ESTEC/ITT AO/1-6491/10/NL/AT

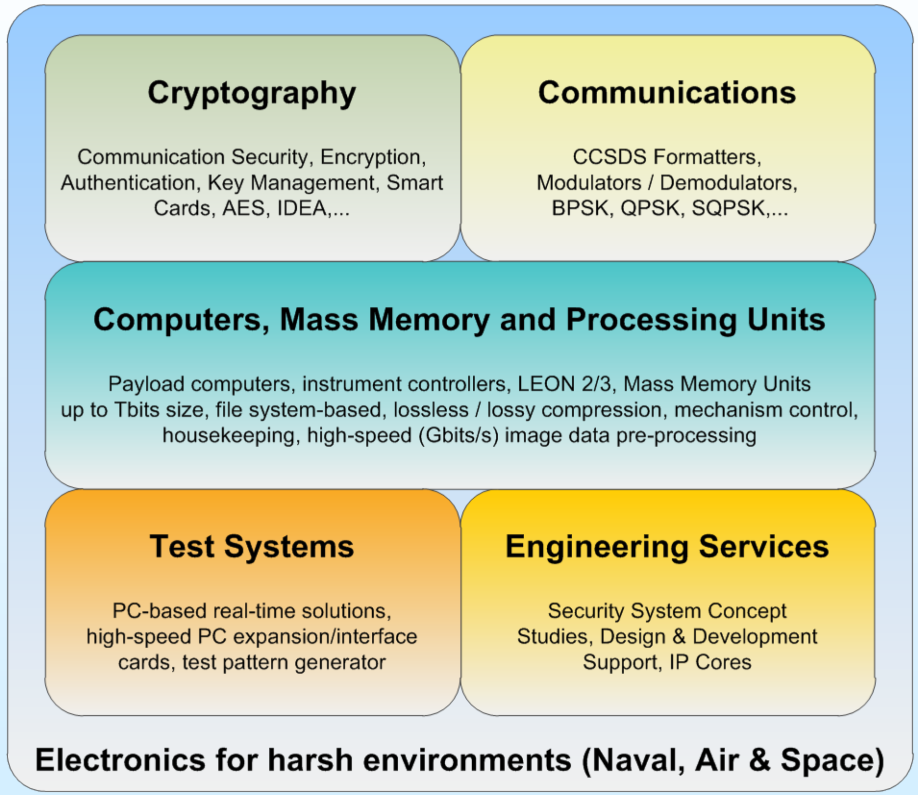
Cryptographic Processor (CP) for the control of Telecom Processing Payloads (CPTPP)

DSI GmbH

Otto-Lilienthal-Str. 1 • D-28199 Bremen • Germany

Phone +49 421 59696-950
Fax +49 421 59696-959
http://www.dsi-it.de

DSI (Digital Signal Processing and Information Technology GmbH) is a SME located in Bremen, Germany which provides high speed electronic units for:



DSI has been developing airborne and space-based designs since 1997 and currently employs around 45 engineers for electronics, software, project management and product assurance.

DSI Informationstechnik

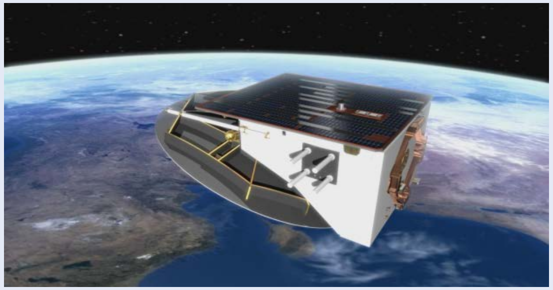
DSI electronic components are part of the major European airborne and space programmes

