A Brief Overview of the ALERT2 Protocol

David Van Wie

Blue Water Design

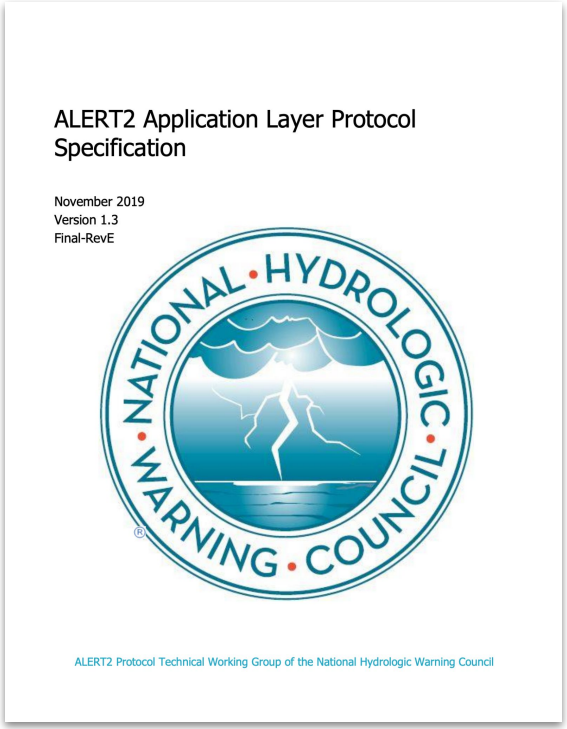
ALERT2 Overview

- ALERT2 is an extremely efficient protocol for transmission of environmental data
- It includes error detection and correction – “good data or no data”
- Designed to work with COTS FM transmitters using TDMA for non-interfering transmissions.
- ALERT2 can be used over cell modem or satellite as well
- ALERT2 is **open protocol** - no vendor lock in!
- Minimal dependence on external infrastructure: transmitters, repeaters, and base stations all communicate over licensed FM frequencies. Minimizes recurring costs and prioritizes reliability.

Protocol Layers

The ALERT2 Protocol consists of four main components:

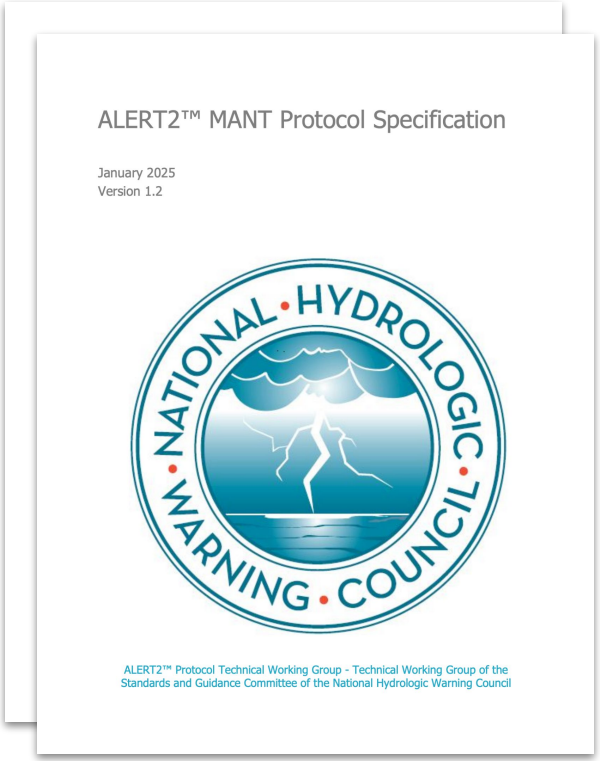
- The **Application Layer** provides a very efficient model for encoding environmental data.



