Isode

Icon-5066 Application Profiles for use with XML Guard

29th January 2024

1 Overview

This white paper specifies two Application Profiles to support use with Isode's Icon-5066 product with an XML Guard. It defines:

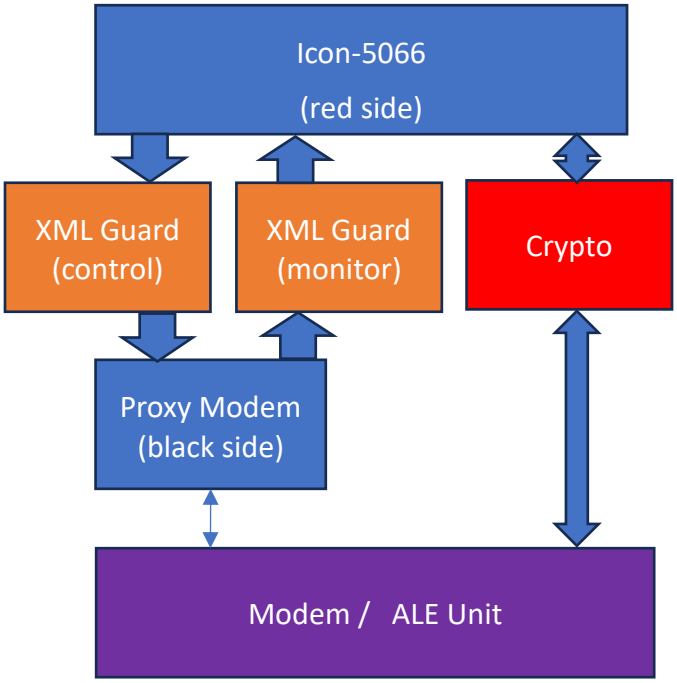
- Schemas for each Application Profile
- Normalization Requirements
- Rules which can be used to constrain the base profiles

Application Profiles are summarized in the Isode white paper "XML Guard Application Profiles". They define a product-independent approach to specify functionality across an XML Guard.

Goals of this specification:

- To provide a clear specification to enable system accreditation of a system using Isode's M-Guard and Isode's Icon-5066 products.
- To enable use of a third party XML Guard with Isode's Icon-5066 product.

2 The Icon-5066 XML Protocols



Icon-5066 is Isode's STANAG 5066 server, providing most functions as a red side product. Data communication with modem (black side) goes through a crypto device.

Proxy Modem is a part of Icon-5066 that sits black side and provides control/monitoring to Modem/ALE units using modem-vendor-specific protocol. It communicates with Icon-5066 through a pair of XML Guards providing control and monitoring flows. There are three broad functions provided:

1. Modem Control. Control of the modem for sending and receiving data. Key functions:
    a. Control: set speed and interleaver before starting a transmission.
    b. Monitoring:
        i. Report SNR on received data
        ii. Report speed and interleaver for received transmissions

2. ALE Unit Control. This is for negotiating outbound and incoming ALE links, which require handshaking. This needs flows of information over both control and monitor links.

3. ALE Unit Configuration. ALE frequencies and addresses can be configured red side. This is important for supporting Mobile Unit mobility, which needs updating of ALE

addressing and scheduling for frequency changes. This configuration information is sent over the control channel when ALE configuration changes.

3 Summary of the Profiles

There are two profiles, one associated with the monitoring flow and the other associated with the control flow.

These profiles are based on XML schemas, which defines the XML messages exchanged and are specified below. The Schemas, specified as an XML Schema Definition (XSD), specify an "outer bound" for what is allowed through the guard.

The associated rules then constrain the schemas, by blocking elements of the schema. This allows the messages being passed to be further constrained.

4 Normalization

Both profiles require the following message normalization:

- Prohibition of XML Comments and XML Processing Instructions.
- Use of Canonical XML. Following Canonical XML Version 1.1 of May 2008.
- Unicode Normalization following UNICODE NORMALIZATION FORMS 13.0.0 using Normalization Form C (NFC) "Canonical Decomposition, followed by Canonical Composition"

5 Isode Icon-5066 Application Profile Products

Isode provides two Application Profile products that follow the two profiles defined in his specification. These profiles enable M-Guard to provide guards compliant to these profiles.

