CPIP

Crypto Processor Intellectual Property

Final Presentation Days - ESTEC

DEFENCE AND SPACE

Arnaud Wagner

11 December 2018

AIRBUS

Agenda

- ❑ What is CPIP ?
- ❑ Project objectives
- ❑ Functionalities
- ❑ Interfaces
- ❑ Performances
- ❑ System implementation example
- ❑ Security assurance
- ❑ Possible future work
- ❑ How to get CPIP ?

What is CPIP ?

❑ CPIP: **Crypto Processor Intellectual Property**

❑ **Soft IP** (VHDL and Verilog)

❑ Implements the Platform **Telecommand Security Layers**

❑ Implements the Platform and low bit rate Payload **Telemetry Security Layers**

❑ Compliant to **CCSDS Space Data Link Security (SDLS) Protocol: CCSDS 355.0-B-1** Blue book, Septembre 2015

❑ **ESA Confidential** classification level

❑ Ready for **an EAL4+ Common Criteria Security Evaluation**

Project objectives

- **CPIP Specification**
  - Many missions security needs to take into account: observation, telecommunications, … (TC, TM and AOS protocols)
  - CPIP shall cope with several architectures: in-line, coprocessor, …

- **Security Assurance**
  - EAL4+ Common Criteria Evaluation anticipation
  - ESA Confidential security level development (secured room, dedicated server, …)

- **RTL development and delivery for ESA catalogue**

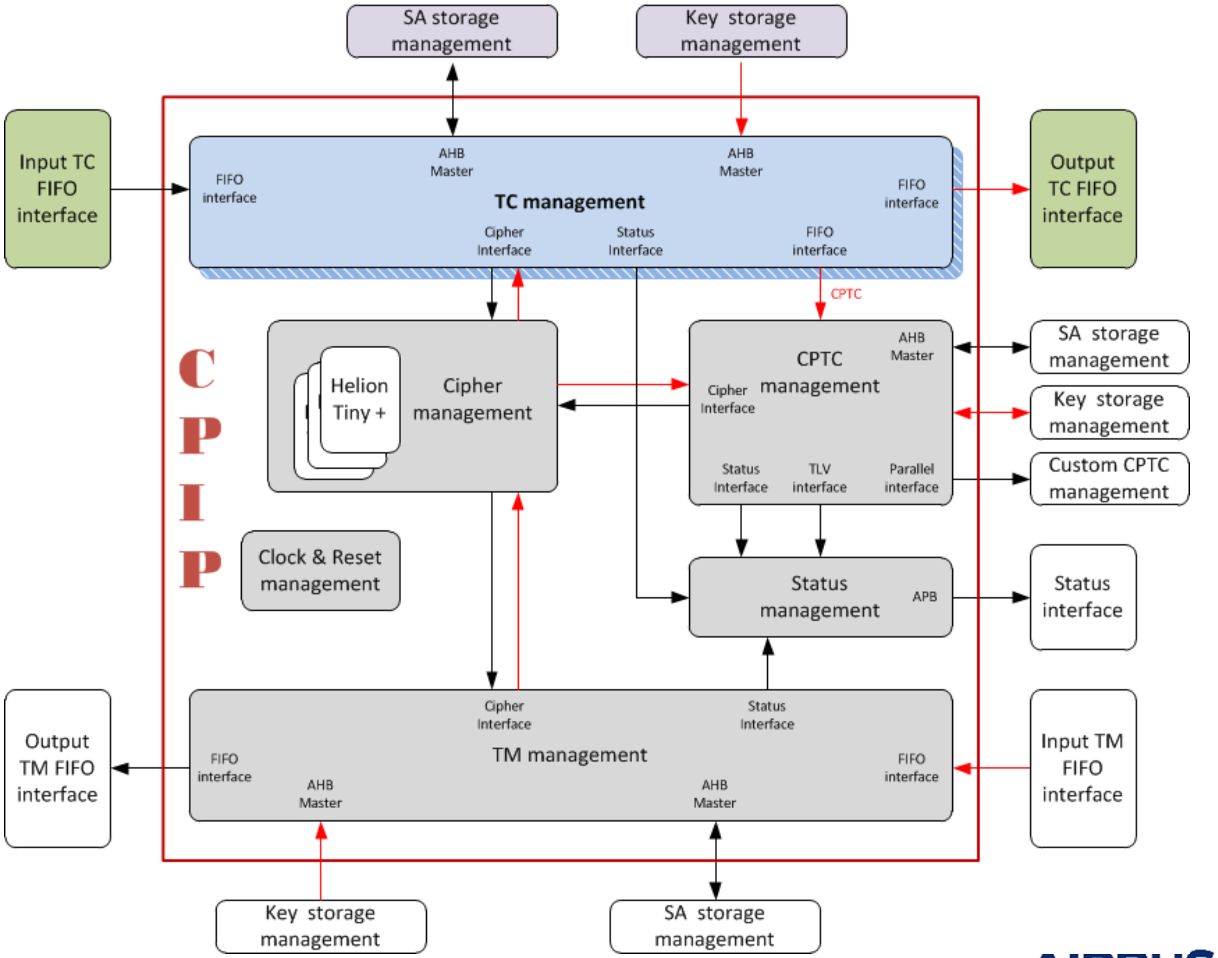
- **System C model (transactional level) development and delivery for ESA catalogue**
  - Used for RTL testing during CPIP development
  - Available for End User System simulations

