

Chapter 9. Ship Security Alert System (SSAS) service

C200M/C700 GMDSS supports SSAS (Ship Security Alert System) functionality. When enabled, the SSAS service allows the transmission of security alerts from the vessel in response to security threats. When activated by the ship's master or crew, the system automatically sends alert messages to predefined recipients including the ship operator and relevant authorities. This system enables rapid response to maritime security threats such as piracy, terrorism, or armed robbery.

9.1 SSAS Box Alert and SSAS Box Test

SSAS Box Alert



The SSAS Box Alert, as shown in the illustration, has a single red latched button with a built-in LED light. When you press the button once, it stays pressed; pressing it again will release it back to its original position. There is a clear over that protects the button from being accidentally pressed.

You can use this button in two ways:

- When used alone, it activates the SSAS Alert.
- When used together with the Test button, it triggers a Test Alert.

SSAS Box Test



The SSAS Box Test has a single green button with a built-in LED indicator. This is a momentary button, so it returns to its original position immediately after you release it.

When you use this button together with the SSAS Box Alert, it activates the SSAS Test Alert, and the LED blinks to indicate that the test alert is active.

9.2 Activating a SSAS Alert

Activating a SSAS Alert:

1. Firmly press one of the SSAS Box Alert buttons so that it latches into the down position.
2. If the SSAS Alert was activated by mistake or you wish to cancel the alert before the message is sent, press the button again within the 30-second window (the SSAS Box Alert button uses a latched mechanism) to release the button.
3. If the button remains latched for 30 seconds, a SSAS Alert message is automatically transmitted to the designated recipient.
4. After this, the alert message will continue to be retransmitted at the interval configured in the SSAS configuration menu.

Cancelling an SSAS Alert (after transmission):

1. Press the SSAS Box Alert button again (the SSAS Box Alert button uses a latched mechanism) to release the button and stop the active SSAS Alert.
2. The system then sends a cancellation message to the recipient.

9.3 Activating a SSAS Test Alert

Activating a SSAS Test Alert:

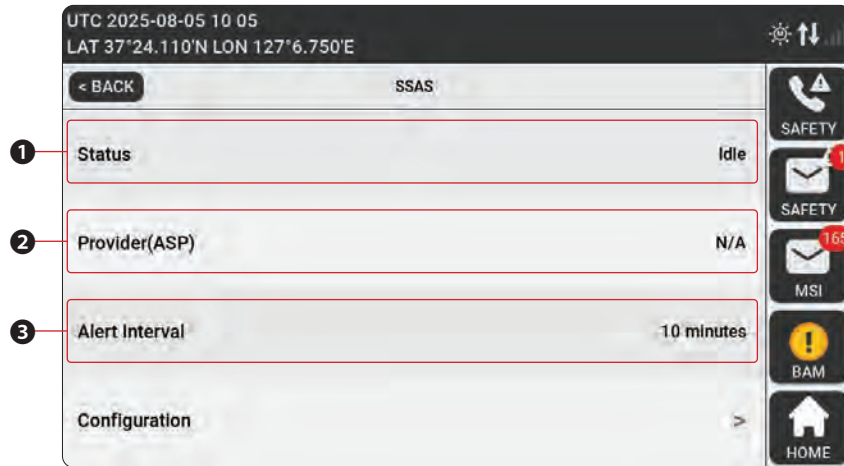
1. Press and hold the SSAS Box Test button.
2. Continue holding the SSAS Box Test button, and press one of the SSAS Box Alert buttons so the it is latched in the down position.
3. When the SSAS Test Alert is activated, the LED on the SSAS Box Test button will blink at 250ms intervals. You may then release the SSAS Box Test button, but the SSAS Box Alert button must remain latched.
4. To cancel before transmission: If the test was activated by mistake, press the SSAS Box Alert button again within the 30-second window to release the button. The SSAS Box Test button LED will turn off when deactivated.
5. Automatic transmission: If the SSAS Box Alert button remains latched for 30 seconds, a test alert message is automatically transmitted to the designated recipient, and the LED on the SSAS Box Test button will blink more quickly at 100ms intervals.
6. After transmission, the test alert message will continue to be retransmitted at the configured interval.

Cancelling a SSAS Test Alert (after transmission):

1. Press the SSAS Box Alert button again (the SSAS Box Alert button uses a latched mechanism) to release the button and stop the active test alert. When the test alert is stopped, the LED on the SSAS Box Test button will turn off.
2. The system then sends a cancellation message to the recipient.

9.4 SSAS Status

Go to **Menu** → **Non-GMDSS Function** → **SSAS**. The SSAS Status section provides information on the SSAS service status. The key parameters shown in the SSAS Status display are:



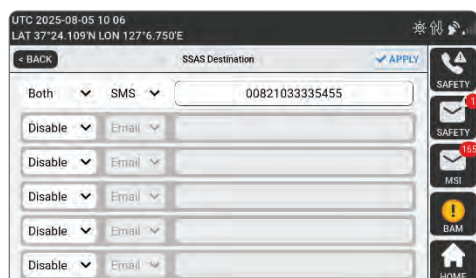
No.	Item	Description
①	Status	Displays the current status of the SSAS service. • Not Configured: Required settings have not been completed, so the service is unavailable. • Idle: The system is on standby, ready to send an alert or test alert as needed. • Alert ready: The system is waiting to send an alert. Cancellation is possible before transmission. • Alert test ready: The system is waiting to send a test alert. Cancellation is possible before transmission. • Sending alert: The system is in the process of transmitting an alert. • Sending alert test: The system is in the process of transmitting a test alert. • Sending alert cancellation: The system is in the process of canceling an alert after it has been sent. • Sending alert test cancellation: The system is in the process of canceling a test alert after it has been sent.
②	Provider (ASP)	Displays the Application Service Provider (ASP) responsible for handling SSAS transmissions. If no ASP is assigned, it shows "N/A" Otherwise, it displays the assigned ASP name (e.g., polestar).
③	Alert Interval	Displays the configured alert message sending interval. • If no alert interval is configured, it shows "No alert interval configured." • If an alert interval is set, it displays the configured value (e.g., 10 min, 20 min, 30 min, etc.).

9.5 SSAS Setting

Go to **Menu** → **Non-GMDSS Function** → **SSAS** → **Configuration**. The SSAS Setting section allows you to configure the following parameters for the vessel's SSAS system. The key settings are:



No.	Item	Description
①	Destination	Designate the contact information (Email or SMS) for the recipient or center that receives an alert message.
②	CSO (Chief Security Officer)	Enter the name and phone number of the Chief Security Officer. This information is not used for transmitting SMS; it is for reference only.
③	Secondary CSO	If the flag state requires that information, enter the name and phone number of the Secondary Chief Security Officer. This information is not used for transmitting SMS; it is for reference only.
④	Alert Interval	Set the repeat sending interval for the alert message. Available options are in 10-minute increments, ranging from 10 minutes to 60 minutes.

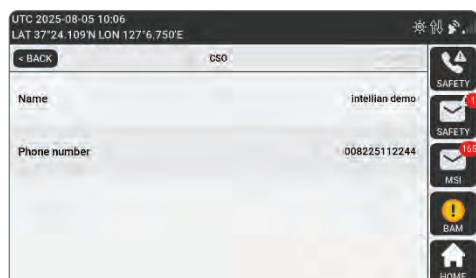


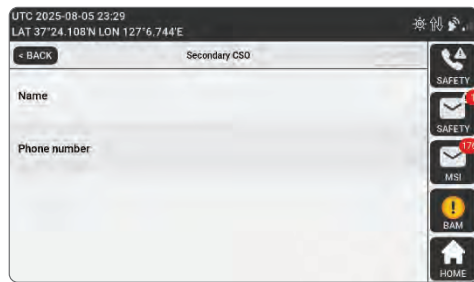
Destination

1. Select the **Destination** in the SSAS section.
2. Specify the destination using the following types.
Disable: This destination is not used.
Test: When a Test Alert is triggered, it is sent to this destination.
Alert: When an Alert is triggered, it is sent to this destination.
Both: When either an Alert or a Test Alert is triggered, it is sent to this destination.
3. Designate the contact information (Email or SMS) for the recipient or center that will receive an alert message.

CSO (Chief Security Officer)

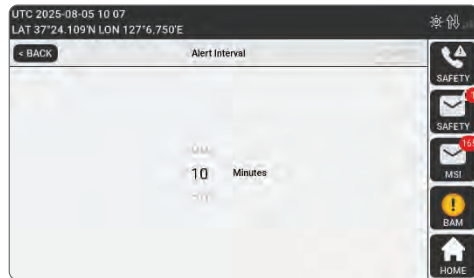
1. Select the **CSO** in the SSAS section.
2. Enter the name and phone number of the Chief Security Officer. This information is not used for transmitting SMS; it is for reference only.