6 Icon-5066 Monitoring Profile

6.1 Black to Red Protection Requirements

The primary security requirement for black to red information flow is to prevent malware or other attacks. The Icon-5066 monitor protocol messages are highly structured XML and this structure is an effective way to prevent malware.

No rules are needed in addition to the base schema.

6.2 Schema

The Icon-5066 Monitoring protocol schema is specified below. It defines the <Icon-5066Monitor/> message sent from black to red.

6.2.1 Example Messages

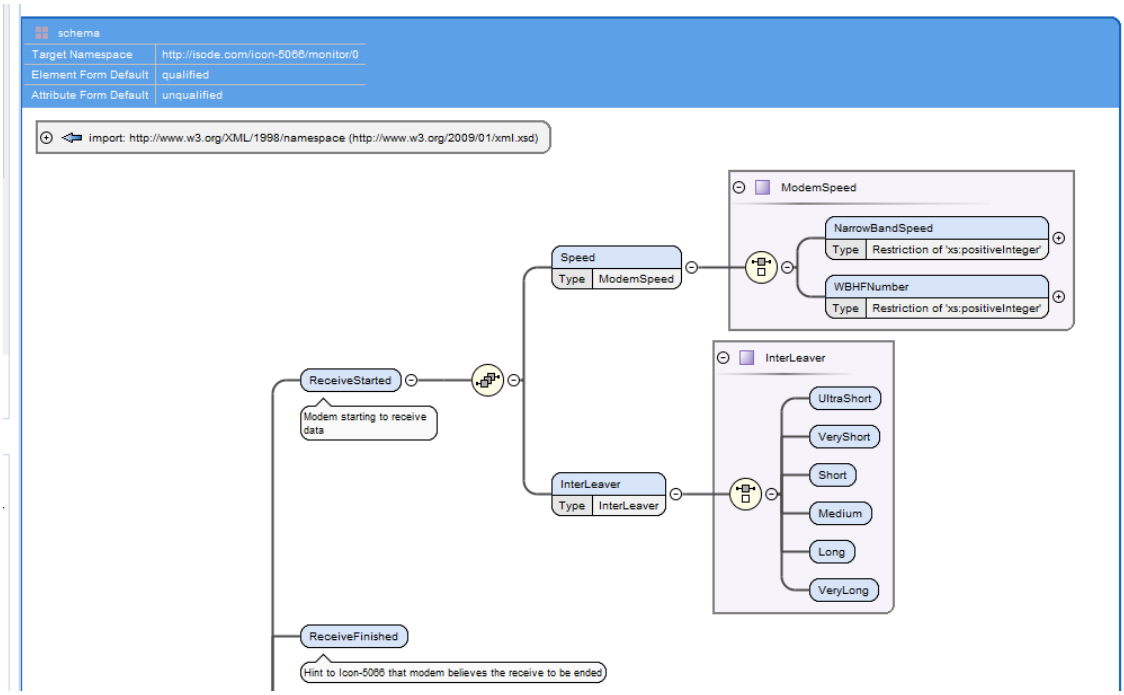
This section shows an example message, correctly normalized following this specification, but folded to make easier to read. This message shows a reported SNR of 5.66. Note that the integer represents SNR*100, so that SNR can be specified to two decimal places.