- **Back end** on several **space FPGAs targets** feasibility performed

- **Breadboard Implementation**

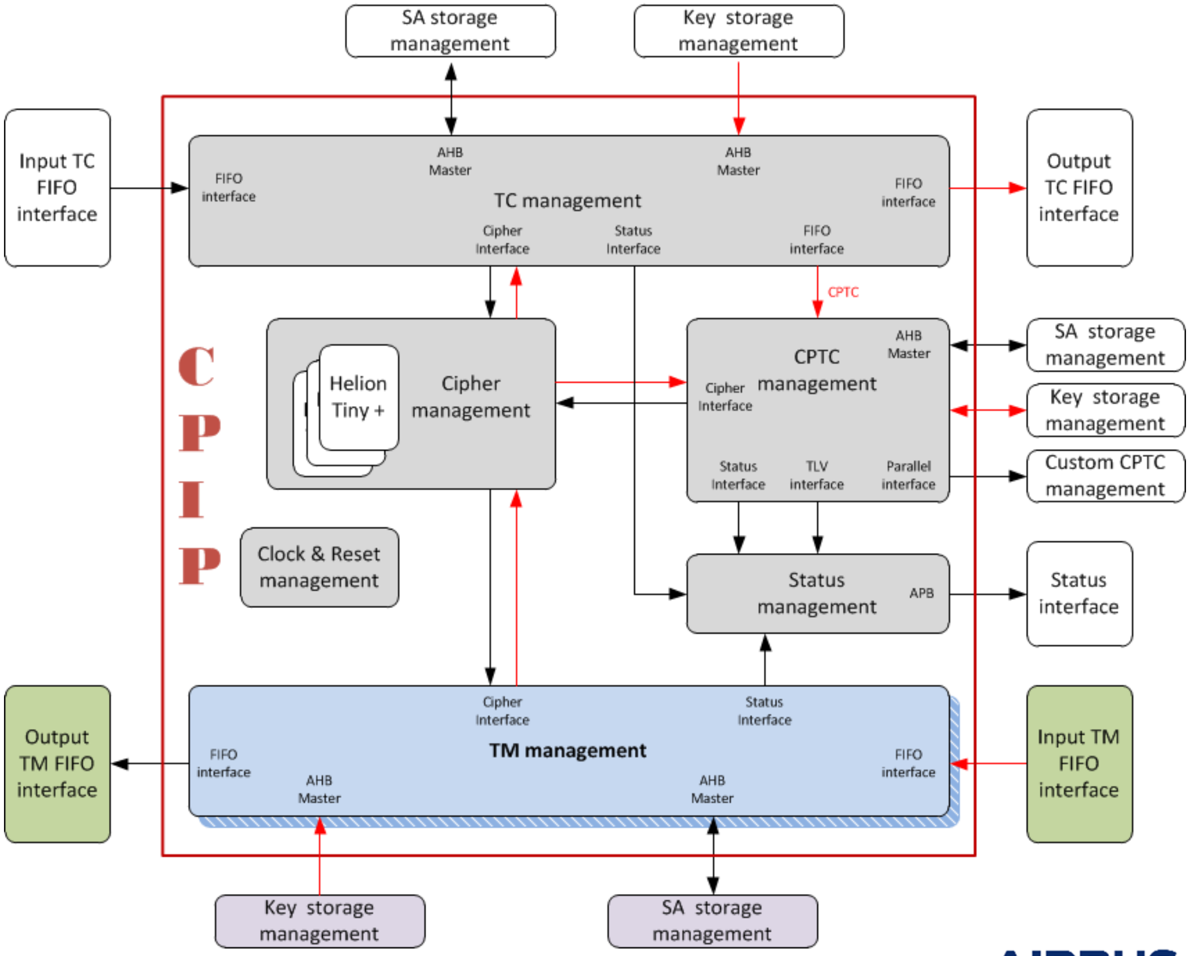
Functionalities: TC Management

- ❑ **Security protection of the platform TeleCommand (TC)** using the Space Data Link Security (SDLS) protocol standard
  - ❑ Up to 8 Secure Channels
- ❑ **AES GCM** for Authentication/Encryption and **AES CMAC** for Authentication only
- ❑ **128 or 256 bits** Keys length



