STANAG 5066 Ed4

Isode

This whitepaper provides an overview of the changes brought in with Ed4 of STANAG 5066, a NATO standard protocol for data applications over HF Radio networks.

This whitepaper gives an overview of new capabilities introduced in STANAG 5066 Ed4.

STANAG 5066 is the NATO Standard HF Link Level protocol, summarised in the Isode whitepaper STANAG 5066 The Standard for Data Applications over HF Radio. STANAG 5066 Edition 4 is a full (promulgated) standard. For anyone seeking the Ed4 specification, please contact your NATO representative.
There were two primary drivers for this new edition:

1. Support of Wideband HF. The new higher-speed HF protocols in STANAG 5069 needed changes to work with STANAG 5066.
2. Use of ALE (Automatic Link Establishment). Although ALE is widely used with STANAG 5066, this was not specified in the STANAG. The changes needed to STANAG were non-trivial.

At the same time, a number of secondary goals were addressed:

1. Restructuring of the STANAG, in particular to give each application specified an independent Annex and to merge text from other annexes.
2. Editorial improvements throughout.
3. Adopt a number of small and "safe" technical changes.
4. Remove or deprecate a number of features not needed.
5. Add an annex on a new crypto mechanism.

This whitepaper assumes some familiarity with STANAG 5066, which can be obtained from the referenced whitepaper or the introduction section of the Ed4 specification.

Edition 3 Compatibility and Interoperability

A primary goal of Ed4 is to retain full interoperability with Ed3 systems. Significant care has been taken to ensure this and to clearly document how this is achieved.

Wideband HF

The first primary driver for the new edition is to support the new contiguous Wideband HF as specified in STANAG 5069. Two issues are addressed.

Frame Sequence Number Extension

Ed3 has a maximum window size of 128 based on an 8-bit frame sequence number. This limits ARQ performance at the higher speeds of narrowband HF and leads to unacceptable performance at the higher speeds available in Wideband HF. The Ed4 change is straightforward: increase the frame sequence number to 16 bits, which will remove the issue. This small, but critical, change is key to the use of Wideband.

Data Rate Selection

Ed3 uses a Data Rate Change process which is controlled by the receiving server. Ed4 replaces this with a Data Rate Selection process, where the data rate is chosen by the sender, taking into account information provided by the receiver. The receiver can use Ed3 compatible mechanisms or new Ed4 mechanisms. The new mechanism is critical for Wideband, as it enables specification of Wideband data rates, which is not possible with the Ed3 mechanism. The new mechanism offers a number of advantages:

- It provides the sender with more information than the Ed3 mechanism.
- The process works for duplex communication.
- The process works for non-ARQ multicast protocols such as ACP 142.
- It allows sender to choose initial speed.
- It allows sender to choose conservative speeds when there is not much data to send. Isode has shown that this is advantageous in operation.

This is discussed further in the Isode whitepaper Optimizing STANAG 5066 Parameter Settings for HF & WBHF.

STANAG 5066 Use of ALE

ALE (Automatic Link Establishment) is commonly used for Skywave HF communications and is vital for Wideband HF to negotiate bandwidth. Ed3 does not specify the use of ALE, so specifying this was the second primary driver for Ed4.

1:1 ALE

The most important use of ALE is to connect to a single peer, choosing from a pool of frequencies. A number of vendors, including Isode, did this with Ed3, and so it was anticipated that adding ALE would be a straightforward change. This turned out to be the most complex change, supported by two models of operation:

1. Multiple Simultaneous Peer Access. This is where data can be transmitted to multiple peers, with links maintained to multiple peers. This is the only model specified in Ed3.

2. Single Peer Access. This constrains access to a single peer, which is essential when using ALE. We believe that a number of existing STANAG 5066 implementations work this way, rather than following the Ed3 standard.