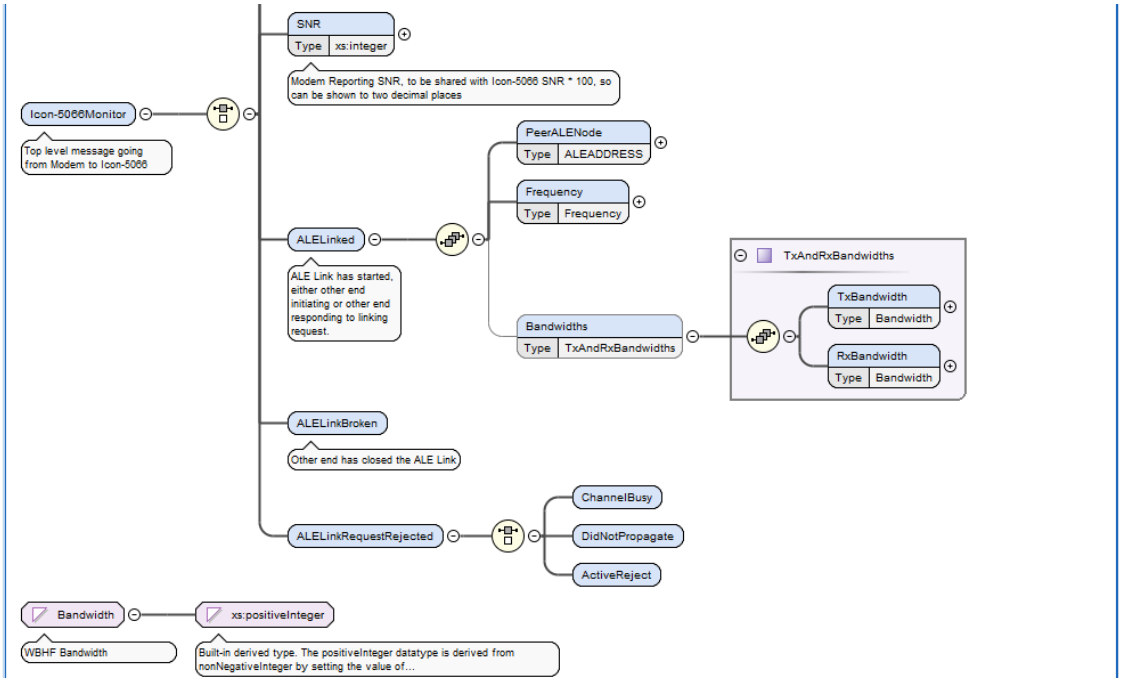
```
<Icon-5066Monitor xmlns="http://isode.com/icon-5066/monitor/0">
<SNR>566</SNR>
</Icon-5066Monitor>
```

6.2.2 Schema Visualisation

This section shows the schema, as visualised by the oXygen XML editor.