Protocol Layers

The ALERT2 Protocol consists of four main components:

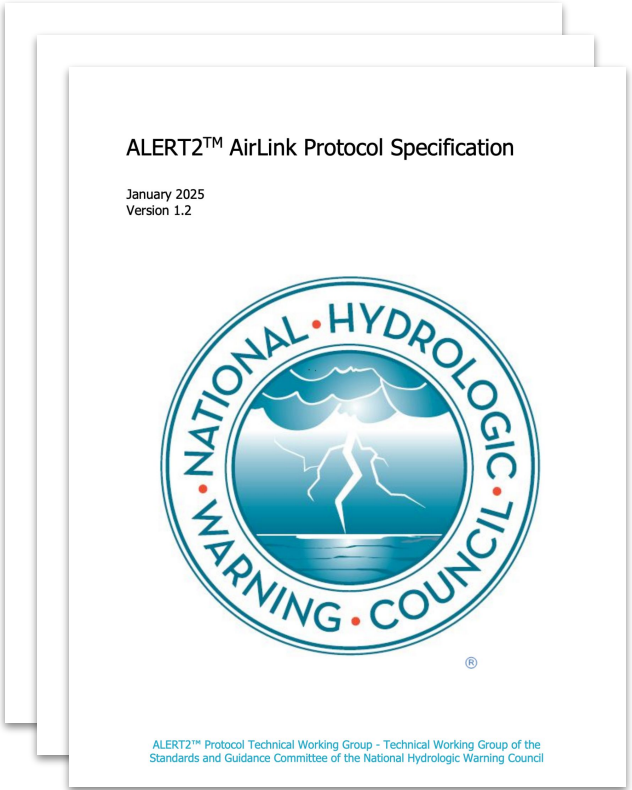
- The **Application Layer** provides a very efficient model for encoding environmental data.
- The **MANT Layer** provides information about how a message navigates the ALERT2 network.



Protocol Layers

The ALERT2 Protocol consists of four main components:

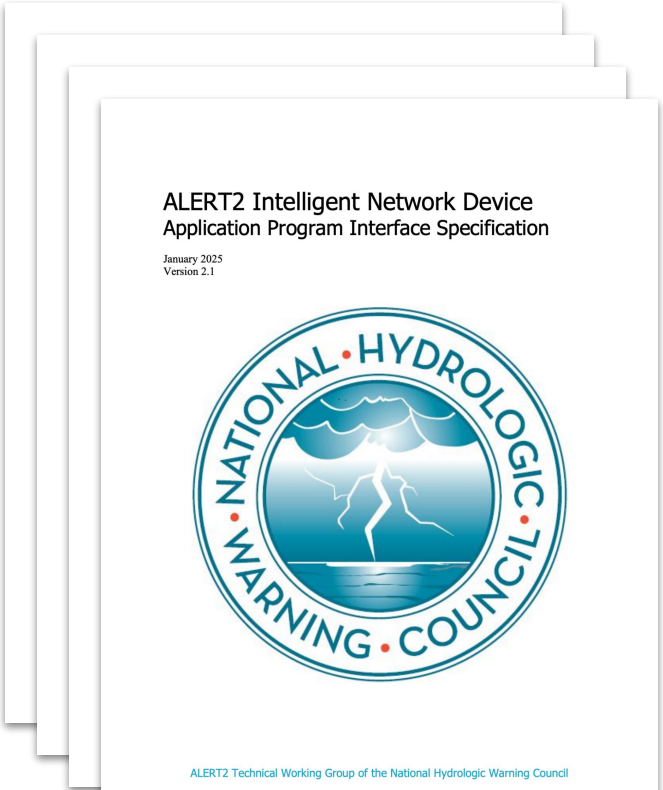
- The **Application Protocol** provides a very efficient model for encoding environmental data.
- The **MANT Protocol** provides information about how a message navigates the ALERT2 network.
- The **AirLink Protocol** defines how to send a message over FM radio.



Protocol Layers

The ALERT2 Protocol consists of four main components:

- The **Application Protocol** provides a very efficient model for encoding environmental data.
- The **MANT Protocol** provides information about how a message navigates the ALERT2 network.
- The **AirLink Protocol** defines how to send a message over FM radio.
- The **IND API** defines how ALERT2 devices communicate with things outside of the ALERT2 network.



