TEK 880 LTE Radar Level Sensor

Edit History

Date	Edited by	Description
6/6/2/23	S Normoyle	First edit
22/6/23	D Lintzgy	Amendments
23/6/23	S Normoyle	Updates
3/7/23	Danny Lintzgy	Further updates

Contents

1. Product Description

The TEK 880 LTE "free space" Radar Level Sensor is a flexible and configurable battery-operated distance sensor with integrated Cellular modem supporting GSM (2G), LTE-CAT M1 & NB-IoT networks. The TEK 880 utilises pulse radar technology to accurately measure tank ullages in the range 8cm to 6.75m and communicates this information in a binary payload message to a remote server via a TCP connection.

The sensor contains a reed switch for activation and initiating manual measurements and a Bluetooth Low Energy (BLE) module for interacting with the device during installation. The device provides feedback to the user via a buzzer.

1.1 Abbreviations/Definitions

The following is a list of terms that may be found in this document.

RSSI	Received Signal Strength Indicator
SRSSI	Radar Received Signal Strength Indicator
RRC	Radar Results Code
CRC	Cyclic Redundancy Check
RTC	Real Time Clock
HW	Hardware
FW	Firmware
Ack	Acknowledgement from the server
Message	The data packet / payload / datagram sent across the network
MSB	The Most Significant Bit is the left-most bit in the string
Payload	Data transmitted between sensor and network
0x	Identifies the number as hexadecimal. Note: numbers are assumed decimal unless specified otherwise.
0b	Identifies the number as binary. Note: numbers are assumed decimal unless specified otherwise.
Unsigned byte	Will only allow you to represent numbers in the positive range
Signed byte	Will allow you to represent numbers both in the positive and negative ranges
IoT	Internet of Things
Dormant	Dormant units are inactivated to ensure the longest battery service life
POR	Power Out Reset
BOR	Brown Out Reset
BLE	Bluetooth Low Energy
PLMN	Public Land Mobile Network (Combines of MCC and MNC)
MCC	Mobile Country Code
MNC	Mobile Network Code
RAT	Radio Access Technology
Server	Network endpoint/server where payload data is received
Ullage	The distance from the underside of the sensor to the surface of the liquid.
Blind-zone	The area < 14cm where conventional radar scanning is problematic. Requires blindzone scanning to be enabled.

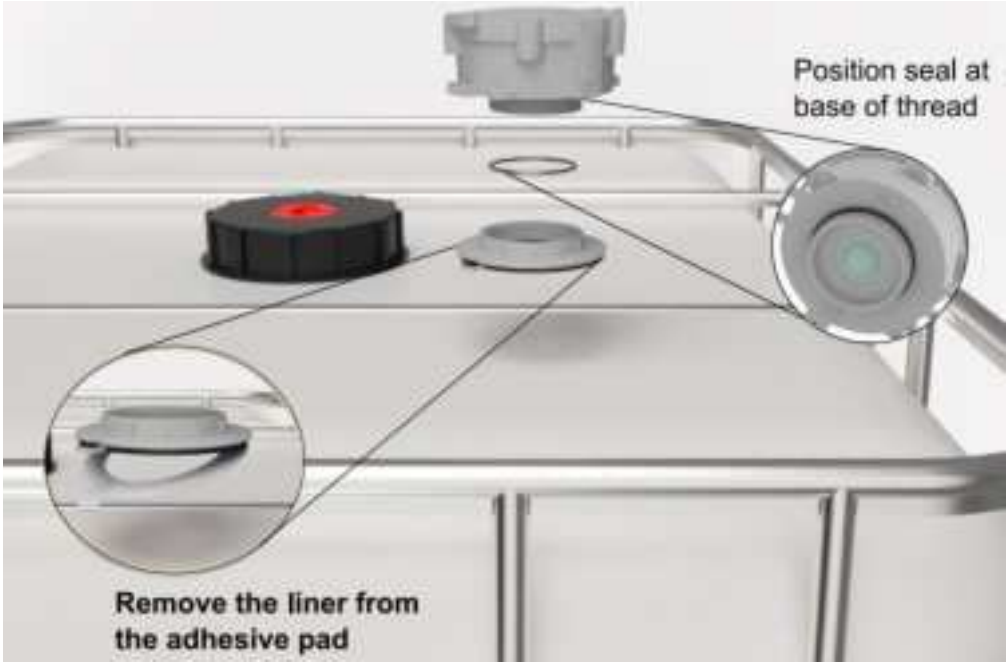
2. Installing the device

The device has a 2” BSP thread opening to allow it to be screwed into the traditional 2” opening which is present on many tanks. This application is known as an invasive measurement as the device requires a pre-drilled hole to gain direct access to the liquid surface.

If the 2” opening is not available and the tank is made of plastic, it is possible to use a threaded adapter to attach to the top of the tank and screw in the device. This application is known as a non-invasive measurement as no pre-drilled holes are required. However, this solution will only work with plastic bodied tanks without any obstructions beneath the sensor.
It is also strongly advised to avoid this application when measuring aqueous liquids due to problems with condensation that can build up on the underside of the tank body.

Conventional attachment into a 2” threaded adapter (invasive)

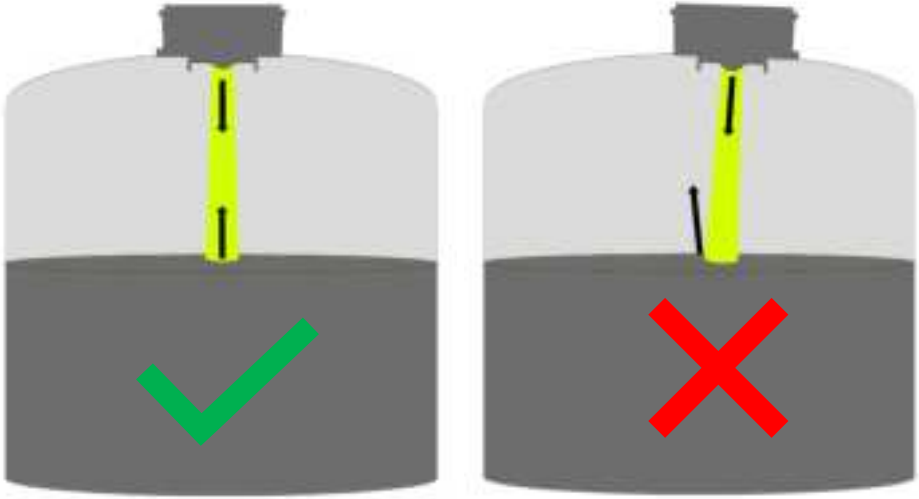
Using the threaded adapter (non-invasive).



2.1 Sensor Alignment

The Radar sensor itself transmits a narrow “beam” of high frequency energy directly downwards towards the surface of the liquid. The energy is then “reflected” back towards the radar sensor and the time of flight is measures in order to determine the distance.

In order to maximise the quality of the radar reflection, as well as to minimise any potential erroneous readings it is essential the sensor is seated flat above the surface of the liquid, located in a central location within the tank and is free from any obstructions such as reinforcing bars.



2.2 Interacting with the device

The device has a magnet sensor located just below the “Tekelek” logo. Hold a magnet across this logo for > 1 second to initiate Bluetooth (BLE) mode. It is then possible to use a smartphone app to perform the requisite steps to activate the device.

Typically, the activation process is as follows:

1) Install sensor onto tank
2) Connect to sensor via BLE App.
3) Set Tank Height
4) Perform test measurement
5) Perform test cellular connection to server
6) Activate device

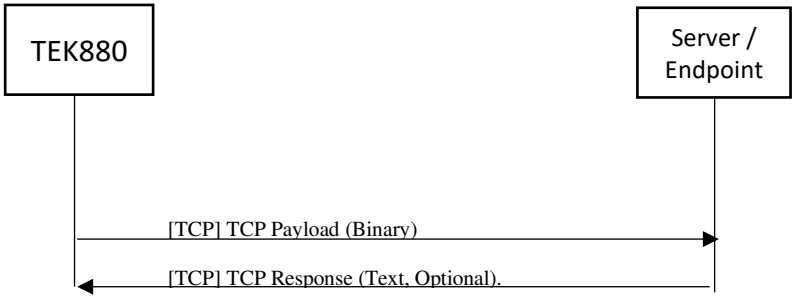
Please see *Radar Installation and User Guide* for more information.

3. Data Payloads and responses

The TEK880 sends its data payloads to a server endpoint using a URL and Port pre-configured into the device at production.

Each time the server receives a payload, it has the option to send one or more responses to the device. These responses may include changing the current time, connection schedule or changing the height of the liquid tank.

For more information on the types of response that can be sent to the device, please refer to section 4 for more information.



3.1 Message Type Overview

Message Type	Description
Message 32	**Diagnostic Data** A message 32 contains raw measurement data, typically used when investigating problems with the radar sensor. This message should only be used by engineers.
Message 34	**Standard Payload Message** The standard message 34 payload contains up to 28 readings with intervals determined by the Logger Speed parameter. The time and day of connection is determined by the Scheduler configuration.

Message 36	**Dump all Settings.** A message type 36 can be requested from the sensor with the command R1=02. A message type 36 sends the contents of the S registers (and may be truncated to 140 bytes if configured to send data via SMS). The response to R1=02 is the full settings starting from S0
Message 38	**Unscheduled payload (Alarm or Install)** A message type 38 is an unscheduled message, typically due to a distance level threshold being broken, or during the installation process when the device is being commissioned.
Message 40	**Ack / Nack message** A message type 40 is sent in response to an Over The Air (OTA) firmware update event. It will notify the server of a successful or unsuccessful update even.
Message 42	**Device info** Contains basic information about the device such as the number of resets and counts of message deliveries/failed deliveries and power consumption.
Message 44	**ICCID and modem information.** A message type 44 contains the cellular modem information such as firmware version and sim card numbers.
Message 47	**GPS details.** A message type 47 contains the GPS data retrieved from the device just prior to the data being sent to the server.

Basic structure of the payload message

Message Header (36 Bytes)	Contains IMEI number, message number, status flags, battery status and other indications.
Payload (Length Varies)	Contains the actual payload data. See message descriptions for more information.
CRC (2 bytes)	2-byte CRC-16 XMODEM/CCITT

3.2 Message header

Each message type is preceded with a common message header, which contain critical information about the device and its operational characteristics.

Sample Payload in Hexadecimal.

The message header is displayed in grey. In this example a message 34 was sent.

22050A0100000D176008610590675550230109082 76E0010190D96C7D100000F162200B20217060C0E000000000
00100192A009101001724009301001 72A00920100172A009200000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000016D7

Byte overview of message header

Byte#	Value (HEX)	Description	Notes	Result
0	22	Defines the product type	0x22 HEX = 34 Decimal	TEK880
1	05	Defines the Hardware Revision		PCb Revision 5
2	0A	Defines the Firmware Revision	Minor 4 bits = FW Major Revision Major 4 bits = FW Minor Revision	0.10
3	01	Defines the reason for contact		Scheduled
4	00	Defines the Status of Alarms	Limit 1, Limit 2 and Limit 3 flags.	No alarms set

5	00	N/A	Not implemented	
6	0D	Defines additional Status Flags	Contain flags relating to the current status of the device such as the GSM connection type	RAT = 2G GSM Roaming RTC Set Device active
7	17	Defines modem Signal Strength	Converts to signed byte (-127 -> 127)	-23dBm
8	60	Battery Remaining percentage	Converts to unsigned byte, limited 0 – 100%	96%
9 - 16	0861059067555023	Defines the IMEI number	Binary Coded Decimal (BCD) Format	IMEI: 086105906755 5023
17 & 18	0109	Message Count	Count of all outgoing messages	265
19 & 20	0827	Energy Used (ENU)	Count of energy used In Milliamps / Second from the previous upload	2087 mA/s
21	6E	RTC Hour / Try Tickets	Count of how many attempts it took to send the message in upper 3 bits Current RTC hours in lower 5 bits	3 Tries 14 Hours
22	00	RTC Minutes	Convert to Decimal	00 Minutes
23	10	RTC Seconds	Convert to Decimal	16 Seconds
24	19	Ambient Temperature	Converts to signed byte (-127 -> 127)	25 °C
25 & 26	0D96	Battery Voltage	Minimum voltage of battery, saved at end of previous data drop	3478mV
27 & 28	C7D1	Settings CRC	CRC of current Settings String. Can be used to compare settings integrity to known device configuration	CRC = 0xC7D1
29 & 30		N/A	Not implemented	
31	0F	Radar Firmware version	Minor 4 bits = FW Major Revision Major 4 bits = FW Minor Revision	Version 0.15
32	16	Simplified accelerometer orientation	Simple number indicates how flat the sensor is mounted.	22
33	22	Message Type	Message type	Message 34 (Normal measurement)
34 & 35	00B2	Payload Length	Number of bytes in the payload not including the message header	178

3.2.1 Product type

Product	Product ID (Hexadecimal)
TEK880 Radar sensor	0x22

3.2.2 Contact Reason

Byte 3 Binary breakdown for contact reason:

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
N/A	N/A	N/A	Reboot	Manual	Server Request	Alarm	Scheduled

- Bit 7 – 5 N/A – Read as 0
- Bit 4 Reboot
  - 0 = No reboot occurred.
  - 1 = Reboot caused this data payload.
- Bit 3 Manual
  - 0 = No manual connection occurred.
  - 1 = Manual connection occurred via Reed Switch or via BLE App command.
- Bit 2 Server Request
  - 0 = No server request

- 1 = Previous request from the server via an “R” command.

