THALES

INTEGRATION OF IP SERVICES OVER HIGH DATA RATE HF CAPABILITIES

Sweden Nordic HF-19
Jean-Yves BERNIER
Philippe CRAMBERT
Catherine LAMY-BERGOT
Jean-Luc ROGIER

Integration Of IP Services Over High Data Rate Hf Capabilities

Agenda

- Introduction
- CONOPS or typical user environment
  - Data protection and the security architecture
  - Bulk crypto and modern long distance communications
  - SALAMANDRE project and the genesis of STANTAG 5070
- HF-XL High Data Rate Waveform and HF Radio
  - Media access control : TDD, DRC, ALE and ALM
  - STANAG 5070 ARQ
  - IP-PEP
  - Client and AES definition
  - Case study : email over HF
- Conclusions

Introduction

High data-rate HF wave-forms – for what usage ?

- Since the advent of HF-XL, 110C waveforms the question was raised about how to use the higher throughputs in the HF environment ?
- The first simple answer was : plug the new modem in current systems, and expect a faster data transmission …
- This approach was not a success for many reasons
  - Just a new waveform did not address the link establishment
  - Existing ARQ were designed to operate with low data-rate, and were not well suited for bigger data packets.
  - Existing HF was performing data transmission the way it was done in late 80's, …
- From the beginning of the HF-XL research program, we needed to address all the layers in the OSI model, from the applications down to the radio media.
  - It was not possible to develop just a new MODEM waveform
  - XL also means "cross-layer"

CONOPS or typical user environment

CONOPS

- CONOPS stands for CONcept of OPerationS.
- Traditional Military way to describe the mission description and the intended equipment use.

The user

- On the ground, fixed or mobile, on the sea or in the air.
- Missions are often in coalition between many countries : NATO and more …
  - There is a need to share mission sensitive information within the coalition members.
  - There is also a need within each nation to manage its own assets, for logistic purposes for instance.
- Typically, each platform has many segregated data domains.
  - Each of these domains needs to communicate with other platforms and shares data.
- Average user expectancy is just dial a number and speak, write an email and hit the send button, open a chat window and start texting, open its mission specific software and simply work.

No more “radio” guy, but IT tech

CONOPS or typical user environment

Data protection and the security architecture

- Data protection objective is to protect information, the operations and operational means and methods needed for the accomplishment of the mission.

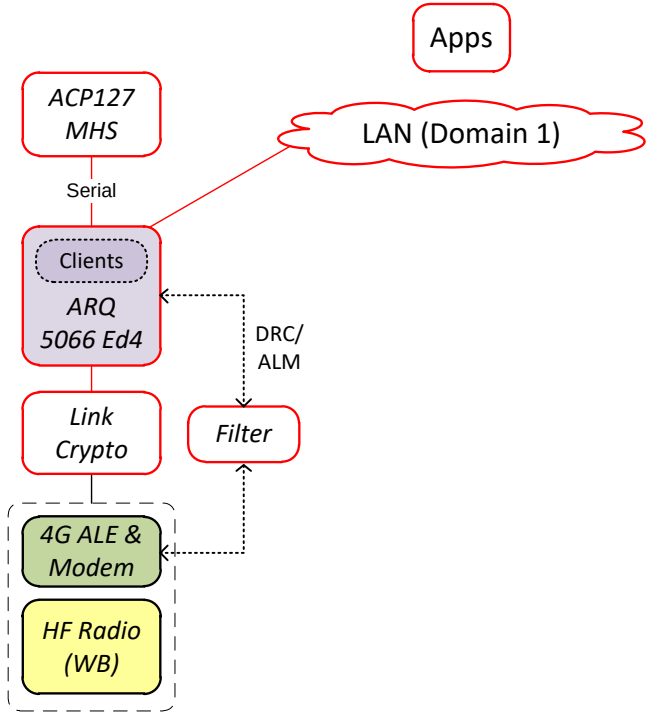
Share data in a trusted and reliable way between partners.

- Many ways to protect information
  - Bulk crypto : the traditional way by inserting a cryptographic equipment to cypher plain text before transmission and decipher it on the other side.
  - IP crypto : In the IP world, new needs for protecting information emerged, with the need to route information form various segregated LANs through a single common carrier.