Functionalities: TM Management

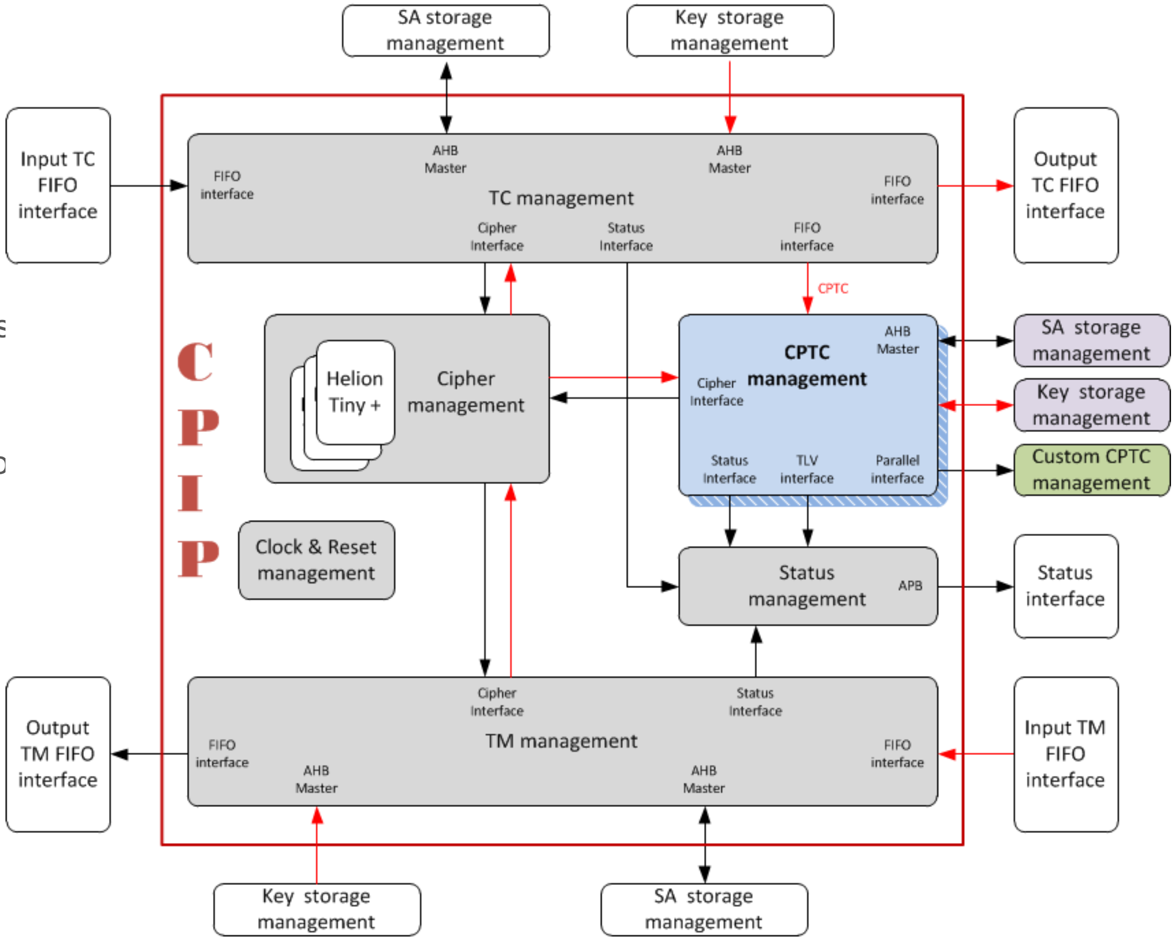
- ❑ **Security protection of the platform TeleMetry (TM)** or low bit rate payload TeleMetry using the SDLS protocol
  - ❑ Up to 8 Secure Channels
  - ❑ TM or AOS protocols
- ❑ **AES GCM** for Authentication/Encryption and **AES CTR** for Encryption only
- ❑ **128 or 256 bits** Keys length



Functionalities: Commanding

- ❑ **In-band Commanding through dedicated TCs** (CPTCs: Crypto Processor TeleCommands)
  - ❑ Standard format: one packet containing one TLV (Tag Length Value) structure
  - ❑ A set of commands are processed by CPIP for keys and parameters management
  - ❑ Custom commands capability (Custom CPTCs): extracted by CPIP from the TC flow and provided to User through a dedicated interface

- ❑ **Over The Air Rekeying** (OTAR)