Ed4 allows an implementation to support one or both of these models, noting that an HF deployment needs to choose the same model for all nodes. Single Peer Access has two modes, "EXPLICIT CAS-1" and "IMPLICIT CAS-1", which are provided to facilitate interoperability with Ed3 systems using ALE in different ways. IMPLICIT CAS-1 is more efficient and recommended where all systems support it.
When using ALE between a pair of nodes, there is often a need to terminate the link. Ed4 provides two mechanisms:

1. A clean "wind down" mechanism that can be requested by either node, that is used when a node wishes to start communicating with a different peer.
2. A quick close mechanism so that the same pair of nodes can use ALE to attempt to get a better frequency.

ALE for Multiple Nodes

1:1 ALE is the most important use of ALE by STANAG 5066. Ed4 also specifies three additional uses of ALE:

1. Multicast. This uses ALE to multiple nodes to deliver PDUs with multicast addresses.
2. Duplex. This supports link pairs so that ALE can be used to support duplex communication.
3. MAC. This negotiates ALE for all nodes on the network so that the MAC protocols discussed later can be used on a frequency negotiated by ALE.

It is currently unclear how useful these will be.

Crypto Support

Ed3 provides support for crypto using the synchronous serial interface specified in Annex D for use with crypto devices such as KIV-7. Ed4 adds a new capability specified in Annex T "STANAG 5066 TRANSEC Crypto Sublayer using AES and other Protocols". This enables a modern approach and avoids performance issues of crypto using synchronous serial.

MAC Layer Changes

STANAG 5066 has two Media Access Control (MAC) capabilities, both of which are updated in Ed4.

CSMA (Annex K)

Annex K uses timers to control MAC access – there is no protocol. Ed3 uses a jitter-based approach, which is suitable for large networks. Modern large networks are likely to use ALE 1:1 rather than CSMA to control access. Ed4 retains the Ed3 approach but also adds a slotted approach, which avoids conflict by assigning a "slot" to each node. This is a simple approach which is efficient for a lightly loaded network with a small number of nodes. It complements WTRP, which is more suitable for heavily loaded networks.

WTRP (Annex L)

Analysis of Ed3 WTRP found that many details were unimplementable and that interoperability would be unlikely. The WTRP in Ed4 has the same top level model and a similar state machine, but the detailed protocol is completely different.
Further information in the Isode whitepaper Token Ring Protocol (WTRP).
WTRP provides a MAC level mechanism to control which node transmits and supports partially connected topologies, such as "three ships in a row". However, it does not support data transfer between nodes that are not directly connected. Annex R: "Routing Sublayer" is a new annex that addresses this by specifying a data relay capability.

Applications

The most visible structural change in Ed4 is that each application is now given its own Annex to improve modularity and maintainability. A number of Ed3 applications have been dropped from Ed4, as they are not seen to be useful moving forward.
The following applications are broadly unchanged from Ed3 but given their own annex.

- Annex O: HF Operator Chat
- Annex P: ACP 127 & Character-Orientated Serial Stream
- Annex V: Compressed File Transfer Protocol

The following annexes also have technical changes:

ACP 142

Annex Q specifies use of ACP 142 over STANAG 5066, which is a general-purpose multicast protocol. This is to support two specific services:

1. Military messaging using STANAG 4406 Annex E. This is as specified in Ed3.
2. SMTP-based messaging using MULE (Multicast Email) as specified in RFC 8494. This can be used to provide both email and military messaging.

IP Client

IP Client, which provides a simple mechanism to run IP over STANAG 5066, is specified in Annex U. The core is identical to Ed3, noting that various unnecessary complexity has been removed and some aspects clarified. Ed4 defines support for IPv6, whereas Ed3 was IPv4 only.

Annex F – SAP Registration

In Ed3, all application protocols are specified in Annex F. In Ed4, Annexe F's primary role is to specify the assignment of protocols to the 16 SAPs that STANAG 5066 allows to specify protocols. This includes all of the applications defined in Ed4, as well as some older applications only specified in Ed3 and XMPP specified in "Server to Server communication over STANAG 5066 ARQ". Ed4 also adds in default priorities for each application, which gives a framework to specify the relative priorities of different applications running over STANAG 5066.

Other Changes

There are a number of other Ed4 changes that are worth noting.

