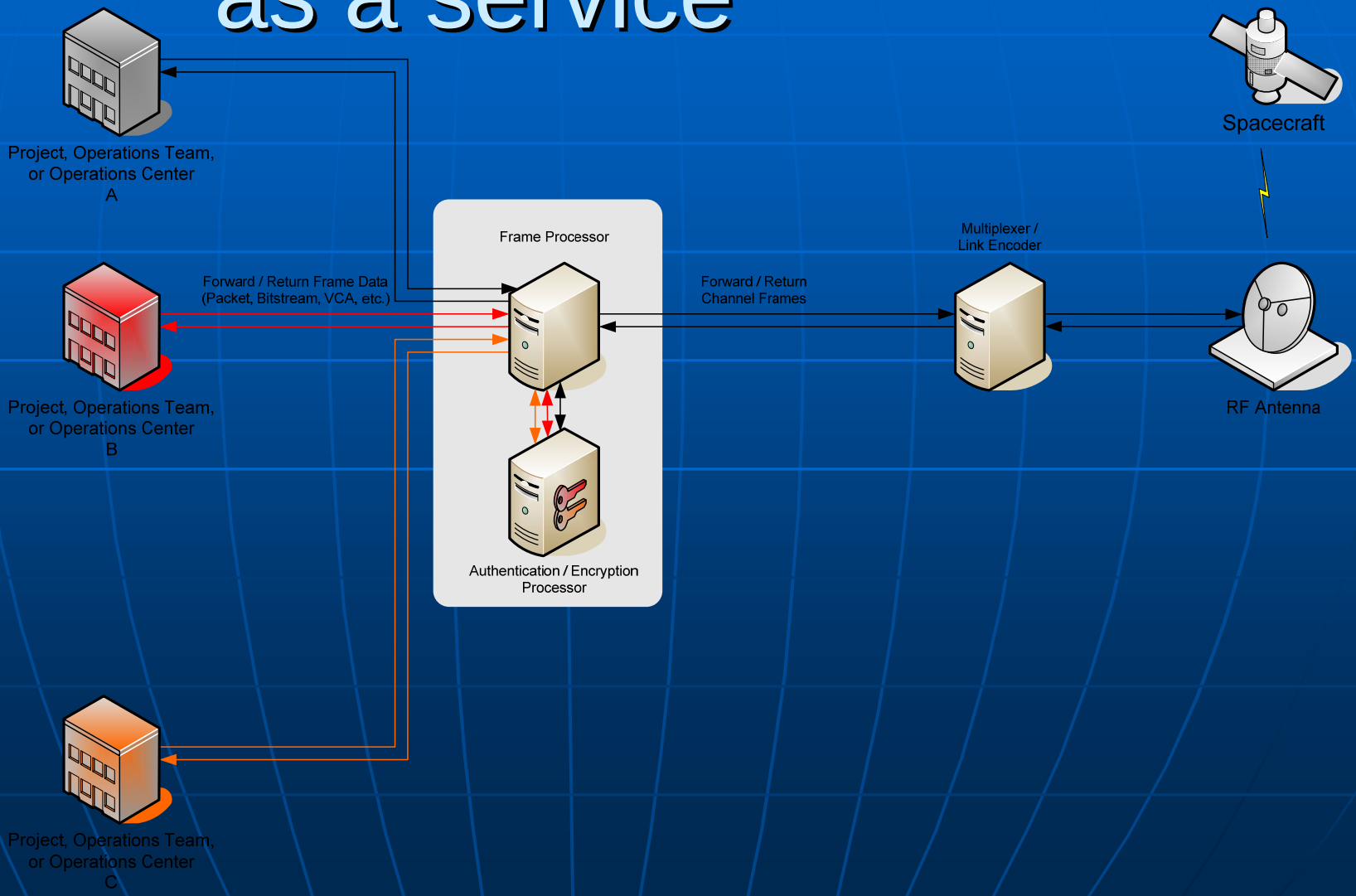
LEGEND:

