STANAG 5066 Edition 5

Isode

This white paper provides an overview of the new capabilities anticipated to be introduced in STANAG 5066, Edition 5.

STANAG 5066 is the NATO Standard HF Link Level protocol, summarized in the Isode white paper STANAG 5066: The Standard for Data Applications over HF Radio. STANAG 5066 Edition 4 is the promulgated (official) version of STANAG 5066. Edition 5 will introduce a substantial number of optional changes. These changes are now stable, and it is anticipated that the formal NATO ratification process will start in early 2026.

This white paper assumes some familiarity with STANAG 5066.

STANAG 5066 Availability

STANAG 5066 specification is NATO UNCLASSIFIED. Edition 3 was publicly distributable. Edition 4 and the drafts of Edition 5 are not publicly distributable but are distributable to selected other nations, including Australia, New Zealand, and Norway. Individuals from these nations and NATO nations may access the specification through a NATO representative.

This white paper provides a publicly distributable summary of the Edition 5 changes.

Edition 3 and Edition 4

Edition 4 introduced two major changes:

1. Support of Wideband HF (STANAG 5069)
2. Use of ALE (Automatic Link Establishment).

There were some other additions and significant restructuring. More details are provided in the Isode white paper STANAG 5066 Edition 4.

Compatibility with Previous Editions

All of the changes in Edition 5 are optional. They build around the core of Edition 4. The option for backwards compatibility with Edition 3 remains, but this is no longer mandatory to support.

Changes to Existing Annexes

This section looks at each of the Edition 4 annexes with non-editorial changes in Edition 5.

Annex A (SIS)

Added an optional performance optimization of client acknowledgement, as the current mechanism is inefficient, although not commonly used. The new mechanism is straightforward and fully backwards compatible.

Annex B (CAS)

An ALE Collision Avoidance Procedure is added to improve resilience.

The ALE Service Definitions are expanded and clarified, primarily to support the new Annex AF. There are no CAS interoperability implications, as service definitions are not normative.

Annex C (DTS)

Added an optional alternative End of Transmission (EOT) approach based on modem block count. There is no protocol change, but this semantic change needs to be agreed a priori by all nodes; a network-wide choice.

Further information is provided in the Isode technical proposal Block Based EOTS (S5066-EP8) on which this change is based.

Annex D (Sync Serial Interface to Modem/Crypto)

This annex is mandatory in Edition 4 and made optional in Edition 5. This is because Edition 5 provides a number of valid options with annexes T and AF to work without annex D.

Annex F (Assignments)

Changes made to reflect new annexes.

Annex S (SIS Access Protocol)

A new optional security layer using TLS and Strong Authentication Security is added. It is specified as a new "Security Layer" profile option so that it can be procured.

A new option framework is specified so that a SIS client can determine which new options are supported by a server. This enables smooth and backward-compatible use of new extensions.

Seven new optional SIS extensions are specified. These are mainly to improve control and monitoring. They will enable significant improvement of some applications.

Extended addressing provides an optional extension to allow more than 16 applications. This change is needed to enable the use of the extended addressing in Annex Q (ACP 142) and applications built on Annex W (SLEP).

Annex T (Encryption Layer)

A number of detailed changes have been made to Annex T. In particular, it adds:

1. Reliable Mode to optimize performance over reliable modems. This is an important optimization for use with modem layers from STANAG 5657 and STANAG 4538 in conjunction with Annex AF.
2. Agreed Key mode to enable working with pre-agreed keys.

Core Annex T is defined as a layer service. This is convenient for Annex T implementation integrated with the STANAG 5066 server. A new protocol interface is defined for interfacing a "crypto box" running Annex T with a modem and red side STANAG 5066. This is helpful when Crypto Box is provided by a third party. A simple protocol is defined for use with crypto/modem and 5066/crypto. It is a simple protocol with TLS security and Strong Authentication. It can support crypto boxes running the Annex T protocol but also works for other crypto protocols.

New Annexes

Edition 5 adds twelve new Annexes, summarized here:

Annex W – SIS Layer Extension Protocol (SLEP)

SLEP provides three key protocol building blocks:

- Reliable Datagram
- Unreliable Datagram
- Streaming Service

SLEP is used by Annexes X, AB, AD, AE, and AH. It is also used by XEP-0365 to provide XMPP chat services over HF.

Further information is provided in the specification "S5066-APP3 SIS Layer Extension Protocol (SLEP)" on which Annex W is based.

Annex X – HF-PEP

HF-PEP provides optimized TCP transfer over HF following the Performance Enhancing Proxy (PEP) model. It is based on the Annex W streaming service. It can support applications such as C2 and Web Browsing over HF.

Details provided in the Isode white paper Providing TCP Services over HF Radio.

Annex Y – IP Crypto

Annex Y enables the use of IP Crypto to encrypt user data. The central approach is that STANAG 5066 runs black side, with all data from the red side going through an IP crypto.

There are two modes. IP Only Mode operates with only IP services being provided red side. This provides a "Compatibility Mode". It is suitable for supporting low-volume traffic.

Full-Service Mode adds a red-side SIS so that all of the STANAG 5066 applications and layer services can be run red-side. It is critical for bulk applications and heavier loads. This mode enables full STANAG 5066 capability. It needs to use Crypto Bypass to work correctly.

