Hybrid modular hardware-software solution for securing ground-satellites communication

Enrico Petraglio, REDS institute, HEIG-VD

Security for Space Systems (3S) - 6.11.2025

Part of the project REACCESS

CYSEC

HEIG-VD

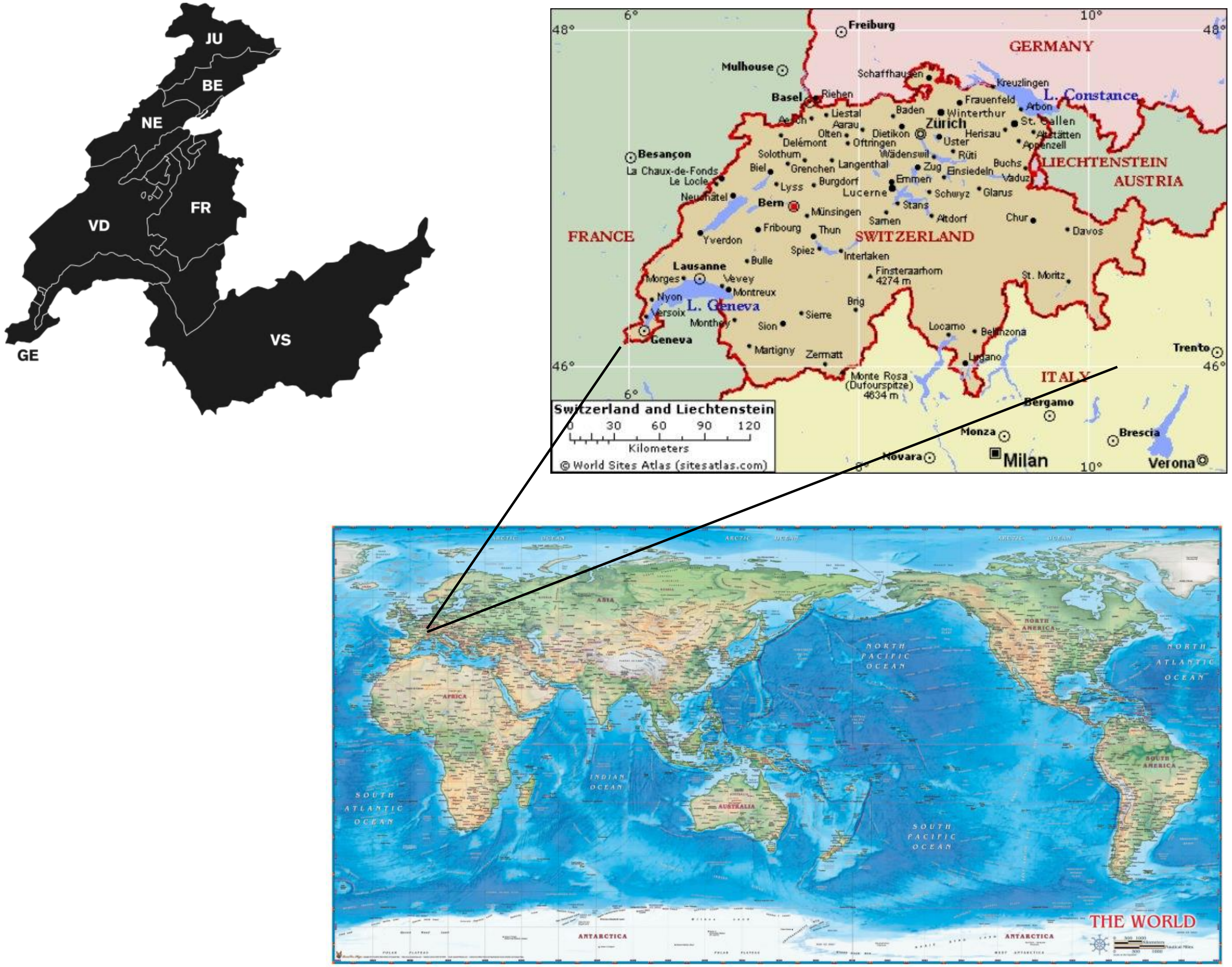
- Prof. Alexandre Duc (cryptography)
- Prof. Yann Thoma (embedded systems + FPGA)

2.5 years

Hes·so

70 bachelor and master programs
>20’000 students
6 faculties

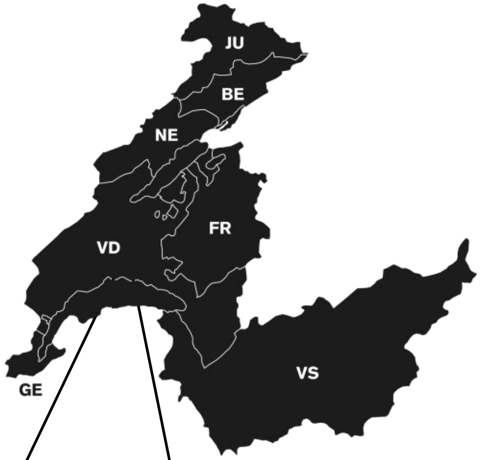
- Design and Visual arts
- Business and Services
- Engineering and Architecture
- Music and Performing Arts
- Health Sciences
- Social Work

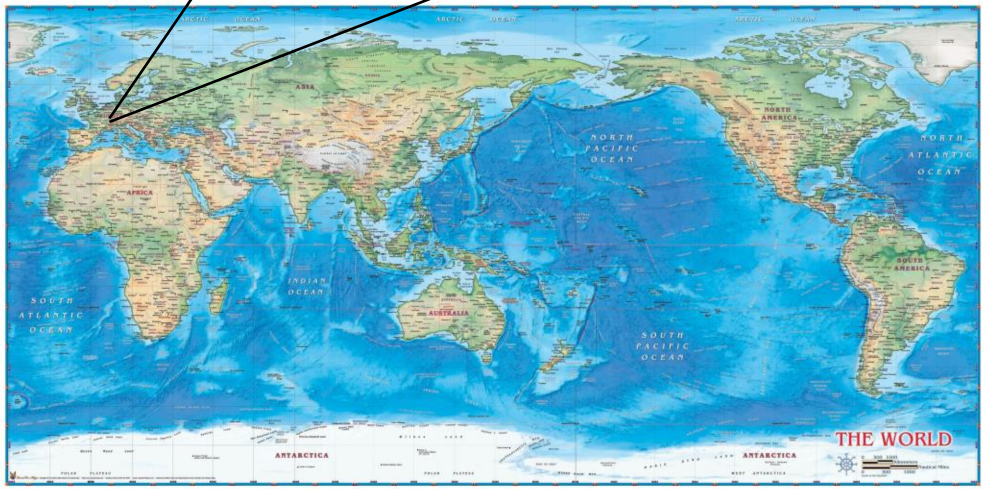


Hes·so

70 bachelor and master programs
>20’000 students
6 faculties

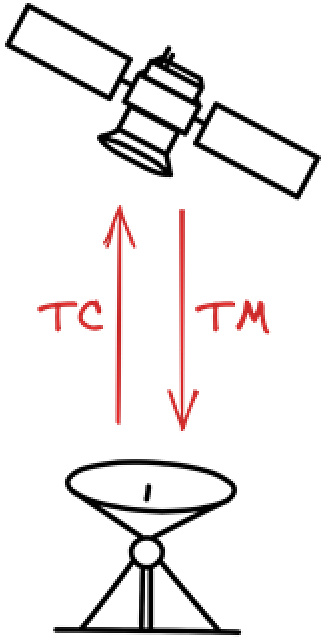
- Design and Visual arts
- Business and Services
- Engineering and Architecture
- Music and Performing Arts
- Health Sciences
- Social Work





REACCESS Context

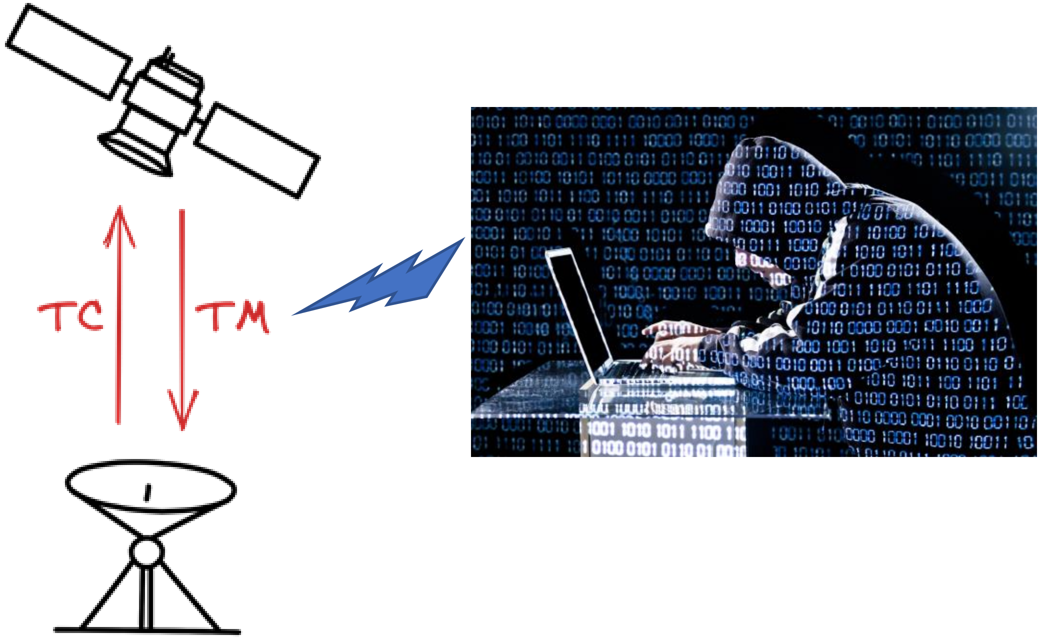
- → Telemetry and telecommand data
  - Monitor and control the spacecraft and its payload



REACCESS Context

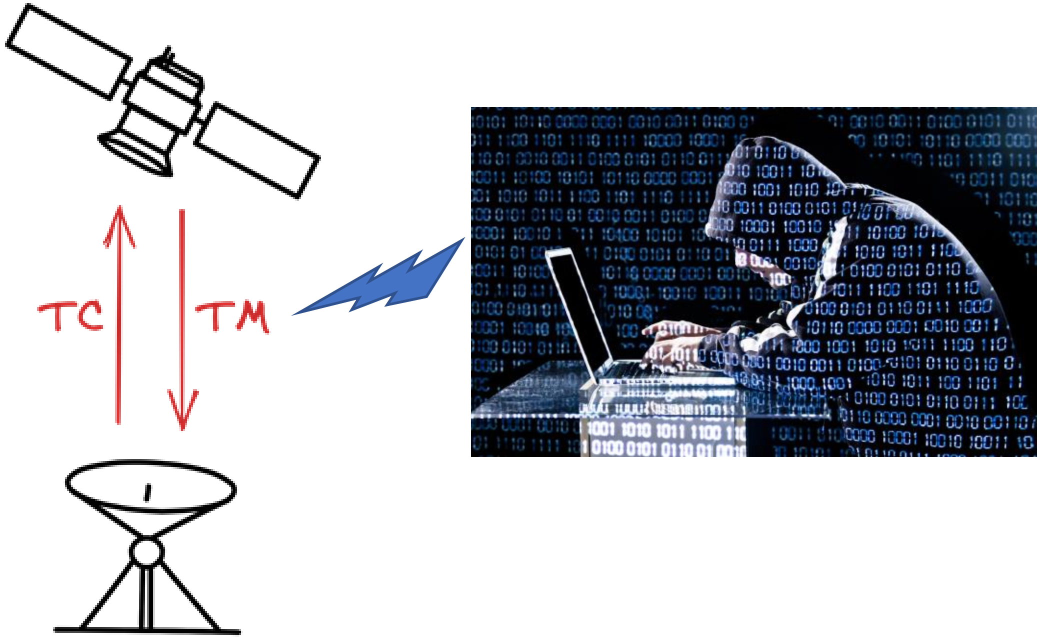
→ Telemetry and telecommand data

- Monitor and control the spacecraft and its payload



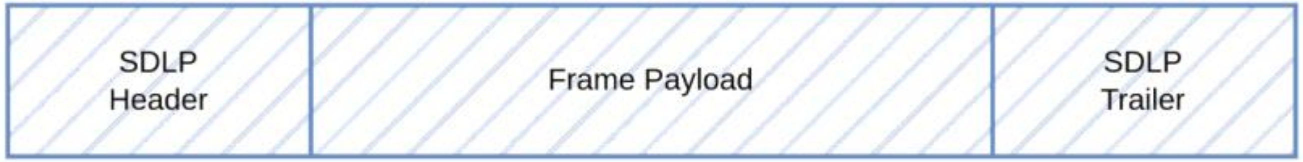
REACCESS Context

- → Telemetry and telecommand data
  - Monitor and control the spacecraft and its payload
- → Need to be secured
  - Else: access to data, loss of satellite control, …