White = required
Yellow = optional
Black = encrypted

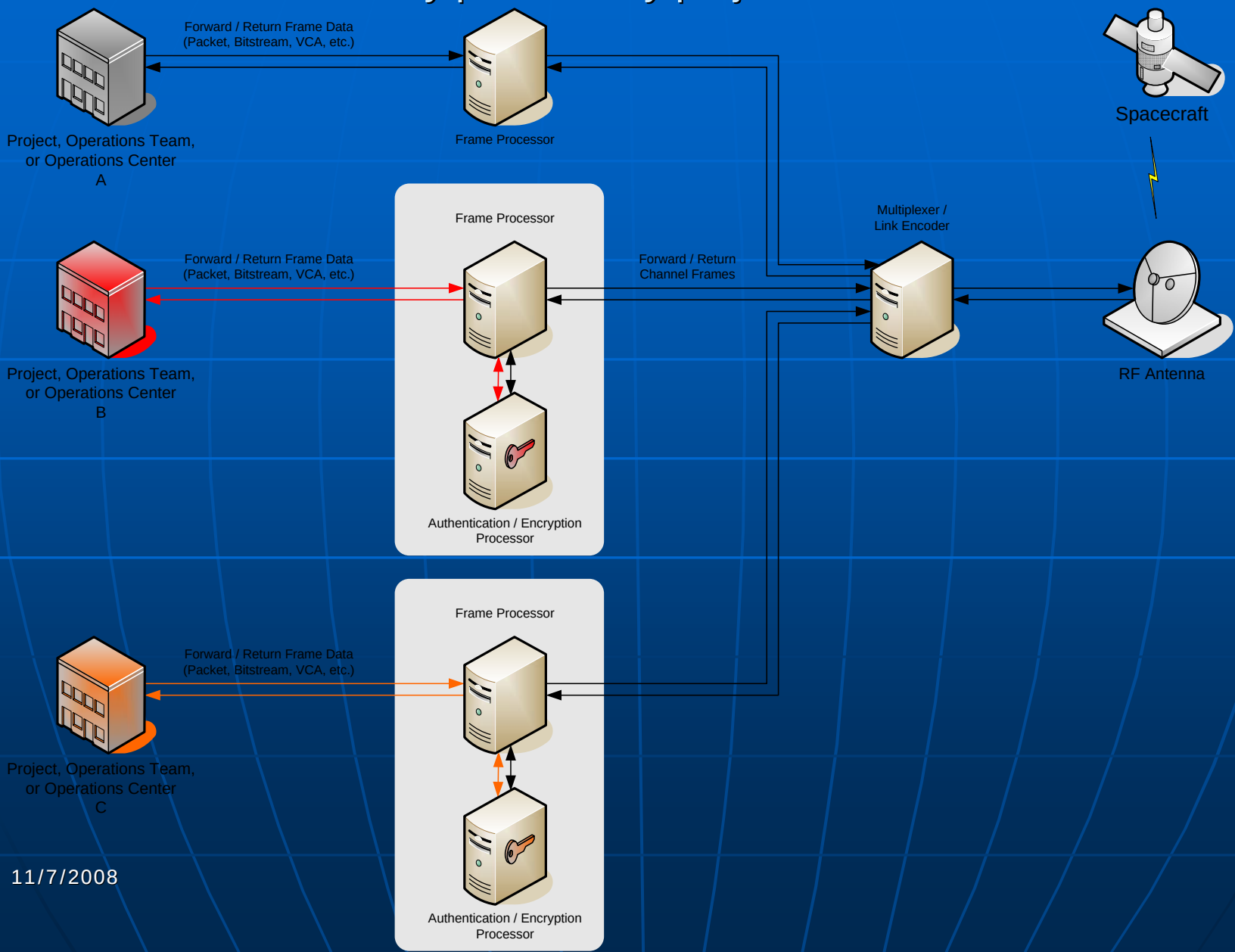
Spacecraft Onboard Scenario



Ground Scenario #1: Cryptographic security provided as a service



Ground Scenario #2: Cryptographic security provided by project or location



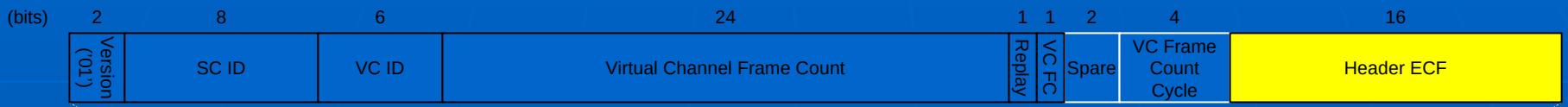
Impacts to CCSDS Space Link Extensions (SLE)