Application Layer Introduction

Application Layer messages begin with a “Control Byte” and a timestamp, then contain one or more “reports”. There are several different report types, and they contain the actual measurement data.

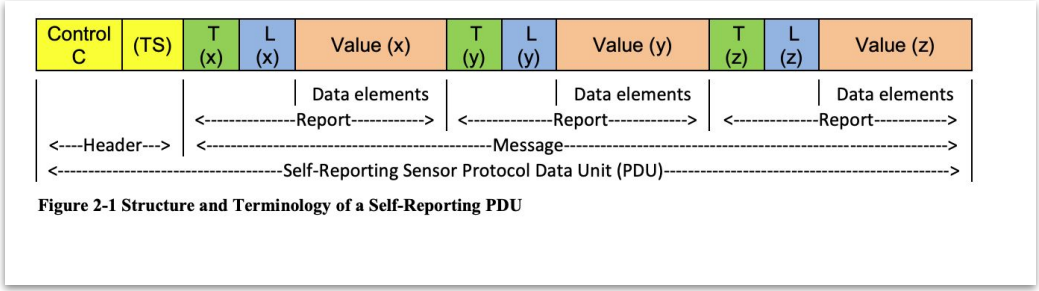
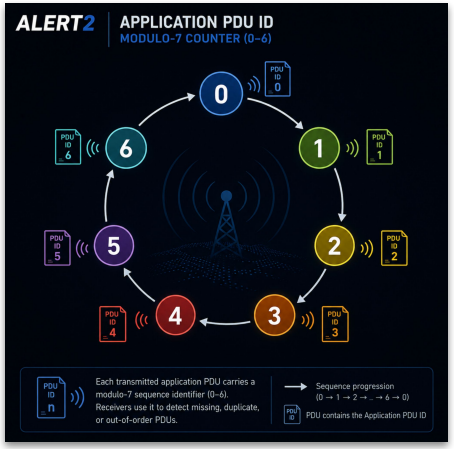


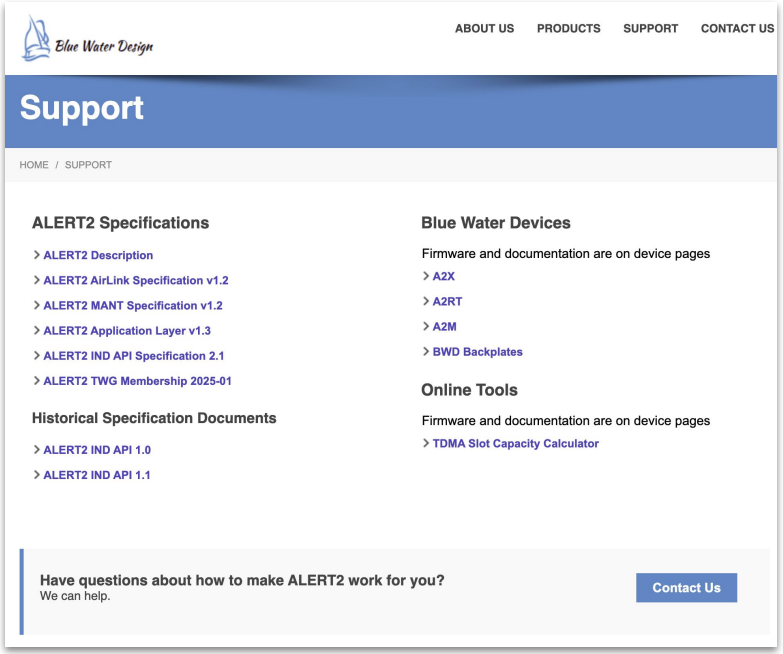
Figure 2-1 Structure and Terminology of a Self-Reporting PDU

The control byte contains an “Application PDU ID” which we can at the base station to identify missing messages.