Separate SIS Protocol Specification

The SIS Access Protocol is defined to support applications using STANAG 5066. In Ed3, the specification is split across Annex A and Annex F. In Ed4, it is given its own Annex S. This improves modularity. Looking forward, it provides a framework for anticipated necessary updates to Annex S, which will not impact the core Annex A.

Padding D_PDU

A new Padding D_PDU is added to fill the blank space in a transmission. This improves performance and resilience.

Extension D_PDU

The core data transfer protocol specified in Annex D is limited to 16 different D_PDUs to transfer information. Ed4 makes use of a D_PDU to enable a large number of additional D_PDUs to be added. This framework is used by WTRP and is available for future protocol changes.

General Editing

Some parts of the Ed3 protocol were well specified, and some less so. Ed4 has provided a new introduction, general text improvements, and specifying functionality that is needed but was not included in Ed3.

Profiles

Ed3 was unclear as to which elements of the specification were mandatory and which are optional. Ed4 introduces two concepts to make this clear:

1. Profile Options. These are explicit labels for optional features of the STANAG 5066 layer services. These can be used by vendors to make clear which optional capabilities are offered.
2. Profiles. Each profile specifies a list of profile options and annexes. These are intended as useful combinations. A deployment of STANAG 5066 will generally operate following a single profile.

Things Removed

Ed4 removes a number of things which are not needed moving forward. Two concepts no longer used are:

1. Rank. This was defined, but did not actually do anything.
2. Hard Links. These have not been used and are not useful moving forward.

The following annexes present in Ed3 are removed in Ed4:

1. Annex E: HF Modem Remote Control Interface. This simple interface is not useful for modern modems.
2. Annex G: Use of Waveforms at Data Rates Above 2400 bps. This was folded into the core.
3. Annex H: Implementation Guide and Notes. Useful parts of the annex were folded into other annexes as appropriate.
4. Annex I: Messages and Procedures for Frequency Change. This has been replaced by the new ALE procedures.

Isode's Role in Edition 4

Isode has had a central role in producing STANAG 5066 Ed4, noting that there were useful contributions from other members of the NATO BLOS Comms Technical Group and that Sweden (FMV) led the Ed4 activity.
Isode started to provide input on STANAG 5066 requirements in 2012. This was initially done informally and subsequently by a series of protocol specifications (the STANAG

5066 EP (Extension Protocol) series), which Isode offered as input to NATO. These specifications have provided the core of the new Ed4 functions:

1. The following were the basis for Wideband HF support in Annex C:
   – Data Rate Selection in STANAG 5066 for Autobaud Waveforms (S5066-EP4)
   – STANAG 5066 Large Windows Support (S5066-Ep5)
2. The following were incorporated into Annex C:
   – STANAG 5066 Padding DPDU (S5066-EP2)
   – Advertising Extended Capabilities (S5066-EP7)
   – Extension DPDU (S5066-EP10)
   – Variable C_PDU Segment Size (S5066-EP11)
3. Slotted Option for STANAG 5066 Annex K (S5066-EP6) was added to Annex K.
4. HF Wireless Token Ring Protocol (S5066-EP12) was the basis for Annex L.
5. STANAG 5066 Routing Sublayer (S5066-EP13) was the basis for Annex R.
6. STANAG 5066 TRANSEC Crypto Layer using AES and other Protocols (S5066-EP14) was the basis for Annex T.

Isode originally anticipated that a third party would produce Ed4. Steve Kille, Isode's CEO, became editor of STANAG 5066, and so most of the technical changes in Ed4 were provided by Isode.

Isode Product Support for Edition 4

Most of the technical changes in Ed4 were added to Isode's Icon-5066 product ahead of the standard. Full compliance information is specified here. All of the applications specified in Ed4 are supported by the Isode product set.

What Next?

STANAG 5066 Ed4 provides an important interoperability base for HF communications. Isode sees this as an important step forward from Ed3. However, it is not an end point, and further improvements are anticipated in Ed5.

Isode

www.isode.com

14 Castle Mews, Hampton
Middlesex, TW12 2NP

Secure, Seamless Communication Solutions