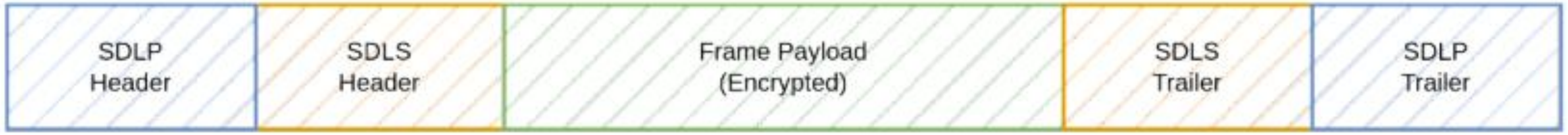
CCSDS →SDLS

- → Currently: CCSDS Space Data Link Protocol (SDLP)



SDLP Header | Frame Payload | SDLP Trailer

- → Future: Space Data Link Security Protocol (SDLS)



SDLP Header | SDLS Header | Frame Payload (Encrypted) | SDLS Trailer | SDLP Trailer

Project main goals

→ SDLS library implementation for ground and space

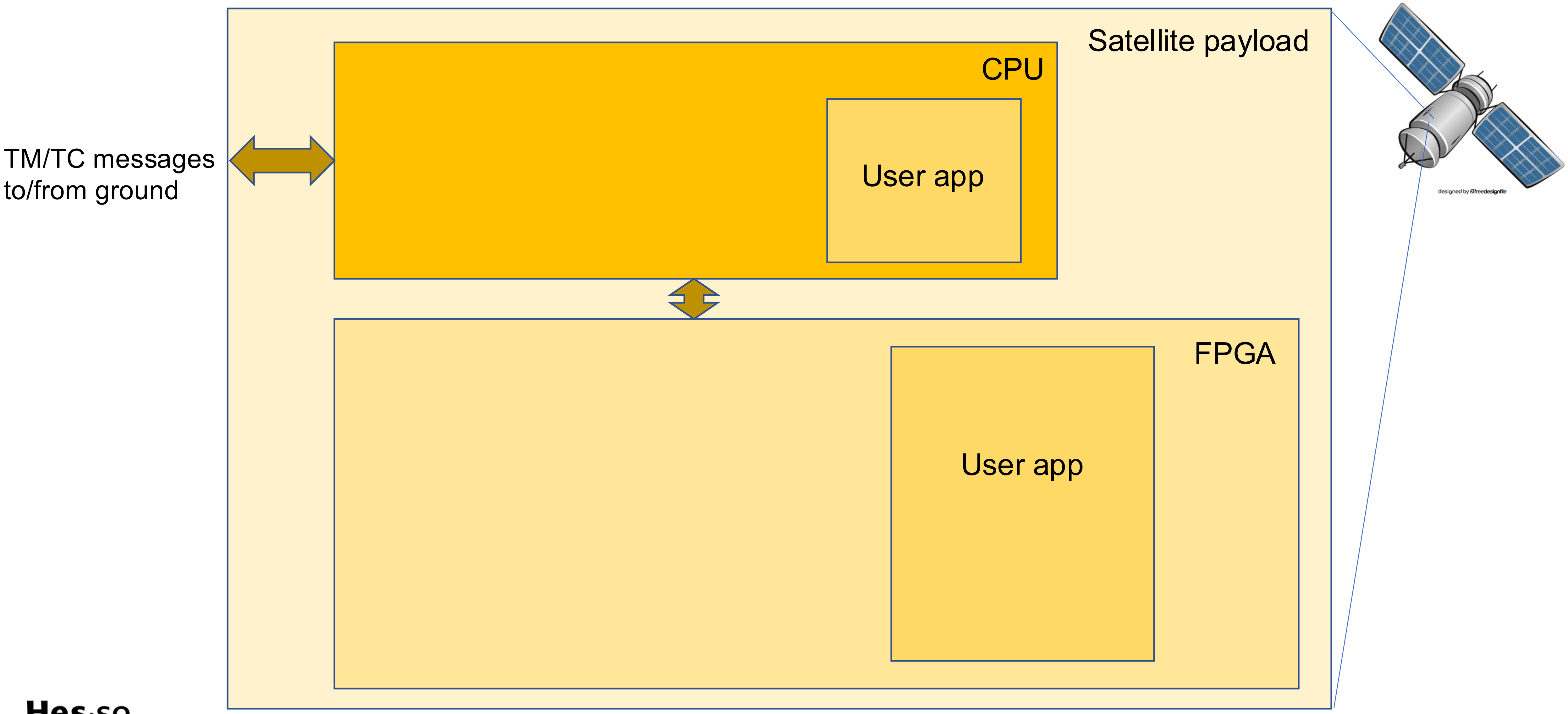
→ Modular architecture for heterogeneous hardware (CPU-FPGA or FPGA-SoC)

→ Asymmetric key cryptosystem

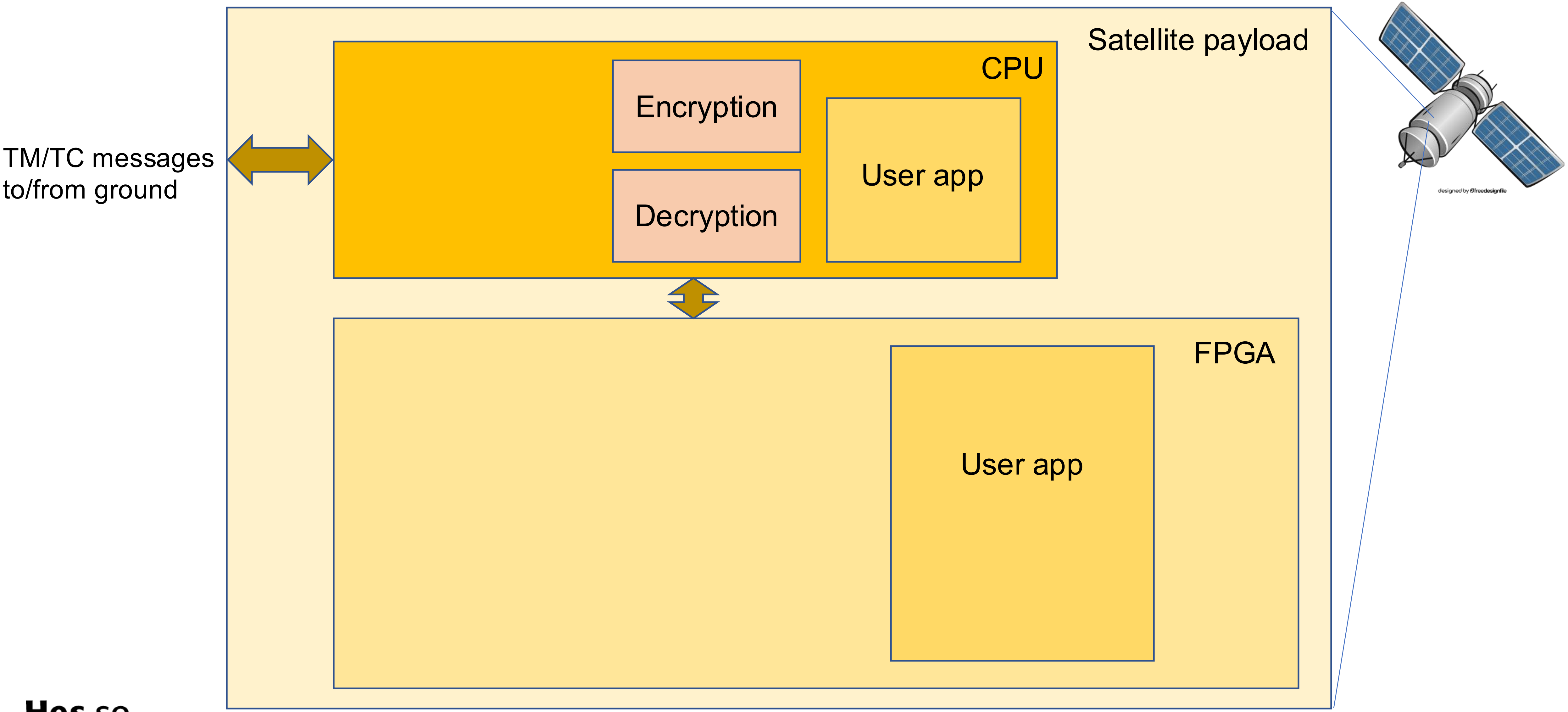
→ Over the Air Reconfiguration

What are we proposing?

