INTEGRATION OF IP SERVICES OVER HIGH DATA RATE HF CAPABILITIES

Jean-Yves BERNIER
Philippe CRAMBERT
Catherine LAMY-BERGOT
Jean-Luc ROGIER

SUMMARY

The HF community has been working on defining and developing a new generation of HF standards to improve the throughput capability and the reliability over HF channels. This has led to the definition of two physical layer solutions, currently under standardization by NATO, using up to 48kHz worth of bandwidth, contiguous or not. Corresponding proposals for link establishment and maintenance are currently proposed.

Furthermore, the current HF third generation system (STANAG4538) exhibits difficulties around the security solution due to its non-explicit definition. This generates the need, in NATO BLOS group, to define a fourth generation solution to take into consideration the need for interoperability between nations and forces, while using a NATO agreed cryptographic solution. The solution will capitalize on the success of the definition of STANAG 5066 at system level for HF second generation systems.

This proposal is currently under discussion at NATO BLOS level to improve the 2020’s HF capability with resilient and interoperable systems complementary to SATCOM links.

Our article will detail the proposed the STANAG 5070 approach architecture, which includes ease of HF IP integration and a crypto solution compatible with the NINE current standardization efforts (see illustration in figure Figure 6).

A first implementation of the proposed architecture, and in particular the capability to connect with both standard IP clients and legacy ACP and CFTP clients has been successfully demonstrated with the SALAMANDRE project sponsored by French MOD. Further tests have been successfully carried out with the UK MOD in June 2018, for both day and night time. Results of 2018 will be integrated in the article.

1 INTRODUCTION

With the new high data rate HF waveform proposition, from the beginning of the studies that resulted in the new HF-XL and 110-C definition, the question was raised about how to use these higher throughputs in the HF environment. The answer was not as simple as it seemed to be.

We first started to analyse the available standards such as the STANAG5066 and the STANAG4538. These were available, well tested and subsequently were good candidates for the future higher data rate waveform in study. But soon, by the moment the demonstrators started to show the feasibility of the HF-XL waveform, we started to analyse the way to select the good ARQ. This is when the limitations of these standards started to show the way it will limit the good results we were getting with our new MODEM.

The ARQ standard, and the way the intended user is planning to use the HF link has a big impact on the success of a new waveform. Very early in the development cycle, the HF-XL development team realized that the whole data stack needed to be addressed, from the end user application side down to the antenna.

But let’s diverge a little. Within the HF radio community, one way to distinguish between a network engineer and a radio engineer is just to note where the antenna lies in the illustrative drawings. If the antenna is on the top of the drawing, you are talking to a radio engineer and, with if the antenna lies on the bottom, a network engineer is in front of you (the higher the antenna, the best is the transmission will say the radio engineer). Personally, I, (the author) am a radio engineer, but for the present article I will switch to the “network” OSI representation for the data stack, with the media physical layer, so the antenna, on the bottom. The other title for this article could be “Networking For HF Radio Engineers”.

As the project went further, realizing that we needed a better ARQ, inevitably, we were addressing the user point of view. This was already the path followed during the HDR-HF EDA research project where all the ISO layers were developed from start, but with the new standard waveform proposition for NATO, it became clear for us that we should start from the user experience and the application layer down to the physical layer. On the other hand, we wanted to borrow as much as possible from existing standards from the HF-House. This path is the genesis of the STANAG 5070.

The following point to address was the fact that the target users for these new HF standards are the NATO countries. None of these users are transmitting plain text in clear. Security, data integrity, network segregation are the basis of all practical radio architecture. Happily, both existing NATO standards STANAG5066 and STANAG4538 address this cryptographic issue. Nevertheless, the proposed security architecture supported by these standards were relying on old security concepts, using bulk crypto devices. This was far from state of the art today’s security architecture using IP crypto. The “old fashioned” bulk crypto is not compatible with modern multi-level security networks and the increasing need for the end user to use state of the art, standard applications, like email, chat, or standards protocols like ftp, http, etc …

2 <u>CONOPS OR TYPICAL USER ENVIRONMENT.</u>

CONOPS (Concept of Operation) is the traditional user word for the intended use of a piece of equipment. We will not dive too deeply in it, just to understand the requirements on the ISO stack we need to address.

The user is either on ground, mobile or fixed, on the sea, or in the air. We need to address all of these environments. During the last decades, all NATO operations were in coalition between many countries. Each mission has to share mission sensitive information, within the coalition but also, in the same time with the nation of origin of each asset, ea. for logistic purposes. Many segregated data domains are existing and need to communicate on each platform, a ship, an aircraft, a vehicle or in a tent.

One of the main issues we faced also during the test trials is that radio operators are mainly IT tech, educated to install and operate modern computer environment. The expertise is now much broader than 30 years ago; the focus of the people is in the mission, with little or no time for network setup or trouble shooting a radio link. All operators are still able to manipulate a Morse key, but only if there is no other possibility. The military end user expectancy is the same as any iPhone user, just take it and dial a number, write an email or open a chat app to communicate without any other technical tweaking. We needed to make the new HF high data-rate system as user friendly as any smartphone, or modern laptop.