- Bit 1 Alarm
  - 0 = No alarm event occurred
  - 1 = Limit Alarm threshold broken, active alarm generated
- Bit 0 Scheduled
  - 0 = No scheduled contact
  - 1 = Scheduled contact

Note - Only one of these flags can be set at any one time.

3.2.3 Alarms

The alarm status register indicates the cause of any alarm event. There are three alarm flags which correspond to the three threshold alarms described in section 0.

Byte 4 Binary breakdown for alarm status:

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
N/A	N/A	N/A	N/A	N/A	Alarm flag Limit3	Alarm flag Limit2	Alarm flag Limit1

- Bit 7 – 3 N/A – Read as 0
- Bit2 Alarm flag Limit3.
  - 0 = Limit 3 alarm not set.
  - 1 = Limit 3 alarm set.
- Bit1 Alarm flag Limit2.
  - 0 = Limit 2 alarm not set.
  - 1 = Limit 2 alarm set.
- Bit0 Alarm flag Limit2.
  - 0 = Limit 1 alarm not set.
  - 1 = Limit 1 alarm set.

Note – It is possible for more than one alarm flag to be set at any time if the measurement breaks more than one threshold limit.

Note – The alarm flags can be set due to an active or passive alarm condition depending on whether the alarm enable flag is set in the alarm threshold parameter. Check the status flag to indicate whether the alarm is generated via an active alarm condition, or whether the alarm flag is set via a scheduled data payload.

3.2.4 Status Flags

This section describes other important status values such as the device active state and the Radio Access Technology (RAT) used to send the payload.

Byte 6 Binary breakdown for additional status flags

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
N/A	N/A	RAT		Roaming	Real Time Clock Set	Reserved	Active

- Bit 7 & 6 N/A - read as 0
- Bit 4 & 5 RAT – Radio access technology (for current connection).
  - 0 = 2G GSM/EDGE

- 1 = LTE NB-IoT
- 2 = LTE CATM1

- Bit 3 Roaming (for current connection)
  - 0 = device is registered to the home cellular network.
  - 1 = device is registered roaming on the cellular network.
- Bit 2 Real Time Clock Set.
  - 1 = RTC value has been set by server (usually via a response to an uploaded message).
  - 0 = RTC value not set (typically occurs after the device has rebooted and has not retrieved a new RTC value).
- Bit 0 Active.
  - 0 = Device is essentially dormant. The scheduler is not operational and the device will not connect to the server unless explicitly instructed.
  - 1 = Device has been activated. The scheduler will instruct device to connect to server according to its configuration.

3.3 Cyclic Redundancy Check (Payload)

Each message payload is terminated by a 16-bit Cyclic Redundancy Check (CRC) which is derived from the preceding data payload. This allows the server to validate the integrity of the payload.

CRC Details:

- Type – CRC-16/XMODEM (CCITT)
- Initial value – 0x0000 (x16+x12+x5+1)
- Polynomial – 0x1021

Sample payload (Message 40) with the corresponding CRC-16 appended to the end.
2201050474001D5D0008697380692887640 0E938C06B3201000D3F9EF80000006C280002080 1580B

```
//https://crccalc.com/ use xmodem CRC16
uint16_t host_crc_calc(char *buffer, uint16_t length){
	uint16_t i;
	uint16_t crc_calc = 0;

	for(i=0; i<length; ++i){
		crc_calc  = (uint8_t)(crc_calc >> 8) | (crc_calc << 8);
		crc_calc ^= buffer[i];
		crc_calc ^= (uint8_t)((crc_calc & 0xff) >> 4);
		crc_calc ^= (crc_calc << 8) << 4;
		crc_calc ^= ((crc_calc & 0xff) << 4) << 1;
	}
	crc_calc &=0x0000FFFF;
	return crc_calc;//CRC-16/XMODEM
}
```

3.4 Message 32 – Diagnostic payload

Message 32 is an extended measurement payload. It contains the same results are a primary payload, but with additional raw data which may be used by engineers to diagnose any issues that may have occurred. This is particularly useful in measurement environments where there is evidence of multiple erroneous signals or internal tank obstructions detected.

The payload consists of a single distance reading which is chosen from the accompanying raw distance and amplitude data (up to 8 individual samples).

Message Initiation:

- Sent via "R6=01" via a payload response or BLE command.

Payload breakdown:

- Message header – Common header precedes all message types See section 0 for more details.
- Distance reading – For more information on the contents of the distance reading, see Distance reading 3.5.2
- Raw Data (up to 8 occurrences)– For engineering use only.
    - Raw Ullage 1..8 – The raw distance measurement. Not necessarily the selected reading.
    - Raw Amplitude 1..8 – The corresponding non-normalised amplitude reading for the given distance.
    - Profile Used – Indicates the corresponding power profile used to perform the measurement.
- CRC – A 2-byte cyclic redundancy check is appended to the end of the message. See 3.3 for more details.

Byte 0 – 35	**36 - 40**	**41 - 45**	**46 - 50**	**51 - 55**	**56 - 60**	**61 - 65**	**66 - 70**	**71 1-75**	**76 - 80**	**81 – 82**
Header	Distance reading	Raw Data 1	Raw Data 2	Raw Data 3	Raw Data 4	Raw Data 5	Raw Data 6	Raw Data 7	Raw Data 8	CRC

Full diagnostic message example (HEX String):

2201130400001D4E5F0863257069887752017520366B320F000CCBA02000000CFF20002D97043A0F009704A6050
10000000000000000000000000000000000000000000000000000000000000000000000000007D71

3.5 Message 34 – Primary payload

Message 34 represent the primary payload. This is typically delivered to the server according to the pre-configured message schedule, though it can also be requested via an "R" command.

Message Initiation:

- Sent according to the "S2" schedule parameter.
- Sent via "R1=01" via a payload response or BLE command.

Payload breakdown:

- Message header – Common header precedes all message types See section 0 for more details.
- Timestamp reference.
- Up to 28 pre-logged readings.
- CRC – A 2-byte cyclic redundancy check is appended to the end of the message. See 3.3 for more details.

Byte 0 - 35	**36 - 41**	**46 - 51**	**52 - 58**	**…**	**202 - 207**	**208 - 213**	**214 - 215**
Header	Timestamp Reference	Logged reading #1	Logged reading #	….	Logged reading #27	Logged reading #28	CRC

Full message example (HEX String):

22050A0100000D1C60086973806937313701360 78E680011130DC767AC00000F082200B20217061008000000000
00100138A00FA0100127A00F90100107800FA0100107800FA0000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000E972

3.5.1 Timestamp Reference

It is possible derive the timestamp for each logged reading by taking the timestamp reference value and corresponding logger interval and counting backwards according to the reading #.

For example, if the Timestamp reference is 16/6/2023 08:00 and the logger interval is 30 minutes, then the first reading in the logger buffer will have been logged immediately prior to connection to the server. The 2nd reading would be 30 minutes prior to the first reading. The 3rd reading would be 30 minutes prior to the 2nd reading.

Reference Timestamp	16/6/2023 08:00	Calculated Timestamp
Logger interval	30 Mins	
Reading #1	= Ref Timestamp	16/06/23 08:00
Reading #2	= Ref Timestamp – (1 * Logger Interval)	16/06/23 07:30
Reading #3	= Ref Timestamp – (2 * Logger Interval)	16/06/23 07:00
…	…	…
Reading #27	= Ref Timestamp – (26 * Logger Interval)	15/06/23 19:00
Reading #28	= Ref Timestamp – (27 * Logger Interval)	15/06/23 18:30

3.5.2 Distance reading

The primary payload consists of 28 individual distance readings, separated according to the logger interval.
The record contains information that relate to the individual measurement event such as distance, temperature and additional data.

Byte 0	1	2	3	4	5
Ullage H	Ullage L	RRC / RSSI	Temperature	Status flags	Reserved

- Ullage – The distance in mm from the surface of the sensor to the surface of the liquid.
- RRC – The Radar Result Code is used to indicate the reliability of the reading. Higher is better.
    - See separate chapter on interpreting these result codes.
- Radar RSSI – The strength of the radar measurement normalised in a from 1 – 10. Higher is better.
- Status flags – The status flags are received from the Radar sensor and notify of any potential problems during the measurement process.
    - Bit0 – Radar amplitude saturated.
    - Bit1 – Invalid setup.
    - Bit2 – Scan failed to complete.
    - Bit3 – Gain auto-adjusted.
    - Bit4 – Too many peaks detected
    - Bit5 – N/A
    - Bit6 – Blindzone scan missing or invalid. See section xxx for more information on the blindzone.
    - Bit7 – N/A

Example distance reading:

0100107800FA

- 00FA = 250mm
- 78 = RSSSI 7 / RRC 8
- 10 = 16 Degrees C
- 00 = No additional status flags
- 01 – Reserved

3.6 Message 36 - Settings message

Message 36 is a long message containing all of the readable S-parameters. Its total length will vary but would typically exceed 500 bytes.

Message Initiation:

- Sent via "R1=02" via a payload response or BLE command.

Payload breakdown:

- Message header – Common header precedes all message types See section 00 for more details.
- Comma separated S-parameter string, decoded to ASCII.
- CRC – A 2-byte cyclic redundancy check is appended to the end of the message. See 3.3 for more details.

Byte 0 – 35	36 …n	Length - 2
Header	S0=82,S1=01,S2=7F0057,S3=01…..	CRC

Full message example (HEX String):

2201130400001D5A5E0863257069887752019523FD6C2F00000B854400000000FF2401D42C53303D38322C53313D30312C53323D3746303035372C53333D30312C53343D4434303345382C53353D3030303030302C53363D3030303030302C53373D30302C53383D30302C53393D2C5331303D2C5331313D54454B3838302C5331323D6E6264312E6B6F72656D326D2E636F6D2C5331333D2C5331343D2C5331353D6C6576656C2E74656B656C656B2E636F6D2C5331363D393030312C5331373D2C5331383D3638352C5331393D2C5332303D31392C5332313D32373230312C5332323D38303030302C5332333D31332C5332343D30312C5332353D2C5332363D30322C5332373D30312C5332383D54454B3838302D2C5332393D30302C5333303D373230302C5333313D2C5333323D32343535413530302C5333333D3134373034323830 2C5333343D3135413432303738 2C5333353D3135394131383238 2C5333363D37443030303945372C5333373D3039323746423543 2C5333383D4243353446446342C5333393D3346413235313141 2C5334303D3436463042334344 2C5334313D4242304244314442 2C5334323D3436463542433941 2C5334333D42413443304539442C5334343D3436374139454344 2C5334353D4239343535334342 2C5334363D30302C5334373D2C5334383D2C5334393D2CDB24

Decoded Payload example (ASCII String):

,S0=82,S1=01,S2=7F0057,S3=01,S4=D403E8,S5=000000,S6=000000,S7=00,S8=00,S9=,S10=,S11=TEK880,S12=nbd1.korem2m.com,S13=,S14=,S15=level.tekelek.com,S16=9001,S17=,S18=685,S19=,S20=19,S21=27201,S22=80000,S23=13,S24=01,S25=,S26=02,S27=01,S28=TEK880-
,S29=00,S30=7200,S31=,S32=2455A500,S33=14704280,S34=15A42078,S35=159A1828,S36=7D0009E7,S37=0927FB5C,S38=BC54FDF4,S39=3FA2511A,S40=46F0B3CD,S41=BB0BD1DB,S42=46F5BC9A,S43=BA4C0E9D,S44=467A9ECD,S45=B94553CB,S46=00,S47=,S48=,S49=,

https://www.rapidtables.com/convert/number/hex-to-ascii.html

3.7 Message 38 – Unscheduled measurement message

Message 38 has the same general structure of a standard message 34 albeit shorter in length and represents an unscheduled connection. These can occur in the event of an alarm event, or during an installation where a quick "snapshot" of measurement data is taken rapidly and delivered to the server.