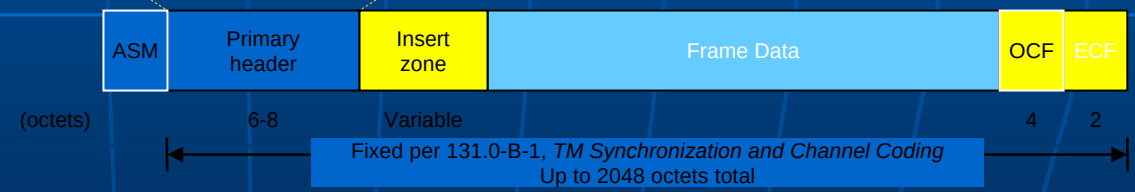
- Unaffected Services – these SLE Services work, regardless of whether Cryptographic Service processing is implemented at SLE server end or at SLE client end
  - Return All Frames (RAF)
  - Return Channel Frames (RCF)
- Affected Services – these SLE Services work with the Cryptographic Service, *if and only if* the Cryptographic Service processing is implemented at the SLE *client* end
  - Forward Coded Transfer Frame
  - Forward Telecommand Frame
  - Forward Communications Link Transmission Unit (CLTU)
- Affected Services – these SLE Services work with the Cryptographic Service, *if and only if* the Cryptographic Service processing is implemented at the SLE *server* end
  - Return Operational Control Field (ROCF)
  - Return Frame Secondary Header (RFSH)
  - Return Insert
  - Return Bitstream
  - Return Space Packet (RSP)
  - Forward Insert
  - Forward Bitstream
  - Forward VCA
  - Forward Space Packet
  - Forward Proto Transfer Frame
  - Forward Telecommand VCA (TC-VCA)
  - Forward Space Packet

Application to AOS Frames

AOS Frame Header (per 732.0-B-2)