CONOPS or typical user environment

Bulk crypto and modern long distance communications

- Typical "bulk crypto" architecture
  - There is only one protected domain, with only one level of protection (in red).
  - No possibility to implement IP routing in the unprotected public side (in black)
  - A cryptographic filter is needed to allow automated DRC (Data Rate Control) and ALM (Automatic Link Management) information exchange between radio and ARQ.
  - This filter is a critical bidirectional security element and many users/implementation prefer to disable the DRC and ALM to mitigate any security risks introduced by this filter.

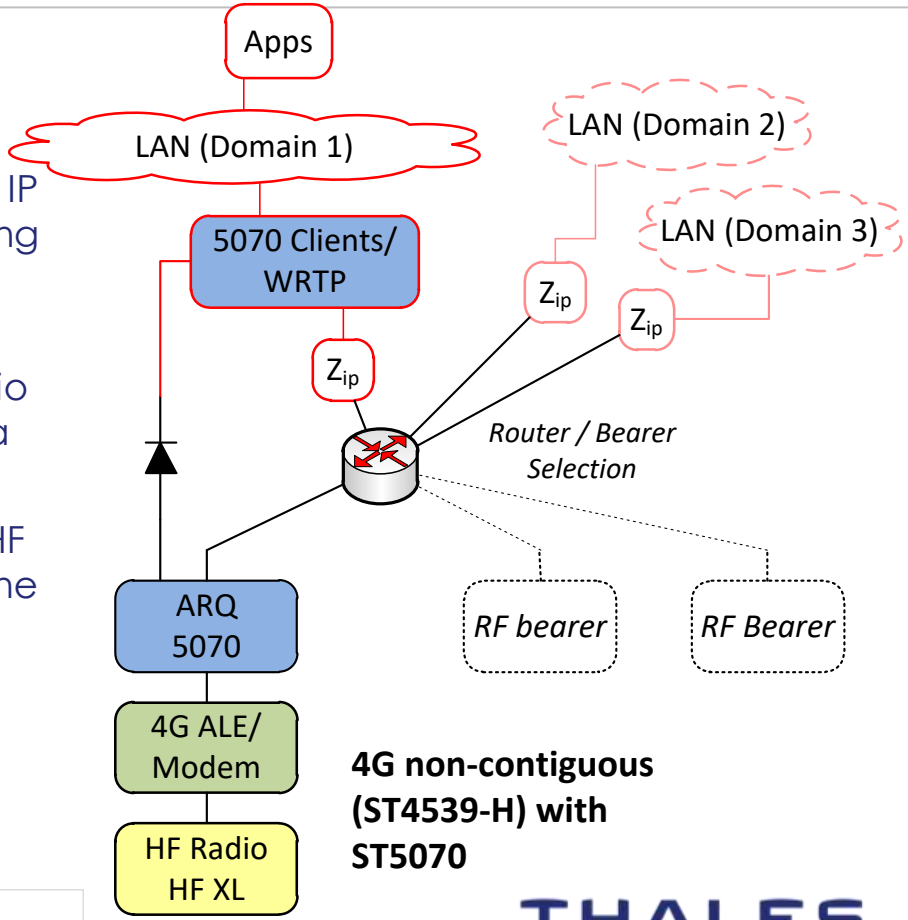


4G contiguous with STANAG 5066 Ed 4

CONOPS or typical user environment

SALAMANDRE project and the genesis of STANTAG 5070 main features

- Enable a "multiple LAN" architecture based on IP crypto technology that allows standard IP routing through one or more "RF bearers"
- The ARQ, DRC and ALM are close to the radio and does not cross the security border. The radio takes care of the channel and for errorless data transmission
- On the user side, HF specific "clients" receives HF connection information to accommodate for the channel availability trough a "black to red" diode.



