

USER MANUAL & SAFETY REGULATIONS

DIS FARADAY C-V1.0



1. OPERATION OF THE DEVICE

1.1 Collection and Transmission of Information

The device collects and transmits information to, among other things, determine their location. It does this through sensor data. Depending on the configuration, the location can be calculated based on GNSS satellite data and network towers of surrounding masts. The Faraday C-V1.0 can also do this via WiFi access points. The reception of GNSS satellite (better known as GPS) only works when the GNSS antenna is placed in close proximity to the outdoors. In practice, the antenna usually doesn't work indoors due to interference (disturbance in radio waves) caused by metal, concrete, bricks, roof tiles, or wood. The Faraday C-V1.0 can, through specific commands, enable Bluetooth. Additionally, the Faraday C-V1.0 also features WiFi scanning, wherein it collects device BSSID addresses. The transmission of a message works by using the telecom network. The devices are initially configured to send data over LTE Cat M1, and if that fails, they are configured to switch to NB-IoT. The Faraday C-V1.0 also has an additional feature that, if the location message still can't be sent, it buffers the data and tries again at a later time.

	Sending information	Collecting information
Faraday C-V1.0 (6 radiocomponents)	LTE Cat M1 Narrow Band IoT Bluetooth signal	GNSS location WiFi scanning Network masts, Temperature indication Tamper sensor Acceleraiion sensor Sub Ghz beacon receiver

Figure 1: Overview table: operation of the devices

1.2 Possible reasons for failure

There are two possible scenarios where the data wouldn't be able to transmit:

1. There is no telecom tower nearby that can handle the LTE Cat M1/NB IoT protocol.
2. The module is in a so-called 'Faraday cage'. This means that the environment disrupts the signal to such an extent that no radio signals can be transmitted to the telecom tower.

1.3 Triggers

The device only operates when so-called triggers turn active. By default, the device is in 'sleep mode' (this is 99% of the time). The device 'wakes up' and is thus activated by four different types of triggers. When this happens, a message is sent containing information about the status of the device and any sensor data. This data is used to calculate the location.

The four triggers are:

1. Time

A configurable wake-up. Default is once every 24 hours;

In this example, the device wakes up every 24 hours to send a message.

2.

2. Start movement

With a configurable definition of movement (G-forces and duration), the device sends a message;

The basic configuration is 3 events of 1.14 G within 30 seconds.

3. Stop movement

If the status of the device is 'in motion', it doesn't send a message until it has detected no movement for longer than X amount of time;

X time is default 10 minutes; it is however configurable.

4. Tamper sensor

If the magnet on the back of the casing is removed, it sends a message*.

*The device has a configurable message budget. The default is 10. If it has made 10 attempts to send something (successful or unsuccessful), it won't try again within the configured wake-up period (default 24 hours).

1.4 Receiving Data

The devices send data that can be received in three ways:

Option 1

The data is sent to the TIP (The IoT Provider) cloud. This data is accessible at <http://cloud.theiotprovider.com>. You can log in with your credentials. Afterward, you can manage your products, adjust configurations, view information, and utilize the HTTPS API through this platform.

Option 2 (not yet available)

The device is configured to send data to the specified IP address via MQTT. As a customer, you must set up an MQTT server yourself. There is a set of commands to update and configure the product. Refer to the documentation for details on the website, when this service is available.

2. MOUNTING INSTRUCTIONS

Later

01

•

02

•

03

•

04

•

3. LIFESPAN

3.1 Device Lifespan - Base Configuration

The lifespan of the device in base configuration is developed in a way that it's capable of being active for 150.000 event seconds. A configuration that doesn't seek GNSS and is located near a telecommunication tower will be awake for approximately 8 event seconds each time. Consequently, in this case the device should be able to send about 10 messages per day, over a period of 5 years.

3.2 GNSS Lifespan

However, when the device **does** search for GNSS, it has a configurable timeout of 180 seconds. This means that the product goes to sleep after 180 seconds. In practice, this implies that with one message per day, the batteries* will be depleted after 2,5 years (approximately 940 messages in total).

*Battery performance is influenced by temperature. The optimal operating temperature is 20 degrees. The device functions between -20 & +65 degrees.

4. INTENDED USE

- The device is designed in such a way that it doesn't need to be opened. This also isn't recommended due to safety reasons.
- The code on the sticker at the top of the device must remain visible at any time as it serves as the unique identifier and the radiation direction of the antenna.
- The device is IP67 tested. This means that the device is waterproof at a depth of 1 meter for 30 minutes.

5. DISCLAIMER

As the device is normally in 'sleep mode', it doesn't retain the location information of GNSS satellites or LTE Cat M1 network towers. Consequently, it may occasionally fail to establish a connection and at other times succeed to do so.

The device shouldn't be opened. If it is opened anyway, the warranty will be voided.