Secondary CSO

1. Select the Secondary **CSO** in the SSAS section.
2. Enter the name and phone number of the Secondary Chief Security Officer. This information is not used for transmitting SMS; it is for reference only.



Alert Interval

1. Select the **Alert Interval** in the SSAS section.
2. Set the repeat sending interval for the alert message. Available options are in 10-minute increments, ranging from 10 minutes to 60 minutes.



NOTE

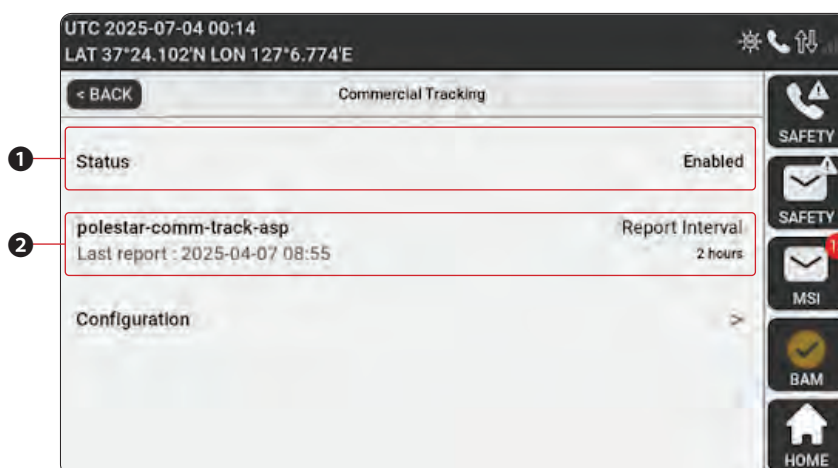
'Destination' and 'Alert Interval' are required settings. If they are not configured, the Status will display "Not Configured" and the SSAS service will be unavailable.

Chapter 10. Commercial Tracking service

C200M/C700 GMDSS supports Commercial Tracking services, which collects, analyzes, and provides information such as vessel position, movement route, and status. While LRIT supports only a single ASP, Commercial Tracking supports multiple ASPs, allowing users to use multiple providers simultaneously.

10.1 Commercial Tracking Status

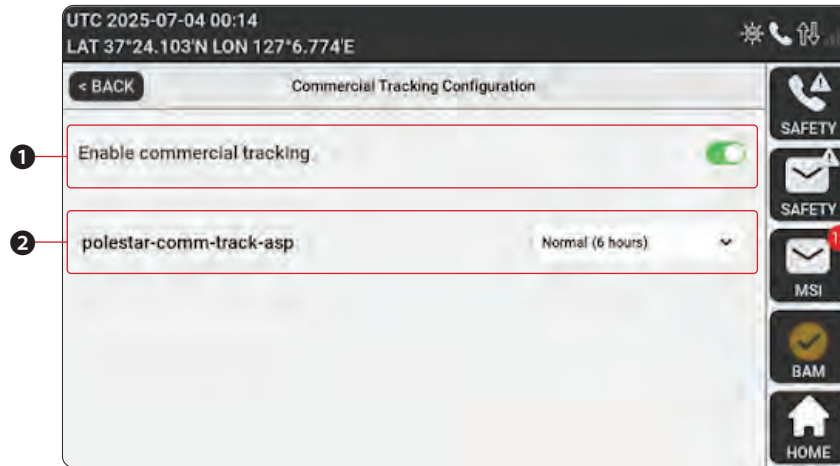
Go to **Menu** → **Non-GMDSS Function** → **Commercial Tracking**. The Commercial Tracking Status section provides essential information regarding the vessel's Commercial Tracking service status. The key parameters shown in the Commercial Tracking Status display are:



No.	Item	Description
①	Status	Indicates whether the Commercial Tracking service is currently enabled or disabled. The default value is disabled.
②	ASP Information	This section provides information about how the Commercial Tracking service is currently set up and managed. This will only be displayed when integrated with the service provider. When the service is provided by multiple service providers, each one appears as a separate entry. • Service Provider Name: Displays the Application Service Provider (ASP) responsible for handling Commercial Tracking transmissions. (e.g., polestar-comm-track-asp) • Report Interval: Report Interval: Represents the frequency at which Commercial Tracking information is transmitted. By default, it shows '6 hours' but it may display either a value set by the user or a value defined by the ASP, and the ASP can modify the value set by the user. (e.g., 2 hours) • Last Report: Shows the timestamp of the most recent attempt to transmit Commercial Tracking information.

10.2 Commercial Tracking Configuration

Go to **Menu → Non-GMDSS Function → Commercial Tracking → Configuration**. The commercial tracking configuration section provides setting for the following parameters:



No.	Item	Description
①	Enable commercial tracking	Enables or disables the Commercial Tracking service.
②	ASP Interval (e.g. polestar-comm-track-asp)	This section provides options to configure the Commercial Tracking service. This will only be displayed when integrated with the service provider. When the service is provided by multiple service providers, each one appears as a separate entry. Each entry includes configurable options that can be set independently. - Set the time interval for reporting ship position information. - Normal: Set the report interval to 6 hours (default). - Reduced (24 hours): Set the report interval to 24 hours, reducing the reporting frequency. - Disabled: Disable the reporting function, no reports will be sent.

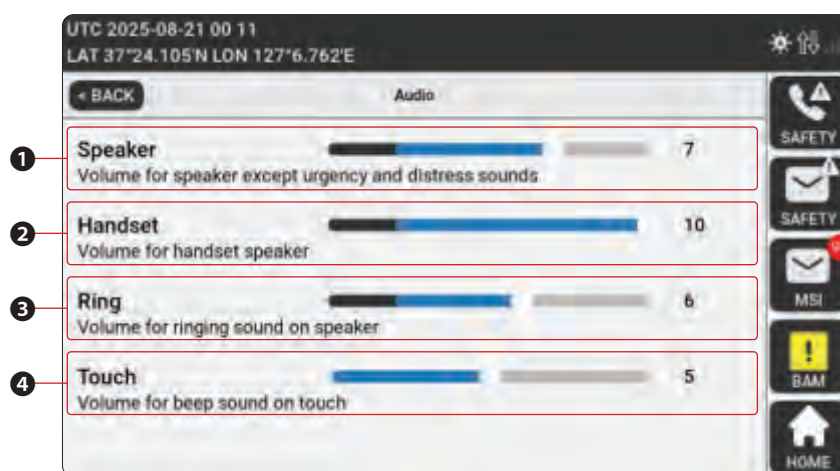
Chapter 11. System Settings

11.1 System Settings

Menu to change system settings for SDT. Go to **Menu** → **System Setting**.

11.1.1 Audio

Go to **Menu** → **System Setting** → **Audio**. The audio level can be adjusted across 11 levels in the Audio settings: most audio functions range from 2 to 10, except for touch sounds which range from 0 to 10:

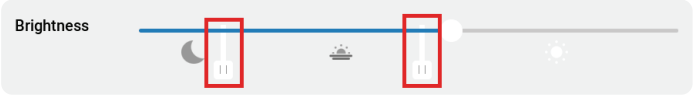


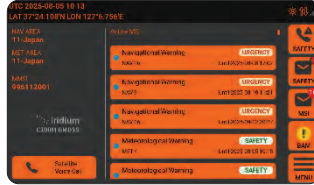
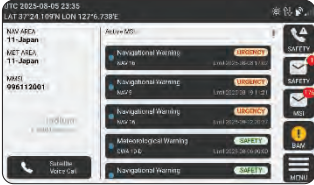
No.	Item	Description
①	Speaker	Adjust the speaker audio level on the SDT. - Available adjustments: Message Notification sound (MSI, Safety), Speaker Phone, Include ④ Touch sound
②	Handset	Adjust the audio level when using the handset. - Available adjustment: Handset audio during calls
③	Ring	Adjust the ringing volume for incoming calls. - Available adjustment: Ringing Tone
④	Touch	Adjust the audio level for button clicks on the screen. - Available adjustments: Touch key, Dial Pad (DTMF)

11.1.2 Display

Go to **Menu** → **System Setting** → **Display**. Change the Brightness and Display Theme:



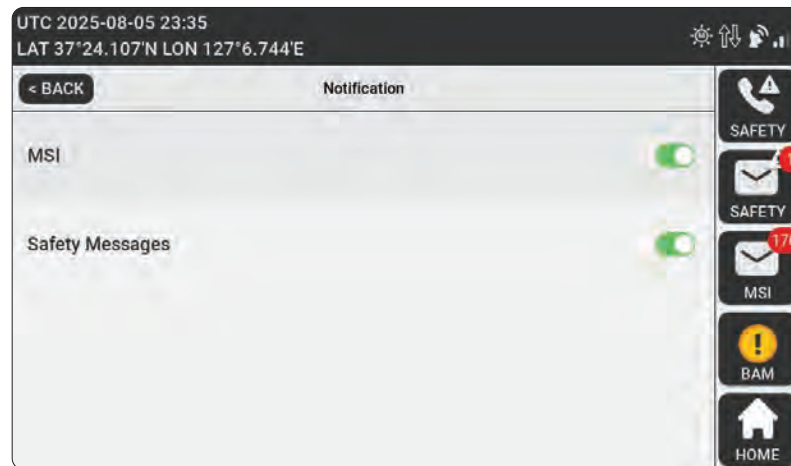
No.	Item	Description
①	Auto Theme	The Auto Theme feature ensures optimal readability in any environment by automatically switching the display theme (Day, Dusk, or Night) based on the brightness level of the display. Users can customize the brightness levels at which the theme changes by adjusting two ‘transition point’ sliders:  • Day/Dusk Transition Point: Sets the brightness level at which the theme switches from the Day theme to the Dusk theme. • Dusk/Night Transition Point: Sets the brightness level at which the theme switches from the Dusk theme to the Night theme. Example: If the Day/Dusk transition point is set to brightness level 4, the theme will automatically change from Day to Dusk when the brightness decreases to level 4. When the brightness increases back above level 4, it will revert to the Day theme. Important Rules for Setting Transition Points: Please note there are two rules for setting these transition points: 1. The Dusk/Night transition point must always be set at a lower (darker) brightness level than the Day/Dusk point. 2. If both sliders are configured to the same brightness level, the system will bypass the Dusk theme and switch directly between the Day and Night themes.

No.	Item	Description
②	Manual Theme	Select the manual theme (Day/Night/Dusk).  <Day theme> <Night theme> <Dusk theme>
③	Brightness	The display brightness can be configured by selecting either ‘Auto’ or ‘Manual’ mode from the Display menu. • Manual Brightness: In Manual mode, you can directly set the brightness to your preference using a finely tuned scale of 20 distinct levels. • Auto Brightness: When Auto mode is selected, the device will use its built-in illuminance sensor to adjust the screen brightness automatically according to the ambient light conditions. For more convenient and immediate control, the Dimmer knob is located on the top-left of the device. • This knob allows you to adjust the brightness from any screen without needing to navigate through the menu. • As you turn the Dimmer knob, the current brightness level is temporarily displayed on-screen for your reference. Note: If you adjust the brightness using the Dimmer knob while the system is in Auto mode, it will automatically switch over to Manual mode at the brightness level you have just selected.   13

11.1.3 Notification

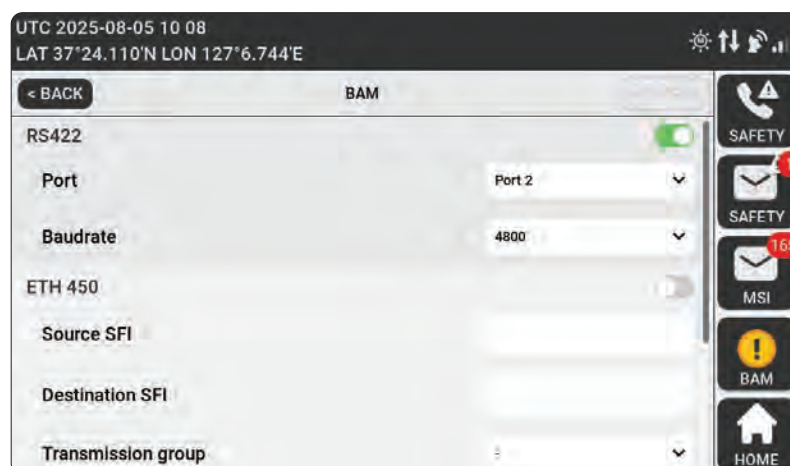
Go to **Menu** → **System Setting** → **Notification**. Choose whether to enable alarms for receiving items such as MSI, or Safety Messages.

Message notifications controllable through the notification menu are limited to safety priority messages. Messages with urgency or distress priority will trigger an audible alert and display a pop-up notification upon receipt, even if notifications are disabled.



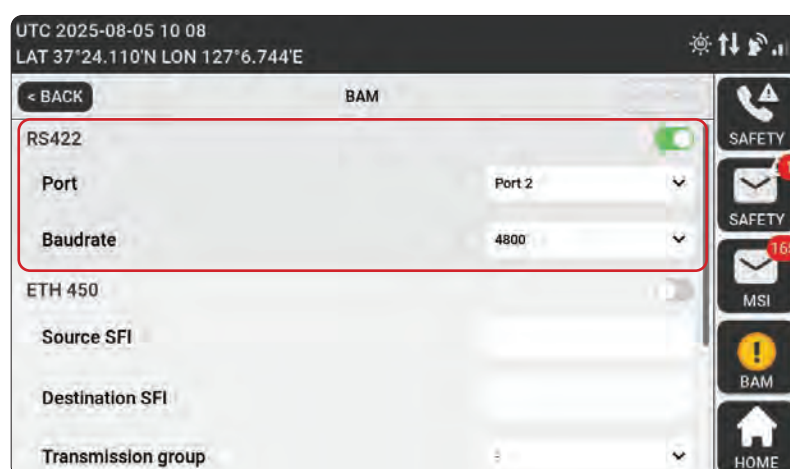
11.1.4 BAM Setting

BAM system is designed to centralize the management and presentation of alerts generated by different sources on the vessel. For the BAM system to function correctly and reliably identify the source of each alert transmitted over the interface, proper configuration of this device is essential. Go to **Menu** → **System Setting** → **BAM**. SDT can be configured with the Central Alert Management (CAM) system and network. When the SDT is connected to the CAM system, BAM Alerts can be received from CAM. You can modify the necessary settings when configuring the network. Available interfaces are Serial Interface (RS422) and Ethernet (ETH 450).



RS422

The C200M/C700 GMDSS utilizes the IEC 61162-1, 61162-2 network standard for communication with other onboard equipment.

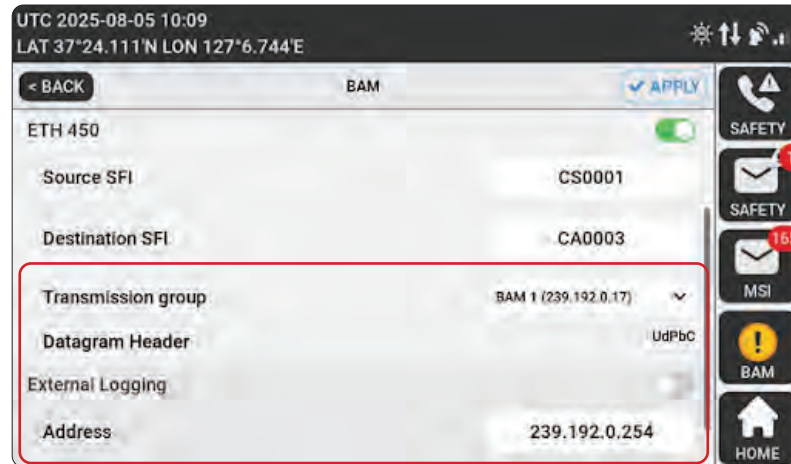


Each port can be configured for a total of 4 baud rates (4800, 9600, 19200, 38400). Refer to the Installation Guide for RS422 connection information. Use the same baud rate as the equipment (e.g., CAM) communicating via RS422. For instructions on connecting the RS422 cable, see section 12.2.2 of the Installation Guide.

- How to set up the RS422
1. Navigate to **Menu** → **System Setting** → **BAM** menu.
 2. Click the Port number to use.
 3. Click the Baudrate to use.
 4. The RS422 toggle switch can be clicked to Enable/Disable it.

Ethernet (ETH 450)

The C200M/C700 GMDSS utilizes the IEC 61162-450 network standard, also known as Lightweight Ethernet, for communication with other onboard equipment.



- **System Function ID (SFI) Configuration**

The SFI must be set correctly during the initial installation process before the ETH 450 BAM functionality is enabled for the first time. Multiple devices generating similar or identical data may be connected to the network. Each SF requires a unique identifier so that other devices on the network can clearly identify the exact source (device and function) of the data. This is called the SFI (System function ID). Using the SFI, receiving devices can select data from desired sources, differentiate data from specific devices, and prevent data conflicts or confusion.