The last element about the expected behaviour is for emergency operation of the radio equipment. It should be possible to dial an emergency frequency, take the mike and speak, just like dialling 911 or 112 on a smartphone.

2.1 DATA PROTECTION AND THE SECURITY ARCHITECTURE

First we need a simple definition or explanation about the data protection. There is often some confusion about data protection that many people confuse with secrecy. Secrecy is a way to control information and its release to general public. On the contrary, data protection is not about secrecy; its aim is to protect information, the operations and operational means and methods needed for the accomplishment of the mission. On purpose, I will not mention any security level such as NATO secret, Nation restricted and so on as this is only a way to express the level of needed protection, and this is not the purpose of this presentation.

The security architecture is the way to protect the data transmitted over the HF means. This is not a mean to build a secrecy fence around operators and users but a way to share information between collaborating crews, or actors in a safe and thrusted environment.

The basic mean for data protection is to use cryptographic equipment that will cypher any plain text before transmission and decipher it on the other side.

Before the World Wide Web that later became the Internet, this protection was simply realized by inserting cryptographic equipment just before transmitting and the corresponding deciphering equipment after reception. This is called the “bulk crypto architecture”. The main idea about this bulk crypto is to protect as much as possible information, the transmitted text, but also who are the originator and the recipient, and how many messages are transmitted.

Since the Internet revolution, with the concept of interconnecting local area networks (LAN), new data protection concepts emerged, and became the basic of our daily experience in practically every part of our personal exchanges with our smartphones, laptop, tablets, bank transactions and so on.

Modern military command and control architecture during operations are using data equipment connected to specialized LANs. Each LAN has a purpose and addresses a community, such as for instance, to share tactical information, share emails, or logistic data for maintenance. For security reasons these LAN are segregated or isolated one from the other. To be able to transmit and interconnect these LAN through a satellite or UHF fast data link, dedicated crypto equipment protects each of these LAN and a specialized router connects them to the WAN (Wide Area Network). This is the mean that connects the ship, the armoured vehicle or the aircraft to the rest of the world. These are named IP crypto, and is part of NATO standardization initiative called NINE (STANAG 4787).

The purpose of each segregated LAN above is to connect terminals, tools, servers and machines to ensure the integrity of the data on each one. For instance, some LAN connects a machine gun and sensors to a remote firing control terminal, other LAN interconnect simple service office laptop.

2.2 THE CLASSICAL "BULK CRYPTO" ARCHITECTURE IS NOT WELL SUITED WITH MODERN LONG DISTANCE COMMUNICATION NEEDS (STANAG 5066) (SEE FIGUREFigure 6)

These data protection concepts above are the basic ideas that govern the design for the HF radio security architecture. The classical security architecture is using a "bulk crypto" (cfr figureFigure 6). In a multi-LAN architecture, we need one HF radio stack with its dedicated bulk crypto per LAN to differentiate, segregate and properly cypher the data originating from these different LANs domains. For instance, one radio stack will be assigned to HF-Email; another will handle ACP127 tactical messaging system, etc. There is no simple way to aggregate communications from multiple LANs through a single HF link.

Furthermore, the "bulk crypto" solution has a many drawbacks when operated with ARQ and automatic link establishment (ALE) systems. These systems need to share information about the quality of the link and addresses of correspondents transiting across the cypher layer. This needs a careful design to avoid any data breach, which is expensive and usually tailor made and certified and individually tested and certified for each system.

2.3 SALAMANDRE PROJECT AND THE GENESIS OF STANAG 5070

Early on, during the development phase of the new HF high data rate waveforms, the SALAMANDRE development team realized that this classical data protection approach is no longer well suited for the intended multiple LAN architecture. We simply borrowed the concepts in use by satellite communications. Our objective was to present the HF link as another transparent data bearer on the same level to UHF and satellite links. In addition to it, we went further by adding Automatic Link Establishment and advanced Hybrid ARQ features.

3 THE HF-XL HIGH DATA-RATE WAVEFORM AND HF RADIO

The purpose of HF-XL high data-rate waveform is to propose a radio platform, which is using the ionospheric propagation effect to enable over the horizon connectivity. This transmission media is known to be difficult to operate, and one of the objectives is to use modern data technology to make it the easier possible. For the user point of view, the HF-XL radio is the physical link layer in the ISO stack. In combination with ALE technology, it takes care of automatically selecting the good frequency band.

The 5070 standard is incorporating all needed to enable HF operation in an interoperable fashion within NATO countries.

Annex A is about the ALE and ALM function and operation description.

Annex B explains the Data Rate Control feature (DRC)

Annex C: (ARQ-Red) Wideband Transport Sublayer

Annex D: (ARQ-Black) Subnet Interface, Channel Access and Data Transfer Sublayers

Annex E: characteristics of IP crypto

Annex F: Client definition (Same as STANAG 5066)

Annex G: AES definition.

Annex H: IP PEP

Here we will go deeper into some of these annexes, to highlight basic improvement in regard to a more classical approach.