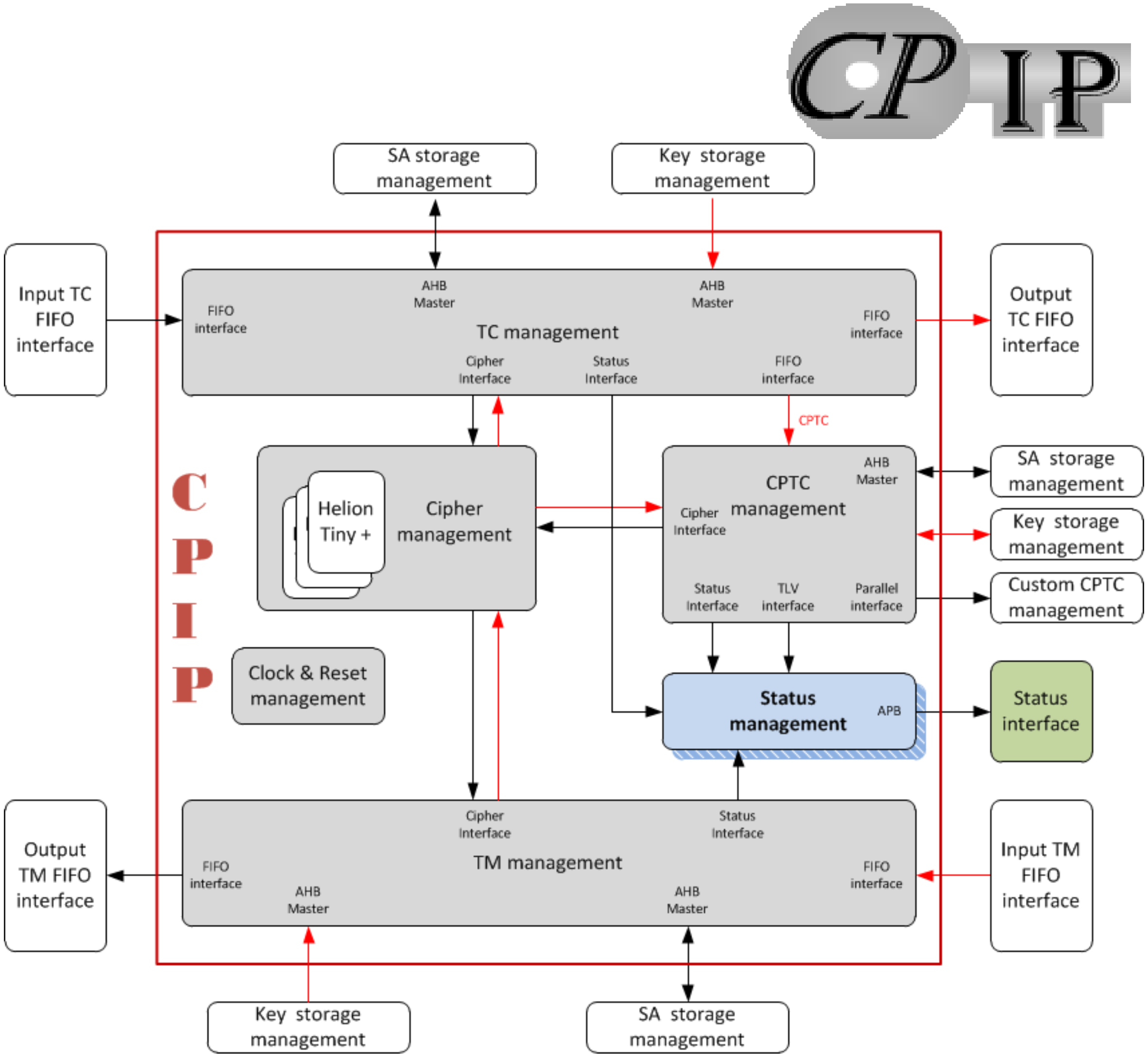


AIRBUS

Functionalities: Status

- ❑ Stores each report coming from other functions
- ❑ Makes reports available to external world
- ❑ **Standard format**: one TLV for each report (Tag Length Value) structure
- ❑ **Optional** implementation of an **Event Log buffer** for storing all CPIP status

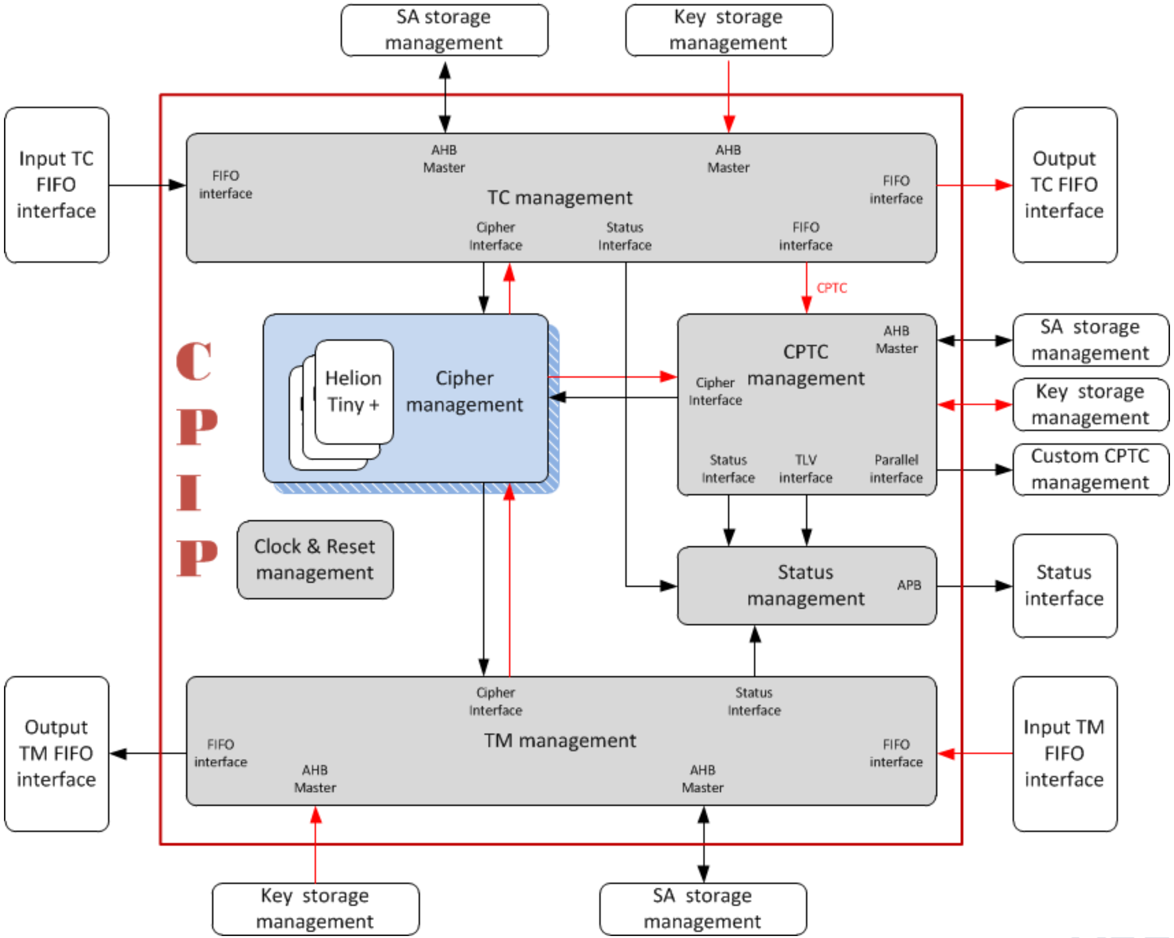
=> CPIP Reports may be put back in the TM flow externally by User