The source of this message can be determined by reviewing the Contact reason and Alarm flags.

Message Initiation:

- Sent via "R1=20" via a payload response or BLE command.

- Long hold on the reed switch > 5 seconds.
- One or more alarm thresholds getting broken.

Payload breakdown:

- Message header – Common header precedes all message types See section 0 for more details.
- Timestamp reference. See section 0 for more information.
- Up to 10 rapidly logged readings. See section 3.5.2 Distance Reading for more information.
- CRC – A 2-byte cyclic redundancy check is appended to the end of the message. See 3.3 for more details.

Byte 0 - 35	36 - 41	46 - 51	52 - 58	…	202 - 207	208 - 213	214 - 215
Header	Timestamp Reference	Logged reading #1	Logged reading #	…	Logged reading #27	Logged reading #28	CRC

Full message example (HEX String):

2205F90801002558000869738069375637006D00004A180614000050E500000DFF2600460F17051A0A1800000000000146A06A80000146A06A70000146A06A80000146A06A70000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000B4C9

3.8 Message 40 - Ack / Nack message

Message 40 is used to Acknowledge/Negatively acknowledge a previous firmware "Over the air" (OTA) update process. Typically, once the OTA process has completed the device will immediately connect to the server and send a message 40 to indicate the status.

Message Initiation:

- In response to an firmware upgrade process.

Payload breakdown:

- Message header – Common header precedes all message types See section 0 for more details.
- Ack Event:
  - 0x02 Failed to retrieve OTA images from server.
  - 0x04 Failed to copy OTA image to memory
  - 0x06 OTA Image CRC Fail
  - 0x07 Incorrect OTA image for device
  - 0x08 OTA Completed Successfully
- CRC – A 2-byte cyclic redundancy check is appended to the end of the message. See 3.3 for more details.

Byte 0 - 35	36	37	38 - 39
Header	Ack Event	Reserved	CRC

Full message example (HEX String):

2201050474001D5D0008697380692887640 0E938C06B3201000D3F9EF80000006C280002080 1580B

3.9 Message 42 - Info and Run History message

The device logs many events and counters during its operational lifetime known as the Info and Run History. Various counters are running to log issues such as successful connections, cumulative power consumption and cellular registration time.

These statistics can be useful at times to diagnose potential problems with the performance of the device.

Message Initiation:

- Sent via "R6=02" via a payload response or BLE command.

Payload breakdown:

- Message header – Common header precedes all message types See section 00 for more details.
- 19 info items of 4-bytes each
- CRC – A 2-byte cyclic redundancy check is appended to the end of the message. See 3.3 for more details.

Byte 0 - 35	36 - 107	214 - 215
Header	Device info and Run History (see table below)	CRC

Info command Items list

Byte #	Item	Description
36 - 39	Message Count	Cumulative count of data payloads successfully delivered
40 - 43	Message Fail Count	Cumulative count of data payloads that failed to be delivered ***Note*** **-** after cellular registration success.
44 - 47	Energy Used Total	Cumulative energy used for all aspects of device operation, in mA/s
48 - 51	Energy Used (Fail)	Cumulative energy used for failed registration and/or connection to server, in mA/s
52 - 55	Energy Used (External)	Cumulative energy used when performing Radar measurements, in mA/s
56 - 59	Registration Time Total	Cumulative time for registering on the cellular network (250ms increments)
60 - 63	Count of BOR	Count of Brown Out Resets (circuit voltage falling below a minimum level).
64 - 67	Count of PIR	Count of Pin Resets
68 - 71	Count of WDT	Count of Watchdog Timer Resets (occurs when device locks up)
72 - 75	Count of SW Reset	Count of Software Resets (Occurs when firmware issues command to self-reset).
76 - 79	Ambient Temp Max	Maximum ambient temperature in °C (Taken from Radar sensor).
80 - 83	Ambient Temp Min	Minimum ambient temperature in °C (Taken from Radar sensor).
84 - 87	Modem Runtime	Total time cellular modem is active (250ms increments)
88 - 91	Message RX Count	Count of received data from the cellular network ***Note*** **–** This is all messages, not necessarily "R" or "S" parameters.
92 - 95	Registration Count	Count of successful registrations to the cellular network
96 - 99	Registration Fail Count	Count of failed registrations to the cellular network. ***Note*** *– Each try ticket can contribute to this count*
100 - 103	Connection Fail Count	Count of failed connections to data services (i.e. failed to establish a TCP link to the server endpoint) ***Note*** *– Each try ticket can contribute to this count*
104 - 107	Count of Modem Crash	Count of incidents when the cellular modem crashed and needed to reboot.

Full message example (HEX String):

2201130400001D5A5E0863257069887752019 20E846B3209000B994400000000FF2A004892010000020000012A90D00BC4F0000406B03007E380000780000 00C600000004000000CA0000001800000000000000E9B5000092010000760100000200000000000000000000003981

3.10 Message 44 - Modem and SIM Card details message

In some specific occasions, it might be necessary to request the telemetry and SIM card and cellular modem firmware details. For example, enabling Azure/IoT-Hub secure communications require an authentication server to issue tokens to the device. The unique data contained within the modem details such as the SIM card IMSI number can be used to identify that device and permit the connection to the Azure/IoT-Hub server.

Note **-** Each element of the payload body is in comma-separated ASCII string.

Message Initiation:

- Sent via "R6=04" via a payload response or BLE command.

Payload breakdown:

- Message header – Common header precedes all message types See section 00 for more details.
- Cellular modem firmware version ASCII string
- SIM Card IMSI (International Mobile Subscriber Identifier) number ASCII string
- SIM Card ICCID (Integrated Circuit Card Identification) Number ASCII string
- Unique ID ASCII string
- CRC – A 2-byte cyclic redundancy check is appended to the end of the message. See 3.3 for more details.

Byte 0 – 35	**36 .. n**	**Length - 2**
Header	Modem FW Version, IMSI Number, ICCID Number, Unique ID [Varying lengths]	CRC

Full message example (HEX String)

2201130400001D5D5E0863257069887752019407DD6B320B000B8A4400000000FF2C004F2C424739354D334C415230324130335F30312E3031362E30312E3031362C39303132383830303532303036322C3839383832333930303030323437313830353031 2C4D795F4E69636B6E616D652C5E75

Decoded Payload example (ASCII String):

,BG95M3LAR02A03_01.016.01.016,901288005200062,89882390000247180501,My_Nickname,

3.11 Message 47 - GPS Message

Some use cases might require the actual location of the device to be identified. This might be in the case of a mobile IBC or to facilitate route or location mapping. A GPS message is initiated by a request from the server or BLE app. It will proceed to register to the cellular network (with is pre-requisite to GPS acquisition) and once registered the device will scan for GPS satellites.

Once the satellite lock has occurred, the device will connect to the server and deliver the payload as an ASCII string.

It is also possible to enable assisted GPS/GPS XTRA via the S3 parameter to allow supporting metadata to be downloaded from the cloud to facilitate the GPS acquisition.

Note – Only select assisted GPS if the SIM card/data provider is known to allow access to the cloud location of the metadata file.

Message Initiation:

- Sent via “R7=FF” via a payload response or BLE command.

Payload breakdown:

- Message header – Common header precedes all message types See section 00 for more details.
- GPS Co-ordinates and Time To First Fix in ASCII string format.
- CRC – A 2-byte cyclic redundancy check is appended to the end of the message. See 3.3 for more details.

Byte 0 – 35	36 .. n	Length - 2
Header	GPS Longitude and latitude ASCII string	CRC

Full message example (HEX String):
2200610400001D4961086435105252500500370000B3216000000BDAA000000002F00320D0A4C61743A35322E37303536312C4C6F6E673A2D382E38393935392C5454463A32352C4750535F454E553A323631320D0AAF9A

Decoded payload example (ASCII String):
Lat:52.70561,Long:-8.89959,TTF:25,GPS_ENU:2612

Note – *GPS acquisition is a battery intensive process. This command should only be initiated sporadically.*

https://www.rapidtables.com/convert/number/hex-to-ascii.html

4. Settings and Request commands

Every time a sensor makes an outgoing status connection to the gateway, the server has the option to respond with special text-based commands to alter the operation of the device.

The device can receive two types of commands which can affect its behaviour.

- Requests or “R Commands” - These are generally instructions for the device to perform a specific task.
- Settings or “S Parameters” – These are saved to memory and affect subsequent operation.

Device Password (6 Chars)	Command String (comma separated)	CRC (HEX)
TEK880	,S16=9001,R1=01,	Z=9C9C

4.1 Device Password

All command types are preceded by a device password. This password is typically 6 ASCII characters long and will be pre-agreed with the customer prior to the production of the device.

Sending commands to the device without device password will cause the command to be ignored.

The device password is inserted at the beginning of the command string, with any comma-separated S or R parameters to follow.

4.2 Command syntax

All R commands and S parameters follow some basic syntax rules. A prefix of “R” or S” immediately followed by the command number itself. Following the command number is an equals symbol followed by the corresponding input value (which will have a specific meaning based on the command number).

SX=YY
RX=YY

- S – Indicates the command is an "S" parameter.
- R - Indicates the command is an "R" command.
- X – The specific setting/request number.
- YY – The command input value.
    - This value could be decimal, hexadecimal or ASCII string depending on the command number in question.

4.3 Command CRC (Cyclic Redundancy Check)

Each concatenated group of commands should be terminated by a 16-bit Cyclic Redundancy Check (CRC) which is derived from the command text. This allows the server to validate the integrity of the payload.

The CRC is formatted as ",Z=ABCD" where ABCD represents the 16-bit CRC in Hexadecimal string format.

CRC Details:

- Type – CRC-16/XMODEM (CCITT)
- Initial value – 0x0000 (x16+x12+x5+1)
- Polynomial – 0x1021

Method – Calculate the CRC over each character from left to right, ensuring a comma and capital "Z" is appended to the end of the command string.

"TEK880,R1=20,Z"

The result can then be converted into a 16-byte Hexadecimal string and appended to the end of the command.

TEK880,R1=20,Z=9C9C

Note – The firmware can be configured to ignore CRC checking when receiving command text, but this is not recommended.

4.4 Combining and concatenating commands

It is possible to concatenate a number of S parameters and R commands within a single contiguous command string. For example, changing a server URL and port simultaneously, and then request a payload is sent to the server.

In the event of combined commands, it is recommended the S parameters are included at the beginning of the string with the R command at the very end just before the CRC. This is to ensure any destined S parameters have already been saved before the R commands are processed.

A typical example of a combined and concatenated command

- R1=01 (Send logged data to server).
- S16=9001 (Change the server TCP Port to 9001).

As there are several S parameters, they must be concatenated together with a comma as a separator.

Example command	Valid/Invalid	Comments
TEK880,S16=9001,R1=01	Valid	
TEK880, S16=9001, R1=01	Invalid	Spaces in addition to Commas are not allowed

TEK880 S16=9001 R1=01	Invalid	Spaces instead of commas are not allowed
TEK880S16=9001R1=01	Invalid	Missing comma separator
TEK880,R1=01,S16=9001	Invalid	"R" command before "S" parameter
S16=9001,R1=01	Invalid	Missing device password

Note – It is recommended all commands are terminated with a CRC (enabled via command 3. See above for more details).