ST5070 updates: v0.4

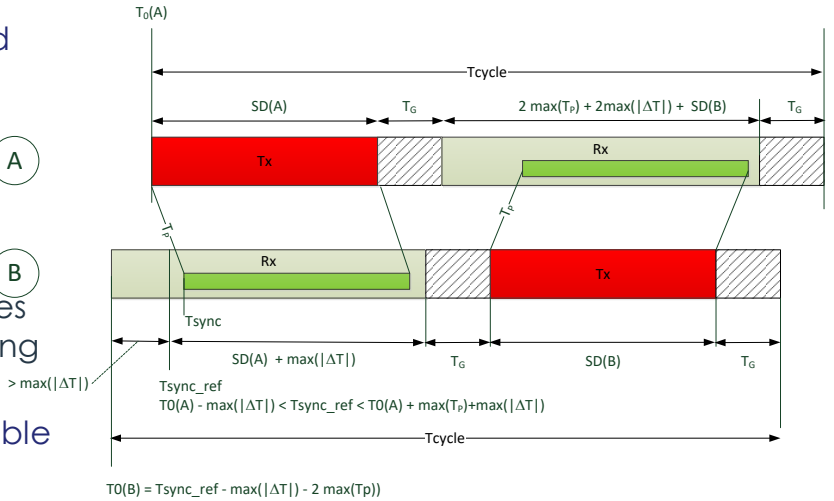
Volume	Contents	V0.4
Main	Overall presentation	Update posted onto web site in July 2019
Annex A	ALE, ALM	
Annex B	DRC + TDD	
Annex C	ARQ-Red	
Annex D	ARQ-Black	
Annex E	IP crypto	
Annex F	5066 clients	
Annex G (new)	AES	In progress
Annex H (new)	IP PEP	In progress

In agreement with FRA MOD, updated draft 0.4 of ST5070 was posted onto BLOS web site in July 2019
Comments are appreciated

HF-XL High Data Rate Waveform and HF Radio

Media access control : TDD

- The Time Division Duplex (TDD) defines a deterministic and periodic way to access the HF media through a predefined allocation of the time resource to each link direction.
- TDD is a layer that provides bidirectional channel access
  - Switching to receive state does not rely on the correct reception of EOT data.
  - Channel quality (Signal to noise ratios, channel occupancy) can be regularly measured, which improves the modem adaptation capability with respect to varying propagation conditions.
- The time that is allocated to each link direction is configurable to fit asymmetrical data rate need.

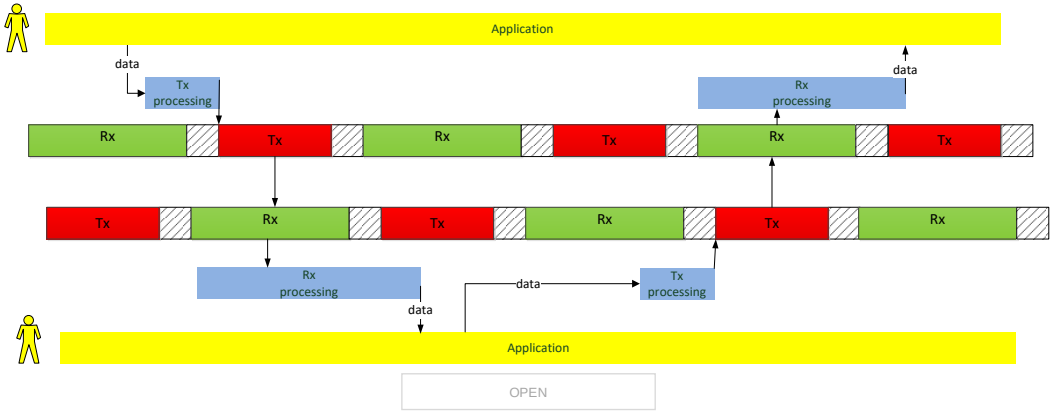


- SD(A) (resp. SD(B)) : superframe signal duration
- T_G : Necessary guard time for receive-to-transmit and transmit-to-receive changeover
- max(T_P) : maximum propagation time
- max(| ΔT_P |) : maximum synchronisation error