Functionalities: Cipher Management

- ❑ Implements 2 Helion AES Tiny+ GCM/CMAC IPs

- ❑ One IP is shared by
  - ❑ TC Management
  - ❑ CPTC Management for OTAR (Over The Air Rekeying)
- ❑ One IP is dedicated to TM Management

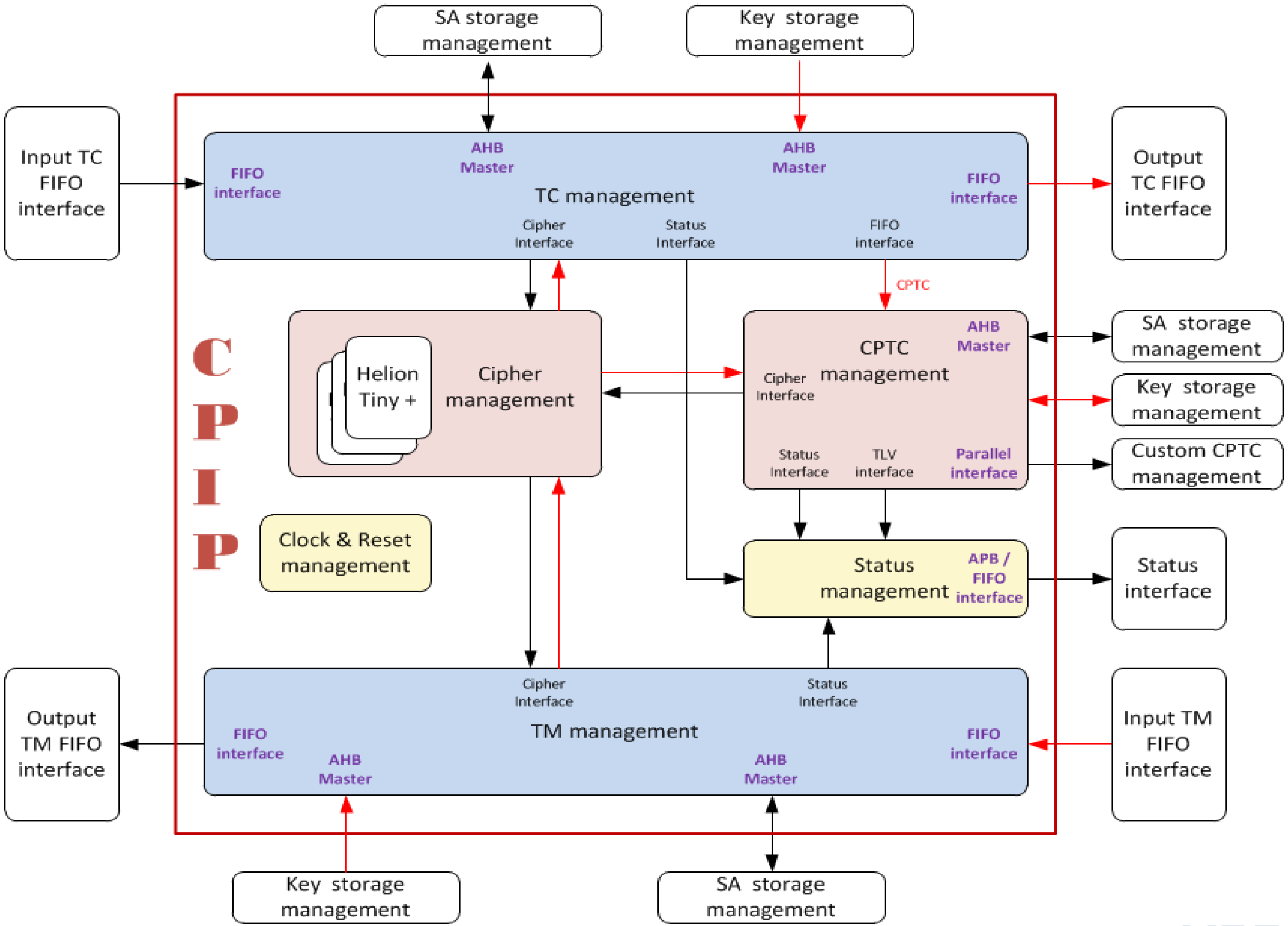


AIRBUS

Interfaces: Functional interfaces

- ❑ **Standard Interfaces**:
  - ❑ FIFO:
    - ❑ TC and TM input and outputs
    - ❑ Event Log buffer if implemented
  - ❑ AHB:
    - ❑ SA storage
    - ❑ Key storage
  - ❑ APB
    - ❑ CPIP Status
- ❑ **Handshake on input TC and input TM FIFO interfaces**