4.5 S-Parameters (Settings)

The sensor is configured using the following S parameters. Blank values are undefined and can lead to inconsistent operation.

Overview

S-	Parameter	Description	Data type
S0	S-Logger Config	• The time interval which each reading is logged into the data payload buffer. • The sampling period between each radar measurement	HEX String
~~S1~~	~~GSM listen Config~~	• ~~How long the unit remains active after powering up~~	~~HEX String~~
S2	Schedule Config	• Sets schedule for when unit is to upload data payload to server.	HEX String
S3	Control configurator	• Access Technology: (NBIOT/CATM1/GSM) • CRC checking • Enable assisted GPS	HEX String
S4, S5 & S6	Static alarms	• Allows low-level/high level alarms to be set. • Configure whether they are active or passive. • Set the hysteresis/tolerance level.	HEX String
S11	Device Password	• Password required to send commands (Settings or Requests) to device.	ASCII String
S12	Mobile data APN (SIM card)	• Access Point Name. Name of the gateway to the server.	ASCII String
S13	Mobile data APN Username (SIM card)	• Username required to access mobile data. Specific to SIM Card provider.	ASCII String
S14	Mobile data APN Password (SIM card)	• Password required to access mobile data. Specific to SIM Card provider.	ASCII String
S15	Destination Server IP address or URL	• IP address or URL for server that unit is required to issue data to.	ASCII String
S16	Destination Server Port number	• Port number for server that the unit is required to issue data to.	Decimal String
S18	Tank height	• Usable tank height (excluding liquid below outlet)	Decimal String
S19	HTTPS POST path	• See secure communications section for more information	ASCII String
S21	MCC MNC (Network Operator Short Code)	• Mobile Country Code / Mobile Operator Code	HEX String
S22	Operating Band Code	• NBIOT only	HEX String
S23	Message deliver try configurator	• How many attempts to make data drop before device returns to low power mode • Time between attempts.	HEX String
S27	Radar measurement quality filter	• Sets minimum Radar Result Code (RRC) used to generate alarms. • Sets minimum Radar RSSI (rRSSI) used to generate alarms.	HEX String

S30	Battery Capacity	• The capacity of the fitted lithium cells in mAh	Decimal String
S31	Operating Band Code	• CatM only.	HEX String
S32 – S44	Radar configuration Profile	• Sets characteristics of Radar measurement algorithm. See separate chapter for more information.	HEX String

4.5.1 S0: Logger Config

The TEK880 collects data according to two time-based parameters. The **Sampling Period** is the time period that determines how often the sensor takes radar measurements and stores the measurement in a sampling buffer. The **Logging interval** states often the sampled readings are saved to the main data logger (and is therefore uploaded to the server).

The configuration of these two settings are dependent on the use-case. A slow-drain environment might have a relatively slow logger speed, linked to a relatively infrequent dial-in schedule. Whereas a faster drain environment might have a faster logger speed and a dial-in schedule of 24 hours or less.

A faster sampling period would be useful if limit-alarms are enabled on the device. This would give a faster notification to the server outside of the logging interval.

If alarms are not required, it is possible to link the sampling period to the logger speed.

- **Logging interval.**
  - 15-minute increments.
  - Max 24 hours.
- **Sampling period.**
  - 1 = Every 15 minutes.
  - 2 = Linked to logging interval.

S0 byte description

Bit15	Bit14	Bit13	Bit12	Bit11	Bit10	Bit9	Bit8
N/A	N/A	N/A	N/A	N/A	N/A	N/A	Samp1

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Samp0	Lint6	Lint5	Lint4	Lint3	Lint2	Lint1	Lint0

- Bit 15-9 N/A – leave as 0
- Bit 8 - 7 Sampling Period
  - 0 = 1 minute (Not recommended).
  - 1 = 15 minutes.
  - 2 = Linked to logging interval.
- Bit 6 – 0 Logging interval
  - 0b0000001 = 15 minutes.
  - 0b0000010 = 30 minutes.
  - 0b0000011 = 45 minutes.
  - 0b0100100 = 60 minutes.
  - …
  - 0b01100000 = 1440 minutes (24 hours)

Note – *Increasing the speed of the sampling period has a direct influence on the battery life. It is recommended to take a radar measurement once per hour by linking the parameter to the logging period.*

Example:
S0=82 (Data sampled once every 15 minutes. Logged every 0.5 hours).
S0=1111104 (Data sampled every hour, logged every hour). (Recommended).

~~*4.5.2 S1: GSM Listen Configuration*~~

~~The time delay for how long the device stays connected to the cellular network in listen mode once the main payload has been delivered to the server. This allows the server to push additional responses back down to the device within the timeout period.~~

~~In normal operation, this function should be superseded by a disconnect command such as R1=80 to disconnect and put the device to sleep.~~

- ~~**Listen period**~~
  - ~~Max of 155 minutes~~
  - ~~Multiples of 5 minutes~~
  - ~~0 = 90 minutes.~~

~~**S1 byte description**~~

~~Bit7~~	~~Bit6~~	~~Bit5~~	~~Bit4~~	~~Bit3~~	~~Bit2~~	~~Bit1~~	~~Bit0~~
~~N/A~~	~~N/A~~	~~N/A~~	~~List4~~	~~List3~~	~~List2~~	~~List1~~	~~List0~~

- ~~Bit 7 – 5 N/A – Leave as 0~~
- ~~Bit 4 – 0 GSM Listen Period~~
  - ~~0b00000 = 90 minutes (Special case).~~
  - ~~0b00001 = 5 minutes.~~
  - ~~0b00010 = 10 minutes.~~
  - ~~0b00011 =15 minutes~~
  - ~~…~~
  - ~~0b11111 = 155 minutes.~~

~~**Example**~~
~~S1=01 (Device listens for 5 minutes after successful connection to server).~~

4.5.3 S2: Schedule Configuration

This multi-part parameter defines the connection schedule for its primary data payload.
It works around the concept of a Monday – Sunday calendar, where each day can be selected or deselected depending on the use case.
The start hour and minute can then be selected, and (optionally) the end hour can be selected if multiple connections per day are desired.

It's worth noting that this parameter needs to be configured in conjunction with the S0 (logger config) parameter to ensure the number of logged readings does not exceed the maximum number 28 of slots within the schedule period.

Note - If the End Time entered is before the Start time, no scheduled data will be transmitted.

- **Connection calendar**
  - Max 0x7F (Each day selected).
  - Min 0x0 (No days selected, scheduled defacto disabled).
- **Connection Hour**
  - Max 23
  - Min 0 (midnight)
- **Connection minute**

- Max 59
- Min 0

Note – *The connection rate can significantly affect the battery performance. It is recommended the device connect to the server a maximum of once per day except in specific circumstances.*

Note – *The schedule should be created with the logging/sampling period in mind*

S2 Byte description

Bit23	Bit22	Bit21	Bit20	Bit19	Bit18	Bit17	Bit16
N/A	Sunday	Saturday	Friday	Thursday	Wednesday	Tuesday	Monday

Bit15	Bit14	Bit13	Bit12	Bit11	Bit10	Bit9	Bit8
Hours5	Hours4	Hours3	Hours2	Hours1	Hours0	Mins1	Mins0

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Mult2	Mult1	Mult0	EndHr4	EndHr3	EndHr2	EndHr1	EndHr0

- Bit 23 N/A – leave as 0
- Bit 22 - 16 22 – 16 – Connection calendar
  - 0b0000000 = No days selected
  - 0b0000001 = Monday
  - 0b0000010 = Tuesday
  - 0b0000011 = Monday & Tuesday
  - …
  - 0b1111111 = Mon, Tues, Wed, Thurs, Fri, Sat, Sun
- Bit 15 – 10 Connection hour
  - 0b00000 = Midnight
  - 0b00001 = 1am
  - 0b00010 = 2am
  - 0b00011 = 3am
  - …
  - 0b10111 = 11pm (hour 23)
- Bit 9 – 8 Connection minute
  - 0b00 = 0 minute
  - 0b01 = 15 minute
  - 0b10 = 30 minute
  - 0b11 = 45 minute
- Bit 7- 5 Multiple connections per day
  - 0b000 = Once every 24 hours
  - 0b001 = Once every 2 hours (Not recommended)
  - 0b010 = Once every Hour (Not recommended)
  - 0b011 = Once every 4 hours (Not recommended)
  - 0b100 = Once every day (Legacy)
  - 0b101 = Once every 6 hours
  - 0v110 = Once every 8 hours
  - 0b111 = Once every 12 hours
- Bit 4 – 0 End hour (end minute equal to start minute)
  - 0b00001 = 1am
  - 0b00010 = 2am
  - 0b00010 = 3am
  - …

- 0b10111 = 11pm (hour 23)

Example 1:
S2=7F0600 (Connect every day at 1.30am)

Example 2:
S2=150655 (Connect Mon, Wed, Friday every 4 hours starting 1.30am and ending 9.30pm (21:30).

4.5.4 S3: Control Configuration

The Control 1 byte is used to set some key parameters such as the cellular network selection or enabling CRC checking to incoming command strings.

- **Network selection** – Allows the preferred cellular network to be selected here. The SIM card and regional network support needs to be factored in when adjusting this setting. For example, NBIOT is not supported in the USA so network registration with this setting would not be possible.
- **CRC checking** – Instructs the firmware to check a valid CRC has been appended to the end of any command string sent from a server or BLE connection.
- **Assisted GPS** – Allows the conventional GPS scanning to be complimented by additional metadata downloaded from a cloud server.

Note – *It is not recommended to adjust the network selection. Misconfiguring this setting could significantly impact the battery life by extending the registration period significantly.*

Note – *Do not use assisted GPS unless specifically advised. It can have a negative effect on the battery life,*

S3 byte description

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
N/A	N/A	GPS	CRC	N/A	Net2	Net1	Net0

- Bit7 N/A – Leave as 0
- Bit6 N/A – Leave as 0
- Bit5 Enable assisted GPS
  - 0 = disable assisted GPS
  - 1 = enable assisted GPS (uses packet data).
- Bit4 Enable CRC checking on command strings
  - 0 = CRC checking disabled
  - 1 = CRC checking enabled
- Bit3 N/A – Leave as 0
- Bit 2 – 0 Network selection mode.
  - 0b000 = CATM Auto (Prefers CATM but can switch network if available).
  - 0b001 = NBIOT Auto (Prefers NBIOT but can switch network if available).
  - 0b010 = 2G Auto (Prefers 2G but can switch network if available).
  - 0b011 = 2G Forced (Forces use of 2G if available - Not recommended).
  - 0b100 = CATM Forced (Forces use of CATM if available - Not recommended).
  - 0b101 = NBIOT Forced (Forces use of NBIOT if available - Not recommended).
  - 0b110 = N/A
  - 0b111 = N/A

Example:
S3=01 (NBIOT Auto only)

4.5.5 S4, S5 & S6: Fixed alarm thresholds

The device has three fixed alarm thresholds. These are used to trigger one or more alarms depending on the liquid level measured by the radar sensor.

The alarm can be configured to be passive (i.e. set a flag that is reported during the normal connection schedule) or active (where an unscheduled alarm payload is sent to the server to immediately inform the user).

Each threshold can be configured with a positive or negative polarity, meaning an alarm can be generated when the level passes BELOW the threshold or ABOVE the threshold and a hysteresis value can be assigned which adds some tolerance to prevent a liquid level exactly on the threshold from repeatedly triggering an alarm due to small variations to the liquid level.
Once the alarm is set, further alarm messages are prevented until the liquid level passes outside of the threshold and then inside the threshold again.

There are three alarm configuration settings. They can be a mixture of positive and negative polarity with different threshold and hysteresis values.