- **SFI Structure (6-character string):**

The SFI consists of a 6-character string. The first two characters are letters and indicate the type of the SF. For the SDT's Default value, "CS", which stands for Communications satellite, is used for the Source SFI, and "CA", an abbreviation for CAM of BAM, is used for the Destination SFI. "CS" in the Source SFI cannot be changed in the SDT.

The last four characters of the SFI are numeric digits. To ensure the SFI of the SF being configured does not conflict with any other SF within the entire network on the vessel, use a number between 0001 and 9998. 9999 is a reserved value for unconfigured SFs and cannot be set. We recommend using an unassigned number in consultation with vessel's network administrator. It is crucial to verify the SFI settings before proceeding, as changing them later requires a full device reset.

- **Transmission Group Selection**

The Transmission group for ETH 450 can be selected between BAM1, BAM2 and RCOM. While the SFI 'CS' used by the SDT defaults to the RCOM transmission group, it is recommended to select BAM1 or BAM2 for its transmission group instead. This is because the SDT fundamentally acts as an alert source device that transmits BAM alerts to CAM, and these groups are specifically designated for such alert communication purposes, allowing for optimized traffic management. Also, only the UdPbC datagram header is supported.

- **How to set up the ETH450**

1. Navigate to **Menu** → **System Setting** → **BAM** menu.
2. Click **Source SFI** and **Destination SFI** to enter the desired string.
3. The ETH 450 toggle switch can be clicked to Enable/Disable it.

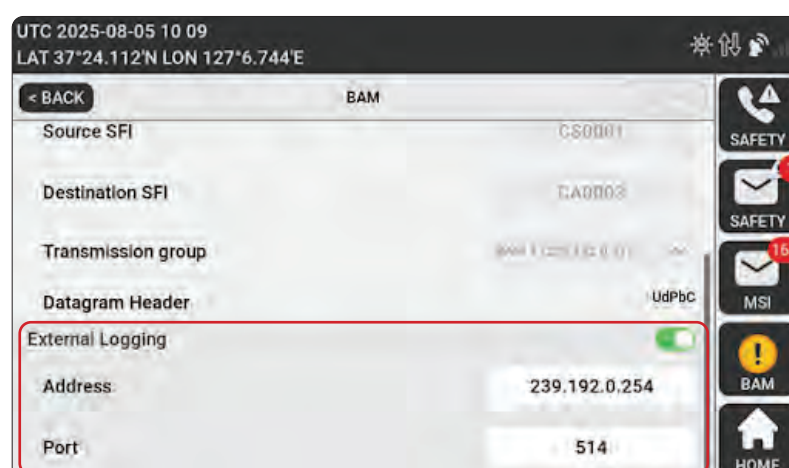
Once SFI configuration is complete, ETH 450 is ready to use.

**WARNING**

Upon enabling the ETH 450 BAM functionality for the first time, the configured Source SFI, Destination SFI and Transmission group values will be permanently locked. Therefore, if a change to a locked SFI is necessary, the only method is to perform a full Factory Reset. This procedure returns the device to its default state, erasing all configurations and requiring the setup process, including SFI configuration, to be completed again.

External Logging

The C200M/C700 GMDSS supports External logging, a function that transmits log information generated internally within the device over the network to another external server.



External logging uses the standard Syslog protocol and transmits via UDP packets to port 514, using the inputted IP address of the external server.

The method to configure External logging is as follows:

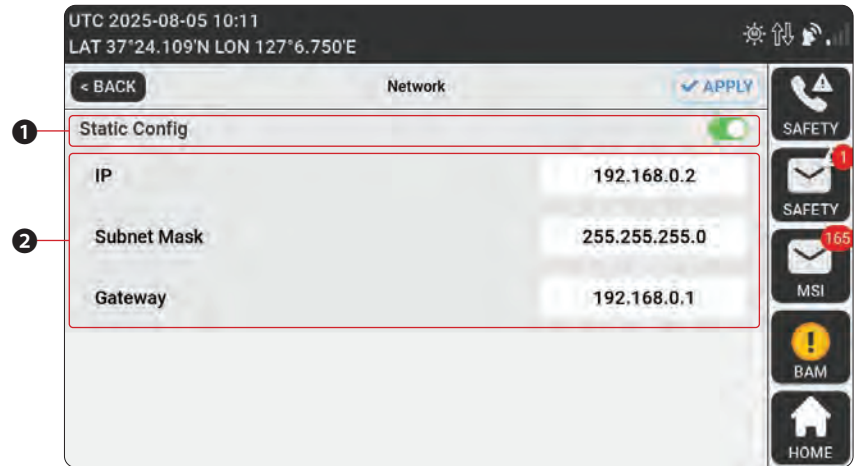
1. Enter the IP address of the external server where logs will be checked into the 'Address' field.
(The default syslog multicast address is 239.192.0.254)
2. Enter the Port number. (The standard port for External logging is 514).
3. Click the toggle switch for External logging to Enable/Disable the function.
4. Generate an error message on the device to which you want to send the error message.
5. Check SDT log for incoming error messages and error counter.
(apps.log is available for download in the SDT Web UI.)

**NOTE**

SDT's BAM ethernet interface does not change its IP address and IP port settings after an OFF/ON power cycle. IP address and port is only changing the BAM setting.

11.1.5 Network

Go to **Menu** → **System Setting** → **Network**. The network settings for ETH 450 can be configured through the Network menu.



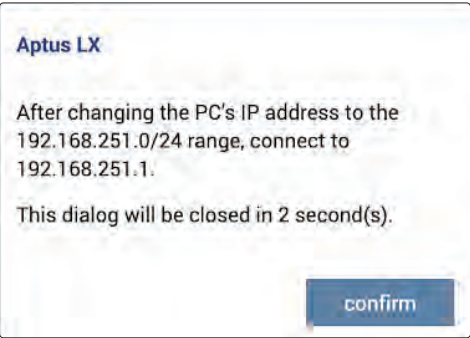
No.	Item	Description
①	Static Config	Sets the static configuration. • Enable: To set a Static IP, enable the Static Config. Configure the IP, Subnet Mask, and Gateway to the desired values. • Disable: To use the automatic IP address assignment method (DHCP), disable the Static Config. (default)
②	Management Network Configuration	Sets the management network configuration. • IP Address: Enter the network IP address (Factory default: 192.168.0.2). • Subnet Mask: Enter the subnet mask (Factory default: 255.255.255.0). • Gateway: Enter the gateway (Factory default: 192.168.0.1). Click the Apply button to apply the settings to the system.



NOTE

When the Static IP is changed to the 192.168.250.xxx IP band already in use by the SDT (Web UI access IP: 192.168.250.1), be aware that the original Web UI access IP will temporarily change to 192.168.251.1.

If the Web UI is accessed and the IP is changed to 192.168.250.xxx, the Web UI will log out and display the pop-up window as shown in the image.

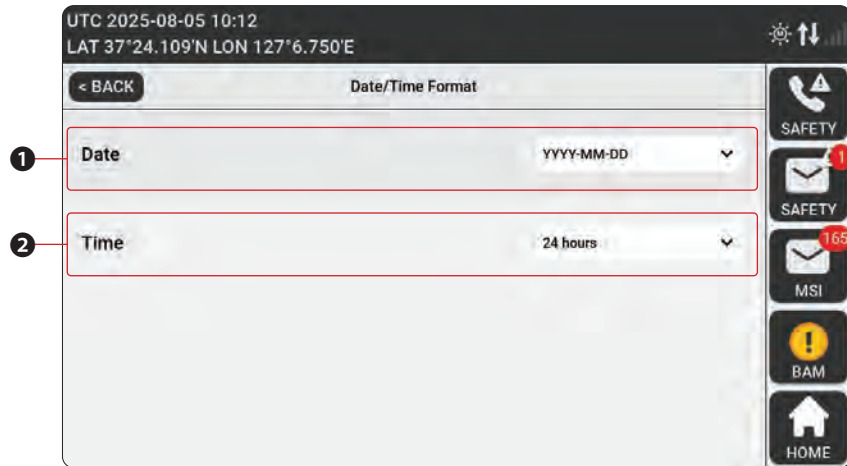


If the band is changed from the 192.168.250.xxx band to another band, the Web UI access IP will revert to its original IP (192.168.250.1).