⇒ CPIP read of clear data may be slowed down by external world



Interfaces: Configuration interfaces

- ❑ **High level of configurability**
  - ❑ Through **generic parameters**:
    - ❑ Reset configuration: synchronous/asynchronous, active level
    - ❑ Event Log configuration: implemented/not implemented, size if implemented

  - ❑ Through **pseudo-static parameters** (Must be static when CPIP is working and a reset is recommended after parameters have been modified, 30 parameters about) :
    - ❑ Examples of parameters:
      - ❑ Number of keys for each Secure channel
      - ❑ Key length for TCs
      - ❑ Key length for TMs
      - ❑ …
    - ❑ Each parameter could be
      - ❑ A constant => design simplification through synthesis
      - ❑ Or on-flight modifiable (a reset is needed after any configuration modification)
      - ⇒ **A lot of possibilities for using CPIP configurability and still optimizing the area**

  - ❑ Through one AHB interface (Access to Security Associations memory):
    - ❑ Sequence Window for Anti Replay Counter,
    - ❑ …

Performances

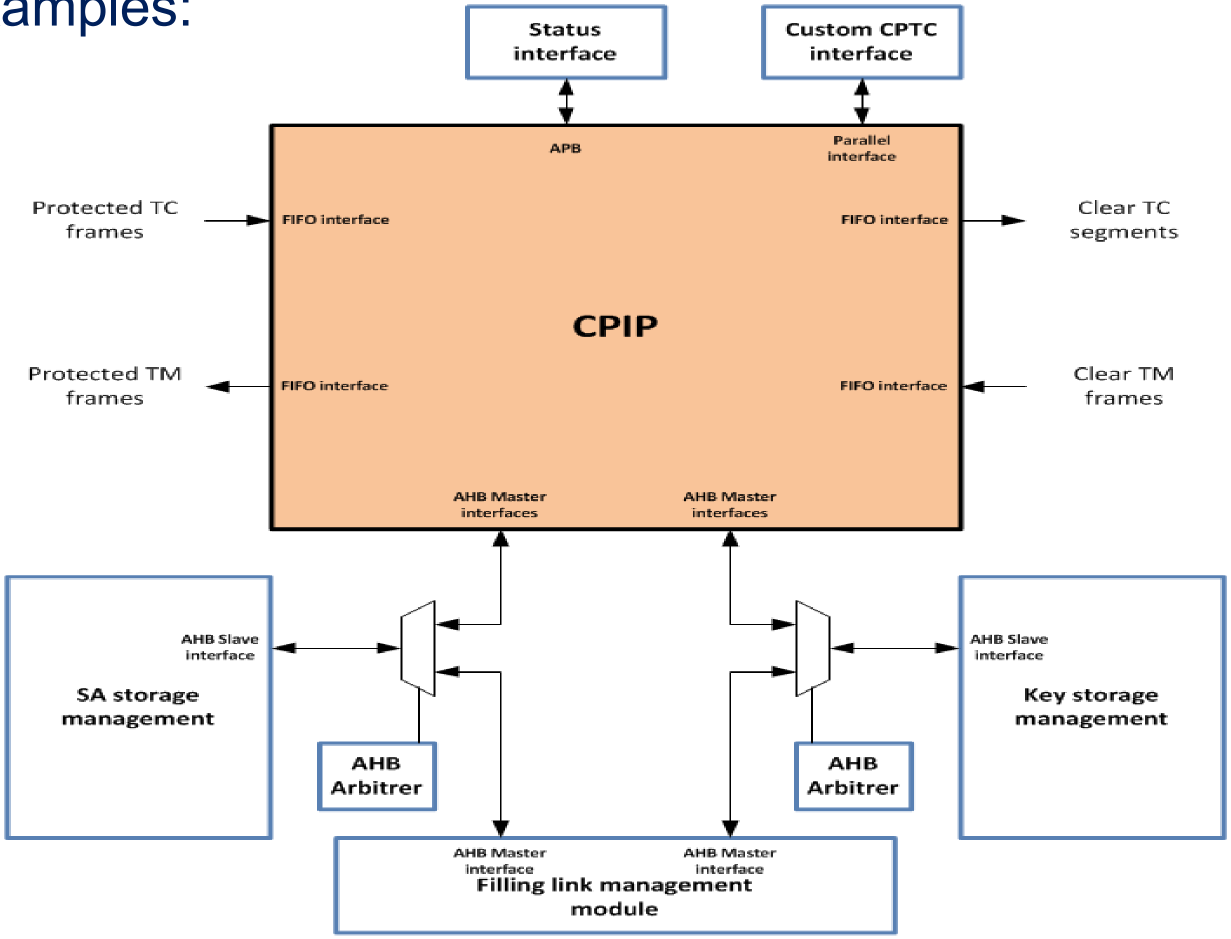
- ❑ **Real Time**
  - ❑ Depends on AHB access time (for getting the keys for example)
    - ❑ TC processing: Up to 10 Mbps at 50 MHz system clock
    - ❑ TM processing: Up to 19 Mbps at 50 MHz system clock