This is the overall schema showing structure of the messages





6.2.3 Schema Specification

This is the formal XML Schema Definition:

```
<?xml version="1.0"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://isode.com/icon-5066/monitor/0"

    xml:lang="en" targetNamespace="http://isode.com/icon-5066/monitor/0"

    elementFormDefault="qualified" attributeFormDefault="unqualified">

    <xs:import namespace="http://www.w3.org/XML/1998/namespace"

        schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>

    <xs:element name="Icon-5066Monitor">

        <xs:annotation>

            <xs:documentation>Top level message going from Modem to Icon-5066</xs:documentation>

        </xs:annotation>

        <xs:complexType>

            <xs:choice>

                <xs:element name="ReceiveStarted">

                    <xs:annotation>

                        <xs:documentation>Modem starting to receive data</xs:documentation>
```

```
                    </xs:annotation>
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Speed" type="ModemSpeed"/>
                            <xs:element name="InterLeaver" type="InterLeaver"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="ReceiveFinished">
                    <xs:annotation>
                        <xs:documentation>Hint to Icon-5066 that modem believes the
receive to be ended</xs:documentation>
                    </xs:annotation>
                </xs:element>
                <xs:element name="SNR" type="xs:integer">
                    <xs:annotation>
                        <xs:documentation>Modem Reporting SNR, to be shared with Icon-
5066
SNR * 100, so can be shown to two decimal places</xs:documentation>
                    </xs:annotation>
                </xs:element>
                <xs:element name="ALELinked">
                    <xs:annotation>
                        <xs:documentation>ALE Link has started, either other end
initiating or other end responding to linking request.</xs:documentation>
                    </xs:annotation>
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="PeerALENode" type="ALEADDRESS"/>
                            <xs:element name="Frequency" type="Frequency"/>
                            <xs:element minOccurs="0" name="Bandwidths"
type="TxAndRxBandwidths"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="ALELinkBroken">
                    <xs:annotation>
                        <xs:documentation>Other end has closed the ALE
Link</xs:documentation>
                    </xs:annotation>
                </xs:element>
                <xs:element name="ALELinkRequestRejected">
                    <xs:complexType>
                        <xs:choice>
```

```
                        <xs:element name="ChannelBusy"/>
                        <xs:element name="DidNotPropagate"/>
                        <xs:element name="ActiveReject"/>
                    </xs:choice>
                </xs:complexType>
            </xs:element>
        </xs:choice>
    </xs:complexType>
</xs:element>
<xs:complexType name="ModemSpeed">
    <xs:choice>
        <xs:element name="NarrowBandSpeed">
            <xs:simpleType>
                <xs:restriction base="xs:positiveInteger">
                    <xs:enumeration value="75"/>