KompSat 2

Space & ground downlink data formatting and crypto system

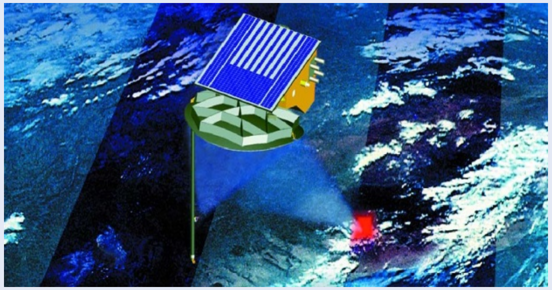
SAR-Lupe 1+2

Space & ground downlink data formatting and crypto system



ESGA

Gound crypto components

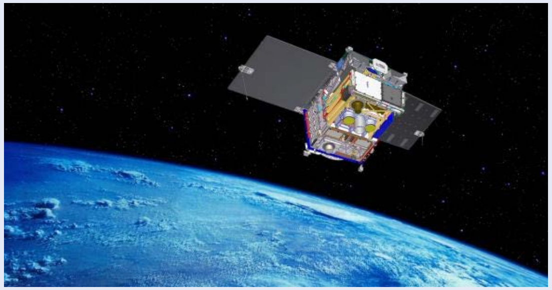


Condor 2

Airborne & ground crypto system

TET

Payload Control Computer and I/O Card



SatComBW II

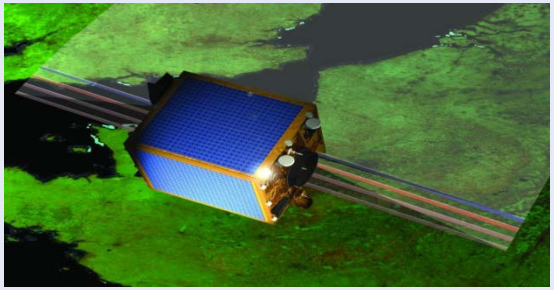
Ground crypto test unit

Galileo

Ground crypto test unit

Proba V

Payload Control Unit incl. compression and downlink formatter



DSI Informationstechnik

DSI electronic components are part of the major European airborne and space programmes

ExoMars

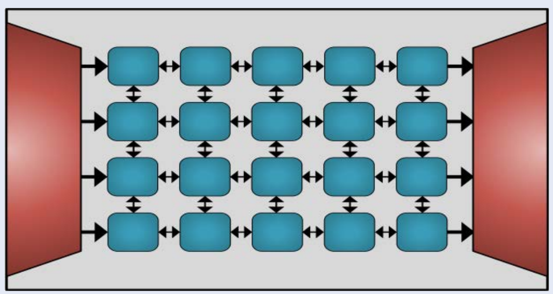
Payload Data Handling Unit incl. Mass Memory design

Euro Hawk

Airborne & ground crypto system

QI2S

Space multicore processor demonstrator system

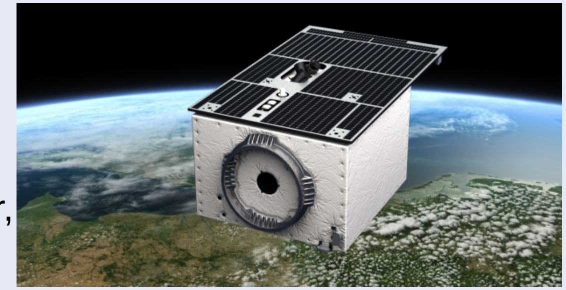


JAXA Hayabusa-II MASCOT

On Board Computer

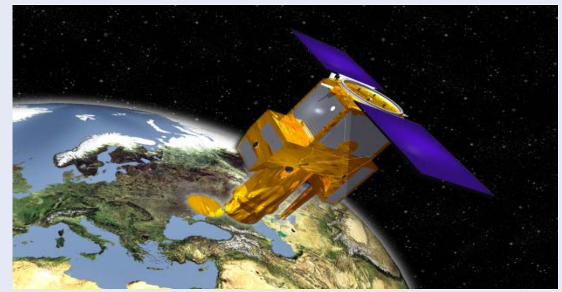
EnMap

Mass Memory incl. com-pression and downlink for-matter, Payload Controller



GökTürk

Space & ground downlink data formatting and crypto system



ICARUS LEO

Standard Platform Computer & I/O board

SAT-AIS

Data protection concept

Contents

Part 1: Background, Concept, Design

- Project Overview – Main Objectives and Requirements
- System Characterisation – Reference Architecture, Use Cases
- Threat/Security Risk Analysis – Threats, Vulnerabilities, Risks
- Risk Countermeasures & Security Mechanisms
- CP Design and Communications Protocol Integration
- Security Assurance

Part 2: Implementation

- CP Architecture
- CP Hardware
- CP EGSE/Tester

- Telecom satellite payload control and configuration (PCC)

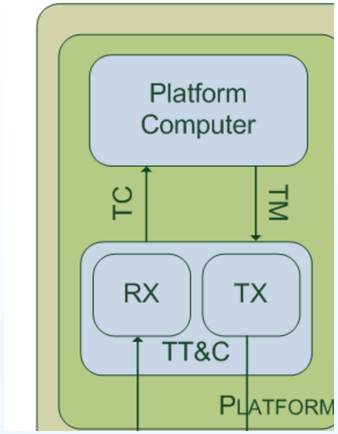
- The PCC space link is used for configuring and monitoring radio- and higher-layer data communications resource management-related parameters, software-defined radio etc.