- **Limit Polarity** – Sets whether the alarm is generated when the measured value is higher than the threshold or lower than the threshold.
  - Bitwise
- **Enable bit** – Sets whether an alarm message is generated or a flag is set within existing scheduled messages.
  - Bitwise
- **Hysteresis** – Sets how many mm outside of the threshold before the alarms state is cleared. Routine adds 3mm to the user setting.
  - Max – 63mm
  - Min – 10mm
- **Threshold value** – sets the distance in mm that the measurement must cross to generate the alarm.
  - Max – 6500 or Tank height, whichever is closer.
  - Min – 200 (Less than 20cm brings the sensor near the blind zone, it is not recommended to set alarms to this threshold).

Note – the polarity figure represents the distance measurement from the surface of the liquid to the sensor. It does not represent the liquid level.

Note – A Threshold value less than 200mm is not recommended.

Note – A Threshold value greater than the tank height will never generate an alarm condition.

S4, S5, S6 Byte description

Bit23	Bit22	Bit21	Bit20	Bit19	Bit18	Bit17	Bit16
Polarity	Enabled	Hyst5	Hyst4	Hyst3	Hyst2	Hyst1	Hyst0

Bit15	Bit14	Bit13	Bit12	Bit11	Bit10	Bit9	Bit8
Thresh15	Thresh14	Thresh13	Thresh12	Thresh11	Thresh10	Thresh9	Thresh8

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Thresh7	Thresh6	Thresh5	Thresh4	Thresh3	Thresh2	Thresh1	Thresh0

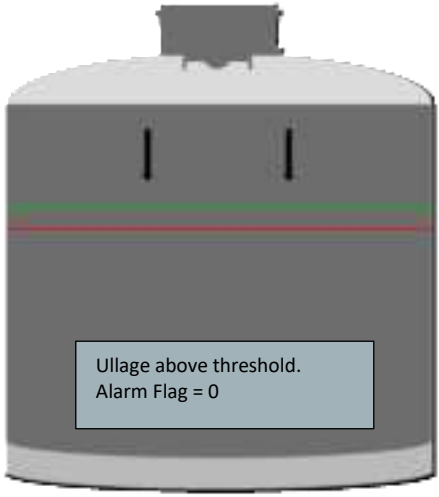
- Bit23 Set threshold polarity.
  - 0 = Alarm when reading is lower than threshold.
  - 1 = Alarm when reading is higher than threshold.
- Bit22 Enable alarm

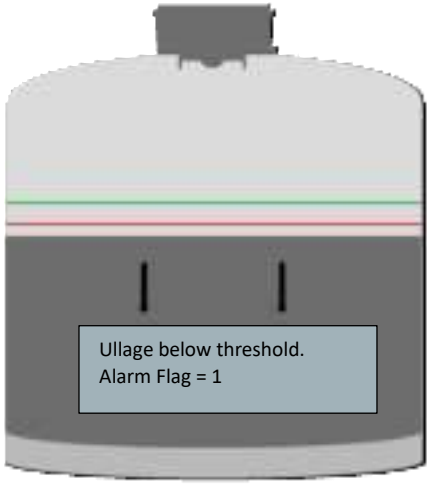
- 0 = Active alarm message disabled. Alarm flag still generated in scheduled message.
- 1 = Active alarm message enabled. Generates unscheduled alarm message.

- Bit 21 – 16 Alarm Hysteresis.
  - 0b000111 = 10mm
  - 0b001000 = 11mm
  - …
  - 0b111110 = 65mm
  - 0b111111 = 66mm
- Bit 15 – 0 Threshold value
  - 0b00000000 11001000 = 200mm (minimum).
  - 0b00000000 11001001 = 201mm.
  - 0b00000000 11001010 = 202mm.
  - 0b00000000 11001011 = 203mm.
  - …
  - 0b00011001 01100011 = 6499mm
  - 0b00011001 01100011 = 6500mm

Example:
S4=F20258 (Val < Threshold, Enabled, Hysteresis 50mm, 600mm threshold).

Enabled: 1 (Generates active alarm once threshold is passed).
Polarity: 1 (Ullage > Threshold triggers alarm).
Green Line: Alarm reset limit (Threshold – (Hysteresis + 3).
Red Line: Alarm Threshold





4.5.6 S11: Device Password

The device password string is up to 6 characters is length and precedes any text-based command string which can be sent to the device during a response from the server, or via the BLE connection.

It is used to prevent unwanted contact with the device by a 3rd party and is typically agreed with the customer prior to production.

The password can be less than 6 characters in length, but cannot exceed 6 characters.

Note – A null terminator is not required.

Parameter	Description	Example
S11:	Unit Password (6 char ASCII)	S1=TEK880

4.5.7 S12, S13, S14: Mobile APN credentials

The device uses mobile data services on the cellular network to deliver data payloads to the server. Most of these cellular networks require login credentials to access the data services. Typically, this include the Access Point Name (APN) which is a gateway through which access to the internet is gained. In some cases a username and password are also required for a successful connection. All three credentials are represented as ASCII strings.

Note – Sometimes no password is required. If this is the case, leave the field blank.

Parameter	Description	Example
S12:	Mobile APN (44 Char ASCII)	S12=live.vodafone.com
S13:	Mobile APN Username (24 Char ASCII)	S13=apnuser
S14:	Mobile APN Password (24 Char ASCII)	S14=apnpass

4.5.8 S15 & S16: Destination server

The primary purpose of the TEK880 is to take measurements, log them and upload them to a server. The server is accessed via a Server URL and a Server TCP Listen Port.

The Server URL/IP Address must be the full path to the web service/TCP listener but excluding the port, which is supplied separately (see below).
The Server Port needs to be an ASCII formatted number between 1 and 65535.

Parameter	Description	Example
S15:	Destination Server IP address or URL (64 Char ASCII)	S15=level.tekelek.com
S15:	Destination Server IP address or URL (64 Char ASCII)	S15=173.212.215.131
S16:	Destination Server Port Number (8 Char ASCII)	S16=9001

4.5.9 S18: Tank Height

It is critical that the correct tank height for the sensor is measured and sent to the device. This is because the radar processing algorithms need to know the overall radar scanning range and ensure phenomena such as water pooled beneath the tank does not result in an invalid measurement.

- **Tank height** – Used to set the maximum extent of the radar scanning process.
    - Min – 50cm.
    - Max = 675cm

Note - The tank height is set in **cm**, rather than mm.

Parameter	Description	Example
S18:	Tank Height (ASCII Number)	S18=128

4.5.10 S21: PLMN Mobile Country Code/Network Code

S21 combines the Mobile Country Code (MCC) and Mobile Network Code (MNC) into a single numeric string of five or six digits (known as the PLMN). It allows the Home Network Identity (HNI) to be identified which when combined with the IMSI number contained within the SIM card allows the device to be subscribed to the correct network for that location.

If the home network is not known or if the device is using a roaming SIM card then leave it blank.

This parameter is applicable for LTE CATM/NBIOT – It has no consequence for 2G GSM connections.

Note – If left blank, first-time registration may take significantly longer as the cellular modem hunts for the best available network.

Note – Entering the wrong PLMN could prevent the device from registering entirely, causing the battery to deplete in the process – extreme caution should be used.

Examples:

MCC	MNC	Operator	PLMN Example
272	01	Vodafone Ireland	S21=27201
272	02	Three Ireland	S21=27202
234	02	O2 UK	S21=23402
234	07	Vodafone UK	S21=23407

4.5.11 S22 NBIOT Band

NBIOT operates on an assortment of frequency bands which depend on the country/region where the device is located. These frequency bands are combined into a Hexadecimal configuration string which is used by the cellular modem to select which bands to scan when attempting to register for data services.

This setting is applicable for NBIOT only – It has no consequence for 2G GSM or CATM connections.

Note – If unsure, it is strongly advised this field is left blank as misconfiguration could significantly affect the registration time, affecting the battery life.

Band	Modem Code (HEX)
B1	1
B2	2
B3	4
B4	8
B5	10
B8	80

B12	800
B13	1000
B18	20000
B19	40000
B20	80000
B25	1000000
B28	8000000
B66	20000000000000000
B71	400000000000000000
B85	1000000000000000000000

Examples:

Region	Value	NBIOT band Example
Europe (B3, B8 and B20)	80084	S22=80084
Australia (B3 and B28)	8000004	S22=8000004
Middle East (B3, B5 and B28)	8000084	S22=8000084
Japan (B1, B8, B18 and B19)	60081	S22=60081

4.5.12 S23: Message Retry Configuration

Registering to a cellular network and delivering data depends on the reliability of the cellular network. Sometimes registering on a network may take longer than normal, and might fail on occasion.
This setting allows the number of retries, and the time period between subsequent attempts to be configured.

Note – Increasing this time can have a significant effect on the battery life.

- **Try Tickets** – Number of attempts per connection session.
  - Min 1.
  - Max 8.
- **Retry period** – Time period between each retry.
  - Min 10 seconds.
  - Max 320 seconds.

S23 Byte Description:

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
RetryPer4	**RetryPer3**	**RetryPer2**	**RetryPer1**	**RetryPer0**	**Tickets2**	**Ticket1**	**Ticket0**

- Bit 7 – 3 Retry Period.
  - 0b00000 = 10 seconds.
  - 0b00001 = 20 seconds.
  - 0b00010 = 30 seconds.
  - 0b00011 = 40 seconds.
  - …
  - 0b11110 = 310 seconds.
  - 0b11111 = 320 seconds.
- Bit 2 – 0 Try Tickets.

- 0b000 = 1 try ticket.
- 0b001 = 2 try tickets.
- 0b010 = 3 try tickets.
- 0b011 = 4 try tickets.
- …
- 0b110 = 7 try tickets.
- 0b111 = 8 try tickets.

Example:
S23=11 (2 tries, 30 seconds between each attempt).

4.5.13 S27: Radar Quality Filter

Generating threshold-based alarms is a handy way of providing an immediately notification that the liquid level has crossed a pre-determined threshold, outside of the normal connection schedule.

However, it is important the readings used to generate the alarm can be trusted.

The Tekelek Radar uses the concept of a Radar Result Code (RRC) and Radar RSSI (rRSSI) to indicate the reliability and strength of the radar measurement. The quality filter parameter applys a minimum RRC and rRSSI value permissible when testing for threshold alarms.

- Radar Result Code – Used to assign a quality score to each reading.
  - Max - 10
  - Min – 0
- Radar RSSI – used to indicate the strength of the radar signal reflection compared to an expected value
  - Max – 10
  - Min - 0

Note – Readings that do not meet the minimum value for the quality filter are still logged and uploaded to the server as normal.

S27 Byte Description

rRSSI3	rRSSI2	rRSSI1	rRSSI0	RRC3	RRC2	RRC1	RRC0
Bit7							Bit0

- Bit 7-4 Radar RSSI minimum value.
  - 0b0000 = rRSSI 0 (Filter off)
  - 0b0001 = rRSSI 1
  - 0b0010 = rRSSI 2
  - 0b0011 = rRSSI 3
  - …
  - 0b1001 = rRSSI 9
  - 0b1010 = rRSSI 10

- Bit 3 – 0 Radar Result Code minimum value.
  - 0b0000 = RRC 0 (Filter off)
  - 0b0001 = RRC 1
  - 0b0010 = RRC 2
  - 0b0011 = RRC 3
  - …
  - 0b1001 = RRC 9

- 0b1010 = RRC 10

Example:
S27=48 (rRSSI = 4, RRC = 8).

4.5.14 S28: BLE Broadcast prefix

The device has a Bluetooth Low Energy (BLE) connection to allow text-based settings and requests to be sent to the device during installation and diagnostics.

Once BLE mode has been activated, the device will broadcast a broadcast name which is detected by a BLE enabled smartphone which initiates the connection process.

The first seven characters of the 10-character broadcast name can be specified by the user. The final three characters are taken from the last digits of the device IMEI number and cannot be changed.

Note – Changing this prefix might prevent the accompanying smartphone app from correctly detecting a device whilst it is broadcasting.

Parameter	Description	Example	Sample BLE Broadcast
S28:	BLE Broadcast prefix (7 char ASCII)	S28=TEK880-	TEK880-615

4.5.15 S30: Battery Capacity

The device monitors its energy consumption in real-time to provide an accurate indication of the remaining battery life. In order to know the percentage of depletion, the battery capacity in Milliamps Hours (mAh) needs to be specified.