- Black to Red is needed for flow control monitoring and correlation.
- Red to Black is needed for modem control.

Details and measurements are provided in the Isode white paper "Using IP Crypto over HF". This work is based on Isode open specifications that are the basis for Annex Y. The model is the same, and measurements are expected to be similar to the results that would be achieved with Annex Y.

Annex Z – IP Optimizations

Annex Z defines two useful (optional) performance enhancements when an IP client is used. Annex Z is primarily intended for use in conjunction with Annex Y.

Annex AA – HF- LISP

HF-LISP (Location and Information Services Protocol) allows the Mobile Unit to report location and related information either by broadcast or point-to-point. It is modelled on AIS (Automatic Identification System) used for Marine traffic. It operates red side and can share an HF link using STANAG 5066.

Further information is available in "S5066-APP10: HF Location & Information Sharing Protocol", which is the open specification on which Annex AA is based.

Annex AB – HF-RIP

HF-RIP (HF Routing Information Protocol) provides a simple HF routing protocol based on the well-known RIP family of protocols. Use of standard IP routing protocols takes too much link capacity. HF-RIP enables operation in MANET-type architecture, which is of growing importance.

Details provided in the Isode white paper "IP Routing Over HF".

Annex AC – Testing and Discovery Protocol

Annex AC provides Simple discovery, ping, and throughput protocols. This supports vendor-independent performance measurements and testing to facilitate demonstration of implementation conformance. Testing with applications or IP can be awkward and gives limited testing, as it uses STANAG 5066 in constrained ways.

Further information is available in "S5066-APP2: HF Discovery, Ping and Traffic Load", which is the open specification on which Annex AC is based.

Annex AD – HFBP

HFBP (HF Broadcast Protocol) follows the ACP 127 BRASS model to provide efficient Broadcast and EMCON support. It provides efficient operation for multiple protocols, including ACP 127; STANAG 4406; SMTP; XMPP.

HFBP fills an important gap in the HF Protocol Suite.

Further information is available in "S5066-APP11: HF Broadcast Protocol (HFBP)", which is the open specification on which Annex AD is based. It gives a rationale for adding this protocol.

Annex AE – File Transfer

HFFTP (HF File Transfer Protocol) specifies a simple file transfer protocol optimized for HF. This capability adds a useful additional component to the HF tool set.

Further information is available in "S5066-APP8: HF File Transfer Protocol (HFFTP)", which is the open specification on which Annex AE is based.

Annex AF – Variable Rate Modem

The core STANAG 5066 approach needs fixed speed modems with speed control and transmission time handled by STANAG 5066.

Annex AF provides a mechanism to support modems different from the "fixed speed" default. The model is that speed is controlled by the modem, and the modem asks STANAG 5066 for data. Annex AF specifies a service interface between STANAG 5066 and modems, which covers both traditional fixed-speed and variable-speed modems.

The annex also specifies a protocol for use between STANAG 5066 and the modem. This protocol is specified using CDDL specified in RFC 8610 "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures". PDUs are encoded in CBOR specified in RFC 7049 "Concise Binary Object Representation (CBOR)".

Key targets for Annex AF are:

- STANAG 4538 using xDL for ARQ. Usage will be specified in a new STANAG 4538 Annex E.
- The new STANAG 5657 waveform uses Packet Protocol for ARQ.

Annex AG – Lightweight DTS

Annex AG Optimizes 5066 ARQ performance when operating over modems that provide ARQ. For example, when using Annex AF with STANAG 5657 Packet Protocol or STANAG 4538 xDL, it avoids duplication of ARQ functionality and improves performance.

Annex AH – UDP PEP

Annex AH specifies HF-UDP-PEP: UDP Performance Enhancing Proxy Protocol. It defines a PEP for UDP (User Datagram Protocol), which is widely used. It provides performance benefits over just using Annex U (IP Client) by:

- Removing the overhead of IP and UDP headers.
- Providing compression.
- Avoiding repetition of addressing information.

Isode's Role in Edition 5

Steve Kille, Isode's CEO, is the editor of STANAG 5066. Isode has provided most of the new specifications in Edition 5 and has validated many aspects in its product set. A number of the new annexes in Edition 5 were initially published by Isode as open specifications and are already shipping in Isode products.

NATO BRIPES Project

The NATO BRIPES (BRASS IP Enhanced Services) is a software package being delivered to NATO for deployment by nations. BRIPES follows the NATO BRE1TA (BRASS Enhancement 1 Technical Architecture). BRIPES is already using two Edition 5 capabilities:

1. The T-Web service uses the Annex X TCP HF Proxy.
2. The T-Chat XMPP service uses the SLEP Streaming Service specified in Annex W.

It is anticipated that more Edition 5 capabilities will be used in due time, as many of the new annexes add capabilities that will be helpful for BRIPES target deployments.

Isode Product Support Edition 5

Isode has added a number of Edition 5 capabilities ahead of standardisation. Compliance information is specified here, which covers both Icon-5066, which is Isode's STANAG 5066 server, and Isode applications that operate over STANAG 5066.

Isode

www.isode.com

14 Castle Mews, Hampton
Middlesex, TW12 2NP

Secure, Seamless Communication Solutions