3.1 MEDIA ACCESS CONTROL: TDD AND DRC (ANNEX B) AND ALE-ALM CONTROL (ANNEX A)

For interactive IP services like web and chat, data rate as well as bidirectional latency (round-trip time) are two major aspects of QoS, whose performance depends on the channel access method.

The Time Division Duplex (TDD) defines a deterministic and periodic way of accessing the HF media through a predefined allocation of the time resource to each link direction.

Conceptually, TDD can be seen as a layer that provides bidirectional channel access to the upper layers, with well-defined characteristics for each link direction in terms of:

- Worst-case latency;
- Maximum waiting time to send a higher priority packet, in a context of multiple services transmission;
- Switching to receive state does not rely on the correct reception of EOT data, avoiding false/non detection issues, and allows designing robust procedures with respect to incorrect data decoding;
- 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 and can differ to fit an asymmetrical data rate need, typically for services such as mail or file transfer, which leads to define a longer slot in the in the preferred link direction.

The trade-off between latency and mean data rate can be manged be computing the cycle duration and the time efficiency, which is defined as the ratio between the mean data rate and the modem data rate.

The optimized cycle duration is computed according to a function dependent of the following parameters:

- 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

The two stations can be synchronized either by an external system or by relying only on modem synchronization. In the latter case, the master station defines the start time of the TDD cycle and the slave station tracks the time at which the beginning of the signal is received, and defines the start time of its own cycle with respect to this synchronisation. In this case, max(ΔT_P) represents the maximum error allowable between the reference position of the tracked signal and its actual position, due to propagation time variation and time drift between the two stations.

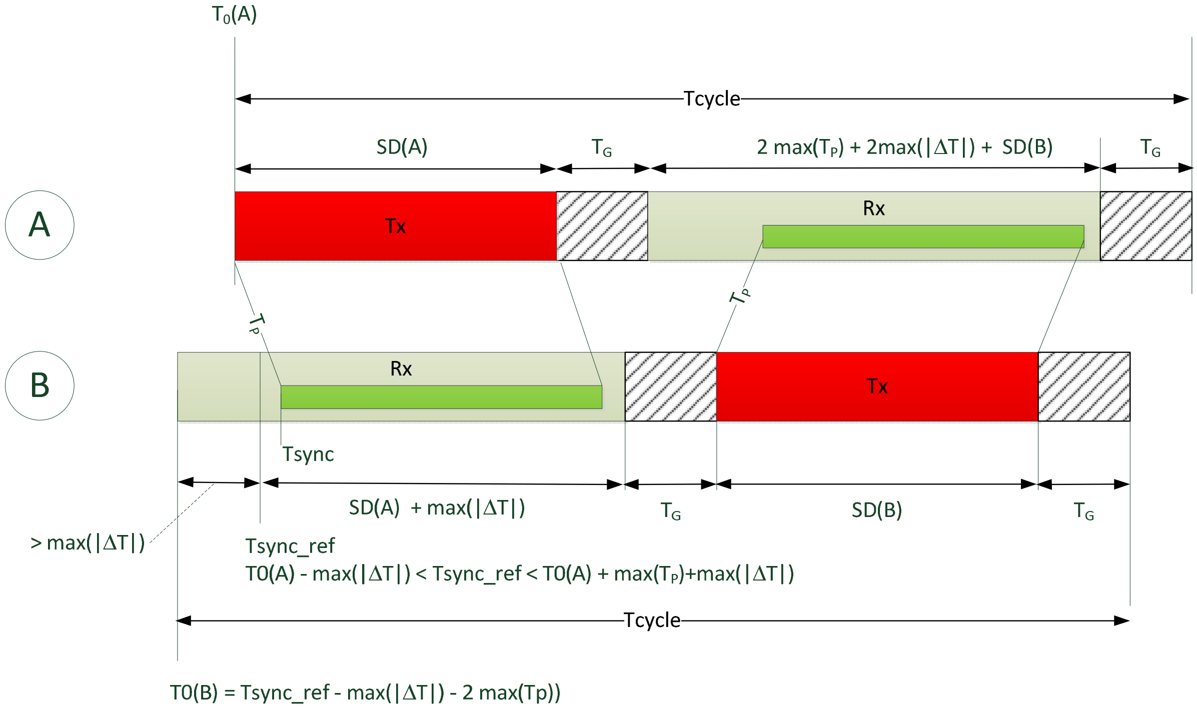

T_0(A)
Tcycle
SD(A)
T_G
2 max(T_P) + 2max(|ΔT|) + SD(B)
T_G
A
Tx
Rx
T_P
T_P
B
Rx
Tx
Tsync
> max(|ΔT|)
SD(A) + max(|ΔT|)
T_G
SD(B)
T_G
Tsync_ref
T0(A) - max(|ΔT|) < Tsync_ref < T0(A) + max(T_P)+max(|ΔT|)
Tcycle
T0(B) = Tsync_ref - max(|ΔT|) - 2 max(Tp))

Figure 1: TDD cycle timing.