AOS Transfer Frame Primary Header



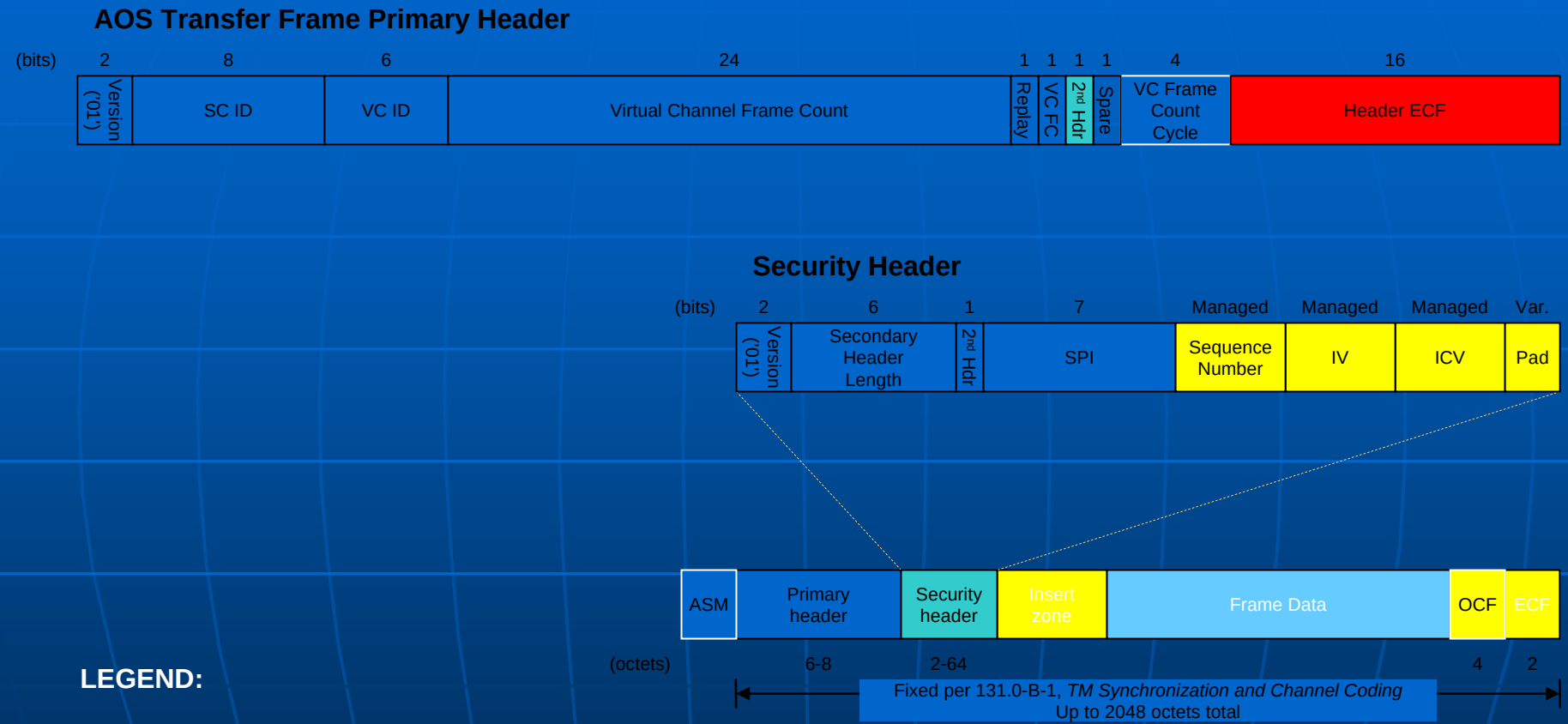


LEGEND:

White = required
Yellow = optional
Blue = user data

11/7/2008

AOS Frame with Security Header (proposed)



LEGEND:

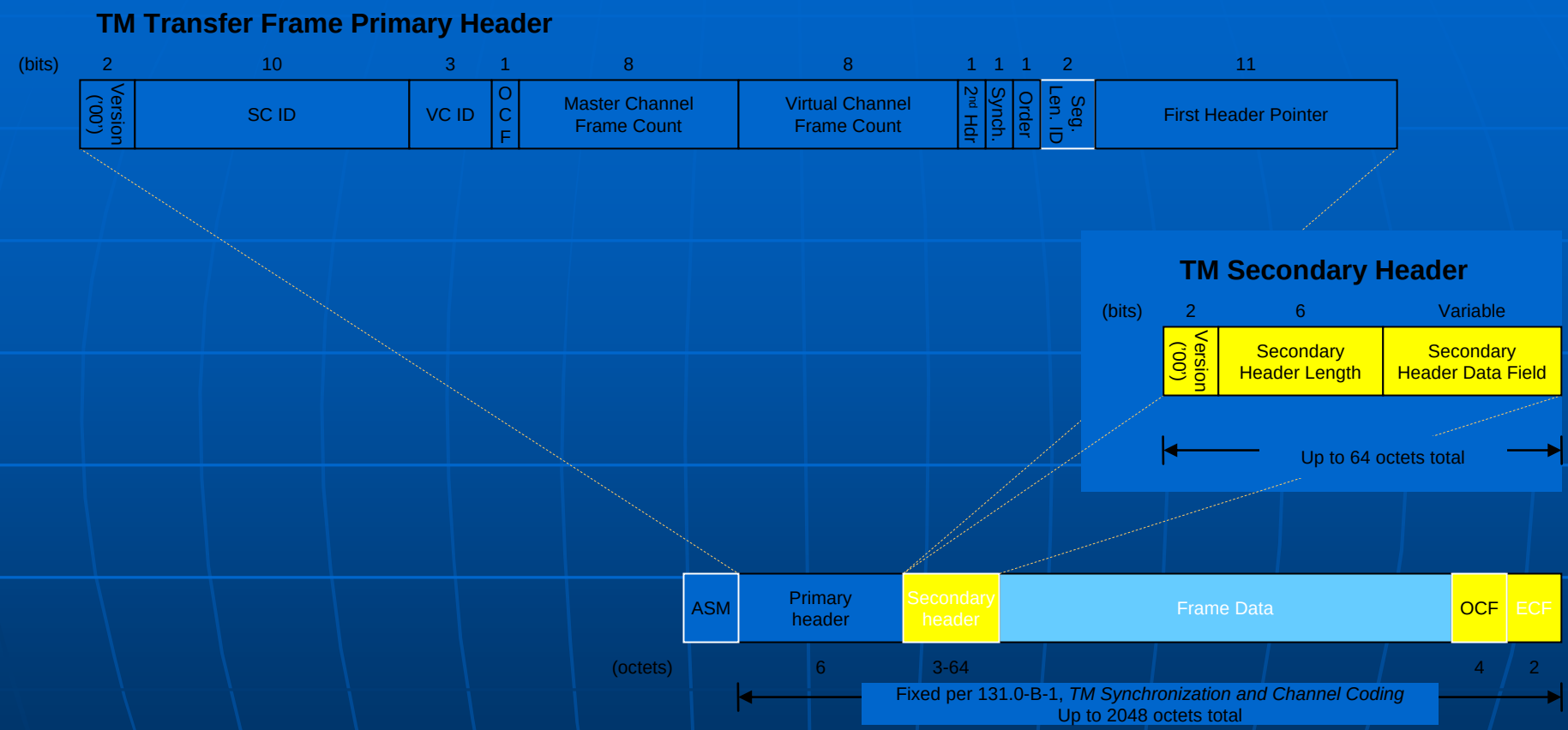
White = required
Yellow = optional
Blue = user data
Green = new / modified
Red = should not be included