Typically, this value will be set during production and should not be changed.

Parameter	Description	Example
S30:	Battery Capacity mAh (ASCII Number)	S30=7200

4.5.16 S31: CATM Operating band

CATM1 also operates on an assortment of frequency bands which depend on the country/region where the device is located. These frequency bands are combined into a Hexadecimal configuration string which is used by the cellular modem to select which bands to scan when attempting to register for data services.

This setting is applicable for CATM1 only – It has no consequence for 2G GSM or NBIOT connections.

Note – If unsure, it is strongly advised this field is left blank as misconfiguration could significantly affect the registration time, affecting the battery life.

Band	Modem Code (HEX)
B1	1
B2	2
B3	4
B4	8
B5	10
B8	80
B12	800
B13	1000
B18	20000
B19	40000
B20	80000
B25	1000000
B26	2000000
B27	4000000
B28	8000000
B66	20000000000000000
B85	100000000000000000000

Examples:

Region	Value	CATM1 band Example
Europe (B3, B8 and B20)	80084	S31=80084

4.5.17 S32 – S44: Radar Configuration Profile

The Radar Sensor allows a rich assortment of configurations which will be optimized for application-specific characteristics such as liquid type, tank material and installation environment. At this time it is not possible to customize these settings. Upon placing an order Tekelek will provide the customer with an assortment of preset configurations which will give the best performance for the specific application.

4.6 Request commands

"R" or "Request" commands are typically used to instruct the device to perform a specific task.

The commands can be sent as a response to a data delivery to the server, or via a Bluetooth Low Energy (BLE) connection using a smartphone.

***Note** - Whilst it is possible to concatenate multiple "S" parameters together in a comma-separated string, it is advised to issue just one "R" command at a time, with the exception of R2, R3 and R4 which can be used in combination with other "R" commands.*

"R" number	Request	Description	Notes
R1=01	Send logger data to server	Sends previously logged data to server (MSG 34)	These are the readings stored according to the data logger period
R1=02	Dump S parameters to server	Send all S parameters, in comma-separated ASCII to server (MSG 36).	
R1=20	Sends unscheduled message to server	Takes 4 rapid measurements and sends to server (MSG 38)	These are typically "rapidly" saved readings as per the sampling interval
R1=80	Device sleep (Excl BLE)	Shuts off cellular modem and sleep, remains awake if BLE connection is live	
R2=YY/MM/DD:hh/mm/ss	Set device RTCC	Set Real Time Calendar Clock (RTCC) date and time	Recommended to send this as a downlink to response to all payload messages.
R3=ACTIVE	Activate device	Activates device scheduler and allows scheduled connections to server	
R4=DEACT	Deactivate device	Deactivates device scheduler. Scheduled connections to server blocked.	Can be used to temporarily deactivate a device which is out of use to help preserve the battery
R5=01	Register to cell network and connect to endpoint	Instructs device to register to cellular network and set up a TCP connection to network endpoint	This command, typically sent via a BLE App only connects to the server. No data is uploaded unless specifically instructed.
R5=02	Device sleep (Inc BLE)	Shuts down cellular modem including any BLE connection	
R5=03	Dump S parameters to BLE	Sends all the S parameters in comma separated ASCII to the BLE terminal	
R5=04,FF,08	Take rapid diagnostic	Perform 255 diagnostic radar scans and post the	FF is Hexadecimal for 255 (the number of repeated scans).

	measurements for BLE	raw data onto the BLE terminal	It is possible to use a smaller number here if required.
R5=05	Returns device info	Returns device info such as counts of resets, message counters, firmware versions and battery level	
R5=06	Clear all counters	Sets counts of resets, message counters to zero and battery level back to 100%	
R5=09	Reset battery to 100%	Clears battery level only, other counters such as resets and message counts are unchanged	
R5=0C	Return device IDs	Returns IMEI, ICCID, ICCID, Cellular Firmware version to BLE	
R5=0E	Test GPS	Attempts to lock on to GPS and returns results to BLE terminal	Sample GPS message: *Lat:52.70580,Long:-8.90025,TTF:51,GPS_ENU:5678*
R5=0F	Dump sampling log	Displays all measurement data from sampling buffer to BLE terminal	
R5=10	Dump Data log	Displays all measurement data from logging buffer to BLE terminal	
R5=11	Power up cellular modem	Power cellular modem	
R5=13	Get Accelerometer	Returns the X, Y, and Z alignment of the sensor plus a simplified "combo" value to indicate how flat the sensor is mounted	
R5=16,1	Scan Blindzone	Scans the "Blindzone" (first 10-20cm below the sensor face).	Use with S44 to enable/disable Blindzone scan
R5=20	Power down cellular modem	Powers down cellular modem, keeps device awake.	
R6=01	Send radar diagnostic data to server	Performs radar scan and sends raw data of up to 8 reflections to server (MSG 32)	
R6=02	Send device info to server	Sends a message to the server containing counts of resets and messages (MSG 42)	

R6=04	Sends device ids to server	Sends a message to the server containing device ids such as the IMEI number and SIM Card ICCID (MSG 44)	
R7=FF	Sends a GPS message to server	Turns on cellular modem and retrieves GPS location, then uploads the GPS data to the server. (MSG 47)	Assisted GPS may be used, see parameter S3.

5. Radar sensor

The radar sensor has a high degree of configurability which depends on the type of liquid to be measured and the size/shape and characteristics of the tank to be known in order to get the best performance from the sensor.

A scoring and normalization algorithm has been developed to apply a score against each radar measurement to allow for a simple and consistent method of selecting the distance reading and determining the confidence of that reading.

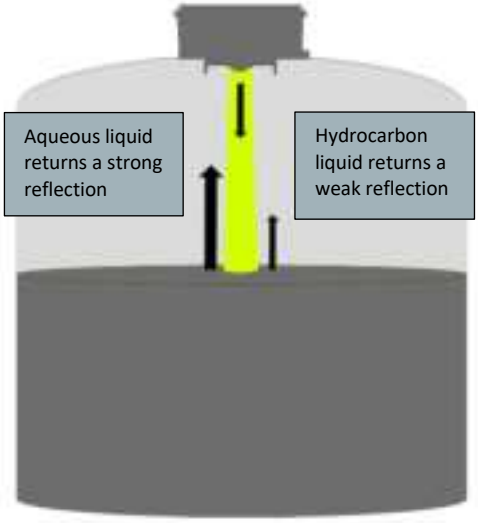
5.1 Reflections and dielectric constants

It is important the basic composition of the liquid is known when installing and commissioning the device. This is because the strength of the radar reflection is related to the type of liquid that is being measured. Different liquid compositions have a varying ability to reflect radar signals back to the sensors.

Liquid composition	Effect on the radar measurement	Maximum distance
Water-based	Very strong reflection	6.75m
Ammonia-based	Good reflection	-
Kerosene / Jet fuel	Weak reflection	4m

Once the liquid type is known, a formula can be used to create a 1-10 score to indicate the reliability of the radar measurement and indicate the strength of the signal.

Pre-set configurations for typical use-cases such as these will be provided by Tekelek.



Note – The signal strength can vary due to external factors such as condensation or whether the sensor installation is non-invasive or invasive (with the signal passing through the tank wall). As such it is important the sensor is installed as flat as possible.

5.2 Condensation effects.

Aqueous or water-based liquids can cause problems when attempting to measure reflections if a condensation layer builds up beneath the sensor. This is because the water droplets act as a barrier to weaken the signal and can often cause an incorrect distance measurement to be returned as the other reflections are suppressed.

This can be a particular problem in “non-invasive” applications where water droplets collect on the flat underside of the tank top.

“Invasive” applications with direct visibility of the liquid surface are less effected due to the shape of the sensor lens,

5.3 Tank shape, construction and unwanted effects

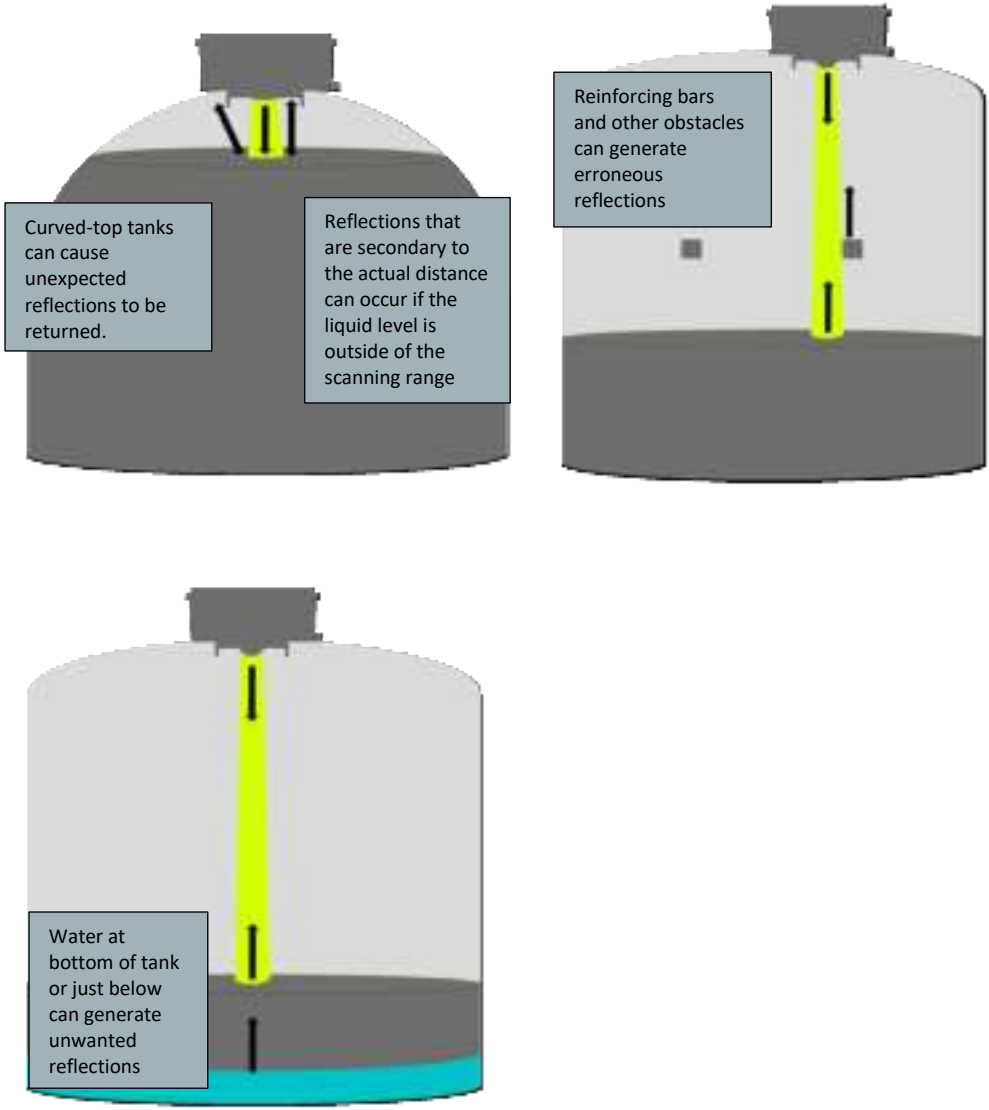
The tank shape and construction material can create unwanted effects. See below for a list of some of the complicating factors when performing radar measurements.

- Metal tanks.
    - Metal can create very strong reflections.
    - Metal can “box in” reflections (particularly in the near zone).
    - Dome-shaped tank tops can cause unusual reflection effects, particularly in the near zone.

- Reinforcing bars and obstructions.
    - Radar sensor needs unobstructed access to liquid surface.
    - Reinforcing bars can create erroneous reflections.

- Water at bottom of tank or just below.

- Liquids with low dielectric constant such as Kerosene allow radar signal to pass through and reflect off the water below.



5.4 Radar Result Code (RRC) - Measurement scoring system

A single strong reflection off the surface of the liquid is desirable, but in many circumstances more than one reflection is returned. The algorithm has been designed to process up to 8 reflections at any one time to attempt to deduce the correct measurement value.