                    <xs:enumeration value="150"/>
                    <xs:enumeration value="300"/>
                    <xs:enumeration value="600"/>
                    <xs:enumeration value="1200"/>
                    <xs:enumeration value="2400"/>
                    <xs:enumeration value="3200"/>
                    <xs:enumeration value="4800"/>
                    <xs:enumeration value="6400"/>
                    <xs:enumeration value="8000"/>
                    <xs:enumeration value="9600"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="WBHFNumber">
            <xs:simpleType>
                <xs:restriction base="xs:positiveInteger">
                    <xs:maxInclusive value="13"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:choice>
</xs:complexType>
<xs:complexType name="InterLeaver">
    <xs:choice>
        <xs:element name="UltraShort"/>
        <xs:element name="VeryShort"/>
        <xs:element name="Short"/>
```

```
        <xs:element name="Medium"/>
        <xs:element name="Long"/>
        <xs:element name="VeryLong"/>
    </xs:choice>
</xs:complexType>
<xs:simpleType name="Bandwidth">
    <xs:annotation>
        <xs:documentation>WBHF Bandwidth</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:positiveInteger">
        <xs:enumeration value="3"/>
        <xs:enumeration value="6"/>
        <xs:enumeration value="9"/>
        <xs:enumeration value="12"/>
        <xs:enumeration value="15"/>
        <xs:enumeration value="18"/>
        <xs:enumeration value="21"/>
        <xs:enumeration value="24"/>
        <xs:enumeration value="30"/>
        <xs:enumeration value="36"/>
        <xs:enumeration value="42"/>
        <xs:enumeration value="48"/>
    </xs:restriction>
</xs:simpleType>
<xs:complexType name="TxAndRxBandwidths">
    <xs:sequence>
        <xs:element name="TxBandwidth" type="Bandwidth"/>
        <xs:element name="RxBandwidth" type="Bandwidth"/>
    </xs:sequence>
</xs:complexType>
<xs:simpleType name="ALEADDRESS">
    <xs:annotation>
        <xs:documentation>2-8 Chars uppercase</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
        <xs:minLength value="2"/>
        <xs:maxLength value="8"/>
        <xs:pattern value="[A-Z]*"/>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Frequency">
    <xs:annotation>
```

```
            <xs:documentation>Frequency 3,000 to 30,000 kHz</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:positiveInteger">
            <xs:maxInclusive value="30000"/>
            <xs:minInclusive value="3000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

7 Icon-5066 Control Profile

7.1 Red to Black Protection Requirements

A key security requirement is to prevent leakage of sensitive information from Red to Black. The minimal information contained in the control messages supports this.

Another security concern may be covert channel, where extraneous information in the protocol is used to convey other information. M-Guard Rate Control is a key tool to minimize this risk.

Rules as part of this application can constrain the information further, in order to reduce potential for covert signaling.