- The PCC link is similar in nature to the traditional TM/TC links, although its criticality is somewhat lower

- The industry expects usage of dynamically reconfigurable payloads and hence PCC links in future fixed and mobile broadband satellite service missions

Assumed Telecom Payload and PCC Link Uses

Payload Use Case Class No./Type	Example Use Cases	Corresponding assumed PCC link use case examples
1. General public communications/ entertainment	Voice, television	Dynamic (re)allocation of logical voice channels and capacity as calls begin and end
2. Commercial/ scientific asset/sensor monitoring	Collecting meteorological, environmental, unmanned installation monitoring data from remote locations	Unlikely to be dynamically tuned due to low communication resource requirements, but PCC link could be used for monitoring data flow i.e. logical channel usage
3. Real-time commercial data communication	Financial and production data uplink	Tuning individual data flow scheduling parameters
4. Emergency communications	Destroyed communications infrastructure replacement for rescue services	Freeing up capacity and allocating the freed capacity to the emergency communication channels as the situation develops. Tuning quality-of-service-affecting parameters, to bound e.g. communication delay.
5. Military scenario	Conflict surveillance, sortie organisation	Virtual circuit set-up and tear-down, dynamic flow or packet scheduling parameter tuning, protocol mode switching, fast capacity reservation adjustments


Platform
Computer
TC
TM
RX
TX
TT&C
PLATFORM

Study Objectives (1)

- To analyse the threats (and hence security risks) to the PCC space link in order to define:
  - Requirements for security of the link
  - A system security concept for its protection

➢ Note that only the space link is in scope and physical layer is out of scope (e.g. jamming threats not considered here, but in another ESA study)

- To define how to integrate the security solution with CCSDS data link communication protocols and to develop a requirements specification for a space-borne cryptographic processor (CP) supporting the protection of the PCC link

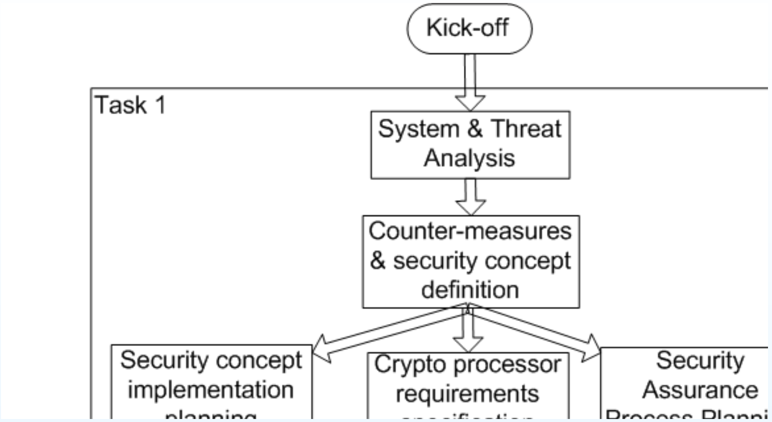
Study Objectives (2)

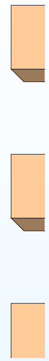
- To design and manufacture a breadboard model of the CP
- To design and manufacture the test equipment for the validation & verification (V&V) of the CP
- To perform the V&V of the CP
- To define a process for security assurance (SA) of the development of a commercial product version of the CP

Main Constraints & Requirements

- CP for geostationary satellites
- TC and TM data rate: 200kbps max.
- CCSDS space data link protocols used for TC and TM
- Security services:
  - Data origin authentication
  - Data integrity
  - Data confidentiality
  - Access control for sending TCs
  - Flexible cryptographic key management
- TC/TM interfaces: RS-422
- Technology for demonstrator: reprogrammable FPGA