User Settings (Ship Network IP)	System Automatic Actions	Management Address (Web UI Access IP)
Set the address to an IP outside of the 192.168.250.x band (e.g., 10.0.0.5)	No Change	192.168.250.1 (Default)
Set the address to an IP within the 192.168.250.x band (e.g., 192.168.250.20)	Management IP will be automatically changed upon IP Conflict Detection.	192.168.251.1 (Temporary Change)
Change the address back to an IP outside of the 192.168.250.x band.	Management IP will be automatically recovered upon conflict resolution.	192.168.250.1 (Default Revert)

11.1.6 Date / Time

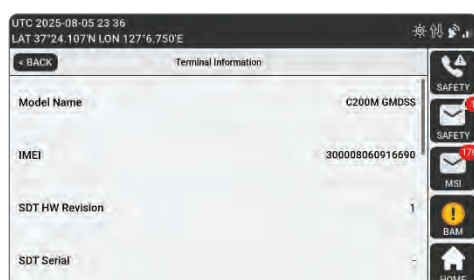
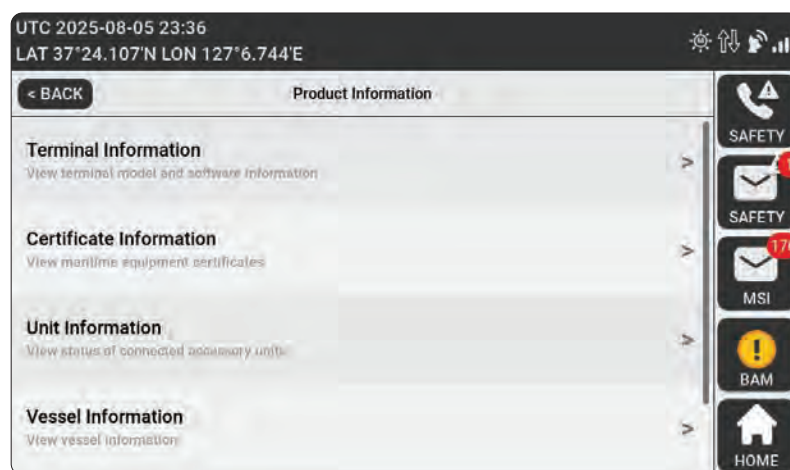
Go to **Menu** → **System Setting** → **Date/Time**. Change the display format for Date and Time on the screen:



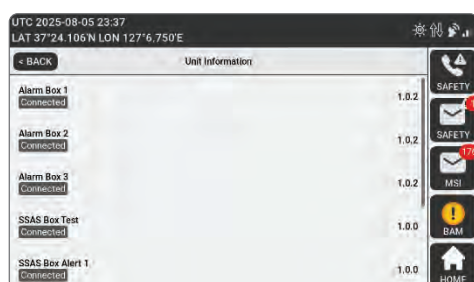
No.	Item	Description
①	Date	Select the date format (YYYY-MM-DD, MM-DD-YYYY, DD-MM-YYYY) from the Data drop-down list.
②	Time	Select the time format (12-hour, 24-hour) from the Time drop-down list.

11.1.7 Product Information

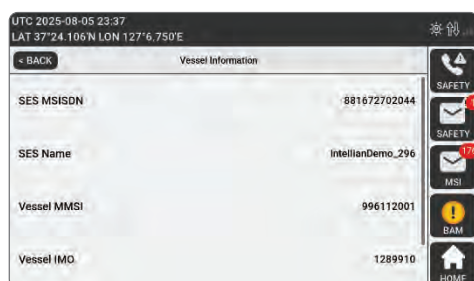
In Product Information, verify details about the GMDSS system. This menu consists of four sub-menus: Terminal Information, Certificate Information, Unit Information, and Device Environment Information. Go to **Menu** → **Non-GMDSS Function** → **Product Information**.



Terminal Information: Information about the C200M/C700 GMDSS equipment can be verified. This includes the equipment's serial number, software version information, and more.



Unit Information: Verify accessory information connected to the GMDSS system. This includes connection status, version information, etc.



Vessel Information: Users can check the registration information of the SES (Ship Earth System – regulatory name for the satcom GMDSS systems installed on vessels). The registration information is stored in the device during commissioning at the time of initial activation. The SES Information includes details such as the SES Name, SES MSISDN, Vessel MMSI, Vessel IMO Number, and Vessel Call Sign.



Device Environment Information: Verify the current temperature and voltage for ADU, BDU, and SDT.

Chapter 12. Tools

Execute the SDT test and reset the system. Go to **Menu** → **Tools**.

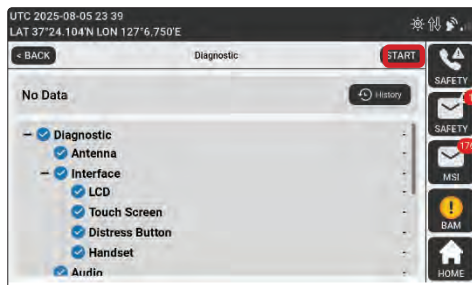
12.1 Diagnostic

C200M/C700 GMDSS provides a diagnostic function to verify whether the hardware and accessories are working properly. Users can check the GMDSS system hardware through this function and request technical service if any failures are detected. Each item can be tested individually.

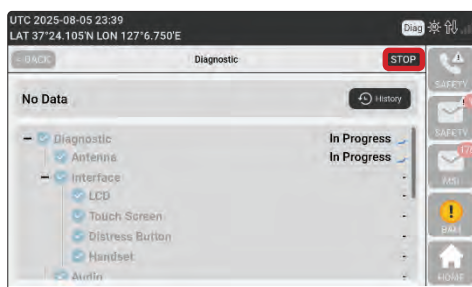
The diagnostic tests include the following:

- Antenna (ADU)
- Interface (LCD, Touch Screen, Distress Button, Handset)
- Audio
- Sensor (Light Sensor, Temperature Sensor)
- Accessories (Alarm Box, Alarm Unit, SSAS Box Alert, SSAS Box Test, Printer, Keyboard, Mouse, USB Memory)

1. Select the checkbox for each test that you want to run on the system. You can select all the tests quickly by selecting the top checkbox.

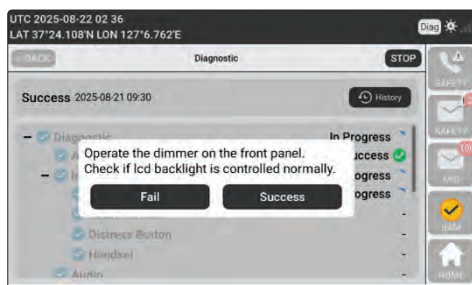


2. Click the **Start** in the upper right hand corner button to begin the diagnostic test



Once the test starts, the page will display “In Progress”.

To stop during the test, click the **STOP** in the upper right hand corner button. Restarting the test may take a few minutes.

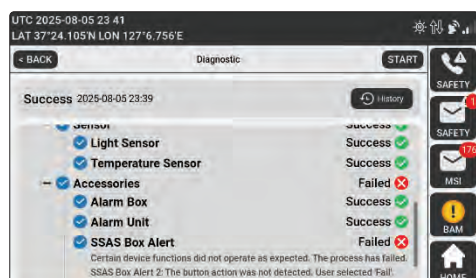


3. Follow the instructions in the pop-up window (1):
 - If a **Fail/Success** button appears, follow the test instructions in the pop-up window.
 - After completing the test, click **Fail or Success** to confirm the result.



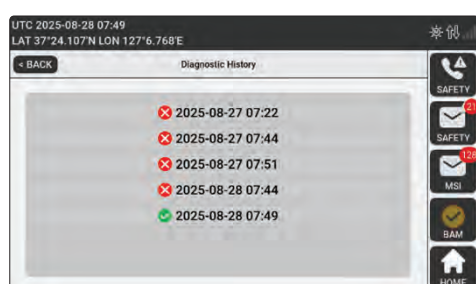
4. Follow the instructions in the pop-up window (2):

- If the **Fail** button appears in the pop-up window, follow the instructions to perform the test manually.
- If the function is working correctly, the system will automatically move to the next test.
- If the function is not working, click the **Fail** button.



5. View test results:

- After the diagnostic test is completed, the system will display the results for each item.



6. View diagnostic history:

- Click the History button to view the diagnostics conducted on each date. Clicking on a date shows the list of diagnostics performed at that time.

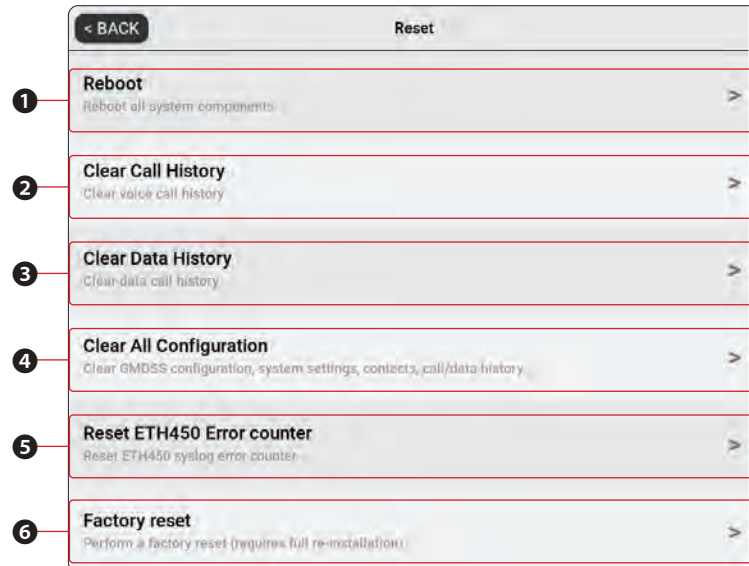


NOTE

When the Diagnostic function starts, the satellite connection will be disconnected and a related BAM alert may occur.