- ❑ **RTG4 performances achieved:**
  - ❑ Resources:
    - ❑ 5300 flip flops
    - ❑ 7300 LUTs
    - ❑ 1 RAM 1K18 + 0 to 2 RAM1K18 depending on Event Log buffer depth
  - ❑ System Clock: up to 82 MHz

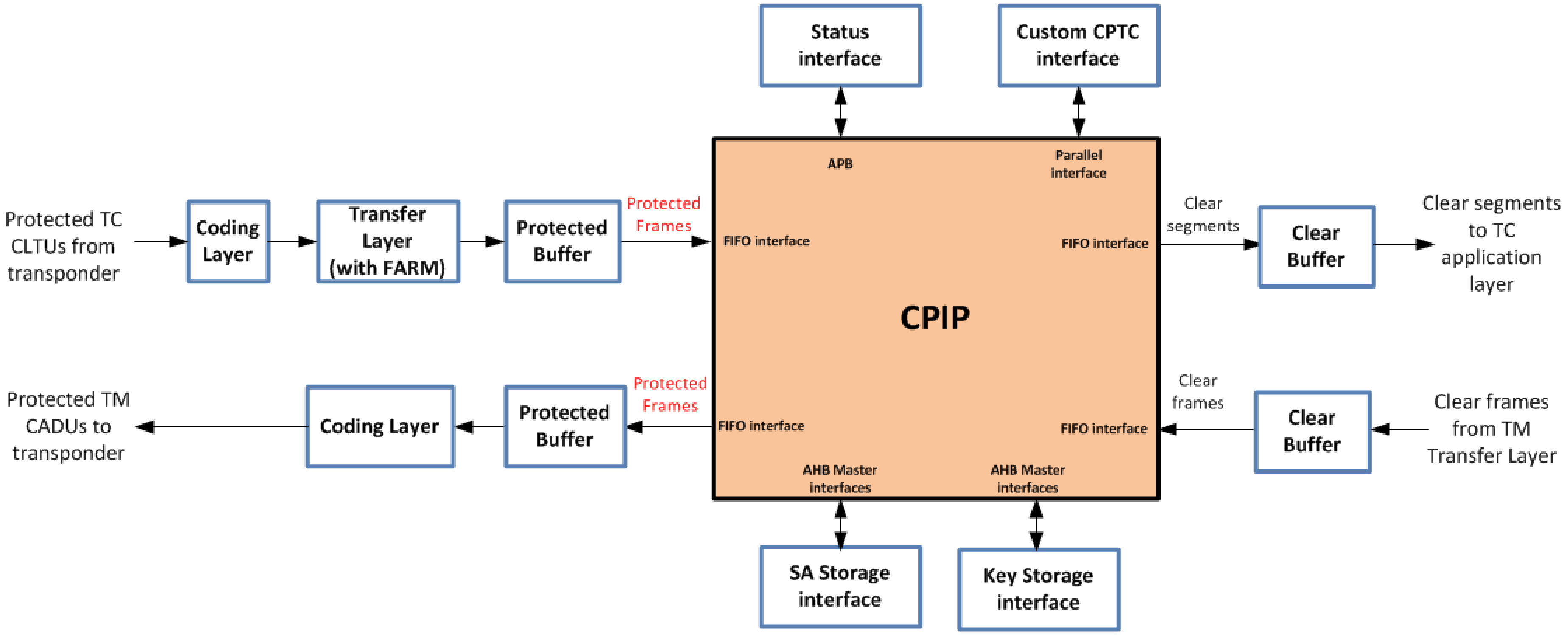
- ❑ **BRAVE NG-MEDIUM performances achieved with an Event Log buffer of 512 bytes:**
  - ❑ Resources :
    - ❑ 5300 flip flops
    - ❑ 11300 4-LUT
    - ❑ 350 XLUT
    - ❑ 170 4-bits carry
    - ❑ 6 Register file blocks
  - ❑ System Clock estimated to 41 MHz

System implementation examples: SA and Key storages

- Two AHB busses are used in the figure but SA storage and Key storage may be grouped in one common storage too which implies the use of only one AHB bus
  - If red/black separation is not needed
  - Or if red/black separation is guaranteed through another way
- CPIP virtual addressing has to be interpreted by SA and Key storage management
- SA and Key storage may contain:
  - Chip memories
  - External memories
  - Registers
  - A mix of all that