Study Logical Flow





Sources of Threats to PCC Link

Threat Source	Motivation / Goal / Cause	Cap-ability	Threat Actions
Foreign (compared to payload user) government (war time)	Obtaining information on communication patterns before imminent attacks Disrupting communications Manipulating payload monitoring	High	Denial-of-service Eavesdropping – data viewing & traffic analysis Command manipulation TM manipulation Command Replay TM replay
Foreign government agency (peace time)	Obtaining information on governmental or commercial data traffic patterns	High	Eavesdropping – data viewing & traffic analysis
Terrorists	Disruption and/or manipulation of commercial or public service, even emergency response services	Medium-high	Denial-of-service Command manipulation TM manipulation
Criminal Organisation	Gaining insight into commercial operational traffic patterns for planning other attacks on e.g. payload data	Medium	Data viewing Command manipulation

Threat Source	Motivation / Goal / Cause	Cap-ability	Threat Actions
Rival satellite/telecom companies	Gaining insight into payload usage, traffic patterns etc. in the hope of using the information for gaining a competitive edge/financial advantage. Lower chance of active attack to disrupt a rival's operations	Medium-High	Data viewing Command manipulation Replay attack
Hacker	Curiosity Challenge/Ego Rebellion	Medium	Denial-of-service Command manipulation
Prankster	Curiosity Challenge/Ego	Low	Denial-of-service Command manipulation
Cryptographic administrator / officer (unintentional)	Inadequate cryptographic knowledge or experience	N/A	Poor management of keys leads to usage of weak sets of keys, aiding some of the above-listed threat actions

Example Vulnerabilities -> Exploiting Threat Actions -> Consequences

- Unencrypted configuration or monitoring information -> Eavesdropping -> Learn communication patterns for which the satellite is used (impact in critical scenarios is high)

- Unauthenticated TCs -> Data manipulation & forgery -> loss of control of communications -> may be extremely detrimental depending on communications scenario

- Unauthenticated TM -> Data manipulation & forgery -> loss of TM integrity -> confusion & undesired TCs sent in response

- Unauthenticated sequence numbers -> Data replay -> manipulated control/monitoring of communications resources

- Improper use of cryptographic algorithms (infrequent key change, keys too short, keys not “random enough”, MAC too short etc.) -> weakening of applied cryptographic measures

Risk Levels

- Risk levels are derived from estimated worst case impact/consequence of a successful vulnerability exploitation and its estimated order-of-magnitude likelihood
- Likelihood depends on motivation & capability of threat source and inherent difficulty in exploiting a vulnerability (depends on environment, inherent baseline security etc.)
- Identified risks are typically low-to-medium level, since the PCC link data is less critical than both the satellite TM/TC link and the payload data link
  - Having said this, we cannot rule out usage of telecom satellite capacity for high-criticality scenarios, even military, and hence impact of manipulation or divulgence of communication resource management information may have a high impact if enough context information is available for an attacker to draw conclusions

Security Goals and Corresponding Services

Security Goal	FWD Link Services	RTN Link Services	Key Management Services
Confidentiality	Selective field confidentiality or connectionless confidentiality	Selective field confidentiality or connectionless confidentiality	Connectionless confidentiality
Integrity	Connection integrity	Connection integrity	Connection integrity
Authenticity	Data origin authentication Peer entity authentication	Data origin authentication	Data origin authentication Peer entity authentication
Availability	Access control	N/A	Access control

Services	Mechanisms
Selective field / connectionless confidentiality	Encryption
Connection integrity	For data integrity: Data integrity check (MAC); Digital signature; Encryption; For flow integrity: Sequence numbers; time-stamping, nonces
Data origin authentication	Data integrity check (MAC); Digital signature; Encryption
Peer entity authentication	Digital signature; Encryption; Authentication message exchange / hand-shaking
Access control	Passwords / presentation of credentials; Digital signature