It is anticipated that the monitoring protocol will send many attributes from all devices with a wide range of encodings. Control over the red/black boundary will be much more restricted. Only selected devices will be controlled; only selected attributes on those devices will be changed. Generally attributes modified will have a tight syntax (typically integer) and often only a constrained set of values are allowed. Rules are specified to constrain the protocol in this way.

7.2 Rules

This version of the Application Profile defines the following associated rules, that may be enabled to further constrain the base schema. These rules are set out to broadly correspond to the schema order, but grouping related functions together. The choice of rules will be deployment-specific.

The broad goal of rules is to restrict control messages to things that it is deemed necessary to control.

Rule	Notes
Narrowband only	Use for Narrowband only deployments. Blocks messages referencing Wideband parameters (Waveform must not be STANAG 5069; Speed must not reference WBHF Number).
Wideband only	Use for Wideband only deployments. Blocks messages referencing Narrowband parameters. (Waveform must not be anything other than STANAG 5069; Speed must not reference narrowband speeds).

Rule	Notes
Fixed Waveform	Block Modem Initialize message.
No ALE	Blocks all ALE control messages
No ALE configuration	Blocks all ALE configuration messages
Valid ALE Addresses	Specifies a list of valid ALE addresses. Any other ALE addresses will be blocked if this list is set.
Valid Narrowband Speeds	Specified a list of valid Modem Speeds. Any other speeds will be blocked.

7.3 Schema

The Red/Black control protocol schema is specified below. It specifies the <Icon-5066Control/> messages sent from red to black.

7.3.1 Example Messages

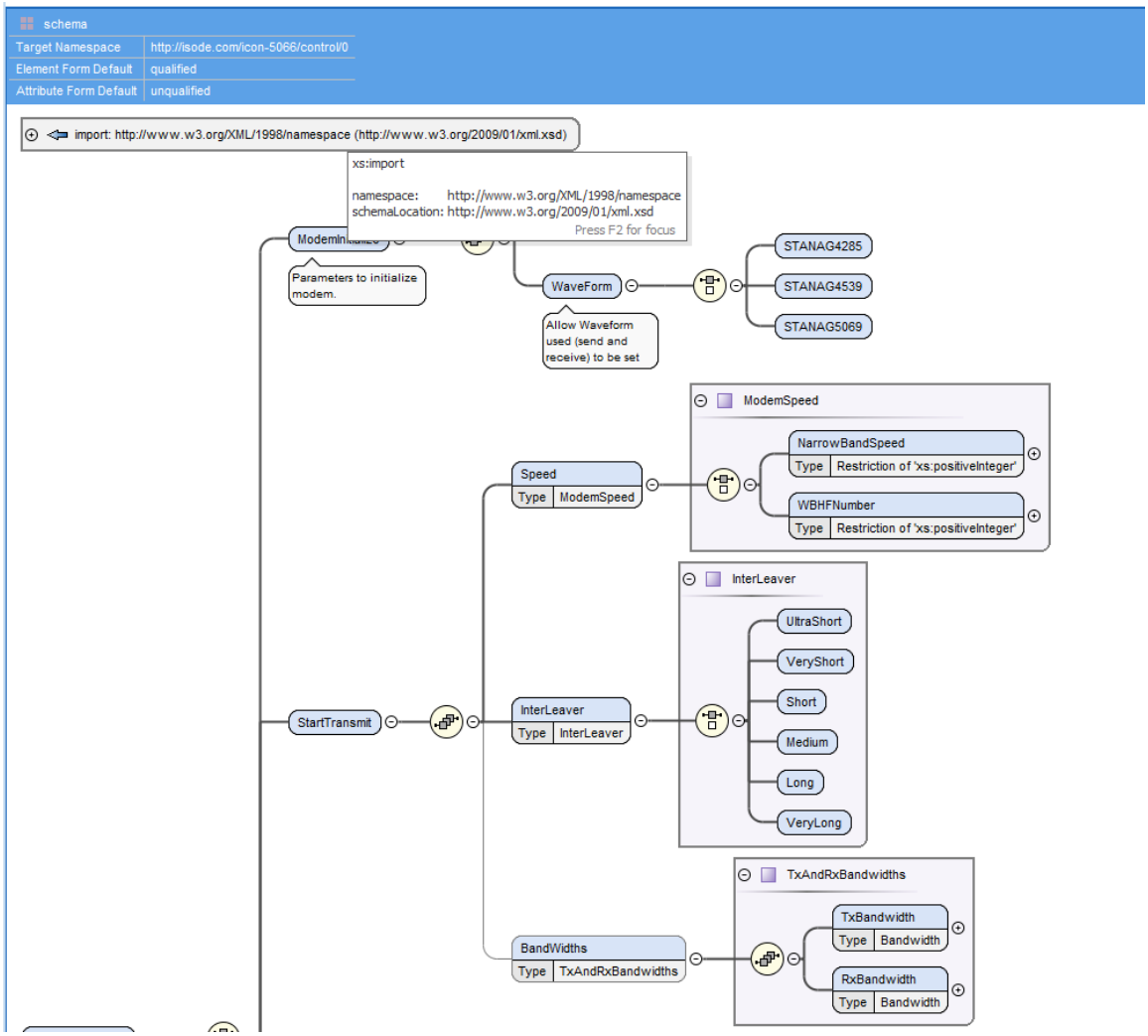
This section shows an example message, correctly normalized following this specification, but folded to make easier to read. This initiates a modem transmission at 1200 bps with short interleaver.

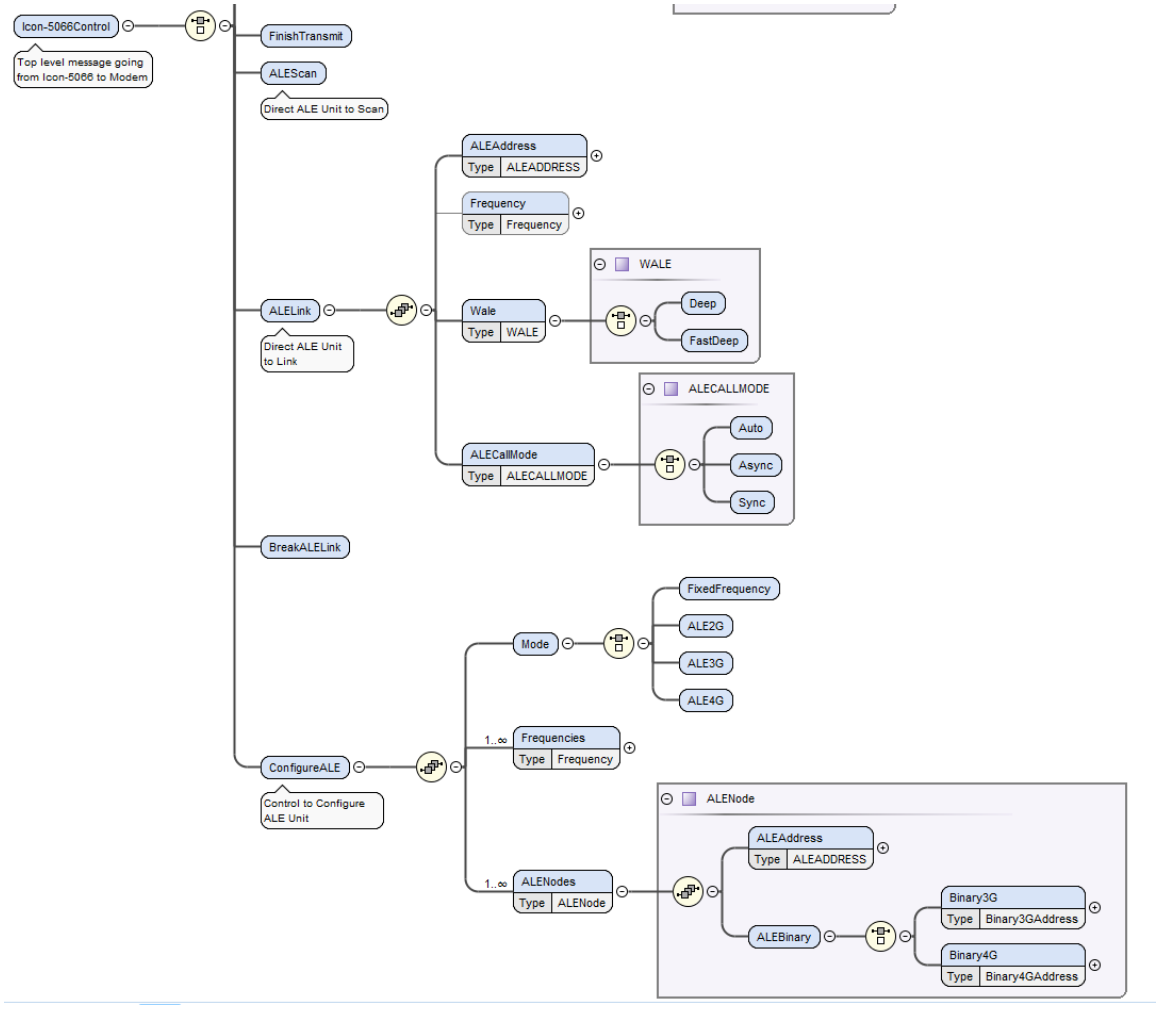
```
<Icon-5066Control xmlns="http://isode.com/icon-5066/control/0">
<StartTransmit>
<Speed><NarrowbandSpeed>
1200
</NarrowbandSpeed></Speed >
<Interleaver><Short></Short ><Interleaver/>
</StartTransmit>
</Icon-5066Control>
```

7.3.2 Schema Visualisation

This section shows the schema, as visualised by the oXygen XML editor.

This is the overall schema showing structure of the messages


schema
Target Namespace
http://isode.com/icon-5066/control/0
Element Form Default
qualified
Attribute Form Default
unqualified
import: http://www.w3.org/XML/1998/namespace (http://www.w3.org/2009/01/xml.xsd)
xs:import
namespace: http://www.w3.org/XML/1998/namespace
schemaLocation: http://www.w3.org/2009/01/xml.xsd
Press F2 for focus
Parameters to initialize modem.
WaveForm
Allow Waveform used (send and receive) to be set
STANAG4285
STANAG4539
STANAG5069
ModemSpeed
NarrowBandSpeed
Type
Restriction of 'xs:positiveInteger'
WBHFNumber
Type
Restriction of 'xs:positiveInteger'
StartTransmit
Speed
Type
ModemSpeed
InterLeaver
Type
InterLeaver
UltraShort
VeryShort
Short
Medium
Long
VeryLong
BandWidths
Type
TxAndRxBandwidths
TxAndRxBandwidths
TxBandwidth
Type
Bandwidth
RxBandwidth
Type
Bandwidth



7.3.3 Schema Specification

This is the formal XML Schema Definition:

```
<<?xml version="1.0"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://isode.com/icon-5066/control/0"
```

```
    xml:lang="en" targetNamespace="http://isode.com/icon-5066/control/0"
    elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xs:import namespace="http://www.w3.org/XML/1998/namespace"
        schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
    <xs:element name="Icon-5066Control">
        <xs:annotation>
            <xs:documentation>Top level message going from Icon-5066 to
Modem</xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:choice>
                <xs:element name="ModemInitialize">
                    <xs:annotation>
                        <xs:documentation>Parameters to initialize
modem.</xs:documentation>
                    </xs:annotation>
                    <xs:complexType>
                        <xs:sequence>
                            <!-- Let us keep init parameters as string for now, we might
need to extract this into single parameters -->
                            <xs:element name="modem_init" type="xs:string"/>
                            <!-- string-encoded table -->
                            <xs:element name="WaveForm">
                                <xs:annotation>
                                    <xs:documentation>Allow Waveform used (send and
receive) to be set</xs:documentation>
                                </xs:annotation>
                                <xs:complexType>
                                    <xs:choice>
                                        <xs:element name="STANAG4285"/>
                                        <xs:element name="STANAG4539"/>
                                        <xs:element name="STANAG5069"/>
                                    </xs:choice>
                                </xs:complexType>
                            </xs:element>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="StartTransmit">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Speed" type="ModemSpeed"/>
                            <xs:element name="InterLeaver" type="InterLeaver"/>
```

```
                        <xs:element minOccurs="0" name="BandWidths"
type="TxAndRxBandwidths"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="FinishTransmit"/>
            <xs:element name="ALEScan">
                <xs:annotation>
                    <xs:documentation>Direct ALE Unit to Scan</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="ALELink">
                <xs:annotation>
                    <xs:documentation>Direct ALE Unit to Link</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="ALEAddress" type="ALEADDRESS"/>
                        <xs:element minOccurs="0" name="Frequency" type="Frequency"/>
                        <xs:element name="Wale" type="WALE"/>
                        <xs:element name="ALECallMode" type="ALECALLMODE"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="BreakALELink">
                <xs:annotation>
                    <xs:documentation/>
                </xs:annotation>
            </xs:element>
            <xs:element name="ConfigureALE">
                <xs:annotation>
                    <xs:documentation>Control to Configure ALE
Unit</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Mode">
                            <xs:complexType>
                                <xs:choice>
                                    <xs:element name="FixedFrequency"/>
                                    <xs:element name="ALE2G"/>
                                    <xs:element name="ALE3G"/>
```