This results in the following value for the duration of the optimized TDD cycle:

$$\text{Tcycle} = \text{SD(A)} + \text{SD(B)} + 2\ T_G + 2\ \max(|\Delta T_P|) + 2\ \max(T_P)$$

The duration of the superframe (SD(A) & SD(B)) is configurable according to the modem waveform (ST4539-H or ST5069), to contain one or several interleaving blocks.

The following figure illustrates the case where one interleaver block per slot is used, and where the guard time is reduced as far as possible, to optimize the cycle duration and the use of the media. When considering the processing of all the layers (modems, protocol stack and application), a response to received data in slot n can be sent in slot n+3. The resulting round-trip-time varies from a little more than two cycles up to a little more than 3 cycles.

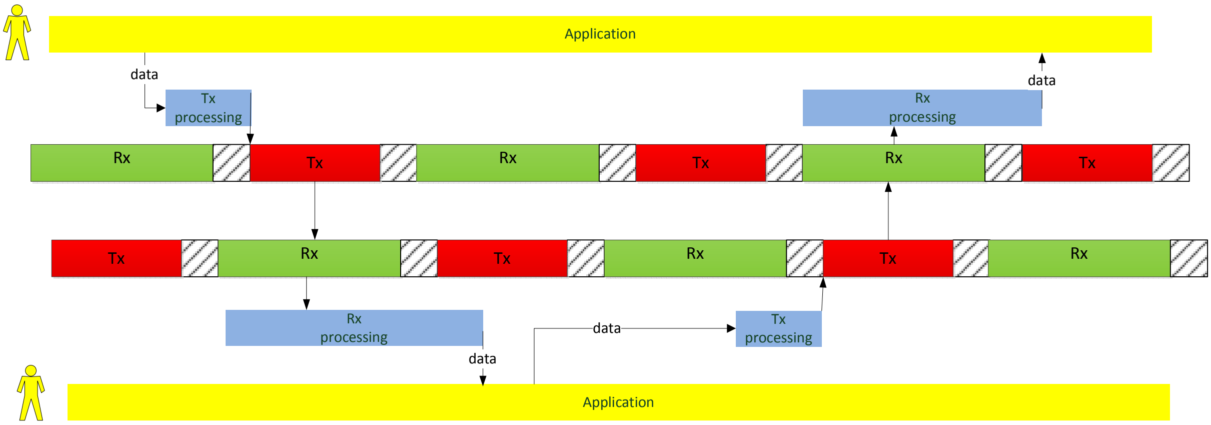


Figure 2: Data transfer over TDD

The modem waveform adjustment, aka Data Rate Control (DRC) is implemented at the TDD level: the waveform parameters can be changed every cycle and independently in each link direction. For the link direction from station A to station B, this adaptation is decided by the station A on the basis of measurements done by station B, which are transmitted to station A at every cycle. This principle guaranties that station A is able to normalize and interpret correctly the measurements done by station B, since it knows exactly the waveforms parameters that were used (notably, power, used or unused channels).

Although the general principle is common to the different possible waveform modems, the adaptation algorithm is specific to the modem waveform.

With regard to ST4539-H modem waveform, the autobaud capability allows to adapt, from slot to slot, the channels in use, their respective modulation as well as the total number of channels. To do this, the receiving station transmits signal-to-noise ratio information and the occupancy level on each channels, in use or not. This allows the transmitting station to monitor the quality of each frequency channel, in a regular fashion that allows to follow the continuous evolution of the propagation.

The data rate adaptation of the modem is carried out at each TDD cycle, in two main steps, the first step consists by the selection of the frequency channels to be used, and the second step by choosing the constellation of each frequency channels. The purpose of these decisions is to maximize the throughput, taking into account the current estimation of propagation conditions:

- The link budget (total mean snr);
- The frequency channels occupancy;
- The equivalent AWGN SNR on each frequency channel.

These metrics are recursively averaged on several slots to obtain statistically consistent estimations over ionospheric varying channels, the quality of these estimates being a key factor for the data rate estimation.

With regard to the evaluation of the SNR, it is worth noting that the mean SNR is not a good metric to choose the modulation. The mean SNR required by the modem to reach a given error rate depends strongly of the nature of the propagation channel (AWGN or CCIR poor for instance and can vary up to 10 dB. So an equivalent AWGN SNR is computed by estimating simultaneously the mean SNR and the dispersion of values over time.

In the figure below (Figure 3), the AWGN equivalent SNR is computed for a CCIR poor channel with 15 dB mean SNR. The equivalent AWGN is estimated at about 8 dB, which lead to choose QPSK constellation most of the time, which is very well suited for such a propagation channel.