In simple terms, the higher the RRC the better. For example, a score of 10 indicates a strong, single reflection which is almost certain to be the correct measurement.
However often there may be additional reflections of lesser strength which sit alongside the correct reflection. The formula looks at the relationship between the reflections and a result codes are explained in the table below.

RRC	RSSI (Normalized)	Notes
10	**1-10**	Single dominant echo. No other echoes detected. Perfect target with ideal conditions.
9	**"10" or "5"**	Detected echo indicates operation in the blind zone (if configured). • RSSI of 10 represents a clear distinct echo above the threshold. • RSSI of 5 indicates multiple echoes within the blindzone.
8	**1-10**	Multiple reflections detected. Dominant reflection RSSI x2 all others.
7	**1-10**	Multiple reflections. Strongest RSSI dominant reflection 20% higher than the rest would be chosen.
6	**1-10**	"Twin Peaks" – similar radar level reflection peaks that exist within 1 – 3cm of each other and either RSSI levels are x2 any other reflections.
5	**1-10**	Multiple reflections. Strongest echo which happens to be at a distance which indicates proximity to or bottom of metal tank.
4	**1-10**	Unclear result – showing multiple reflections across entire scanning range. No reflection is significantly higher than the others (pick strongest reflection).
3 - 1	**N/A**	Undefined
0	**0**	No reflection detected within radar detection range (Tank height + 5cm). The tank height is incorrect or the sensor is pointed towards a non -reflective surface.
15	**15**	No communication with Radar Board. Likely hardware Fault.

5.5 Blind-zone

The area immediately below the surface of the radar sensor can be problematic to measure. This is caused by reasons such as the erroneous detection of inter-related (secondary) reflections and the strength of the radar signal in a very small air space.

These problems can be exacerbated when using curved-top tanks which can create unpredictable reflection effects.

The Blind-zone allows the minimum measurement distance (from the surface of the sensor) to be reduced from 14cm to 8cm by the radar taking a "snapsnot" of the air-space within the Blind-zone and saving the "snapshot" to memory. All subsequent measurements will then subtract that snapshopt from subsequent readings to mitigate the unpredictable reflection effects.

Steps to successfully activate Bline-zone scanning:

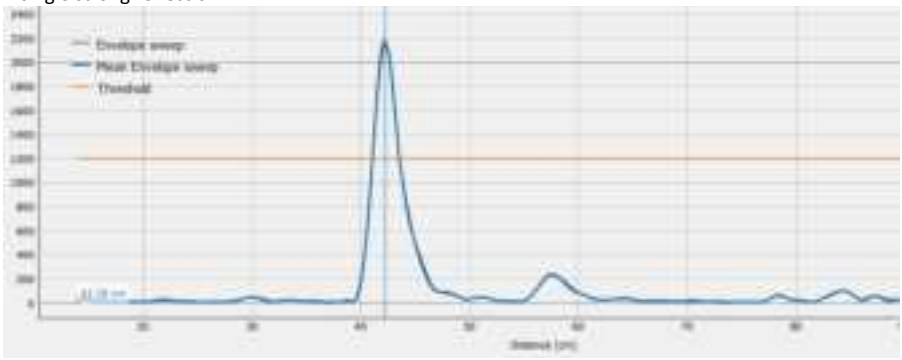
1) Ensure ullage > 250mm to ensure only the "air gap" is scanned.
2) Initiate the Blindzone snapshot by issuing **R5=16,1** to device.
3) Enable routine blindzone scanning be enabled by setting **S46=02**.

Note **-** Disabling blindzone scanning can be performed by setting S46=00.

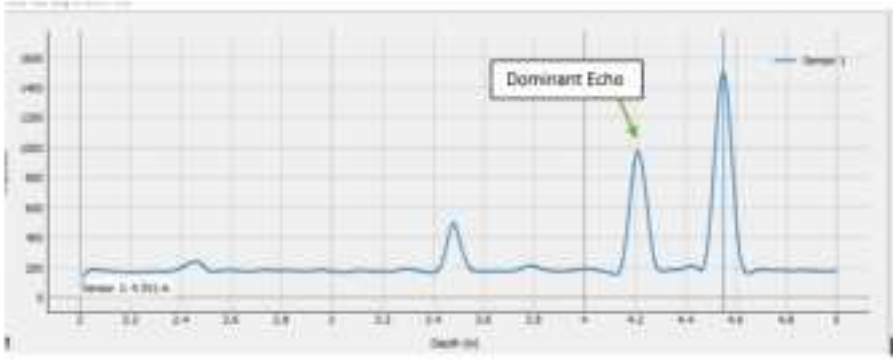
Note – It is recommended to periodically re-scan the Blind-zone as the installation environment may change over time (such as dirt or humidity) which can distort the blindzone snapshot.

5.6 Examples

Ideal measurement.
A single strong reflection.



The importance of correctly defining the tank height.
A metal bottomed tank gives a stronger reflection than the Oil level 20cm above.



6. Secure communications

The device supports two layers of secure alternate communications:

- HTTPS POST (Direct)
- Azure IoT-Hub + HTTPS POST Authentication.

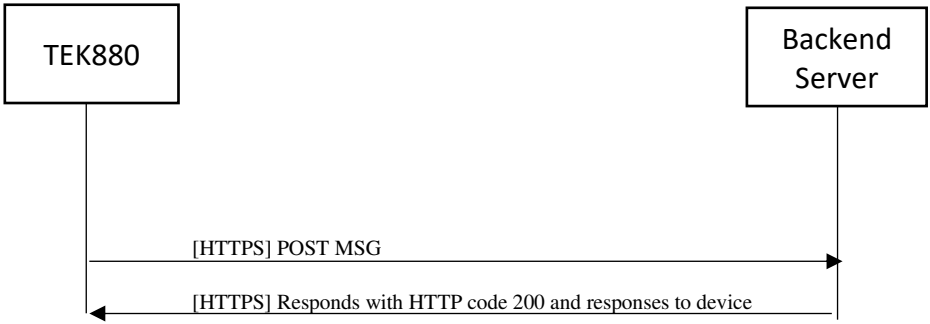
6.1 HTTPS Post (Direct)

HTTPS POST (Direct) is the easiest way to implement a secure communication with a server without requiring a two-stage authentication process and all the associated complexity.

This is the same mechanism as the token retrieval process in the two-stage IoT-hub secure communications, but all payloads are submitted via HTTPS POST rather than being sent via IoT-Hub.

This solution offers TLS 1.2 encryption HTTPS link to a web server using standard HTTP POST to convey the binary payload within message body. An authentication header can be specified to provide an additional layer of protection against unwanted or incompatible requests.

Upon successful receipt of the payload, the server will response with the conventional “200 OK” response. Any additional ASCII responses to the payload should be included in response body.



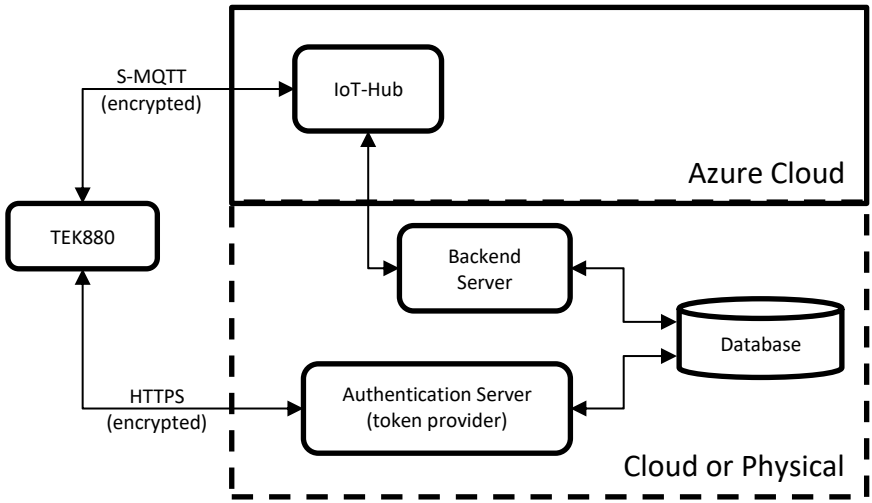
6.1.1 Sample HTTPS POST Payload

POST /authentication/nodered HTTP/1.0
Host: level.tekelek.com
Authorization: AFrT2J7I6A87%7POrrGF3ibcsBrsC2Qll9KSCw
Content-Type: multipart/form-data
Content-Length: 40

2201050474001D5D00086973806928876400E938C06B3201000D3F9EF80000006C2800020801580B

Note – The payload is represented here as a HEX string, in practice it will be a binary payload.

6.2 Azure IoT-Hub



The TEK880 sends payload messages to the backend server using the IoT-Hub service as a broker. Since the IoT-Hub is a highly secure service, it requires devices to authenticate themselves on each connection. The existence of a secondary web service to manage the authentication credentials, here called authentication server, is essential to guarantee a secure and reliable ecosystem.

From the diagram, both servers and database may be hosted in a cloud system or not, depending on the preference of the system architects. From the perspective of the TEK880 it does not make any difference if the authentication server operates in accordance with specifications described in this document.

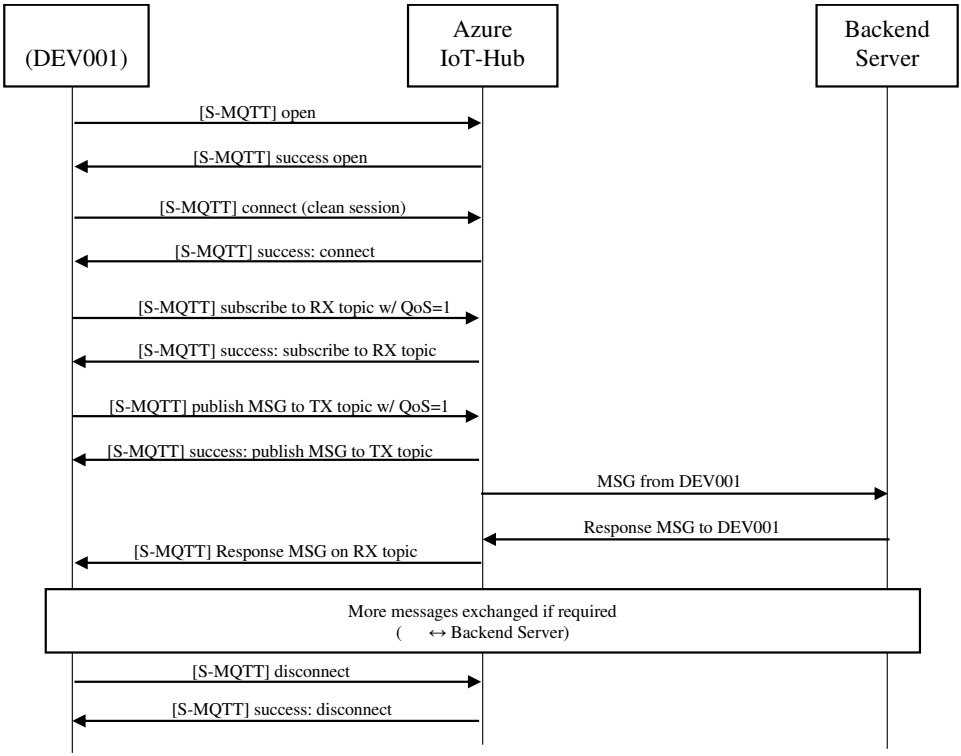
When the TEK880 is configured to operate in Azure IoT-Hub mode, it will transmit data to the hub using S-MQTT protocol, which is the MQTT protocol running over the security layer TLS ver. 1.2, on the standard port 8883. The TLS layer grants encrypted communication between IoT-Hub and TEK880. S-MQTT has been selected over S-AMQP and HTTPS because of its superior performance in the IoT-Hub, especially when compared with HTTPS. Being a lightweight protocol and more standardized than S-AMQP, are the primary criteria for this choice.

Note **-** See separate Azure IoT Hub operation manual for more information.

6.2.1 Device Communication Scenarios

6.2.1.1 Data drop

By default, every time the TEK880 sends a payload to the backend server, it will contact the IoT-Hub using S-MQTT protocol. A connection will be established based on the S-MQTT settings described below. After the message has been submitted to the transmit topic, the unit expects a response from the backend server on the receive topic. It is highly recommended for the backend server to send the shutdown and sleep command (R1=80) to the unit, when there are no more messages to be exchanged.