```
                                    <xs:element name="ALE4G"/>
                                </xs:choice>
                            </xs:complexType>
                        </xs:element>
                        <xs:element maxOccurs="unbounded" name="Frequencies"
type="Frequency"/>
                        <xs:element maxOccurs="unbounded" name="ALENodes"
type="ALENode"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:choice>
    </xs:complexType>
</xs:element>
<xs:complexType name="ModemSpeed">
    <xs:choice>
        <xs:element name="NarrowBandSpeed">
            <xs:simpleType>
                <xs:restriction base="xs:positiveInteger">
                    <xs:enumeration value="75"/>
                    <xs:enumeration value="150"/>
                    <xs:enumeration value="300"/>
                    <xs:enumeration value="600"/>
                    <xs:enumeration value="1200"/>
                    <xs:enumeration value="2400"/>
                    <xs:enumeration value="3200"/>
                    <xs:enumeration value="4800"/>
                    <xs:enumeration value="6400"/>
                    <xs:enumeration value="8000"/>
                    <xs:enumeration value="9600"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="WBHFNumber">
            <xs:simpleType>
                <xs:restriction base="xs:positiveInteger">
                    <xs:maxInclusive value="13"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:choice>
</xs:complexType>
```

```
<xs:complexType name="WALE">
    <xs:choice>
        <xs:element name="Deep"/>
        <xs:element name="FastDeep"/>
    </xs:choice>
</xs:complexType>
<xs:complexType name="ALECALLMODE">
    <xs:choice>
        <xs:element name="Auto"/>
        <xs:element name="Async"/>
        <xs:element name="Sync"/>
    </xs:choice>
</xs:complexType>
<xs:complexType name="InterLeaver">
    <xs:choice>
        <xs:element name="UltraShort"/>
        <xs:element name="VeryShort"/>
        <xs:element name="Short"/>
        <xs:element name="Medium"/>
        <xs:element name="Long"/>
        <xs:element name="VeryLong"/>
    </xs:choice>
</xs:complexType>
<xs:simpleType name="Bandwidth">
    <xs:annotation>
        <xs:documentation>WBHF Bandwidth</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:positiveInteger">
        <xs:enumeration value="3"/>
        <xs:enumeration value="6"/>
        <xs:enumeration value="9"/>
        <xs:enumeration value="12"/>
        <xs:enumeration value="15"/>
        <xs:enumeration value="18"/>
        <xs:enumeration value="21"/>
        <xs:enumeration value="24"/>
        <xs:enumeration value="30"/>
        <xs:enumeration value="36"/>
        <xs:enumeration value="42"/>
        <xs:enumeration value="48"/>
    </xs:restriction>
</xs:simpleType>
```

```
    <xs:complexType name="TxAndRxBandwidths">
        <xs:sequence>
            <xs:element name="TxBandwidth" type="Bandwidth"/>
            <xs:element name="RxBandwidth" type="Bandwidth"/>
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="ALEADDRESS">
        <xs:annotation>
            <xs:documentation>2-8 Chars uppercase</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:minLength value="2"/>
            <xs:maxLength value="8"/>
            <xs:pattern value="[A-Z]*"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Binary3GAddress">
        <xs:annotation>
            <xs:documentation>ALE 3G binary address of the node (0-1023)
</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:positiveInteger">
            <xs:maxInclusive value="1023"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Binary4GAddress">
        <xs:annotation>
            <xs:documentation>ALE 4G binary address of the node (0-65535)
</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:positiveInteger">
            <xs:maxInclusive value="65535"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="Frequency">
        <xs:annotation>
            <xs:documentation>Frequency 3,000 to 30,000 kHz</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:positiveInteger">
            <xs:maxInclusive value="30000"/>
            <xs:minInclusive value="3000"/>
        </xs:restriction>
```

```
    </xs:simpleType>
    <xs:complexType name="ALENode">
        <xs:sequence>
            <xs:element name="ALEAddress" type="ALEADDRESS"/>
            <xs:element name="ALEBinary">
                <xs:complexType>
                    <xs:choice>
                        <xs:element name="Binary3G" type="Binary3GAddress"/>
                        <xs:element name="Binary4G" type="Binary4GAddress"/>
                    </xs:choice>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```