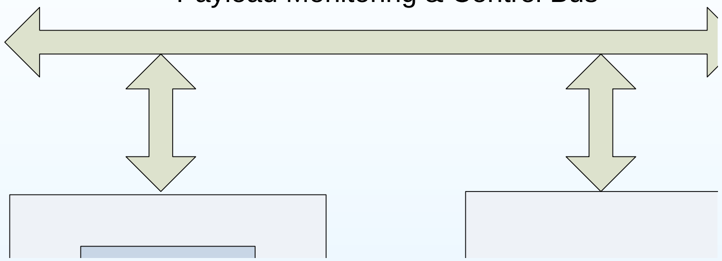
Cryptographic & Security Schemes

Security Mechanism	Countermeasure Type	Candidate Schemes (selected: in bold)
Encryption	Symmetric encryption	AES-CBC; **AES-CFB**; AES-CTR; AES-GCM; AES-OFB
Message authentication code	Hash-based MACs, Encryption-based MACs	HMAC-RIPEMD-160; HMAC-SHA-2; GMAC; **CMAC**
Digital signature	Elliptic Curve (EC), non-EC algorithms	**EC-GDSA,** DSA, EC-DSA, RSA
Connection integrity	Sequence number, time-stamping, nonces	Specific application-level sequence number; **communication protocol frame sequence number**, global clock-based time-stamp, randomly-generated nonce
Authentication message exchange/handshaking	Message exchange protocol + digital signature	Diffie-Hellman-based message exchange with EC-GDSA (or other digital signature, based on what is selected for the above)

CP-Supported Security Services

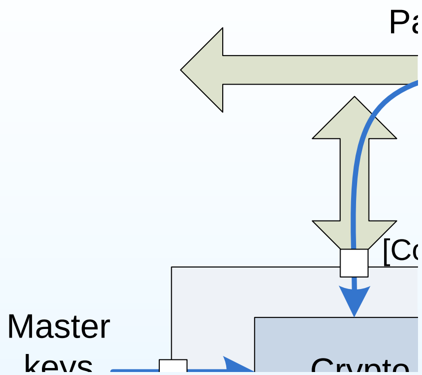
Security Function	Supported Services	Service ID	Input	Output
AES-256 decryption in cipher-feedback mode, AES-CFB-8	Forward link TC selective-field confidentiality	1	CCSDS TC transfer frame with encrypted payload	Decrypted CCSDS TC transfer frame
	Forward link CP TC selective-field confidentiality	2	Encrypted CP command	Decrypted CP command
	CP traffic key-unwrapping (key confidentiality)	3	Encrypted CP traffic key frame	Decrypted CP traffic key frame
AES-CFB-8 encryption	Return link TM selective-field confidentiality	4	CCSDS TM transfer frame	CCSDS TM transfer frame with encrypted payload
	Return link CP TM selective-field confidentiality	5	CP TM	CP TM with MAC
AES-CMAC verification with anti-replay counter	Forward link TC data and connection integrity	6	CCSDS TC transfer frame with MAC	Authenticated CCSDS TC transfer frame without MAC (or rejection of TC transfer frame)
AES-CMAC calculation with anti-replay counter	Return link TM data and connection integrity	7	CCSDS TM transfer frame	CCSDS TM transfer frame with MAC and ARC
AES-CMAC verification	Forward link CP TC data integrity	8	CP command with MAC	Authenticated CP command without MAC or rejection of CP command
	CP traffic key authentication (key integrity and authenticity)	9	Encrypted and MAC-tagged CP traffic key frame	Encrypted CP traffic key frame (or rejected key frame)
AES-CMAC calculation	Return link CP TM data integrity	10	CP TM	Authenticated CP TM with MAC

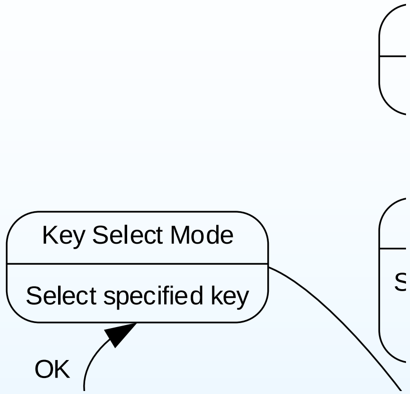
In-band



Out-of-band

Extern. Interfaces, Commanding & Monitoring




Key Select Mode
Select specified key
OK

Key Management

- Common approach, symmetric key infrastructure chosen (after trade-off with public key infrastructure approach)
- Master encryption/authentication keys pre-loaded onto satellite
- Data keys can be uploaded in sets and later activated
- The layered encryption/authentication scheme allows the cryptographic separation of logical channels and hence user privileges
  - i.e. Key manager, CP operator, day-to-day operator