12.2 Reset

Reset SDT information such as Call History, Data History, Configuration, and more.



No.	Item	Description
①	Reboot	Restart SDT & BDU
②	Clear Call History	Clears all Routine voice call and Safety call history.
③	Clear Data History	Resets the data history.
④	Clear All Configuration	Resets all configurations, including call and data history, for the SDT.
⑤	Reset ETH450 Error counter	Resets the error counter that can be checked in the External Logging.
⑥	Factory Reset	Resets the current system to its factory default, including the deletion of provisioning information. <i>This function resets the terminal to its initial factory state and must only be performed by authorized service personnel.</i>

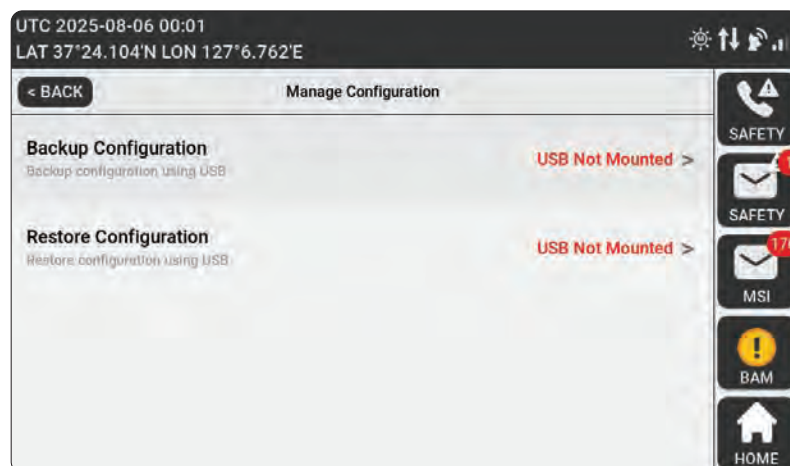
12.3 Manage Configuration

This feature provides a Config Backup & Restore function that allows users to store or load the current SDT settings using a USB flash drive. Before connecting the flash drive to the SDT, it MUST be scanned for viruses and other malware.

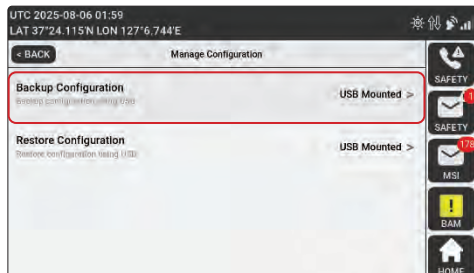


NOTE

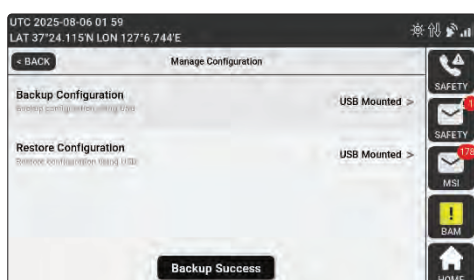
The file system format for USB memory only supports FAT32. It does not support formats like NTFS.



Backup Configuration:

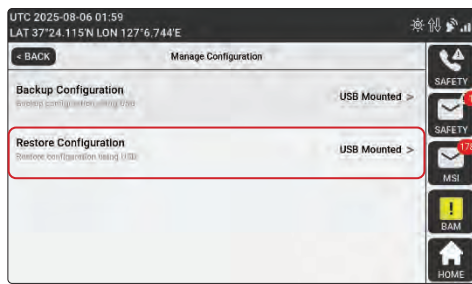


1. Connect the USB flash drive to the USB port on the rear of the SDT. Once connected, “USB Not Mounted” will change to “USB Mounted.”
2. Click the **Backup Configuration** button to save the config file.

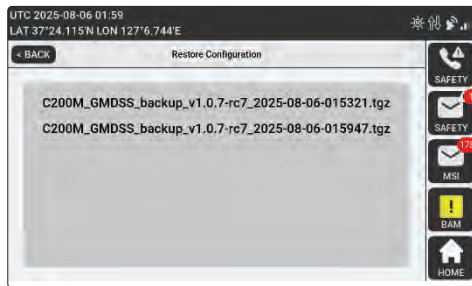


If the backup is successful, a message saying “Backup Success” will appear.

Restore Configuration:



1. Connect the USB flash drive to the USB port on the rear of the SDT. Once connected, “USB Not Mounted” will change to “USB Mounted.”
2. Click the **Restore Configuration** button to view the list of config files stored on the USB flash drive.
3. Select the desired config file. Then the system will start rebooting and restore the settings automatically.



Chapter 13. Software Upgrade

The C200M/C700 GMDSS provides a software upgrade function. Software upgrades can be performed using a USB flash drive or via the Web UI. If upgrading software using a flash drive, you must perform a virus and malware scan on the flash drive before connecting it to the SDT. For instructions on upgrading the software via the web UI, see section 14.5.1.

13.1 Software Upgrade using USB

The C200M/C700 GMDSS software can be easily upgraded using a USB flash drive. Follow these steps:

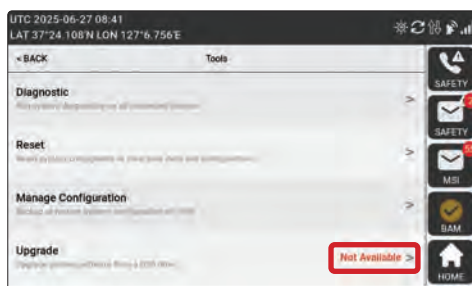
Prepare:

- Get the software file: Obtain the software package file for the C200M/C700 GMDSS, ensuring it is the latest version provided by Intellian.
- There are two types of upgrade files: Unified binary file (containing SDT, BDU, ADU, and modem), and SDT standalone binary file (containing only SDT).
- Prepare a USB flash drive: Transfer the software package file to a USB flash drive.

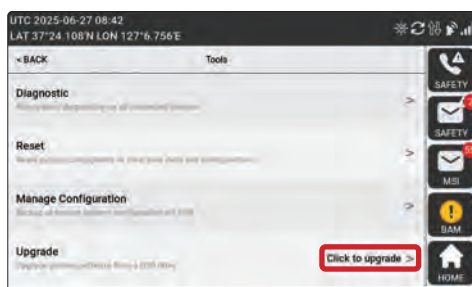
Caution:

- Do not turn off the SDT or remove the USB flash drive from the SDT during the software update. This may cause a malfunction or system damage.
- The software should be upgraded in an environment that guarantees a stable electrical power supply.
- If the upgrade fails, 'Upgrade Fail' will appear in the Status column. Try to upgrade again or use a different upgrade file.
- The file system format for USB flash drive only supports FAT32. It does not support formats like NTFS.

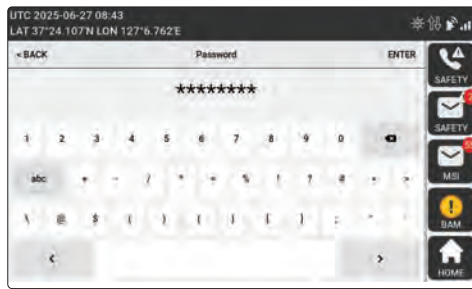
Upgrade Procedure:



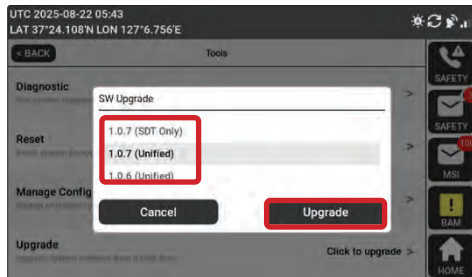
1. Navigate to **Menu** → **Tools**. Verify that the Upgrade menu at the bottom indicates **Not Available**.



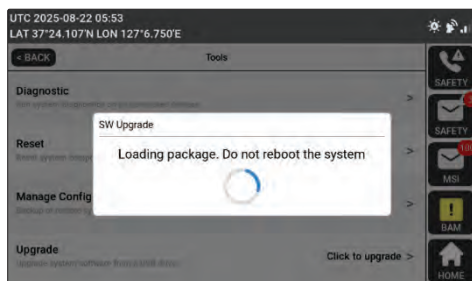
2. Connect the USB flash drive containing the software package file to the USB port on the rear panel of the SDT.
3. Verify that the Upgrade menu at the bottom has changed to "**Click to upgrade**" and click the **Upgrade**.