Message Types

1 - General Sensor Report (GSR)
2 - Tipping Bucket Rain Gauge Report (TBRG)
3 - Multi-Sensor Report - English Units (MSR3)
4 - Multi-Sensor Report - Metric Units (MSR4)
5 - Status Report (MSR5)
7 - Time-Series Data Report (TSD)



Message Types: General Sensor Report

Pros
- Flexible

Cons
- Less efficient
- Easy to misconfigure

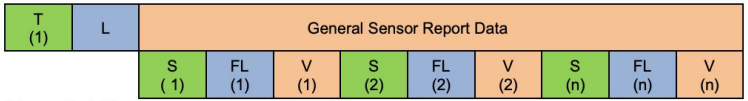


Figure 2-4 General Sensor Data Report

2.2.1 General Sensor Report Sub-Structure

• Report Type (T)	1 byte application layer Message identifier as defined above
• Report Length (L)	1 or 2 byte unsigned integer as defined above
• Sensor ID (S)	1 byte
• Value Format/Length (FL)	1 byte
• Report Value (V)	as specified in Value Format/Length

Pitfalls
- Sending stage using an integer type (insufficient resolution)
- Sending signed data using an unsigned type (what happens when air temperature goes below zero?)
- Sending full weather station data using 4-byte floating points (48 bytes vs 12 for MSR3)

Message Types: Tipping Bucket Rain Gauge Report

Pros
- Receive every tip

Cons
- Variable message length
- Long messages with 0.01” buckets

Figure 2-7 Tipping Bucket Rain Gage Report

Report Sub-Structure:

• Report Type (T)	1-byte application layer message identifier , value 2
• Report Length (L)	1 or 2 bytes, as defined in 2.1.4
• Sensor ID (S)	1 byte
• Value Format/Length (FL)	1 byte, as defined by 2.2.3
• Accumulator value (Accum)	as defined by the FL Field
• Time Offsets (TO)	1 byte (each)

Pitfalls
- Small TBs, high rainfall intensities, and a busy repeater network create a potential congestion problem. Usually ok with bigger tipping buckets, direct paths, or uncrowded repeaters

Message Types: Multi-Sensor Report

Pros
- Very efficient
- Preconfigured with good defaults
- Usually the right answer

Cons
- Inflexible

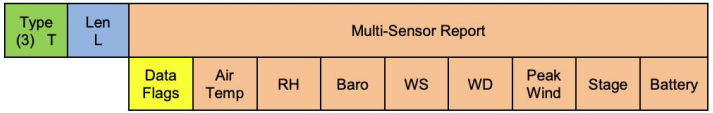


Figure 2-8 Multi-Sensor Report

2.4.1 Report Sub-Structure:

• Report Type (T)	1-byte application layer message identifier, value 3
• Report Length (L)	1 byte unsigned integer
• Data Flags	1 byte representing 8 data flags
• Measurement Suite Variable	number of bytes carrying data from 8 optional sensor types

Sensor	Bytes	Format	Resolution	Units
Air Temperature	2	Signed Integer	0.1	deg F
Relative Humidity	1	Unsigned Integer	1	%
Barometric Pressure	2	Unsigned Integer	0.1	hPa
Wind Speed	1	Unsigned Integer	1	mph
Wind Direction	2	Unsigned Integer	1	deg
Peak Wind	1	Unsigned Integer	1	mph
Stage	2	Signed Integer	0.01	ft
Battery Voltage	1	Unsigned Integer	0.1	V

Figure 2-9 Type 3 Measurement Suite

Sensor	Bytes	Format	Resolution	Units
Air Temperature	2	Signed Integer	0.1	deg C
Relative Humidity	1	Unsigned Integer	1	%
Barometric Pressure	2	Unsigned Integer	0.1	hPa
Wind Speed	2	Unsigned Integer	1	km/hr
Wind Direction	2	Unsigned Integer	1	deg
Peak Wind	2	Unsigned Integer	1	km/hr
Stage	3	Signed Integer	0.001	m
Battery Voltage	1	Unsigned Integer	0.1	V