Key Uploading

Key ID	Pld. TC Enc. Key	Pld. TC Enc. IV	Pld. TC Auth. Key	Pld. TM Enc. Key	Pld. TM Enc. IV

User Roles

Role	Level of Trust	Available Security Services	Usable CP Interfaces
Payload Operator	Knowledge of TC/TM encryption and authentication keys	1, 4, 6, 7	TC_in, TC_out, TM_in, TM_out
CP Operator / Security Officer	Knowledge of CP TC/TM encryption and authentication keys	All except 3 and 9	All except internal master key PROM interface
Key Management Officer	Knowledge of master keys for key encryption and authentication	All	All

Protocol Layer Choice Considerations for Encryption

The lower the encryption layer the more headers and fields are protected,

but:

- More difficult to differentiate security (e.g. different keys) between services on the link
- Counter-productive to encrypt EDAC code blocks or information (so the layer should not be TOO low)
- Hardware vs. software e.g. lower layer implementation may force hardware cryptographic processing (also for performance reasons)

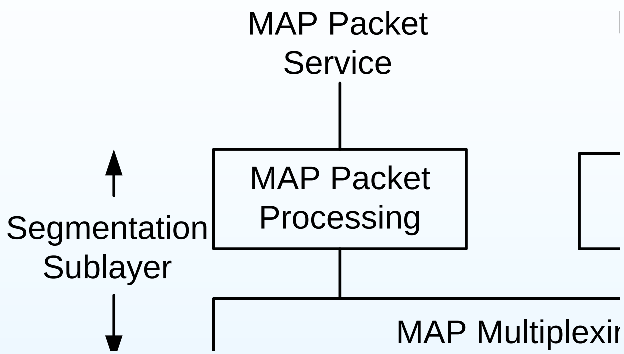
Protocol Layer Choice Considerations for Authentication

Integrity is often more critical than confidentiality for unclassified missions -> thus authentication should cover as many fields as possible i.e. be at as low a layer as possible to avoid control information manipulation,

but:

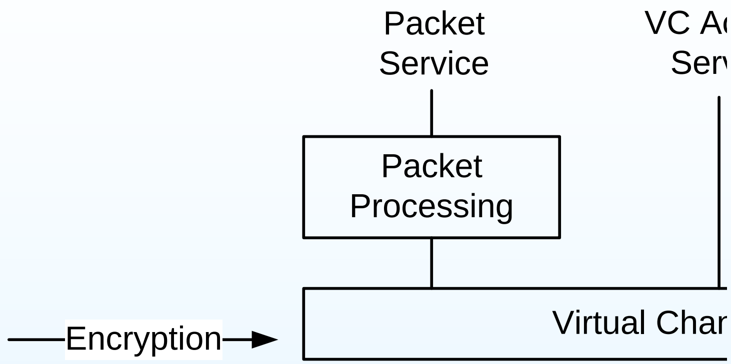
- MAC schemes are sensitive to single-bit errors so it is useless to place MAC below coding layer
- MAC needs space in e.g. secondary header or user payload space

Overall, the integration approach (devised independently) is similar to CCSDS draft standard Space Data Link Security Protocol (SDLSP)



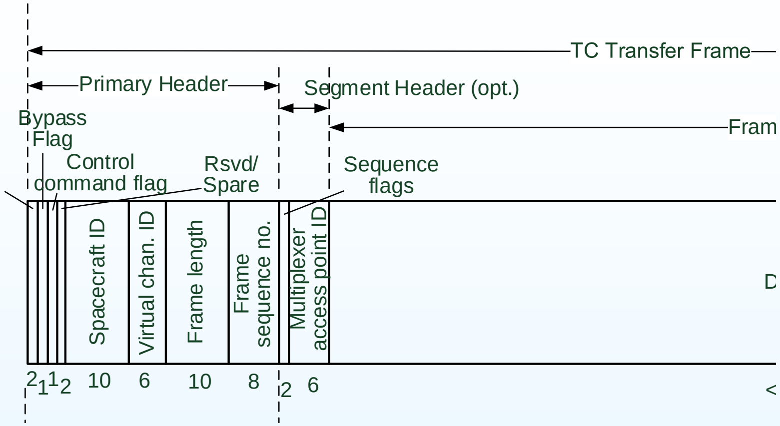
Data field size slightly restricted to make room for security information