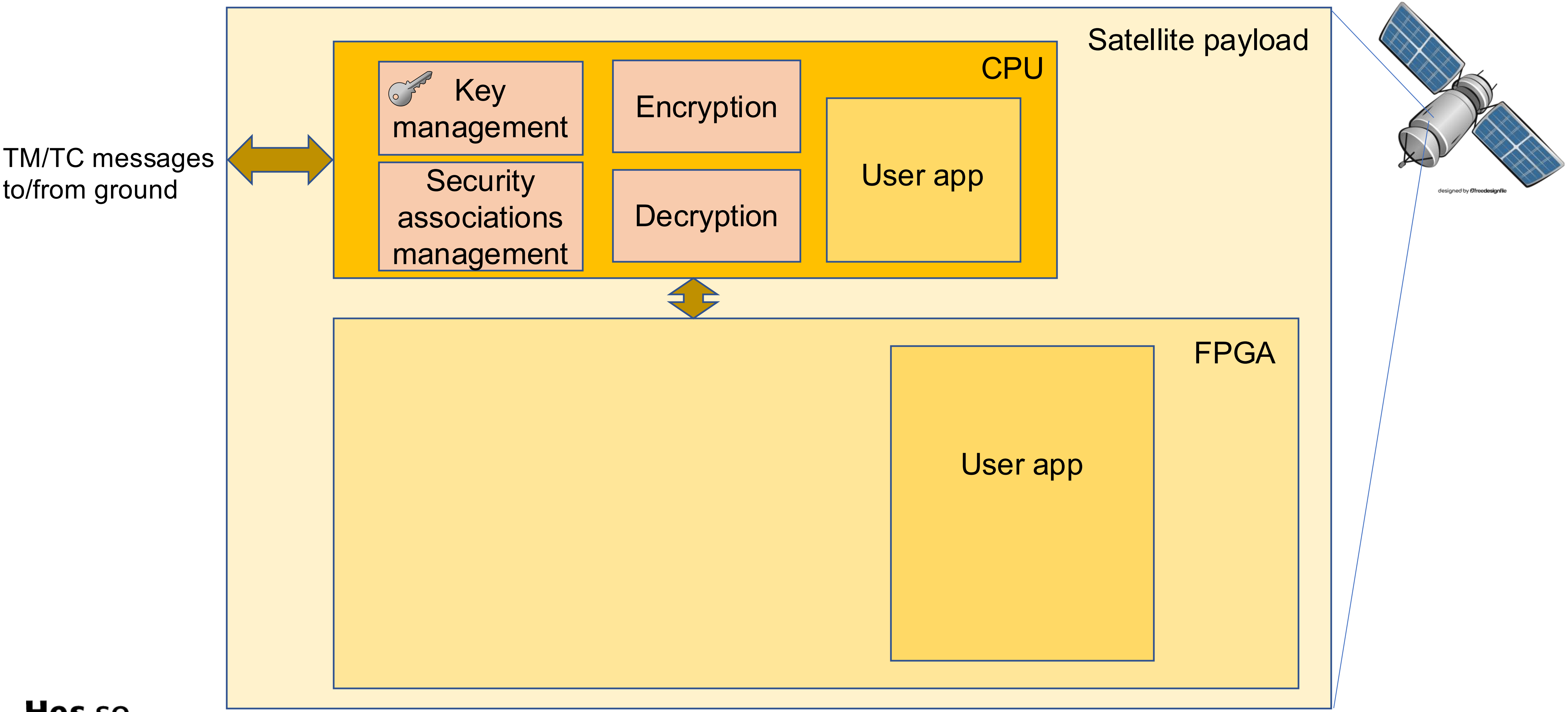
Modular architecture



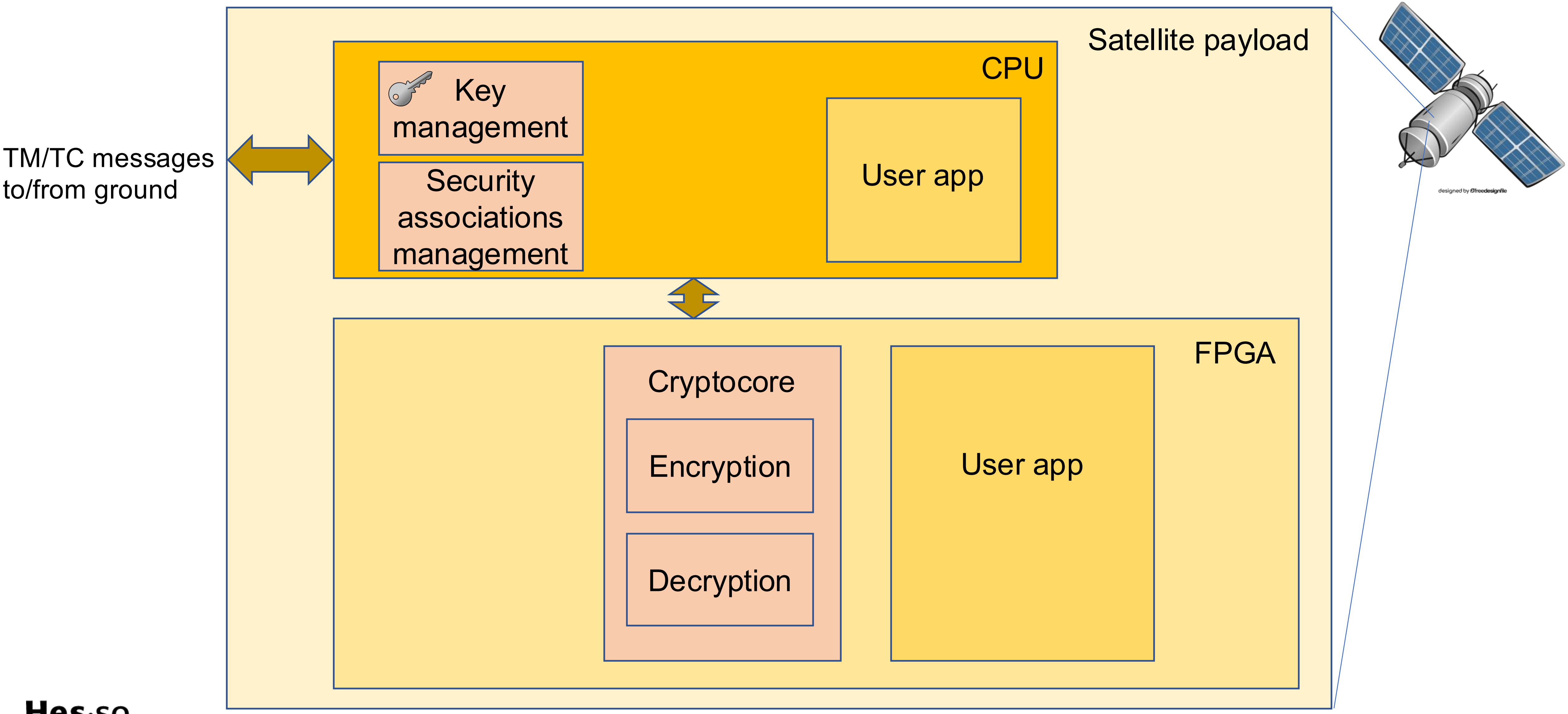
Modular architecture



Modular architecture


Satellite payload
CPU
Key management
Encryption
Security associations management
Decryption
User app
FPGA
User app
TM/TC messages to/from ground
designed by freedesignfile

Modular architecture



TM/TC messages to/from ground

Satellite payload

CPU

Key management

Security associations management

User app

FPGA

Cryptocore

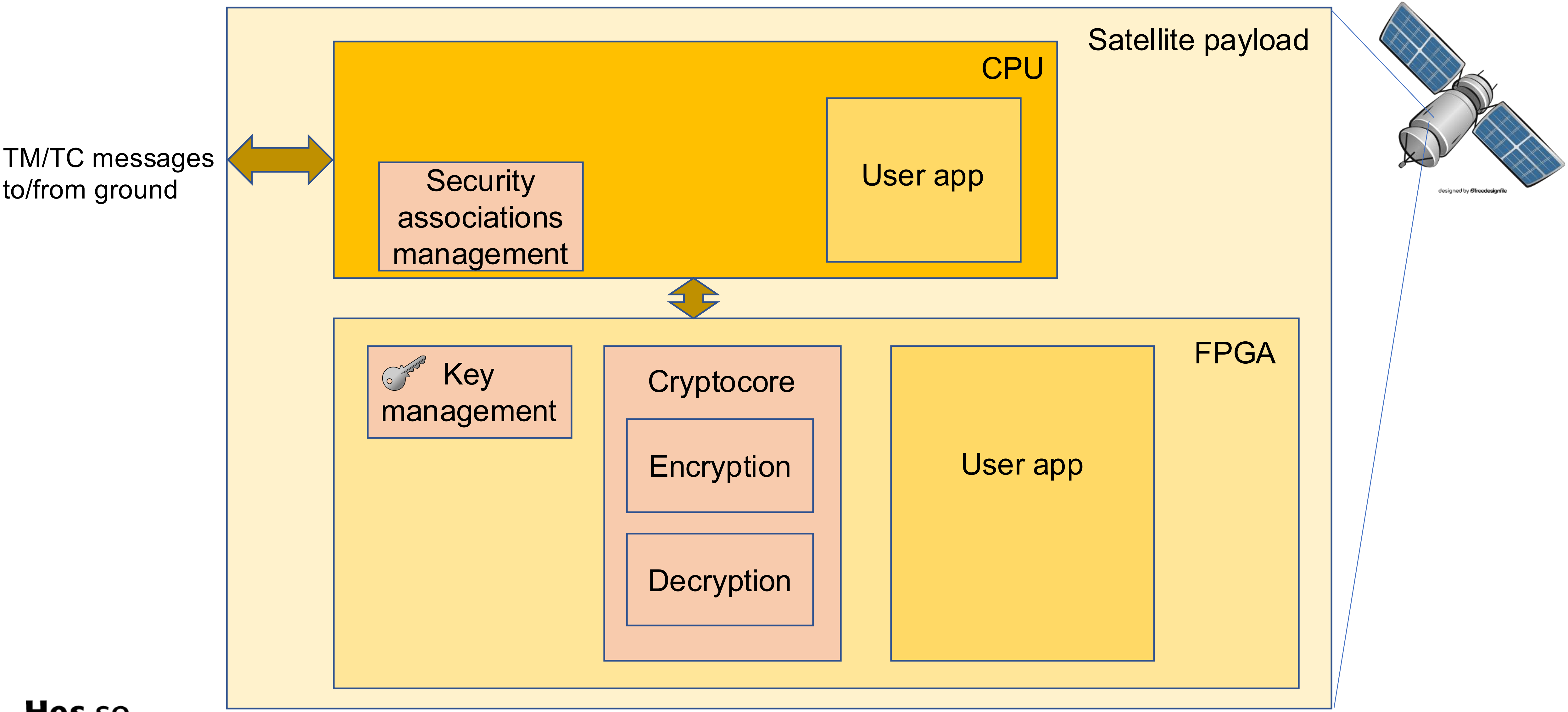
Encryption

Decryption

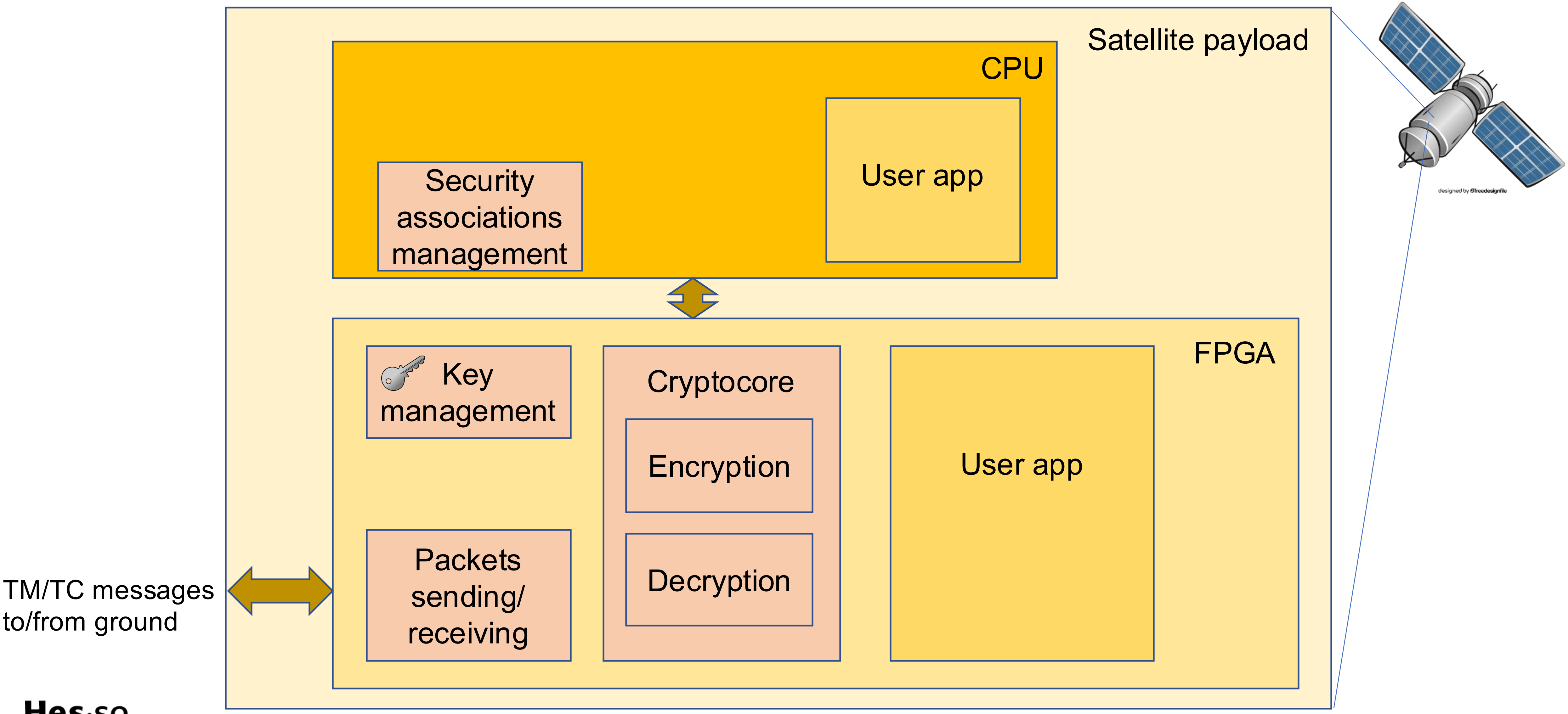
User app

designed by freedesignfile

Modular architecture



Modular architecture



Satellite payload

CPU

Security associations management

User app

FPGA

Key management

Cryptocore

Encryption

Decryption

User app

Packets sending/ receiving

TM/TC messages to/from ground

designed by freedesignfile

Modularity RECAP

→ Minimal Version (cryptographic co-processor)