Application to AOS Frames

- AOS Transfer Frame Primary Header
  - Currently there are 2 unused bits
  - Redefine 1 of these bits to signal the existence of a secondary header
    - (Revision of existing Blue Book CCSDS 732.0-B-2, "AOS Space Data Link Protocol", §4.1.2)
- Security Header
  - Transmitted after Primary Header, and before [optional] Insert Zone and Frame Data field
    - Insert Zone receives same protections as Frame Data contents
  - If Authentication is specified:
    - Authentication ICV is computed over whole frame except for sync mark and [optional] ECF
      - (i.e., Primary Header, Security Header, Insert Zone, Frame Data, and OCF)
  - If Encryption is specified:
    - Encryption is performed upon Pad, Insert Zone, and Frame Data
  - If Authenticated Encryption is specified:
    - Encryption is performed upon Pad, Insert Zone, and Frame Data
    - Authentication ICV is computed over whole frame except for sync mark and [optional] ECF
      - (i.e., Primary Header, Security Header, Insert Zone, Frame Data, and OCF)
  - If Encryption with Validation is specified:
    - Validation ICV is computed over whole frame except for sync mark and [optional] ECF
      - (i.e., Primary Header, Security Header, Insert Zone, Frame Data, and OCF)
    - Encryption is performed upon ICV, Pad, Insert Zone, and Frame Data

Application to TM Frames

TM Frame Primary & Secondary Header (per 132.0-B-1)