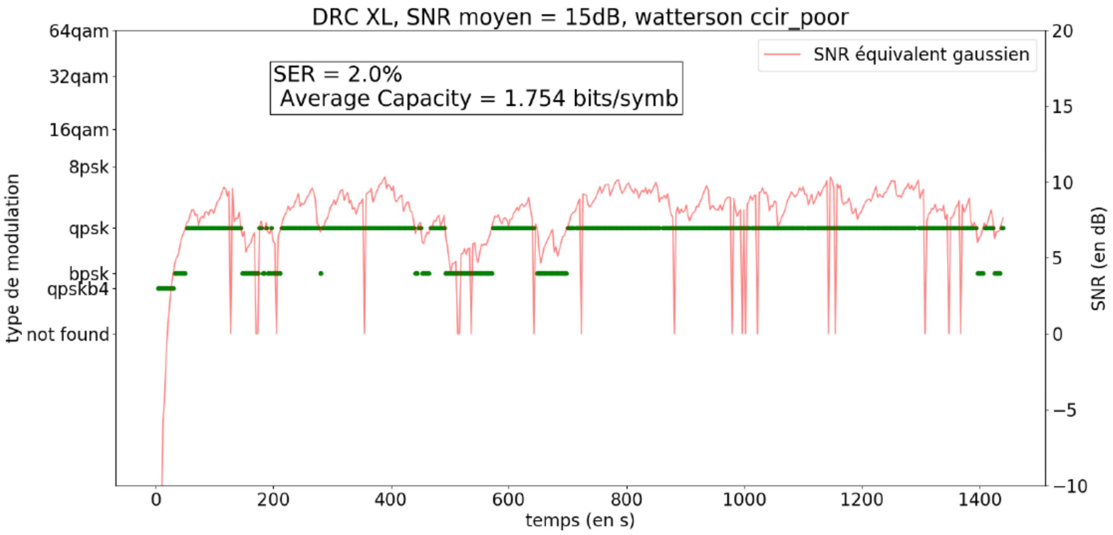
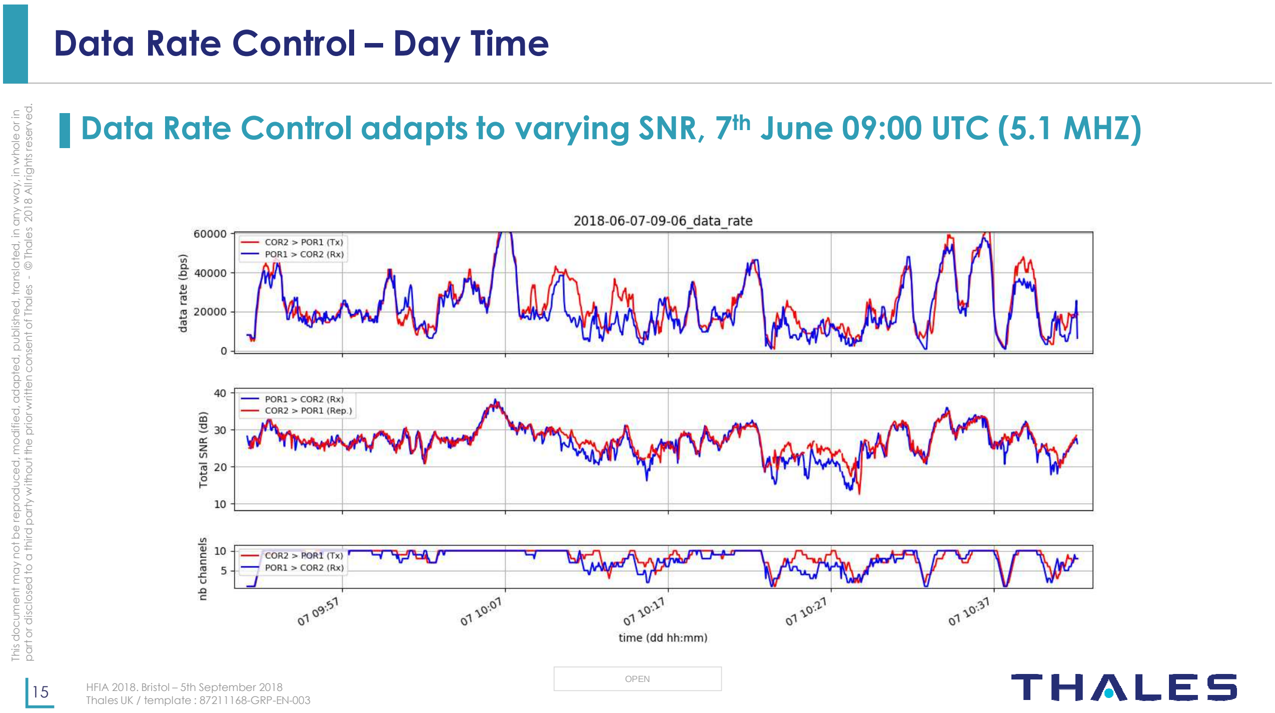


Figure 3: AWGN equivalent SNR

During the SALAMANDRE experiments, this approach proved to be very efficient to follow the ionospheric propagation evolution. Thanks to the HF-XL multi-channel feature, the channels were not fading at the same time. The TDD-DRC scheme reduces the need to switch very often to a better frequency using the ALM process. Even if the whole band was fluctuating with time (See Figure 4), it was just a matter to wait for the channel to come back to its previous capabilities. There was no longer a need to disconnect and reconnect to find a better frequency. ALE-ALM was then only used much less often than initially expected. Its main use is during the initial link establishment and during night and day transitions.