- offloading computationally intensive encryption and decryption

→ Medium Version (cryptographic co-processor + Key management)

- offloading computationally intensive encryption and decryption
- Keys safe storage against unauthorized access
- Integrated Keys sanity check (with error recovering)

→ Full Version (cryptographic co-processor + Key management + SDLS)

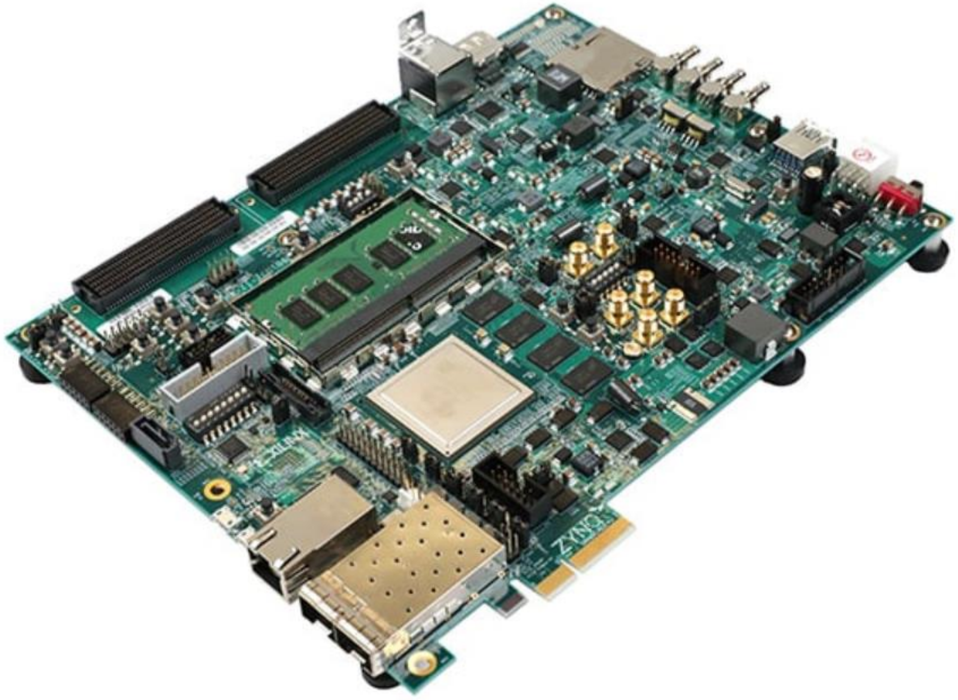
- offloading computationally intensive encryption and decryption
- Keys safe storage against unauthorized access
- Integrated Keys sanity check (with error recovering)
- SDLS packets formatting by the FPGA
- Enhanced data throughput

Implementation on a Zynq SoC

→ Board: SoC AMD Zynq™ 7000 ZC706

→ FPGA: XC7Z045

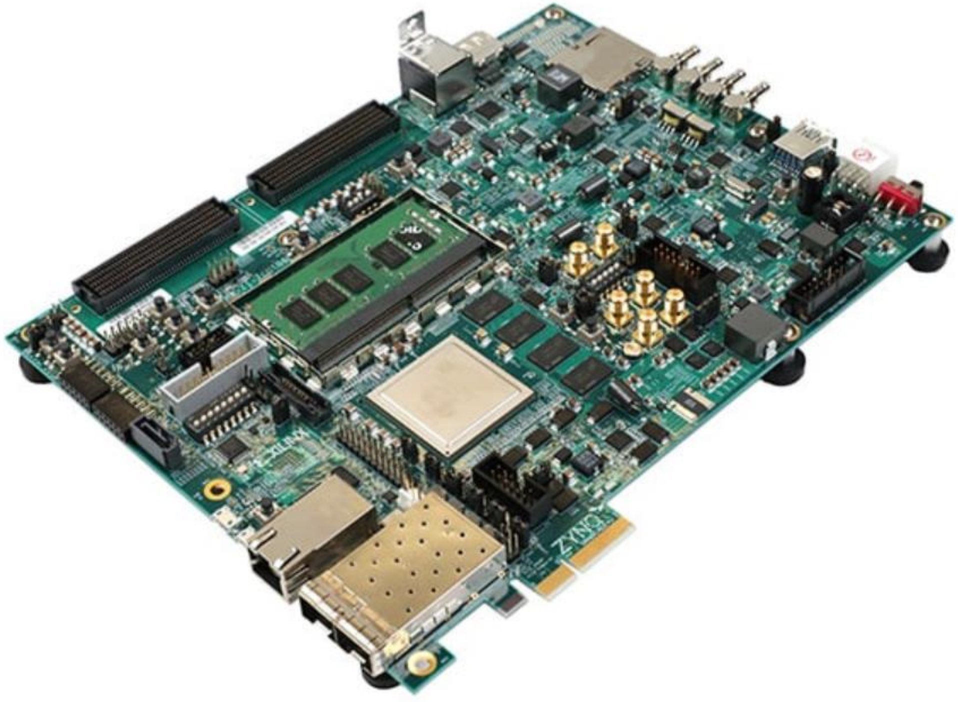
- Logic slices : 350'000
- 6-input LUTs : 218'600
- Flip-Flops : 437'200
- Block RAM : 2.4 MB



Implementation on a Zynq SoC

→ Board: SoC AMD Zynq™ 7000 ZC706

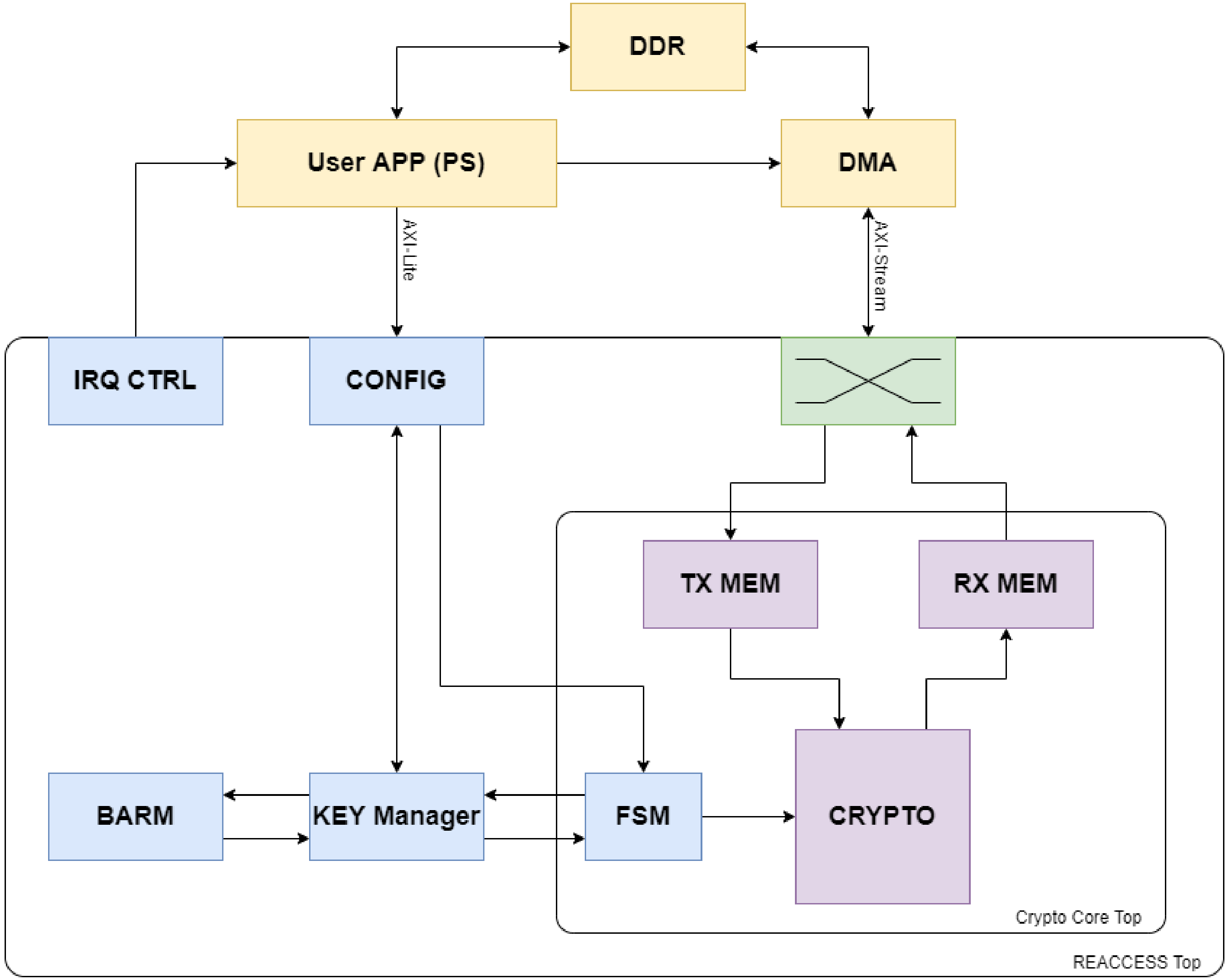
→ FPGA: XC7Z045
- Logic slices : 350'000
- 6-input LUTs : 218'600
- Flip-Flops : 437'200
- Block RAM : 2.4 MB



→ Two crypto engines:
- AES GCM (256 bits)
  - Core from https://github.com/BLu85/AES-GCM-128-192-256-bits
- ASCON (128 bits)
  - Core from https://github.com/ascon/ascon-hardware