Figure 2-10 Type 4 Measurement Suite

Message Types: Status Report

Pros

- Efficient
- Preconfigured with good defaults
- Usually the right answer

Cons

- Not available on all transmitters

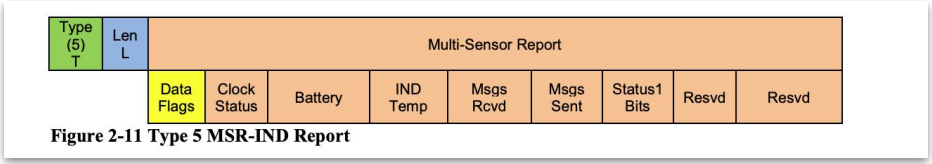


Figure 2-11 Type 5 MSR-IND Report

Sensor	Suggested Sensor ID	Bytes	Format	Resolution	Units
Clock Status	201	1	Unsigned Integer	•	See clock status table
Battery Voltage	8	1	Unsigned Integer	0.1	V
IND Temperature	202	2	Unsigned Integer	0.1	Deg C
Messages Received	203	2	Unsigned Integer	1	Accumulator Value
Messages Sent	204	2	Unsigned Integer	1	Accumulator Value
Status Bits	205	1	Unsigned Integer	-	See status bits table
Reserved	-	-	-	-	-
Reserved	-	-	-	-	-

Figure 2-12 Type 5 Measurement Suite

The MSR5 report is a status report and may not be “user configurable” in the same way that other reports are.

Message Types: Time Series Report

Pros

- Efficient way to send time series data

Cons

- Not a typical ALERT2 use case
- Not widely supported

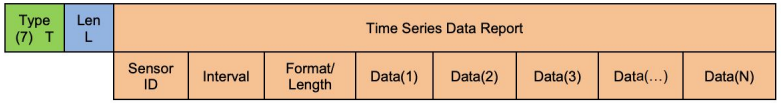


Figure 2-15 Time Series Data Report

2.5.1 Report Sub-Structure

Report Sub-Structure:

• Report Type (T)	1-byte application layer message identifier, value 7
• Report Length (L)	1 or 2 bytes, as defined in 2.1.4
• Sensor ID (S)	1 byte
• Interval	1 byte, as defined in 2.5.3
• Value Format/Length (FL)	1 byte, as defined by 2.2.3
• Data(1) – Data(N)	1 to N Time Series Data Elements

Application Layer Closing Thoughts

Why do we care about message length so much?

What are some things to consider when configuring a remote transmitter?

Application Layer Closing Thoughts

Why do we care about message length so much?

- **Repeater capacity is limited!**
- **Shorter messages are more likely to be received correctly over RF links**
- **Suitable for user over tightly metered links (e.g., satellite)**

What are some things to consider when configuring a remote transmitter?

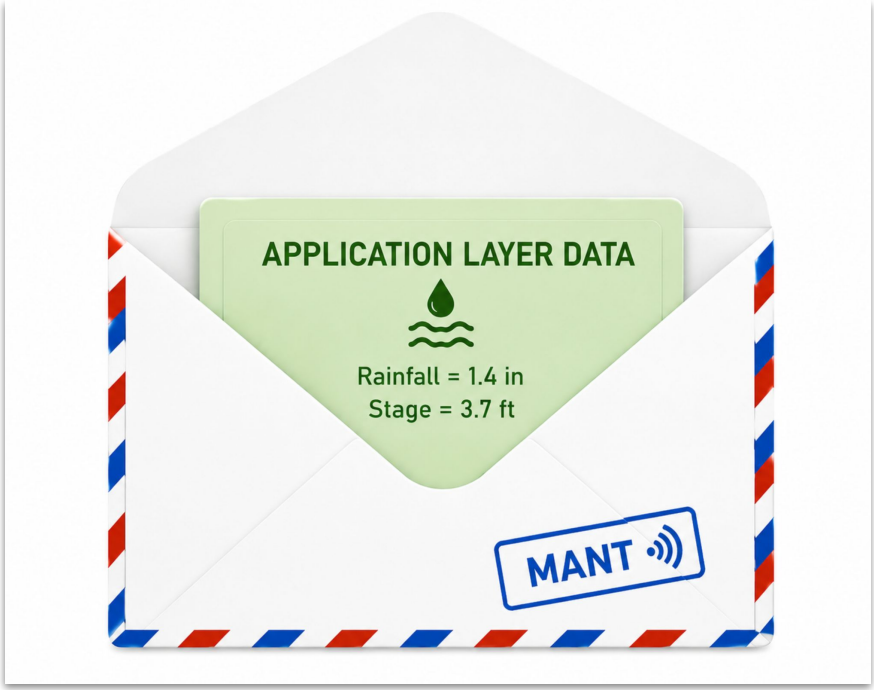
- **Data resolution**
- **Measurement and transmit frequency**
- **Transmit offset**
- **Typical and maximum message length**