On the same level to the DRC, is the ALE-ALM mechanism. This engine has the responsibility to select the best transmission frequency or HF-XL sub-band. Previous ALE implementation, 2G or 3G were extensively used in HF transmissions. This is mainly due to the peculiar fact that ionospheric channel is a natural transmission mean that changes with time. It was quite accepted that the ALE-ALM had to regularly change the channel or that it will search for a new “passing” frequency.



Data Rate Control – Day Time

Data Rate Control adapts to varying SNR, 7th June 09:00 UTC (5.1 MHZ)

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

15

HFIA 2018. Bristol – 5th September 2018
Thales UK / template : 87211168-GRP-EN-003

OPEN

THALES

Figure 4 : Link evolution with time and automatic adaptation.

These features are part of previous papers dedicated on this subject. We will not go further on this issue and we will concentrate on higher stack level related to data protection architecture.

A last point is to note the AES encryption used to mask ALE and ARQ node addresses and on the air providing some protection.

3.2 STANAG 5070 ARQ (ANNEX C AND D)

The main feature about the STANAG 5070 ARQ is its two part construction with standardized IP crypto equipment.

The black ARQ, lies in the black side on the security level, and connects directly to the MODEM.

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, from the black ARQ, mainly about the link status and capabilities.

This is the main advantage for this architecture in comparison to previous IP compatible solutions over HF, where the HF link can be seen like any other link, like the Sub Net Relay (ACP200), SATCOM or simply WAN. It allows the aggregation of multiple data fluxes, maybe with different level of protection (encryption) on the same link.