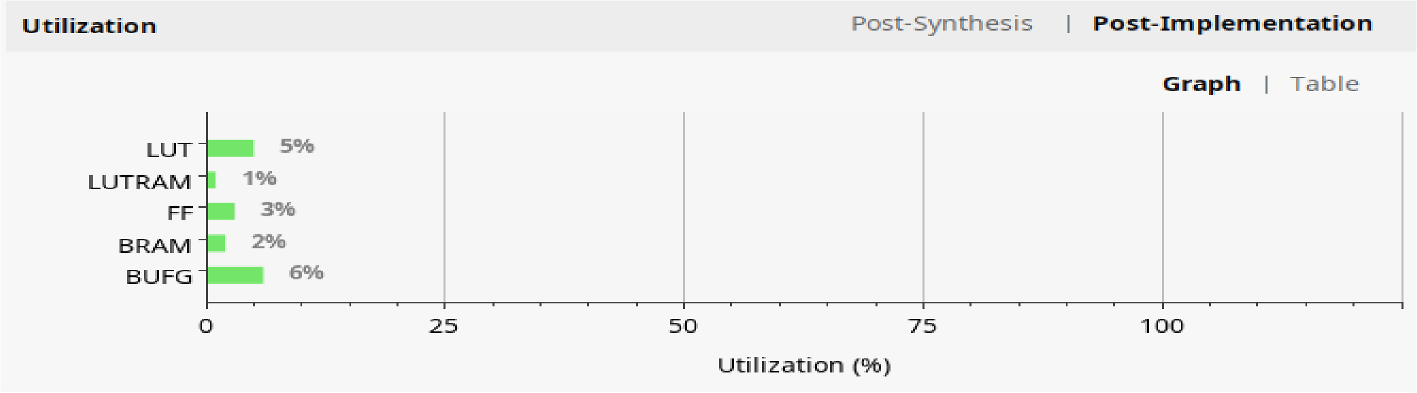
Implemented Design

Hardware crypto engine

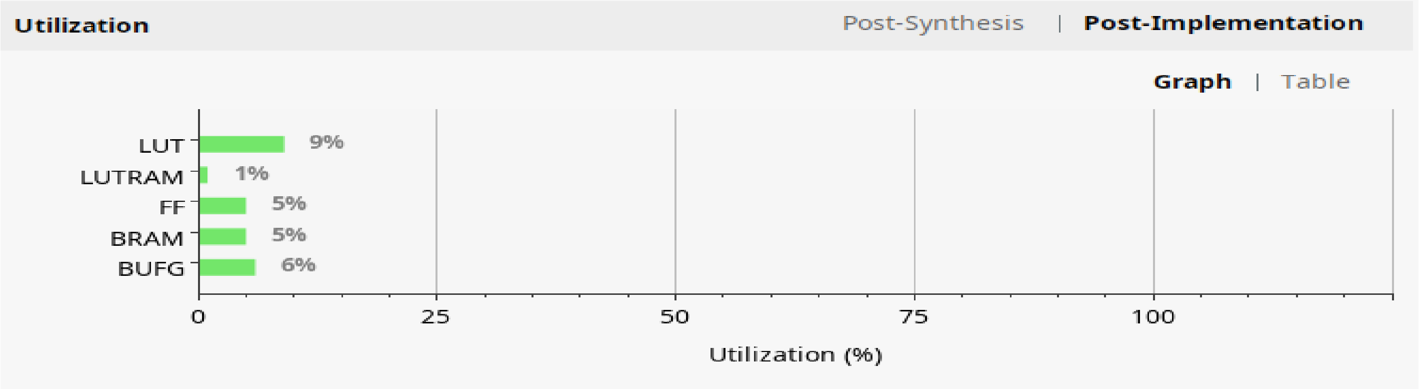


Resources Utilization (impl)

ASCON-AEAD128



AESGSM256



Encryption speed @100MHz

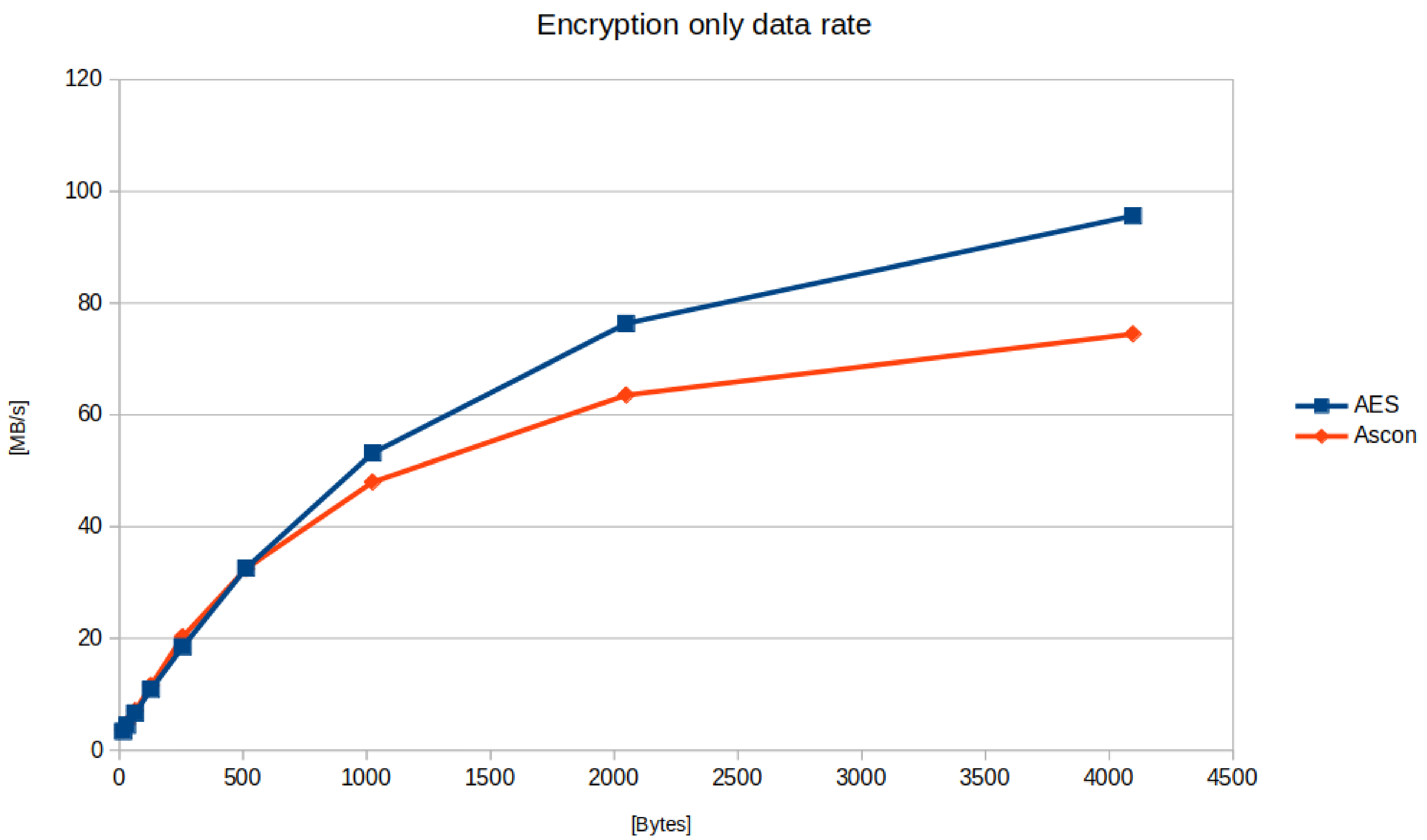
Encryption throughput [MB/s]

	16 B	32 B	64 B	128 B	256 B	512 B	1kB	2kB	4kB
Ascon	3.63	4.75	7.05	11.61	20.28	32.50	47.97	63.55	74.47
AES	3.35	4.45	6.62	10.91	18.48	32.58	53.17	76.36	95.62

Packet size is composed of 32 bits of AAD + 16 to 4kB of DATA

32 bits AXI stream bus

Encryption speed @100MHz



Decryption speed @100MHz

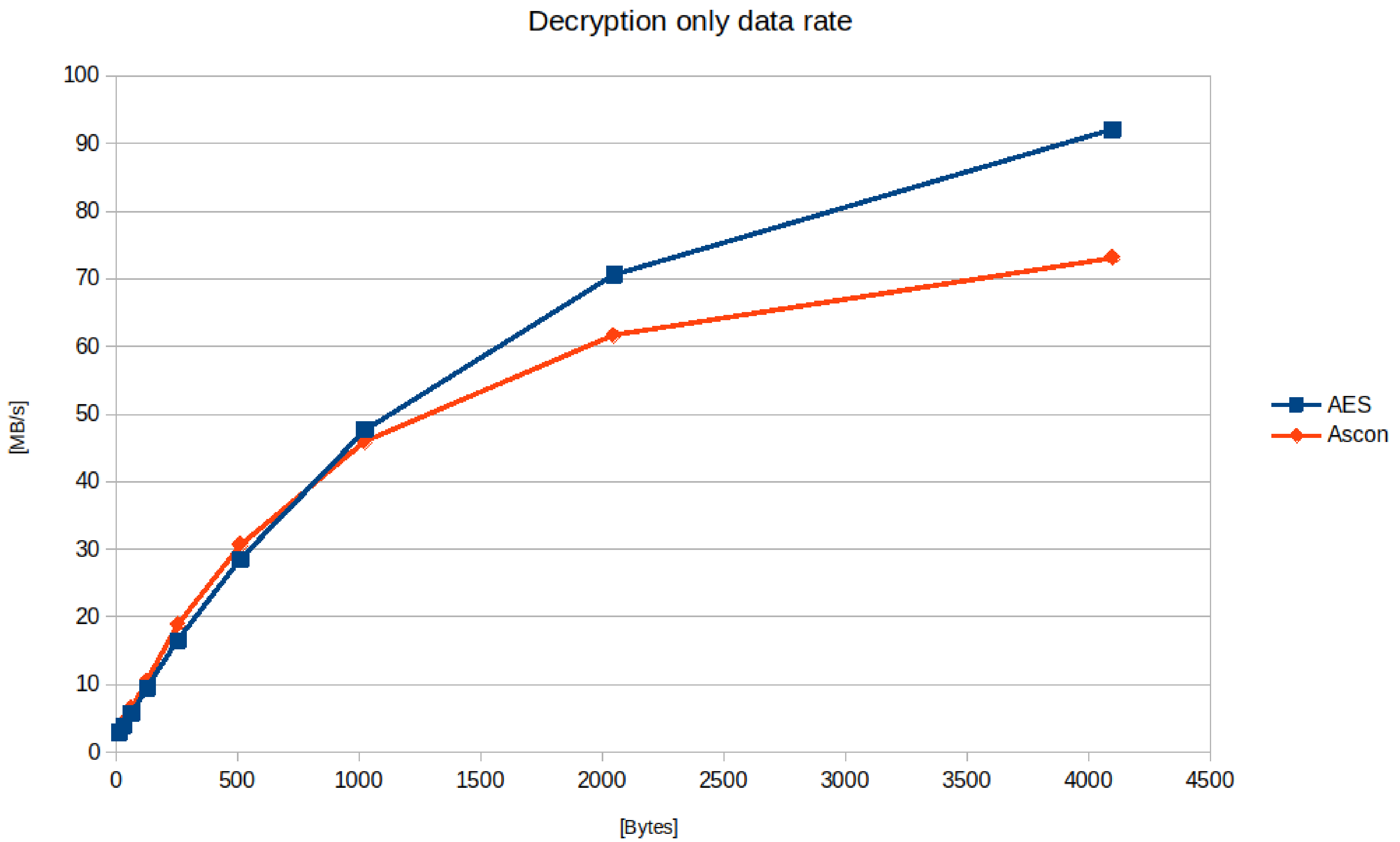
Encryption throughput [MB/s]

	16 B	32 B	64 B	128 B	256 B	512 B	1kB	2kB	4kB
Ascon	3.35	4.43	6.51	10.55	18.9	30.65	45.95	61.6	73.16
AES	2.96	3.89	5.69	9.47	16.51	28.52	47.69	70.56	92.04