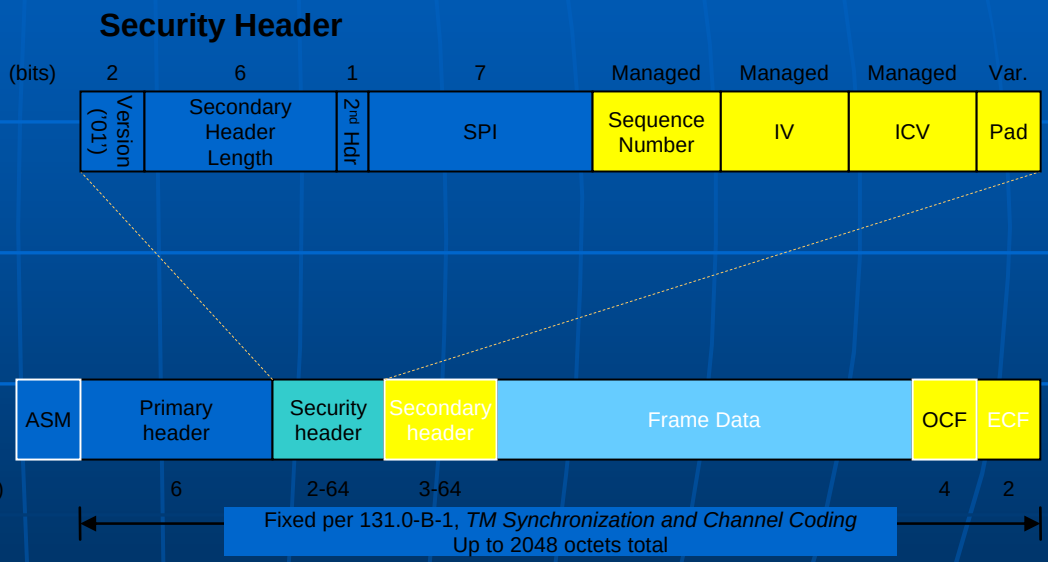


LEGEND:

White = required
Yellow = optional
Blue = user data

11/7/2008

TM Frame with Security Header (proposed)



LEGEND:

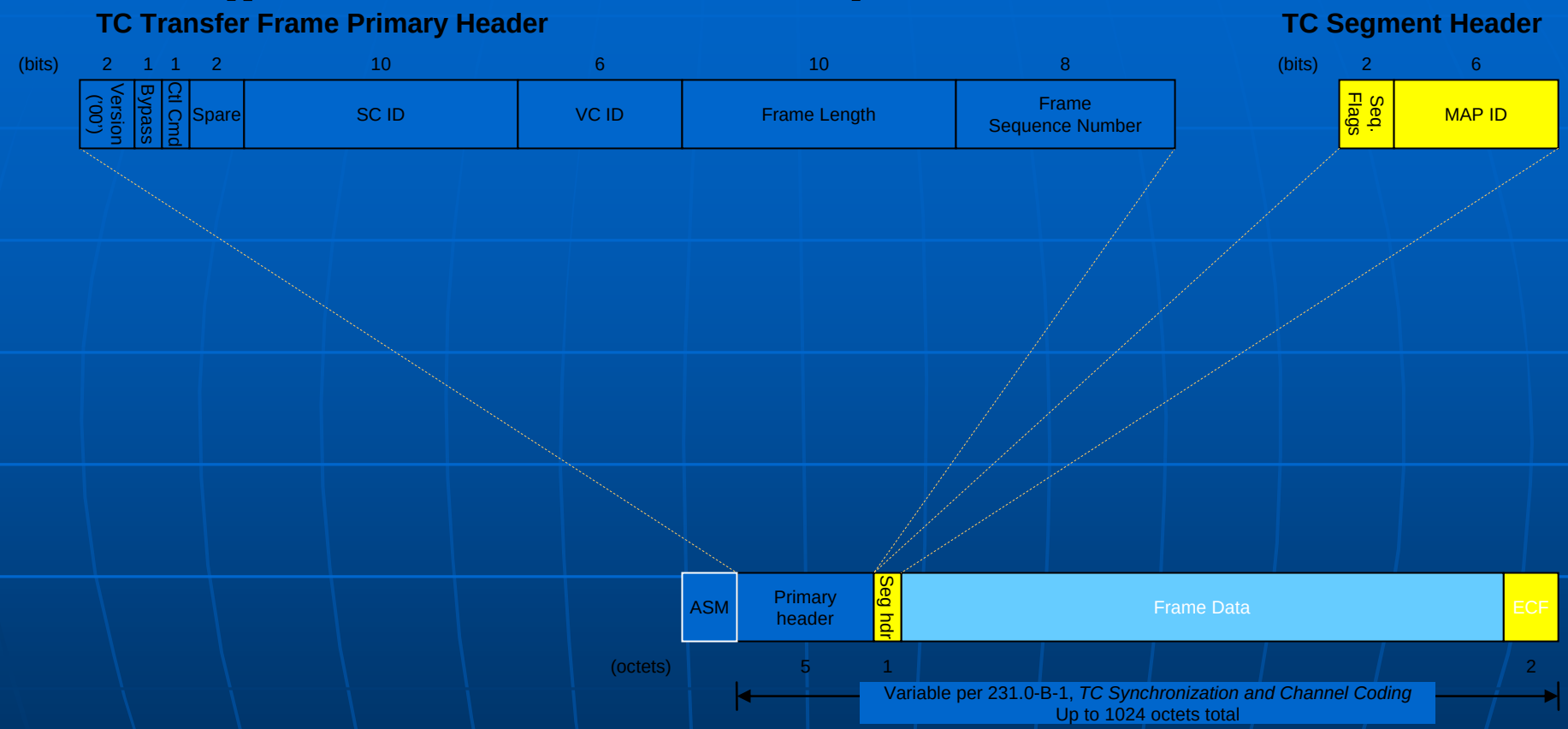
White = required
Yellow = optional
Blue = user data
Green = new / modified
Red = should not be included