HF-XL High Data Rate Waveform and HF Radio

Media access control : DRC

- The MODEM waveform adjustment, or Data Rate Control (DRC) is implemented at the TDD level: the waveform parameters can be changed on each cycle and independently of the link direction.
- On each TDD cycle, radio measurement are averaged on several slots to obtain statistically consistent estimations over ionospheric varying channels :
  - The link budget (total mean SNR)
  - The frequency channels occupancy
  - The equivalent AWGN SNR on each frequency channel to select the best modulation.
- The quality of these estimates is a key factor to maximize the throughput by the selection of the frequency channels and the modulation to be used



OPEN

THALES

HF-XL High Data Rate Waveform and HF Radio

Media access control : ALE and ALM

- The ALE (Automatic Link Establishment) and ALM (Automatic Link Management) engine has the responsibility to select the best transmission frequency or HF-XL sub-band.
  - note : HF-XL allocated spectrum is a set of HF-XL sub-bands each made of 1 to 16 classical 3 kHz channels.
    - The ALE-ALM will simply select the best HF-XL sub-band "centre frequency"
    - The DRC will select and manage the best channels within the sub-band.

Typical Example of Frequency Allocation for 3 HF-XL channels (MHz)

- During the field tests, ALE – ALM selects one operating "centre frequency" and practically keeps its.
  - No need to continuously search for another passing frequency as in 2G and 3G ALE-ALM systems when the channel is changing with time or temporally fading with time.
  - The ALE-ALM is only operating during the link establishment and day-night transitions conditions.
  - In difficult situations, when the link drops, ALE-ALM does not find any better condition, and usually resume transmission on the same frequency, or HF-XL sub-band.

HF-XL High Data Rate Waveform and HF Radio

STANAG 5070 ARQ (Automatic Repeat reQuest)

- The proposed 5070 ARQ is in two parts.

- The ARQ part lies in the “black” side on the security level. It connects directly to the MODEM.
  - It ensure that each transmitted data bloc is transmitted without error.

- This ARQ has a proxy or 5070 client in the red part and acts as a gateway for IP traffic going through HF media.
  - This proxy or client needs to receive information from the HF link : the link status and capabilities
  - All the applications connects to the “red” side.

HF-XL High Data Rate Waveform and HF Radio

IP-PEP (Proxy Enhanced Protocol)

- The IP-PEP layer manages the link QoS, or Quality of Service.
- It is a layer in connection with the application and takes in charge following features:
  - Connection management,
  - Local TCP acknowledgement,
  - End to end packets delivery,
  - The HF link error handling and link failure recovery.
- The main feature of this IP-PEP is to fool the TCP protocol by sending acknowledgment to the application while ensuing the delivery of the packet by the specific HF ARQ process.

This IP-PEP is also called TCP "Spoofer"

HF-XL High Data Rate Waveform and HF Radio

Client and AES definition

- The client, for sake of simplicity and to ensure a maximum compatibility with existing HF applications shares the same definition as the current STANAG 5066 standard.

- AES is here to provide some data protection in the HF link management. It is not here for the payload protection, but to ensure that the link data, the sender and the receiver addresses, receives some protection.

HF-XL High Data Rate Waveform and HF Radio

Case study : email over HF

- EMAIL over HF is a typical example to highlight the evolution for the S5070 from S5066.
- Standard EMAIL servers and clients (such as OUTLOOK, Firebird, …) use multiple IP packets for connection establishment : typically 6.
- To reduce reduces the connection latency, HF-EMAIL in the S5066 goes through the EMAIL-Client that acts as a proxy EMAIL server for the users.
- But
  - The user needs to know that the recipient is accessible through HF, with an HF specific address.
- The 5070 proposal will solve these issues. The EMAIL client to server connection is straight forward via the IP client.
  - EMAIL service can share the same HF radio link as with services with different security levels.

Conclusions

HF is back!

- After many years of decline and disregard, new studies and standards propositions modernize this historic way of communication. To achieve this goal, users and industry teamed in the SALAMANDRE program to build a solution that meets the operational needs while using state of the art technology. The new standard STANAG 5070 proposes an architecture that is designed to suit current customer needs by proposing the integration of IP connectivity and data protection compatible with the ongoing NINE crypto standardization.

THALES

Any Questions ?

Thank-you