Packet size is composed of 32 bits of AAD + 16 to 4kB of DATA

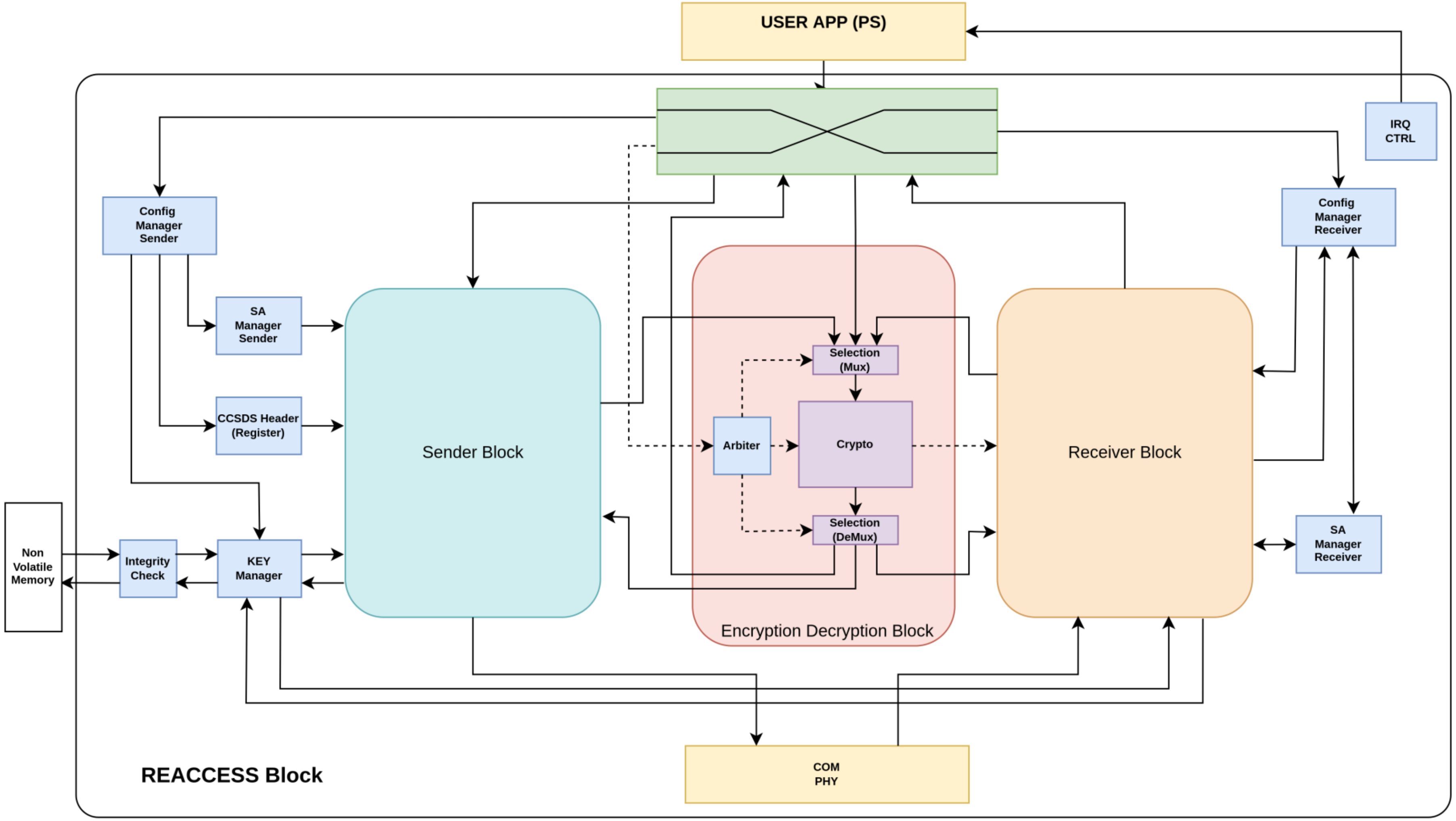
32 bits AXI stream bus

Decryption speed @100MHz



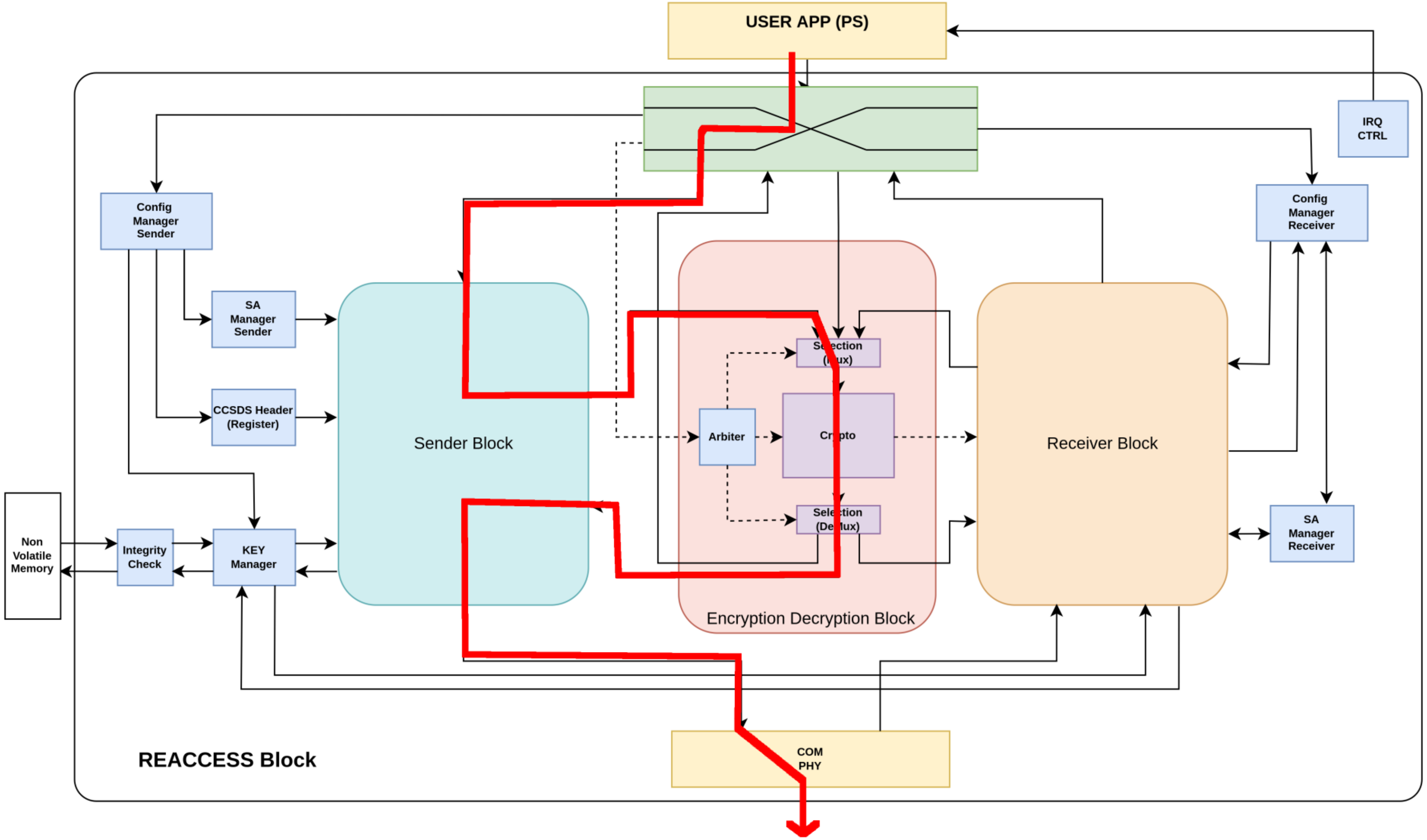
With SDLS packets management

Crypto + SDLS Version



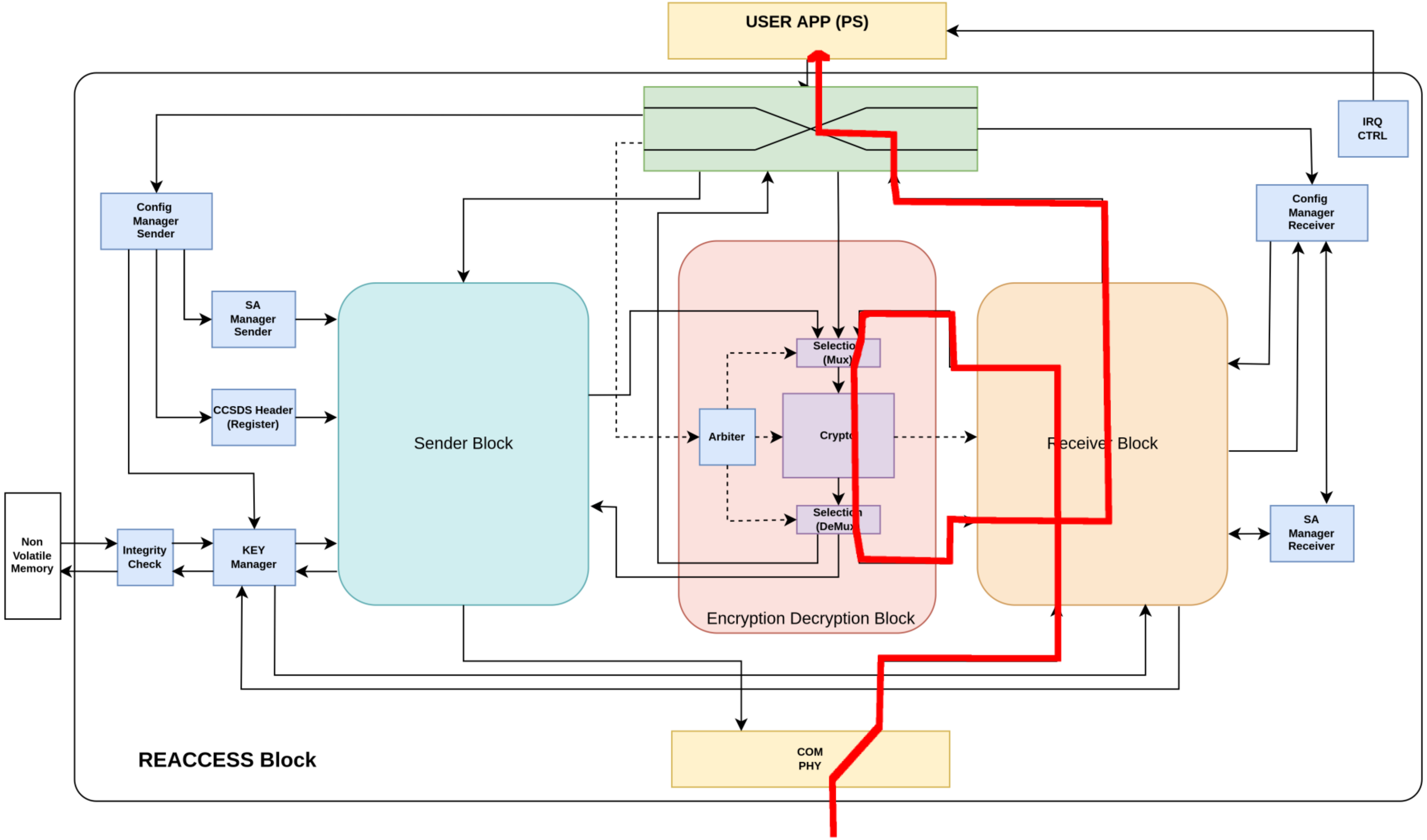
With SDLS packets management

Crypto + SDLS Version



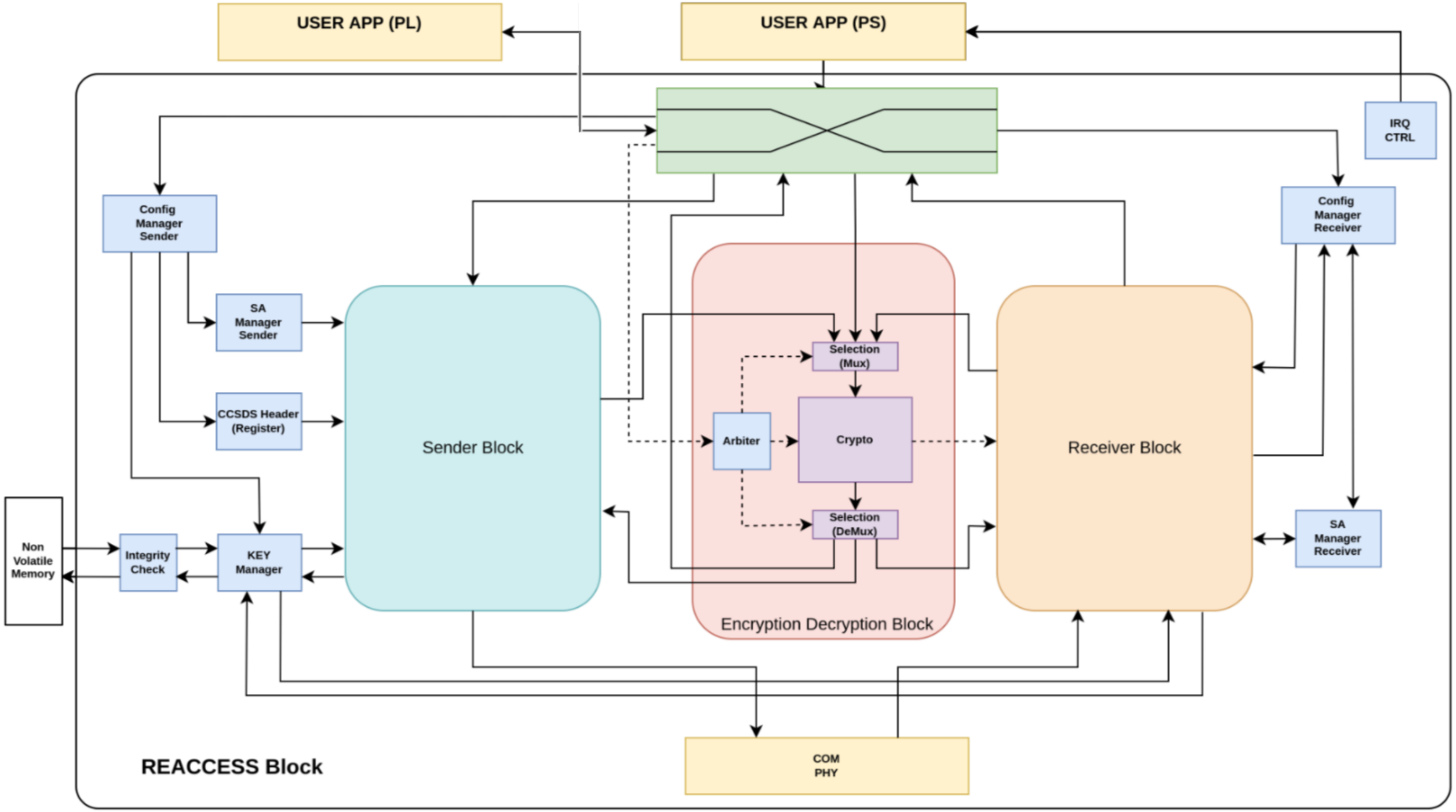
With SDLS packets management

Crypto + SDLS Version



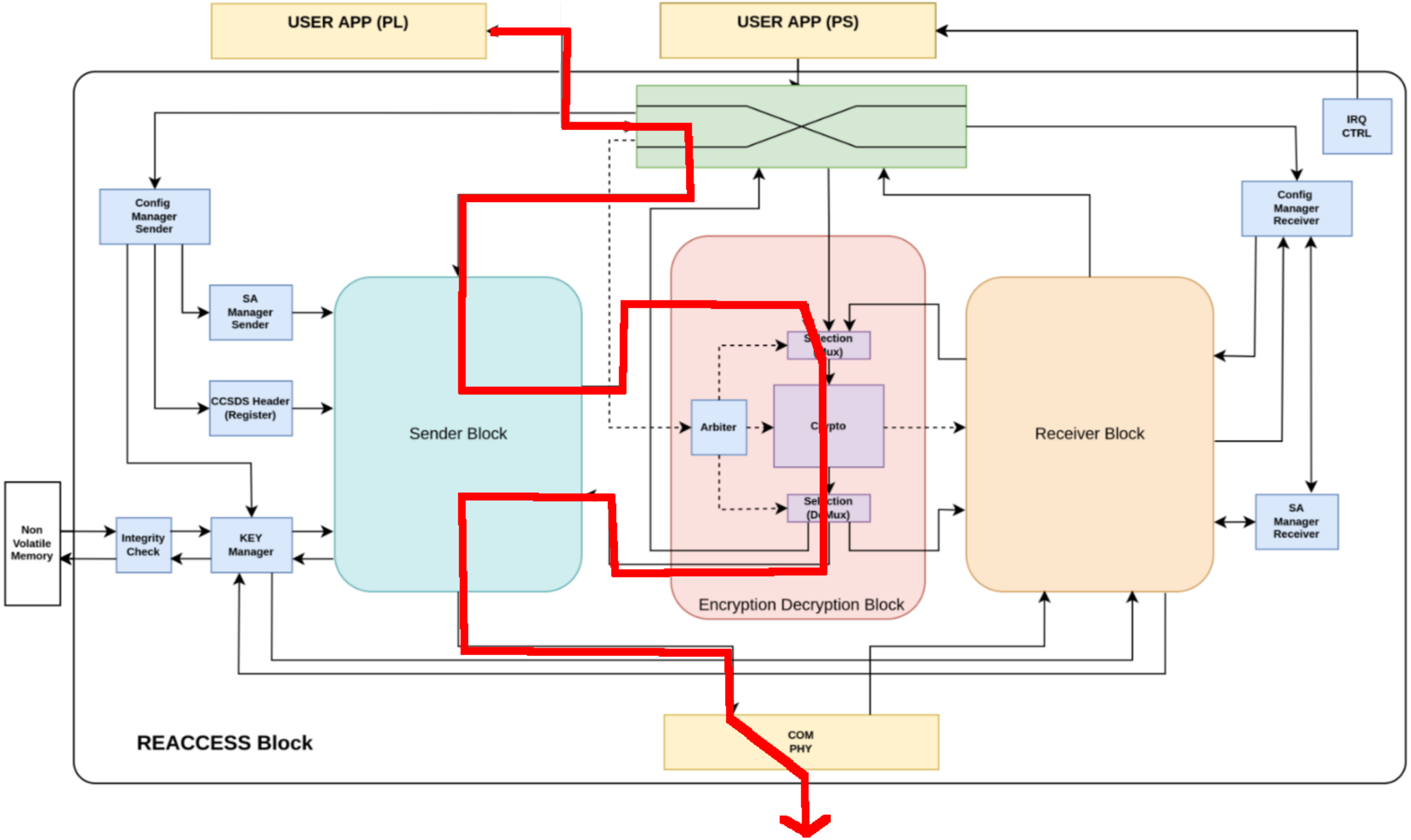
With SDLS packets management

Crypto + SDLS Version



With SDLS packets management

Crypto + SDLS Version



FPGA with SDLS

Version	LUT	FF	BRAM
ASCON + SDLS	10108	9552	10
AES + SDLS	18725	13371	20

FPGA with SDLS

Version	LUT	FF	BRAM
ASCON + SDLS	10108	9552	10
AES + SDLS	18725	13371	20

Zynq Family			
Z-7010	17'600	35'200	60
Z-7015	46'200	92'400	95
Z-7020	53'200	106'400	140
Z-7030	78'600	157'200	265
Z-7035	171'900	343'800	500
Z-7045	218'600	437'200	900
Z-7100	277'400	554'800	2020