Application to TM Frames

- TM Transfer Frame Primary Header
  - Currently uses 1 bit of Data Field Status to signal the existence of a secondary header
  - No modification necessary
- TM Transfer Frame Secondary Header
  - No mandated content other than header length field
  - No apparent benefit to putting existing secondary header ahead of security header
  - No modification necessary
- Security Header
  - Transmitted after Primary Header, and before [optional] TM Frame Secondary Header and Frame Data field
  - If Authentication is specified:
    - Authentication ICV is computed over whole frame except for sync mark and [optional] ECF
      - (i.e., Primary Header, Security Header, TM Frame Secondary Header, Frame Data, and OCF)
  - If Encryption is specified:
    - Encryption is performed upon Pad, TM Frame Secondary Header, and Frame Data
  - If Authenticated Encryption is specified:
    - Encryption is performed upon Pad, TM Frame Secondary Header, and Frame Data
    - Authentication ICV is computed over whole frame except for sync mark and [optional] ECF
      - (i.e., Primary Header, Security Header, TM Frame Secondary Header, Frame Data, and OCF)
  - If Encryption with Validation is specified:
    - Validation ICV is computed over whole frame except for sync mark and [optional] ECF
      - (i.e., Primary Header, Security Header, TM Frame Secondary Header, Frame Data, and OCF)
    - Encryption is performed upon ICV, Pad, TM Frame Secondary Header, and Frame Data

Application to TC Frames

TC Frame Primary & Segment Header (per 232.0-B-1)