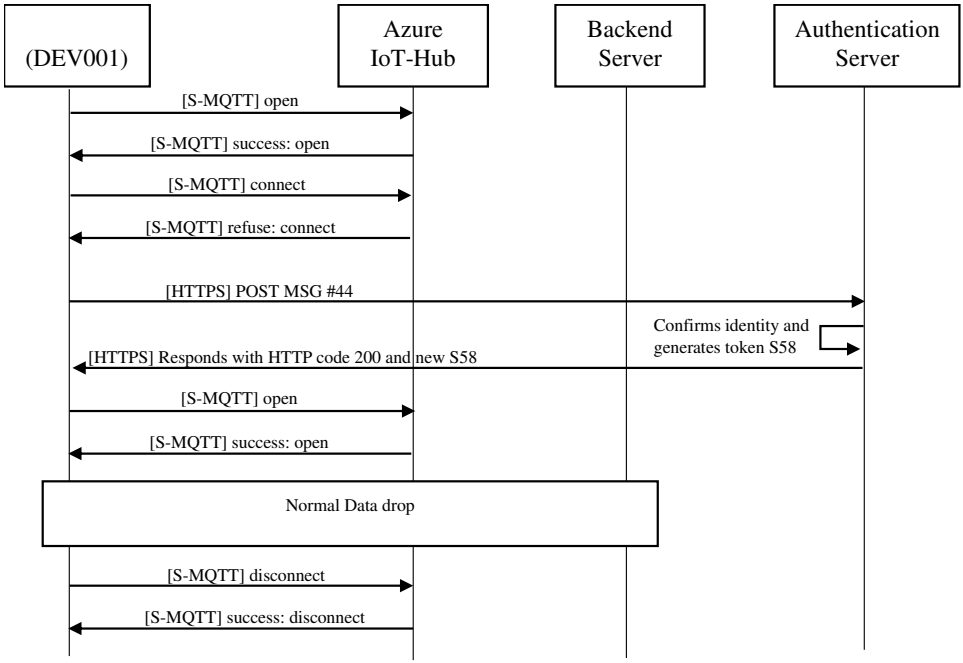


6.2.1.2 Token retrieve

During the process of sending a message to the data server, if the IoT-Hub refuses the S-MQTT connection, the unit will try to retrieve new password (Token) (S58) from the authentication server. The TEK880 will send a message #44 from the device protocol, to prove its identity. With message #44, the authentication server can read, among other things, the following unit details:

- Modem IMEI
- Modem firmware revision
- SIM card ICC-ID number
- Product type
- PCB hardware revision
- Microcontroller firmware revision

The following diagram summarises this process.



After contacting the authentication server and receiving a new token, if the S-MQTT connection with IoT-Hub is refused again, the device will ignore the transaction and return to a dormant state until the next scheduled contact, to save battery. The same will happen if the HTTPS response code from the authentication server is anything other than 200.

It is important to emphasise that, as this is a safety mechanism to retrieve the token S58, if the authentication server credential S62 is used, it must be a long lived one because there is a risk that the unit would otherwise be remotely unreachable.

6.3 Device Configuration Settings

Secure communication requires some additional “S” parameters in order to function correctly. It is very important this is configured correctly to ensure sufficient quality of service and prevent any connection problems.

Please see S-Parameter description for more information.

6.3.1 S3 Control1 Configurator

This parameter is used to set the GSM connection type. The purpose of this is to ensure a fast connection to data services due to the larger data overhead associated with secure communications.

The last 2 least significant bits of this configurator must be set to 4 (CAT-M1 Forced) or 3 (2G-GSM Forced). At the present date it is highly recommended to avoid using NB-IoT (NB1) in Azure IoT-Hub mode due to limited speeds of this technology.

See S3 for more details.

6.3.2 S15 Destination Server Address

IoT Hub address, without the text “http://www.”
See S15 for more details.

6.3.3 S16 Destination Server Port

S-MQTT port 8883 will typically be used.
See S16 for more details.

6.3.4 S23 Retry Control

It is recommended the retry timer to be longer than 30 secs and a retry tickets more than 3. This is translated to S23=12 at minimum.
See S23 for more details.

6.3.5 S53 Alternate communications settings

By default, the device is configured to deliver its payloads over conventional TCP without any end-to-end security. S53 allows for another two communication methods of increasing levels of security (and complexity).

- **Alternate comms mode –** Used to select which alternative communication mode is required
  - Max - 2
  - Min - 0
- **Authentication Server mode –** Used to select whether an Authentication server should be used
  - Maximum 1
  - Minimum 0

S52 byte description

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
Mode3	Mode2	Mode1	Mode0	Comms3	Comms2	Comms1	Comms0

- Bit 7 – 4 Authentication Server Mode
  - 0b0000 = No Authentication Server
  - 0b0001 = HTTPS (IoT-Hub)
- Bit 3 – 0 Alternate Comms Mode
  - 0b0000 = Alternate comms disabled
  - 0b0001 = HTTPS Post (Direct)
  - 0b0010 = MQTT Azure/IoT Hub
  - 0b0011 = N/A
  - …
  - 0b1111 = N/A

Example:
S52=01 (HTTPS Post /Direct)

S52=12 (MQTT Azure / Authentication server)

6.3.6 S54 Secure communications settings

Azure/IoT-Hub is an MQTT broker which facilitates the delivery of data between an IoT device and your server. As such it is possible for occasional messages to lost in the event of network or infrastructure problems.

This risk is mitigated by specifying the Quality Of Service (QOS) to indicate the importance of the message and to what lengths the MQTT broker should attempt to guarantee the delivery of the data. Typically, a higher QoS has additional costs associated with it.

- **Subscribe Quality of Service –**
  - Max - 2
  - Min - 0
- **Publish Quality of Service –** Used to select whether an Authentication server should be used
  - Maximum 1 (2 Not supported in IoT dub)
  - Minimum 0

S54 byte description

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
N/A	N/A	N/A	N/A	Pub1	Pub0	Sub1	Sub0

- Bit 7 – 4 N/A – Leave as 0
- Bit 3 – 2 Publish QoS
  - 0b00 = Pub QoS 0 (“At most once”)
  - 0b01 = Pub QoS 1 (“At least once”)
  - 0b10 = Pub QoS 2 (Not supported in IoT Hub)
  - 0b11 = N/A
- Bit 1 – 0 Subscribe QoS
  - 0b00 = Sub QoS 0 (“At most once”)
  - 0b01 = Sub QoS 1 (“At least once”)
  - 0b10 = Sub QoS 2 (“Exactly once”)
  - 0b10 = N/A

Example:
S54=11 (Set Subscribe and Publish QoS to 1 and 1 respectively).

Note - This parameter is write only. It cannot be read back for security reasons.

6.3.7 S55 Authentication Server Address

Without the text “http://www.” or the resource path.

Parameter	Description	Example
S55:	Authentication Server Address (128 char ASCII)	S55=level.tekelek.com

Note - This parameter is write only. It cannot be read back for security reasons.

6.3.8 S56 Authentication Server port number

HTTPS Port 443 will typically be used.

Parameter	Description	Example
S56:	Authentication Server Port (ASCII Number)	S56=443

Note - This parameter is write only. It cannot be read back for security reasons.

6.3.9 S57 S-MQTT Username

MQTT Username. This credential is issued as part of the connection sequence alongside the Token.

Parameter	Description	Example
S57:	S-MQTT Username (128 char ASCII)	S57=radarhub.azure-devices.net/DEV001/api-version=2018-06-30

Note - This parameter is write only. It cannot be read back for security reasons.

6.3.10 S58 S-MQTT "Token" (Password)

Token to authenticate to IoT-Hub. This will be used as password on S-MQTT settings, in accordance with IoT-Hub specifications.

Parameter	Description	Example
S58:	S-MQTT Token/Password (256 char ASCII)	S58=SharedAccessSignature sr=radarhub.azure-devices.net%2Fdevices%2FDEV001%2Fapi-version%3D2016-11-14&sig=cwpe2Ghu7cM0RJ2OPokwpOXuniEZWLB4wIrgn8hMtqU%3D&se=1677073519

Note - This parameter is write only. It cannot be read back for security reasons.

Note – This must represent the full token string including the unique device ID.

Note – This token will typically be overwritten by the authentication server according to the pre-determined token renewal period.

6.3.11 S59 S-MQTT Subscribe Topic

The S-MQTT subscribe topic is submitted as part of the connection sequence. It allows S-MQTT responses from the server to be received to the device.

Parameter	Description	Example
S59:	S-MQTT Publish Topic (128 char ASCII)	S59=devices/DEV001/messages/devicebound/#

Note - This parameter is write only. It cannot be read back for security reasons.

6.3.12 S60 S-MQTT Publish Topic

The S-MQTT publish topic is submitted as part of the data sending sequence. It allows M-MQTT payloads to be delivered to the server.

Parameter	Description	Example
S60:	S-MQTT Publish Topic (128 char ASCII)	S60=devices/DEV001/messages/events/

Note - This parameter is write only. It cannot be read back for security reasons.

6.3.13 S61 Authentication Server path

HTTPS POST Server resource path without the initial "/" character.

Parameter	Description	Example
S61:	Authentication Server Path (128 char ASCII)	S61=authentication/iothub

Note - This parameter is write only. It cannot be read back for security reasons.

S62 Authentication Server Authorization Header

HTTPS Post Authorization header. This string includes the keyword and the corresponding value.

Parameter	Description	Example

S62:	Unique Device ID (128 char ASCII)	S62=Authorization: AFrT2J7I6A87%7POrrGF3ibcsBrsC2Qll9KSCw

Note - This parameter is write only. It cannot be read back for security reasons.

Note - If used, this credential is recommended to be long-lived or renewed carefully.

6.3.14 S64 Unique Device ID

The unique Device-id will be saved into the device during production and must be separately pre-registered with IoT-Hub. This parameter is used during the handshake process with the MQTT server.

Parameter	Description	Example
S64:	Unique Device ID (64 char ASCII)	S64=DEV001

7. Technical Specification

7.1 Reed switch interface

A magnetically activated Reed Switch is used to interact with the device.
Hold the magnet against the “Hot Spot” for > 1 second to activate Bluetooth Low Energy (BLE) advertisement mode.
This is indicated by a sequence of double beeps.

Holding the magnet against the “Hot Spot” for > 5 seconds forces a quick distance measurement and uploads the data to the server.

7.2 LED output

There is no LED visible on the TEK880 device.

7.3 BLE Interface

This allows the Tekelek BLE App to be used to perform certain activities that relate to commissioning and diagnostic of the device.

BLE mode uses the same “R” and “S” parameter scheme as is used when generating responses to a data delivery to the server.

See separate guide on using the BLE Phone App.

7.4 Accelerometer

The device comes equipped with an accelerometer which can indicate how flat the mounting surface is or whether the device is in motion.

7.5 GSM Connectivity

GSM / Cellular connectivity is provided by an on-board cellular modem. This modem is compatible with 2G, NBIOT and CATM1 data communications.

8. On-site Maintenance Checks

8.1 Mounting

During on-site maintenance, the operator must ensure that the GPS tracker is still securely tightened.

8.2 ATEX / IECEx / Hazloc

Observe ATEX installation instructions guidance.

8.3 Environment

During on-site maintenance, the operator must check that external environment does not degrade the performance of the sensor, such as clay, dust, water, etc.

FCC Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must be at least 20.1 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide.

9. Trouble Shooting

9.1 Buzzer codes

	Function

For further details please see additional documents:

- *DS-5079-XX Datasheet*
- *9-6121-XX Ultrasonic Long Range 4G LTE Installation Guide*
- *9-5965-XX Product ID reference document*
- *9-6140-XX Battery Replacement*
- *9-6141-XX SIM Card Replacement*

SEAMUS NOTE:

Review of work to date.

1. Font size – 8 is small ?
2. NB-IoT bands – explanation.
3. RRC explanation improve.
4. Installation – add section for straps etc.
5. Drawings of devices.