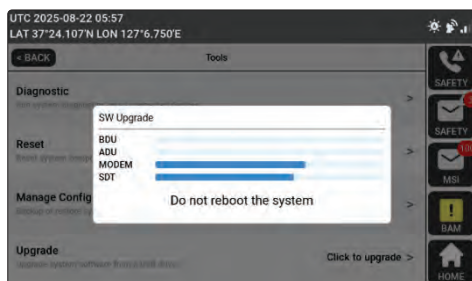
4. Enter your password to upgrade (this is the same as your account password in AptusLX, which defaults to 12345678).



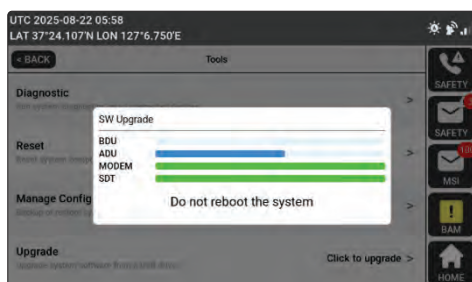
5. Showing the list of software package files, select the desired upgrade file from the list.
6. Verify the file name and click the **Upgrade** button.



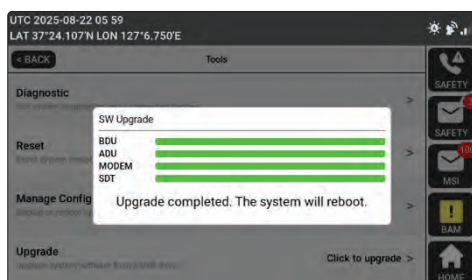
7. Loading The software upgrade package.



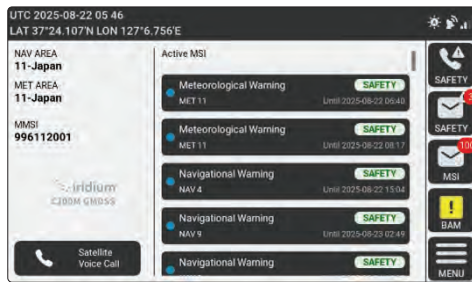
8. The software upgrade will start. During the upgrade process, the window will display the progress and status.



9. The Unified upgrade takes 10 to 12 minutes to complete, while the standalone SDT upgrade takes 5 to 6 minutes.



10. If the software is successfully upgraded, **Upgrade success** will be displayed in the progress window. Then, the SDT will start booting automatically.



11. If the SDT completes the reboot and the window displays the home screen, the upgrade is complete.



NOTE

- When upgrading the software package that includes both the SDT and BDU modules, ensure that neither the SDT nor the BDU is disconnected.
- To verify the applied upgrade status, go to **Menu** → **System Settings** → **Product Information** → **Terminal Information**. User can find the software versions for the SDT, BDU, ADU, and Modem.
- Firmware upgrade files can be downloaded from the Intellian Partner Portal.



WARNING

Do not turn off the equipment power during the upgrade.

Chapter 14. Web UI

Additional functions not provided by the SDT can be accessed through the Web UI. By default, the address to access the Web UI is <https://192.168.250.1>

14.1 Access Aptus LX

To access the AptusLX web interface for system configuration and management, you must first log in with the factory default credentials.

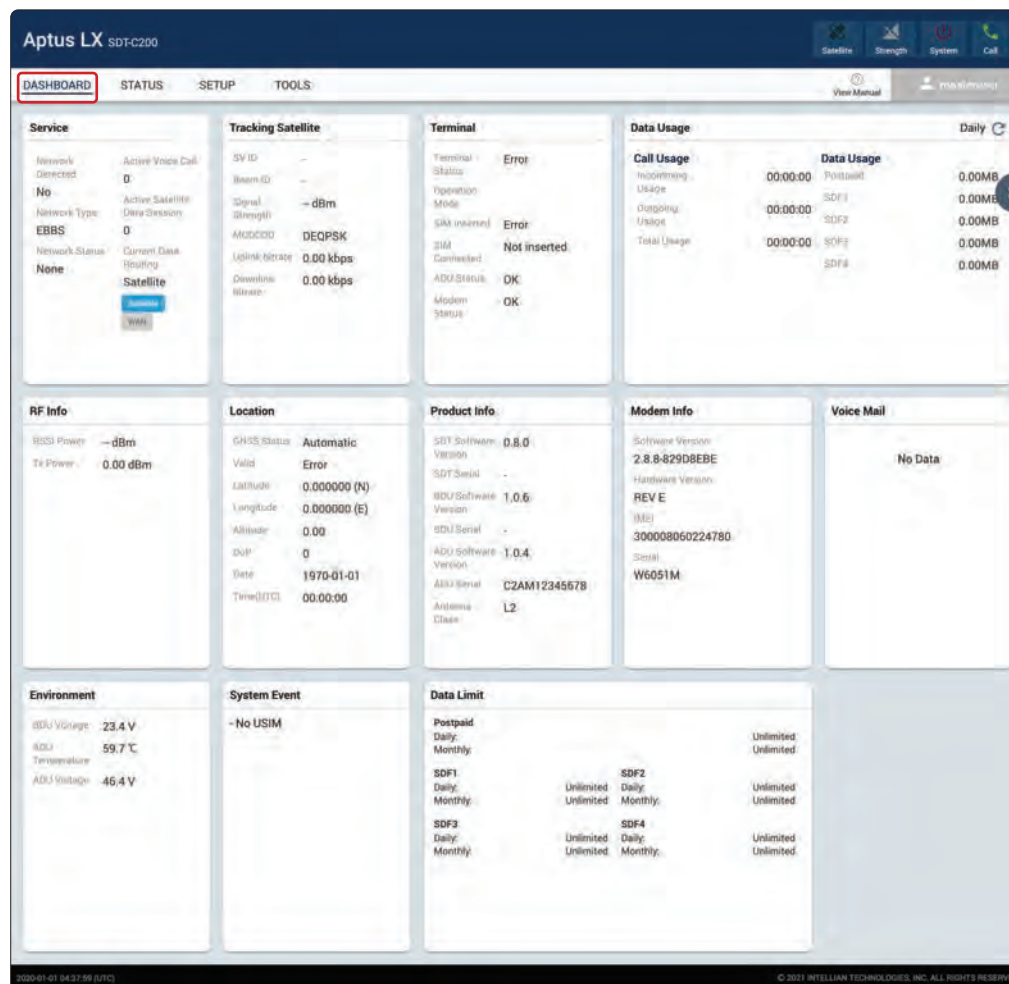
Accessing the Web UI:

1. Connect your computer to the BAM port.
2. Open a web browser and navigate to the following address: <https://192.168.250.1>
3. Log in using the factory default credentials:
 - Username: intellian
 - Password: 12345678

Change the default password immediately after first login to protect the vessel's critical communication system and prevent unauthorized access. Navigate to **Account(intellian)** → **User menu** to set a new, strong password.

14.2 Dashboard

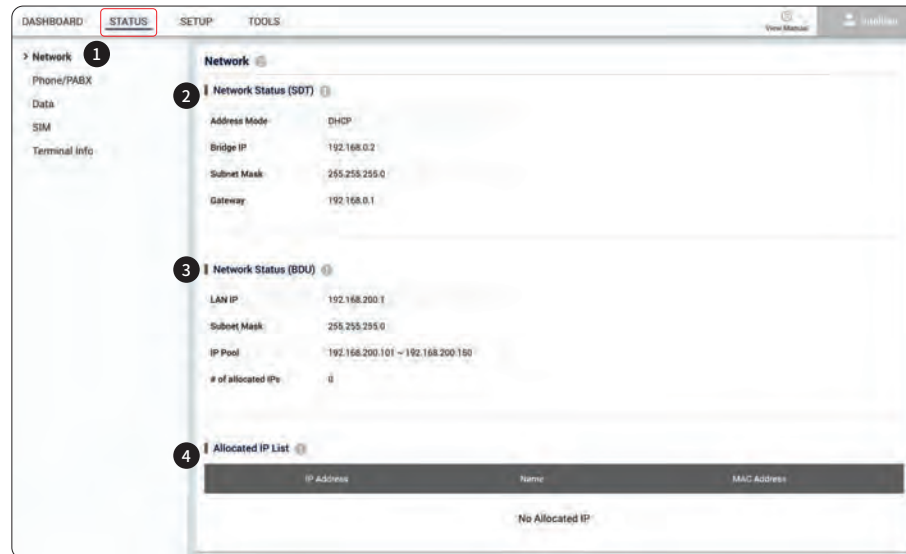
The Dashboard menu item provides access to quick monitoring of the antenna status. Once displayed, the Dashboard helps you arrange panels on a single screen, while providing you with a broad view of a variety of information at once.