System implementation examples:
TC and TM links



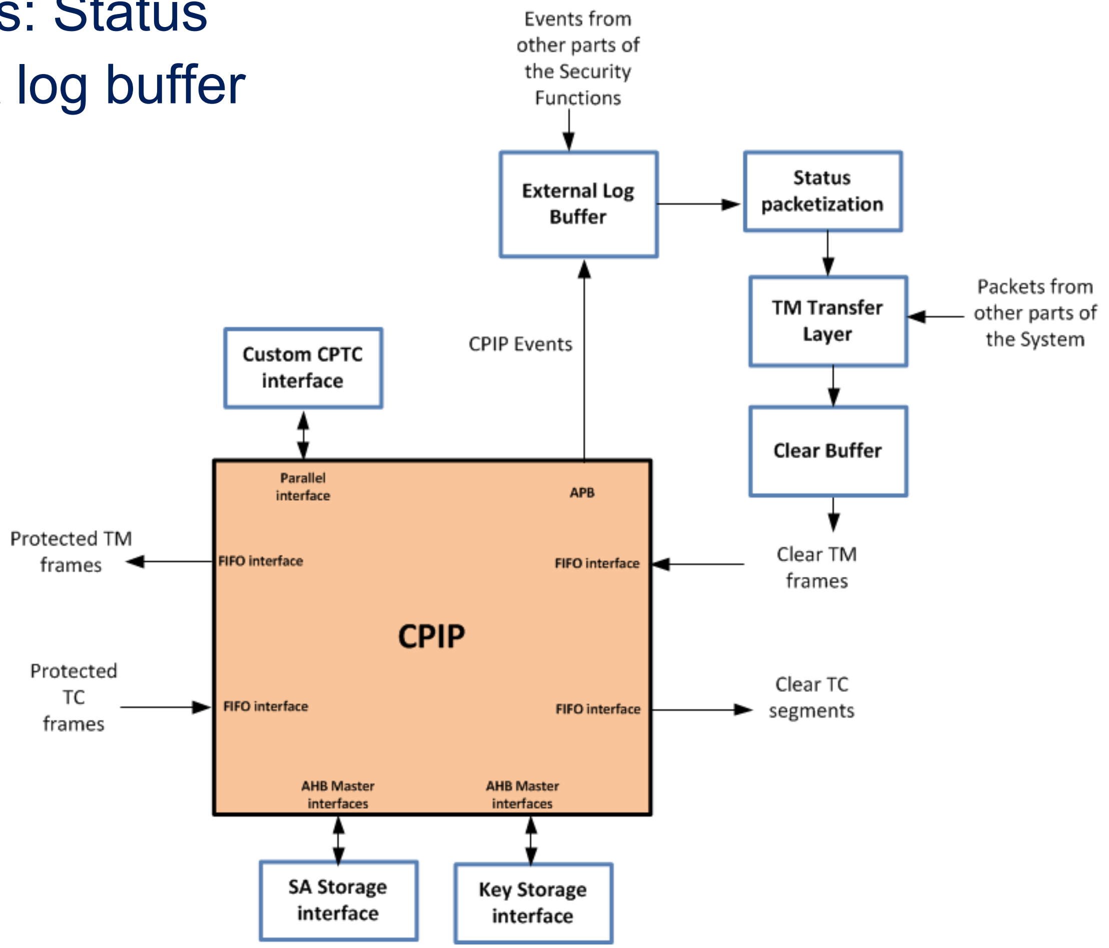
System implementation examples: Status Management with external Event log buffer

- ❑ Hypothesis: the system implements other security functions than CPIP (TMI cyphering for example)

- ❑ External Log Buffer and Status packetization may be manage either by Hardware or by SoftWare

- ❑ Packetization may be made before External log buffer, on each status

- ❑ TM Transfer Layer may be duplicated: one part for managing secured packets, the other part for managing non secured packets
- ⇒ Necessary in some systems (Interface with existing OBCs for example)
- ⇒ Lead to difficulties (Master Channel Frame Count, …)



Security assurance

- **Development has been made in a ESA Confidential environment**
  - Dedicated secured room
  - Dedicated servers

- **Red/Black data functional separation** for the RTL model

- **Documentation for a future EAL4+ Common Criteria Security Evaluation of a design using CPIP has been prepared**
  - Security Target is not in the scope of this documentation because it is specific to each application using CPIP
  - All other Common Criteria documentation which relates to ADV (development) and ATE (test) Common Criteria classes has been prepared
  - Once User (Company/project team implementing CPIP in its product) has his Security Target in hand (written by the user himself or by the end user for instance the final customer), the user is then able to prepare the Security Evaluation documentation by using CPIP documentation.

  - The CPIP has not been evaluated in the frame of this project but a pre-evaluation has been performed during the development.

AIRBUS

Possible future work

CPIP

❑ **Implementation in a Unit**

⇒ TRL improvement

⇒ Feed back on CPIP functionalities and interfaces

⇒ Feed back on CPIP documentation

⇒ Could limit the evaluation to this hardware product and propose a ESA confidential product

❑ **Security Evaluation**

⇒ Security Assurance improvement

How to get CPIP ?

- ❑ **CPIP is ESA Confidential**
  - ❑ National Security Agencies shall be involved
  - ❑ User has to manage CPIP as an ESA Confidential item
- ❑ **Providers**
  - ❑ ESA
- ❑ **Support**
  - ❑ Helion for AES GCM/CMAC and **only if this IP is acquired via Helion**
  - ❑ Airbus for other parts
- ❑ Fees
  - ❑ Helion: 45 K€ about for one multi projects soft license of AES Tiny+ GCM/CMAC IP
    - ❑ May be get via Helion **with support**
    - ❑ May be get via CPIP providers without support
      - ❑ **Fees lowering**
      - ❑ Simpler process
      - ❑ Remove of potential confusion
  - ❑ ESA: 5 K€
  - ❑ For Airbus Support if required

Thank you