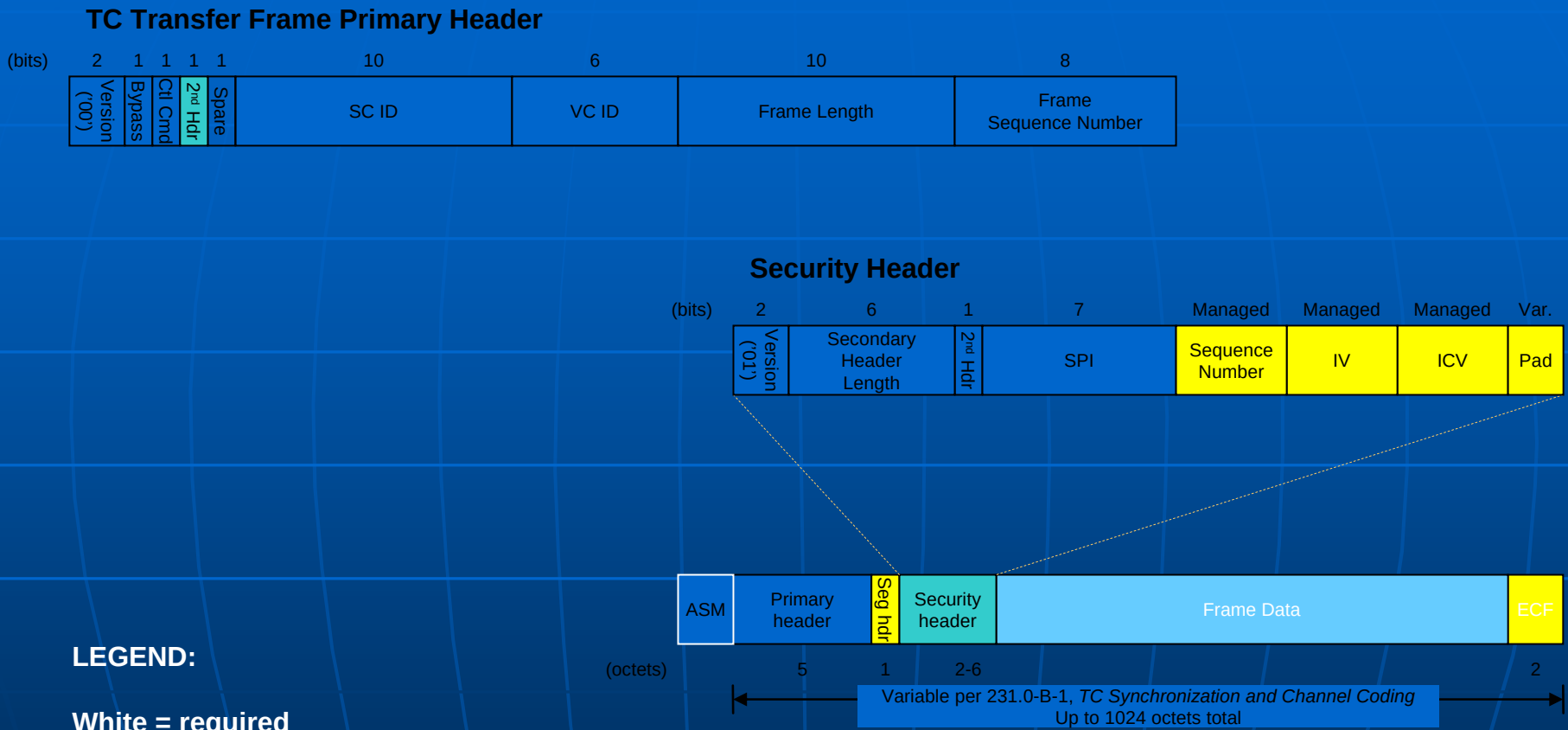


LEGEND:

White = required
Yellow = optional
Blue = user data

11/7/2008

TC Frame with Security Header (proposed)



LEGEND:

White = required
Yellow = optional
Blue = user data
Green = new / modified
Red = should not be included

Application to TC Frames

- TC Transfer Frame Primary Header
  - Currently there are 2 unused bits
  - Redefine 1 of these bits to signal the existence of a secondary header
    - (Revision of existing Blue Book CCSDS 232.0-B-1, "TC Space Data Link Protocol", §4.1.2)
- TC Segment Header
  - No modification necessary
- Security Header
  - Transmitted after Primary Header and [optional] Segment Header, and before Frame Data field
    - Transmitting Segment Header ahead of Security Header permits use of unencrypted Multiplexer Access Point (MAP) ID field by the receiver
  - If Authentication is specified:
    - Authentication ICV is computed over whole frame except for sync mark and [optional] ECF
      - (i.e., Primary Header, Segment Header, Security Header, and Frame Data)
  - If Encryption is specified:
    - Encryption is performed upon Pad and Frame Data
  - If Authenticated Encryption is specified:
    - Encryption is performed upon Pad and Frame Data
    - Authentication ICV is computed over whole frame except for sync mark and [optional] ECF
      - (i.e., Primary Header, Segment Header, Security Header, and Frame Data)
  - If Encryption with Validation is specified:
    - Validation ICV is computed over whole frame except for sync mark and [optional] ECF
      - (i.e., Primary Header, Segment Header, Security Header, and Frame Data)
    - Encryption is performed upon ICV, Pad, and Frame Data