TM Data Link Protocol Integration



Secondary header field used for security information

TC/TM Data Link Protocol – Security Integration



- Analogous to product assurance, runs in parallel to product development
- Based on standard security requirements
    - Selected standard was FIPS-140-2 requirements for cryptographic modules
- FIPS-140-2:
    - Aimed at modules protecting sensitive but unclassified data -> fits the CPTPP scenarios
    - Specifies functional, configuration, documentation, design and verification requirements
- Security level 2 selected as suitable for CPTPP
    - Higher levels require operator identity-based access control and active tamper protection -> not necessary for space unit
- FIPS-140-2 requirements adapted into CPTPP requirements

- When developing a product to be mass-produced and sold to e.g. Government agencies with standard-based security requirements, FIPS-140-2 certification can be sought
- For less formal security assurance, cheaper self-assurance can be pursued
- SA includes checking project outputs to ensure security functional, documentation and verification requirements are upheld, based on the selected security standard
- Prepared Security Assurance (SA) plan, akin to small PA plan, including SA milestone report DRD
- Reported SA activity outcomes in SA milestone reports as well as SA review-of-design (verification) report – including security requirements compliance/verification control matrix

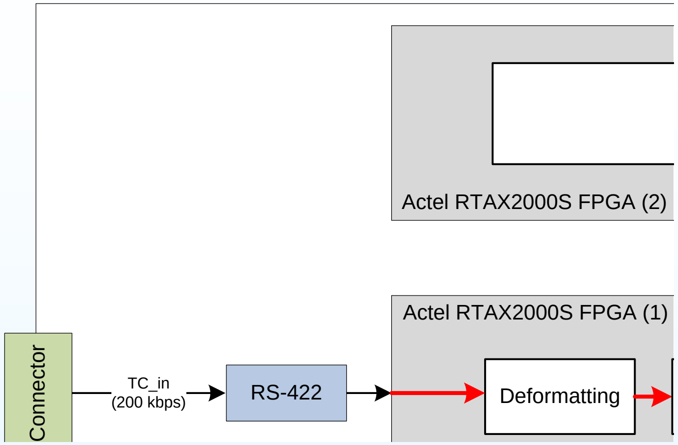
Contents

Part 1: Background, Concept, Design

- Project Overview – Main Objectives and Requirements
- System Characterisation – Reference Architecture, Use Cases
- Threat/Security Risk Analysis – Threats, Vulnerabilities, Risks
- Risk Countermeasures & Security Mechanisms
- CP Design and Communications Protocol Integration
- Security Assurance

Part 2: Implementation

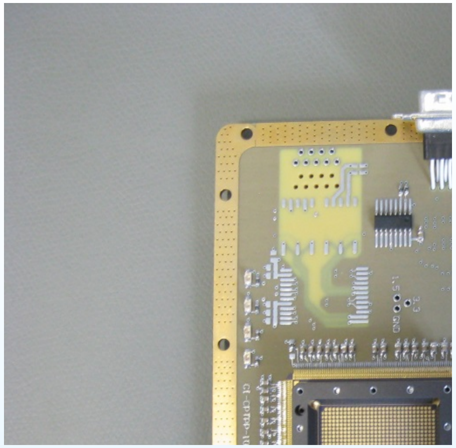
- CP Architecture
- CP Hardware
- CP EGSE/Tester


Actel RTAX2000S FPGA (2)
Actel RTAX2000S FPGA (1)
Connector
TC_in
(200 kbps)
RS-422
Deformatting

Hardware Architecture Overview

- TC/TM serial link data rate 200 kbps
- CCSDS TC CLTU & TM CADU
- Control Interface 115 kbps UART
- External Key Cartridge (EE)PROM I/F
- 32 master keys
- 64 traffic keys. Update via TC command
- EDAC protected internal memory modules
- Anti-replay counter with recovery functions after power-up/reset
- Physical separation of control/data path
  function and cryptographic function
- Power usage ≤ 5W in all modes

Processor Board Layout



Size: 185 mm x 155 mm

FM layout principals with commercial parts used

Prototype adapter used for RTAX footprint


J1
J4
J5
DSI
Informationstechnik
Germany
Model: CPTPP Cryptographic Pr
Serial No.: CI-CPTPP-10.00.00-00