MANT Layer

The MANT layer acts like an envelope around the application layer data, providing metadata about how to route and process the message as it traverses the ALERT2 network.

For typical use cases, there are few key fields in the MANT layer that are worth understanding.

The ALERT2 hardware typically handles creation of the MANT headers, and the user only needs to set a few configuration options.



MANT Layer: Header Structure and Key Fields

Key Fields:

Source Address - The address of the site sending the message.

Hop Limit - How many repeaters this message can pass through. Each time this message goes through a repeater, hop limit is decremented. When it reaches 0, it's no longer repeated.

Add Path Service Request - When enabled, repeaters will add their address to the outgoing MANT when repeating it. Valuable for system health analysis

Field Name	Field Length (bits)	Description
Version	2	Current version is $0x0^2$; used for backward compatibility
Protocol ID	3	Network Protocol requested: best efforts, broadcast = 0; end to end reliable datagram service = 1.
Time Stamp Service Request flag	1	No TS service requested = 0; TS service requested = 1.
Add Path Service Request flag	1	No Add Path Service requested = 0; Add Path Service Requested = 1.
Destination Address (DA) included in header	1	MANT header is not extended to include a 16 bit Destination Address = 0; MANT header contains a 2 byte Destination Address immediately following the Source Address (SA) field.
Port	4	The Application or MANT protocol port number.
Encrypted Payload	1	Payload is not encrypted = 0; Payload encrypted = 1.
Reserved Bits field	2	Reserved for future use: encoded as 0x0 in Version 0.
ACK flag	1	Used to acknowledge a MANT PDU for End to End Reliable Datagram Service
Added Header flag	1	Provided for extensibility; MANT Payload begins immediately following the MANT header = 0; Additional header begins immediately following the MANT header.
Hop Limit	3	The maximum hops before the MANT PDU is discarded; when set to 0x7 the PDU is never discarded.
Payload Length	12	The MANT payload length in bytes.
Source Address	16	The Source Address of the originating IND.
[Destination Address]	[16]	When the DA included flag is set, this is the appended Destination Address.
[MANT PDU ID field]	[8]	MANT PDU ID field must be included when End to End Reliable Datagram Service Protocol ID is requested.
[Number of Added Source Address]	[8]	When the Add Path Service Request bit is set, this counter must be the number of 2 byte SAs appended to the header.
[Source Address list]	[N*16]	The list of appended Source Addresses when the Add Path Service Request bit is set. N is the "Number of Added Source Addresses" field. Note: this field will not exist if N = 0.

Figure 2-2 MANT header field Name, Length and Description

MANT Layer: Practical Thoughts

In the typical use case, the ALERT2 equipment will handle most of the MANT work.

If you have repeaters in your network, it's worth checking that **Hop Limit** is set appropriately, especially if you have multi-hop repeater networks.

I suggest enabling **Add Path Service Request** as a default because it removes any ambiguity for system and message analysis tools.

Command and control applications will make use of **Encryption** and **Destination Address** functionality. The legacy ALERT Concentration Protocol is indicated by use of the **Port** flag.

Additional Q & A

Audience Questions?

Thank you!

Thank you!

Thanks for your interest in ALERT2!

David Van Wie

Blue Water Design