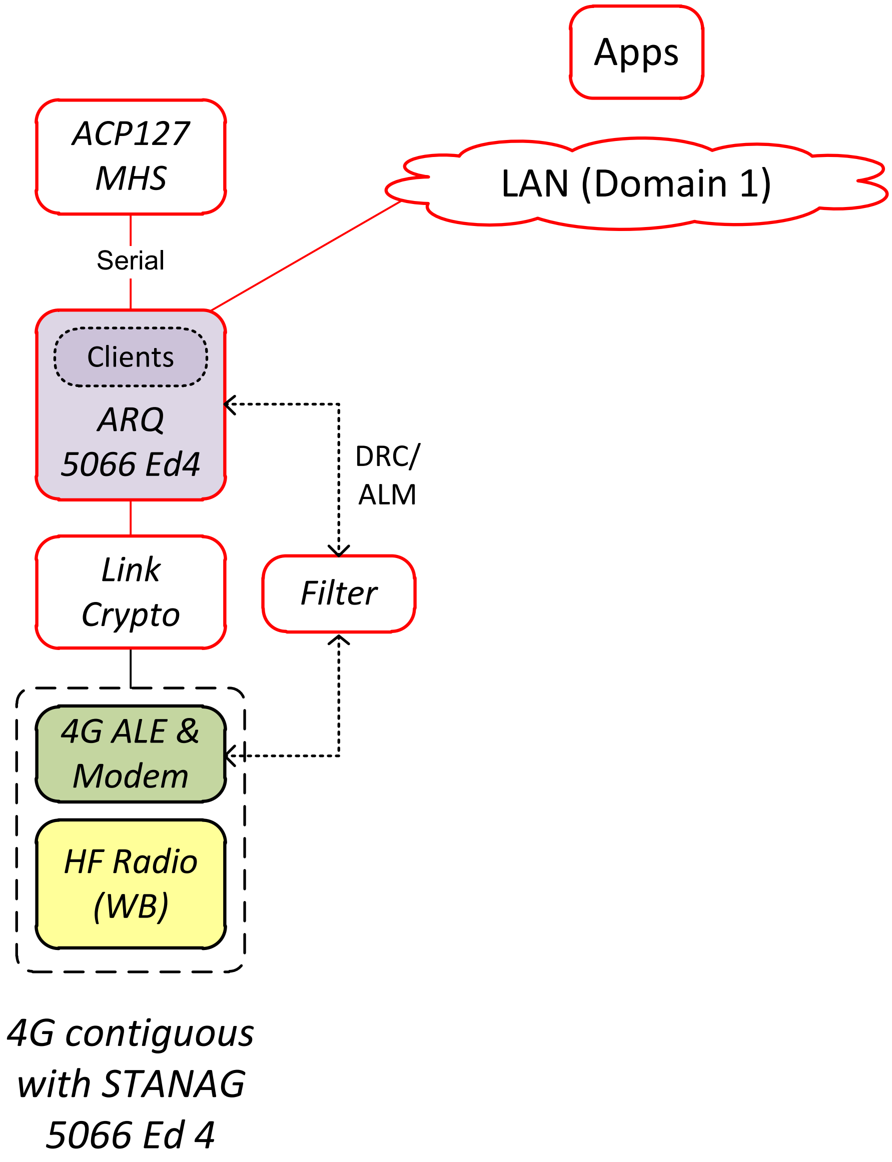
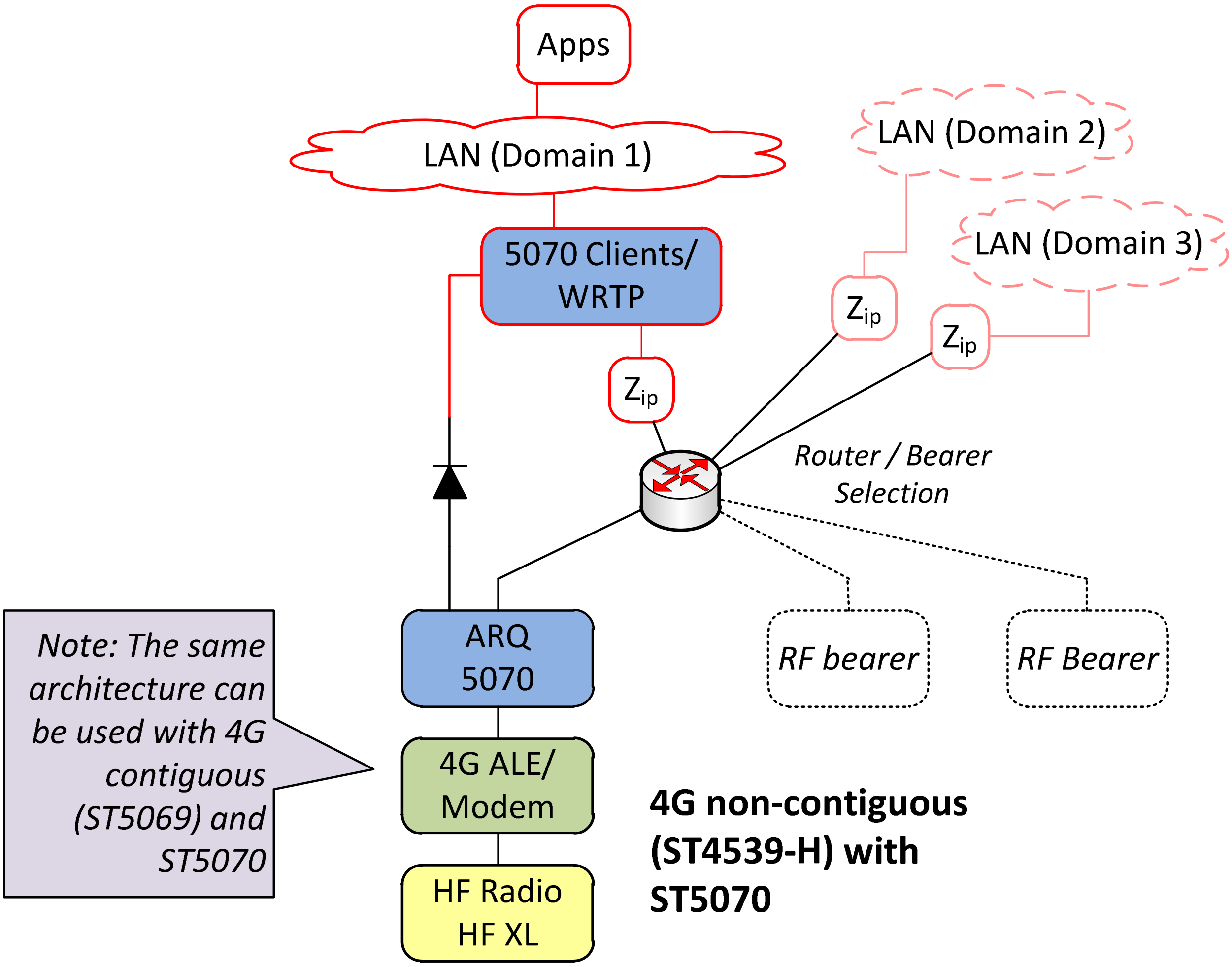


Figure 5: typical STANAG 5066 installation

The proposed solution tries to address and solve another point in sensitive installations about data protection. A typical HF installation that uses a STANG 5066 ARQ in conjunction with a serial bulk crypto, is not capable to use an ALE that will automatically switch frequency when the link is broken. The information about the link quality is in the red part of the architecture, and the ALE control mechanism needs to control the radio equipment on the black side (See Figure 5). Furthermore, the information that the link is up and running on the black side needs to reach the red side to activate any transmission. One way to solve this issue, beside the trivial solution of a manual setup by an operator is to develop specialized security equipment that will exchange this information between the black to the red sides in a “protected” way, ensuring no data breach can happen. Unfortunately this piece of equipment is often very expensive to develop. Moreover, as this equipment is not part of any NATO standard, there is no agreed way to implement it; each NATO country often ends ups with its own specific solution not compatible with the other nations. This tricky little detail prevents in actual world to implement the HF-House stack that would allow no brainer communication between allies.