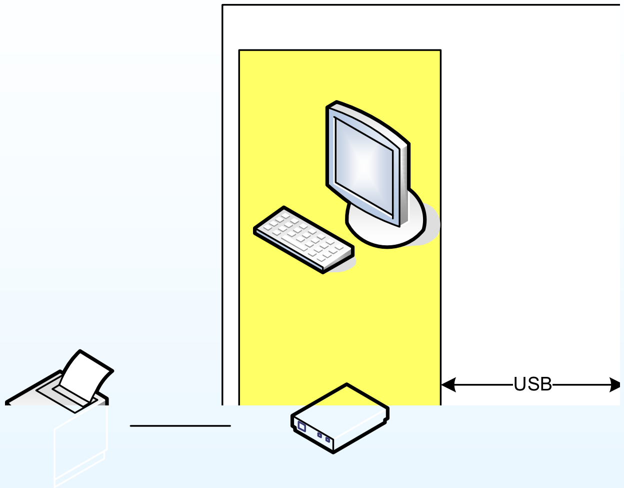
Front

Rear

Verification/Testing Overview

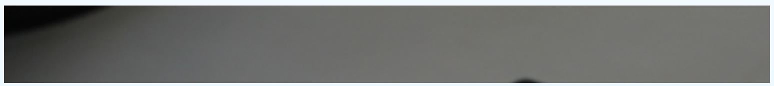
- General verification to check general CP operational correctness:
    - Physical properties
    - Electrical interface tests
    - Functional and performance tests
    - Error cases, failure detection tests

- Validation against requirements:
    - Physical properties tests against requirements and ICDs and checking of correct configuration management
    - Verification of fulfilment of and adherence to functional and performance requirements inc. correct implementation of cryptographic algorithms
    - Review-of-design and inspection to verify fulfilment of non-testable requirements


USB

- **Laptop + interface adaptor box**

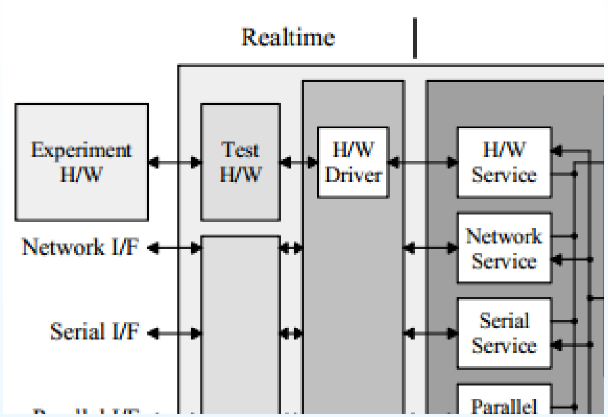
- **Interface box photos:**



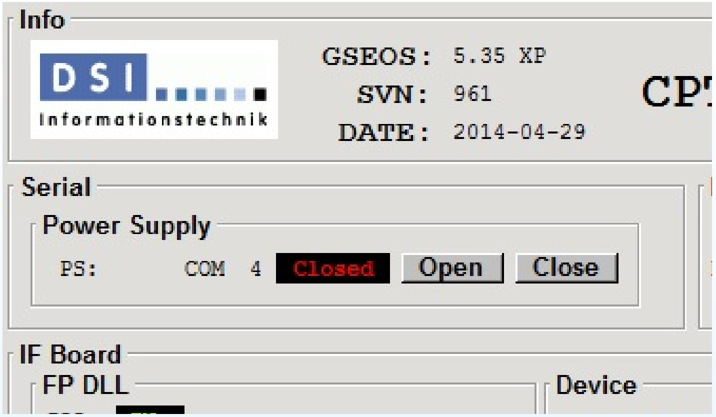
EGSE Capabilities

- Generate and save test sequences (test cases), and execute the defined test sequences / batches
- All different interfaces are operable simultaneously and independently of each other
- Analyze and verify the UUT data stream online and offline (i.e. verify the saved UUT data)
- Simulation of attacks at the interface level (e.g. replay of data),
- Injection of erroneous data into data stream (e.g. simulation of bit errors within the protocols)

GSEOS Software – System Diagram



CPTPP EGSE Test Screen



Summary of Key Project Outcomes

- Security risks and corresponding security measures for the PCC links were analysed
- Security concept developed
- Cryptographic processor (CP) requirements specification established
- CP designed and manufactured
- CP test equipment designed and manufactured
- CP demonstration model tested/verified