ASCON

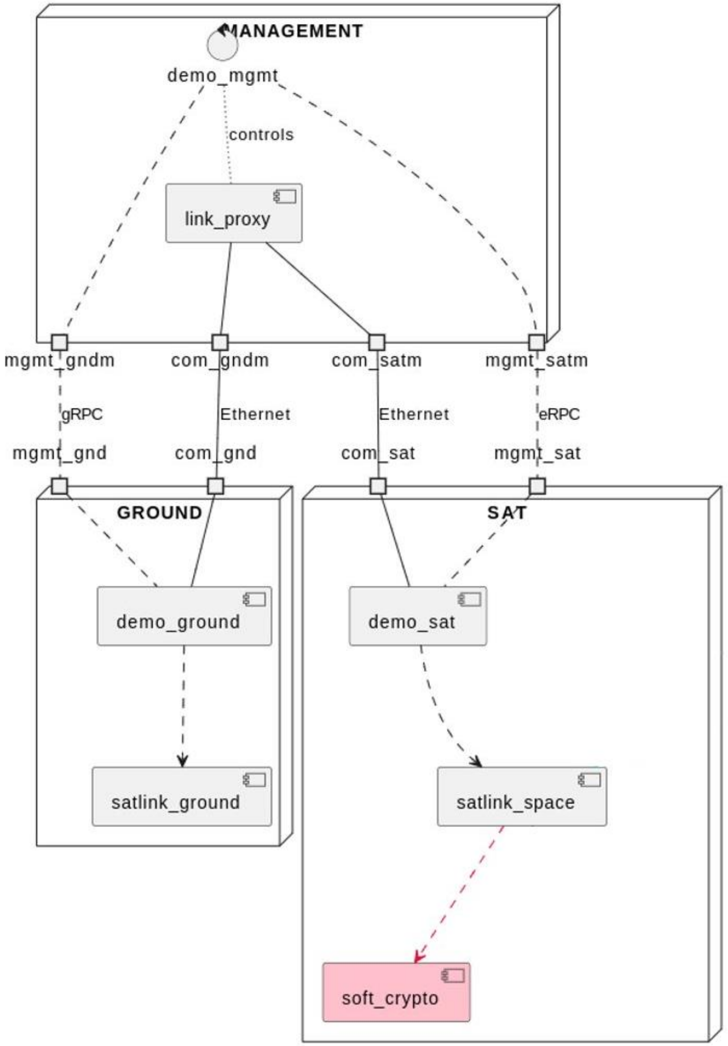
AES

Zybo Z7-10

Test framework

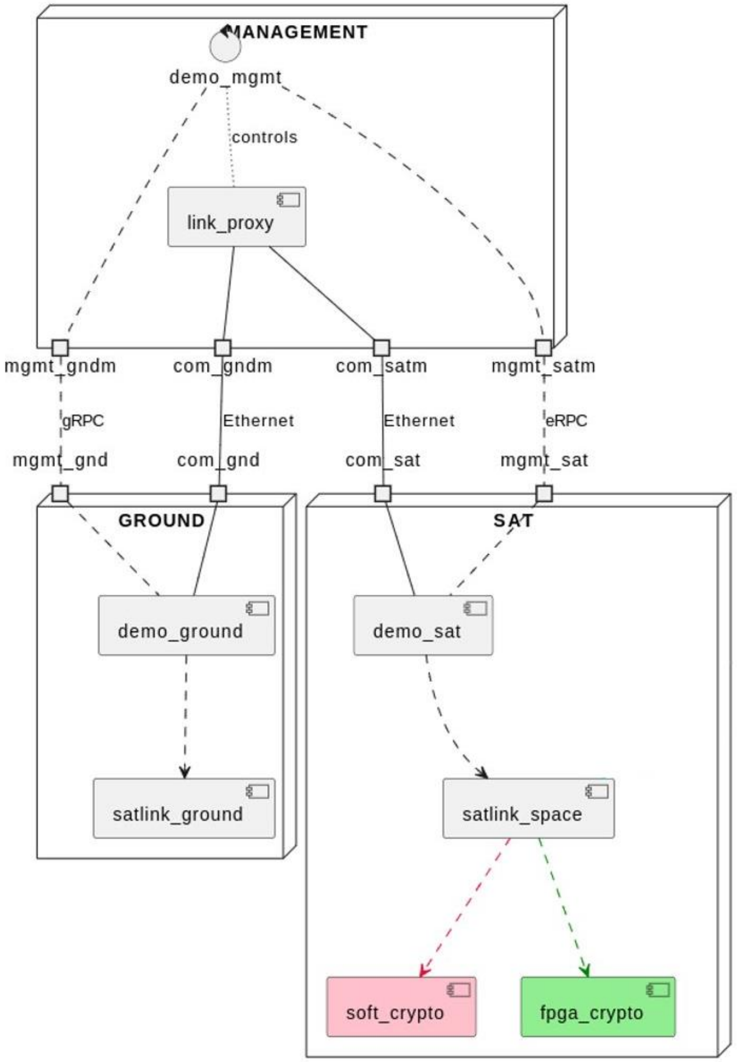
Verification framework

Deployment diagram of an end-2-end demonstrator

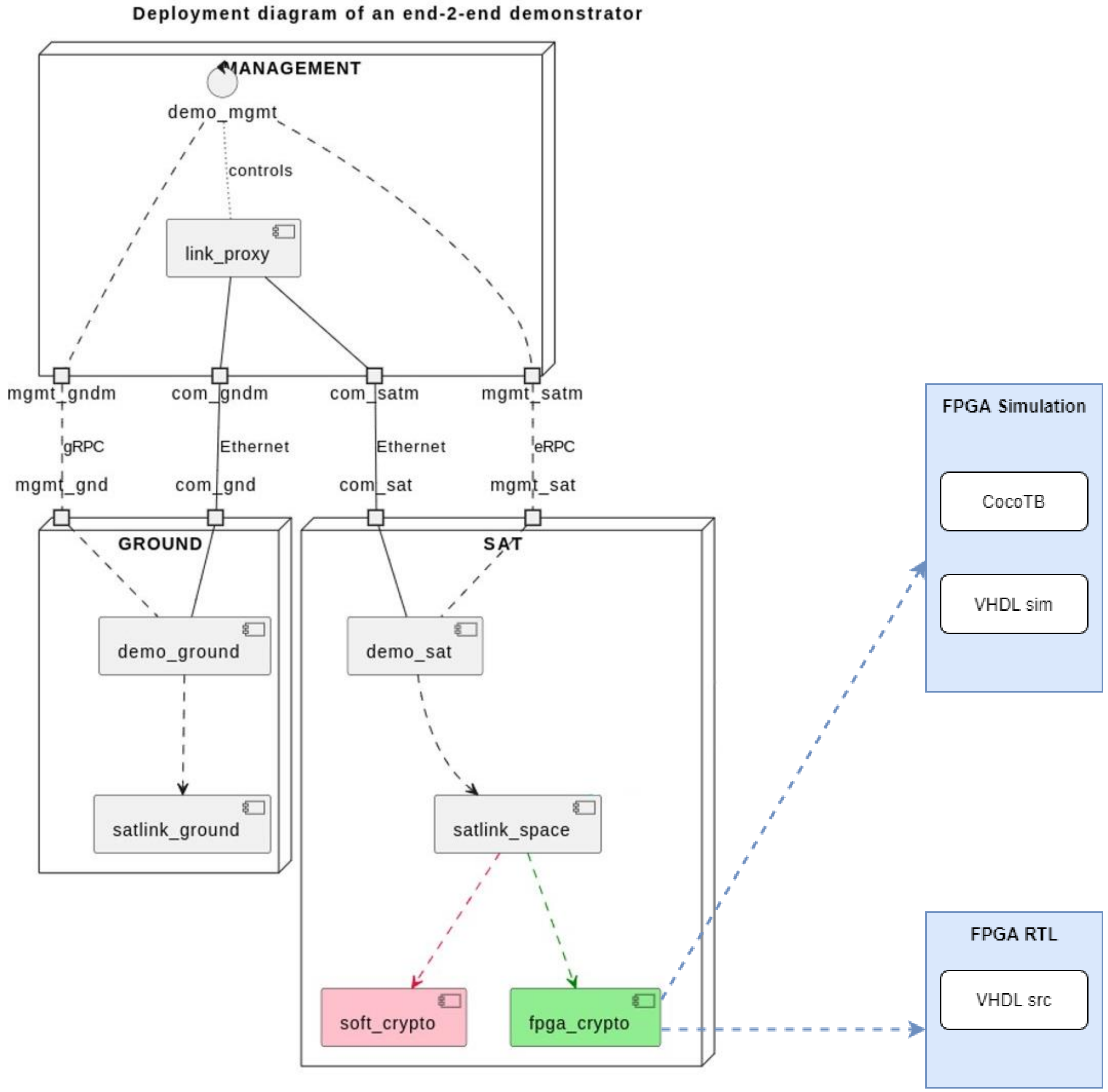


Verification framework

Deployment diagram of an end-2-end demonstrator



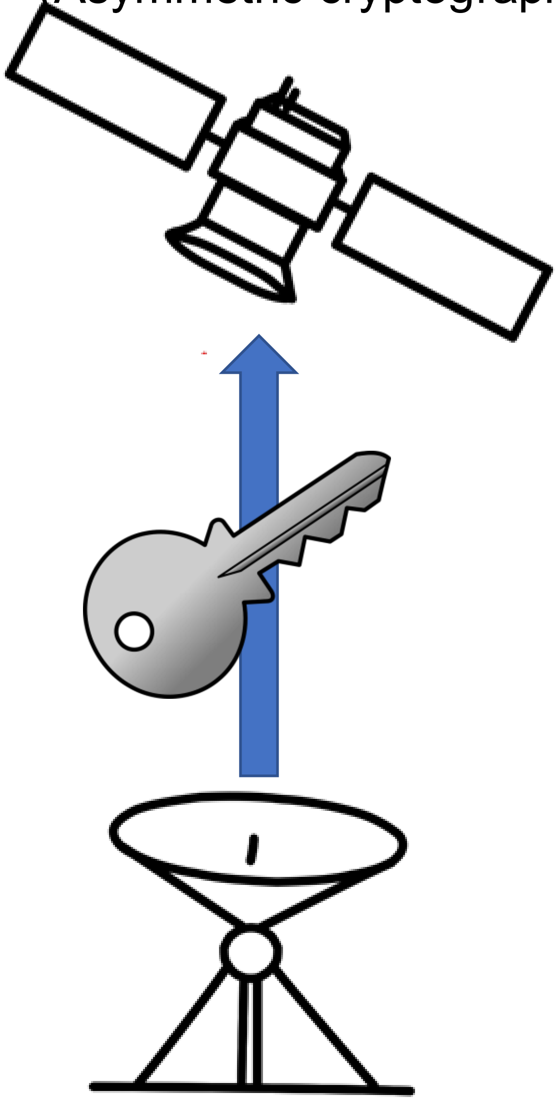
Verification framework



Next steps

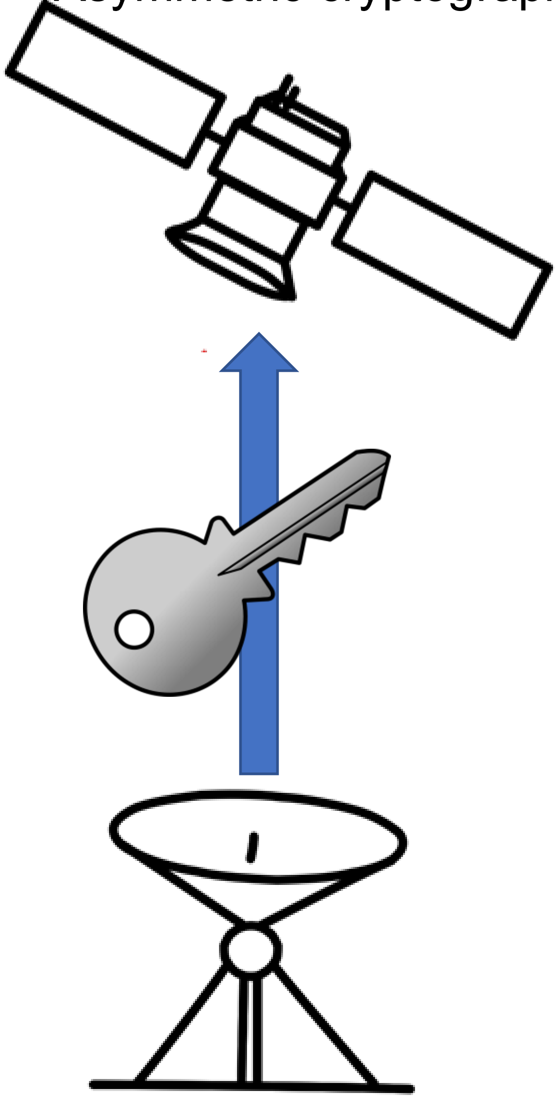
Next steps

Over the air rekeying
(Asymmetric cryptography)

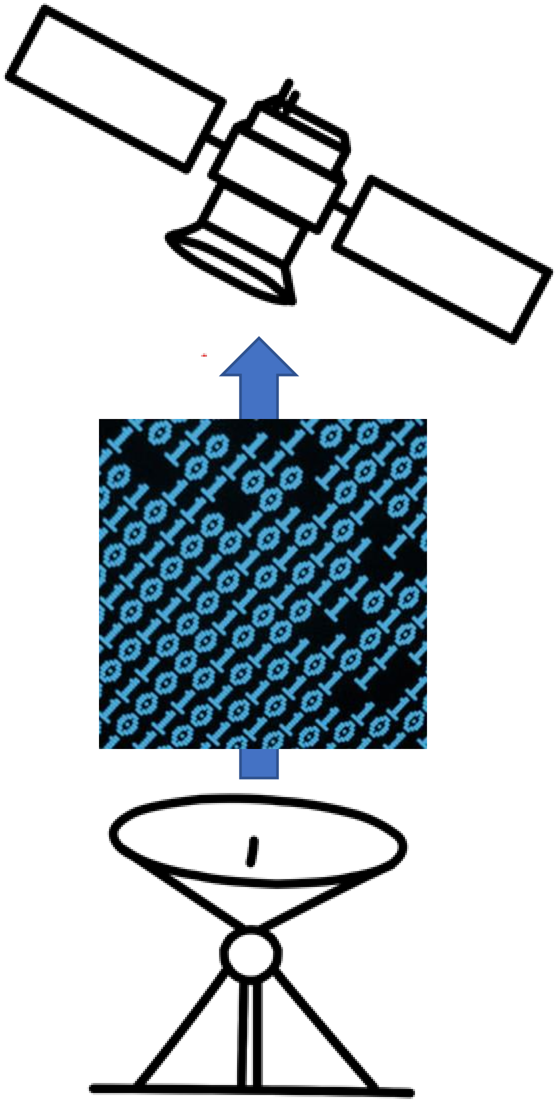


Next steps

Over the air rekeying
(Asymmetric cryptography)



Over the air FPGA reconfiguration



A closing remarks

→ The development of the presented design is proceeding smoothly, and we are pleased with the results achieved so far.

→ The FPGA implementation has already attracted interest among some CYSEC partners.

→ Members of CYSEC and the security team are also present in the room to continue the discussion after the presentation.

Many thanks to the team!

Contact: enrico.petraglio@heig-vd.ch

? ? ? ? ? ? ?

HEIG VD

HAUTE ÉCOLE
D'INGÉNIERIE
ET DE GESTION
DU CANTON
DE VAUD

Hes·so

Contact: enrico.petraglio@heig-vd.ch