The STANAG 4538 standard, that incorporates 3G ALE, and ARQ has the same issue as no provision was agreed between nations about the security issues that are related to it. Today, each vendor proposes a security solution that is not compatible with any other vendor.



Note: The same architecture can be used with 4G contiguous (ST5069) and ST5070

4G non-contiguous (ST4539-H) with ST5070

Figure 6 : proposed STANAG 5070 security architecture

The proposed STANAG 5070, while relying on standard IP crypto proposes to address this security issues and proposes to standardize the solution in a simple and straightforward way. The ARQ mechanism is in the black side, any payload data is encrypted. The modem and the ARQ are exchanging link data information as needed. When the link disappears, the ALE-

ALM is able to automatically take over and find a new set of frequencies. The only need here is to inform the “user side”, the applications in the red world about the link status. This is the reason that the ARQ is on both side of the IP crypto, the red part is able to manage and inform any user of the HF link, or the Quality of Service: QOS. To implement this QOS feature, only a limited set of information has to cross the red-black in one direction. Many vendors propose state of the art safety solutions to meet this requirement that are not specific to a vendor or a nation.

3.3 IP-PEP (Annex H).

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: connexion 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” for this reason.

3.4 CLIENT DEFINITION (ANNEX F) AND AES DEFINITION (ANNEX G).

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

For the last annex, the AES definition 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.

3.4 A CASE STUDY: EMAIL OVER HF.

Email over HF is one of the major candidates for HF links even with the new “wide-band” waveforms remains slow. Email does not require instant transmission and can tolerate some delay in the delivery. Today, the use of Email is wide in armed forces and it meets a real operational need.

Email is using client applications, usually a mail application such as Outlook or Thunderbird, and Email servers that empty the client outbox and fill its inbox. The underlying protocol is IP based email protocol suite.

Email servers are interconnected to transport the mail flow to the recipient.

Normally, any IP mail client and IP server connected to the STANAG 5066 IP plugin (also improperly named 5066 IP client) should do the trick.

Unfortunately, on classical STANAG 5066 ARQ based installations, using narrow band or wide-band waveforms, the SMTP mail exchange traffic is important. Regularly, the mail server connects the mail client by 6 IP packets exchanges, where each packet, is acknowledged individually. This saturates the HF link with only not necessary traffic. In this situation, specialized HF Email relies on specialized Email servers, acting as proxies on each side of the HF link to compact the connection, and keep the exchange to the necessary minimum (HMTP). This usual solution has one major drawback. The user, to send an Email, needs to know if this email has to go through an HF link or through a standard IP compatible link like satcomm for instance, or wired WAN. Each user has two email addresses, one for normal traffic, when non HF IP connection is available, and one specific for HF transport. This is the classical way to circumvent the HF Email “server” issue.

In a STANAG 5070 stack, this is no longer an issue. There is no need to implement an Email proxy server to compact the traffic exchange. The user client is able to connect to an email server through an HF link transparently. The red ARQ acknowledges all the local IP traffic, and takes cares of the transmission to the other side of the HF link. The route selection for email is standard IP traffic routing on the basis of QoS information.

4 CONCLUSION

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.

REFERENCES

[1] Catherine Lamy-Bergot, Jean-Luc Rogier, Jean-Yves Bernier, Jean-Baptiste Chantelouve, Patrice Stevens, Philippe Crambert, "Time-division approach in HF wideband: Surfing the wave to offer a better performance", *Military Communications Conference (MILCOM) MILCOM 2017 - 2017 IEEE*, pp. 653-658, 2017.

[2] "Technical standards for wideband HF waveforms (Draft 1, version 1", NATO STANAG 5069, Feb. 2017.

[3] "Interoperability and performance standards for data modems", MIL STD 188–110C, Sept. 2011.

[4] "Technical Standards for Single Channel HF Radio Equipment, draft A for ED 4", NATO STANAG 4203, Feb. 2016.

[5] "interoperability and performance standards for medium and high frequency radio systems", Department of Defense, 1999.

[6] A. F. R. Gillespie, S.E. Trinder, "Performance characteristics of the STANAG 5066 HF data link protocol", Proceedings of IEE Colloquium on Frequency Selection and Management Techniques for HF Communications, pp. 8/1-8/6, 1999.

[7] "Technical standards for an automatic radio control system (arcs) for HF communication links, Ed", NATO STANAG 4538, 2000.

[8] E. E. Johnson, "Staring link establishment for high-frequency radio", Proceedings of IEEE Military Communications Conference, pp. 1433-1438, 26–28 Oct. 2015.

[9] C. Lamy-Bergot, J-B. Chantelouve, J-Y. Bernier, H. Diakhaté, J-L. Rogier, "HF XL: adaptive wideband HF transmissions", Proceedings of Nordic HF 2013 Conference, August 2013.

[10] C. Lamy-Bergot, J-B. Chantelouve, J-L. Rogier, H. Diakhatéand, B. Gouin, "Improved error correction for Stanag 4539 appendix H proposal: HF XL", Proceedings of IEEE Military Communications Conference, pp. 1182-1187, 26–28 Oct. 2015.