14.3 Status

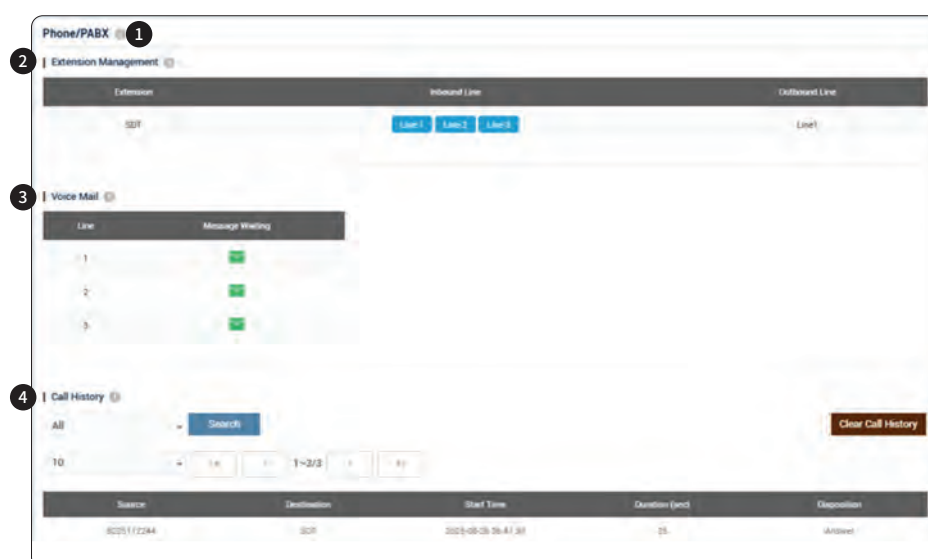
This menu displays the Network, Phone/PBX, Data, SIM and Terminal Info function.

14.3.1 Network



No.	Item	Description
①	Network	Displays the information about a network and IP.
②	Network Status(SDT)	Displays the network information currently in use by the SDT. • Address Mode: Displays the current setting mode (Factory default: DHCP). • Bridge IP: Displays the current IP for the SDT. • Subnet Mask: Displays the subnet mask for the SDT. • Gateway: Displays the gateway for the SDT.
③	Network Status(BDU)	Displays the network information currently in use by the BDU. • LAN IP: Displays the IP address for the BDU. • Subnet Mask: Displays the subnet mask for the BDU. • Gateway: Displays the gateway for the BDU.
④	Allocated IP List	Displays the allocated IP addresses and information for devices connected to the BDU.

14.3.2 Phone/PABX



No.	Item	Description
①	Phone/PABX	Displays the phone and Private Automatic Branch Exchange (PABX) status.
②	Extension Management	Displays the extension number and details. - Extension: Displays the registered extension. - Inbound Line: Displays the inbound line in use through the blue indicator. - Outbound Line: Displays the outbound line.
③	Voice Mail	Displays the received new voice mail.
④	Call History	Displays the received call history. You can set view details from the drop-down list. Remove the history by clicking the Clear Call History button.

14.3.3 Data



No.	Item	Description
①	Data	Displays the current data setting status.
②	Routing	Displays the connection status with the satellite.
③	Data Service	Displays the activation status for each data service.

14.3.4 SIM

SIM ①

② **Configuration** ②

Connected: Normal

IMSI: 901037270000313

Messaging Provisioned: Normal

③ **Voice** ③

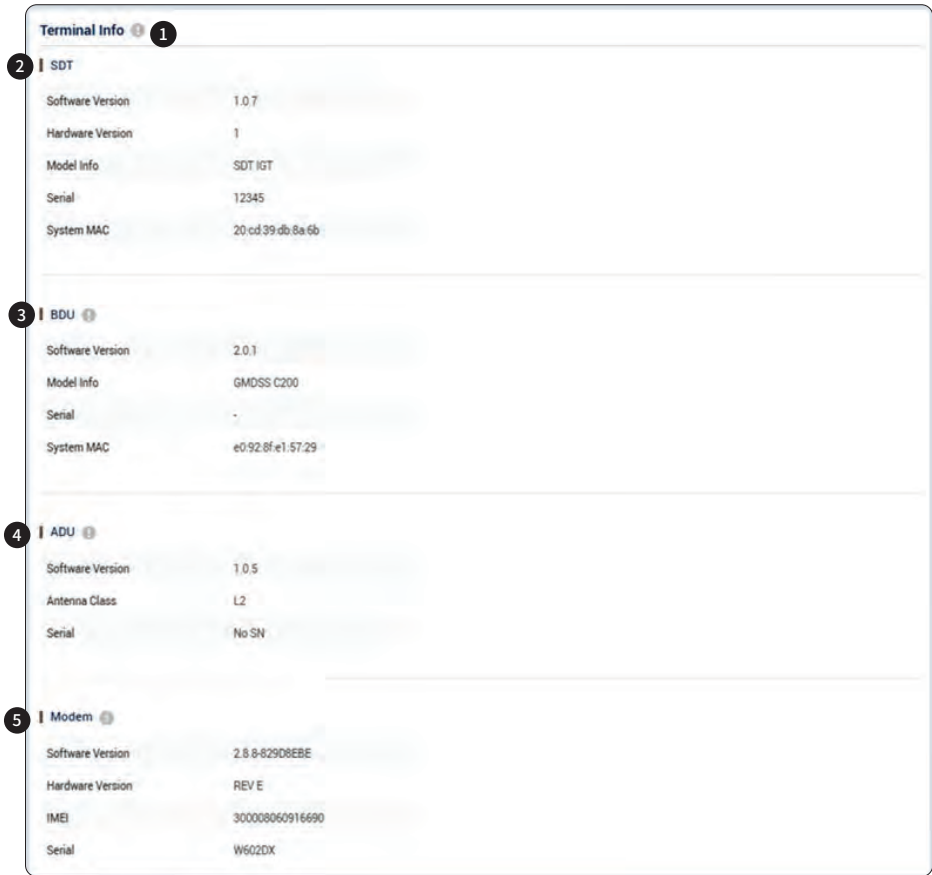
Line	Type	MSISDN
1	Safety	881672702044
2	Postpaid	881677101066
3	Postpaid	881677100015

④ **Data** ④

Type	Provisioned
postpaid	True
devmgt	False
secondary1	False
secondary2	False
secondary3	False
secondary4	False
prepaid	False

No.	Item	Description
①	SIM	Displays information about the SIM card, and the voice and data status.
②	Configuration	Displays the SIM card information in use. - Connected: Displays the connection status of the SIM card. The SIM must be inserted. - IMSI: Displays a unique identifier to the SIM card.
③	Voice	Displays the active status of the voice.
④	Data	Displays the status of data communications.

14.3.5 Terminal info



No.	Item	Description
①	Terminal info	Displays the system terminal information.
②	SDT	Displays SDT information in use.
③	BDU	Displays BDU information in use.
④	ADU	Displays ADU information in use.
⑤	Modem	Displays the core module information in use.

14.4 Setup

This menu sets and displays the Network, Phone/PBX, Data Limit, and Location function.

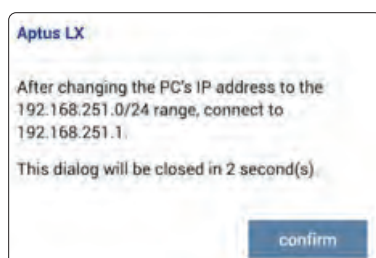
14.4.1 Network

No.	Item	Description
①	Network	Sets the information about a network.
②	Bridge Network	Address Mode: Select the network mode to be used for the Bridge Network (Dynamic/Static). Click the Apply button to apply the settings to the system.
③	Static Config	When setting to Static in Address Mode, set the IP manually. • IP: Enter the IP address to be used. • Subnet Mask: Enter the subnet mask. • Gateway: Enter the gateway address. Click the Apply button to apply the settings to the system.



NOTE

- When the Static IP is changed to the 192.168.250.xxx IP band already in use by the SDT (Web UI access IP: 192.168.250.1), be aware that the original Web UI access IP will temporarily change to 192.168.251.1.
- If the Web UI is accessed and the IP is changed to 192.168.250.xxx, the Web UI will log out and display the pop-up window as shown in the image.



- Firmware upgrade files can be downloaded from the Intellian Partner Portal.

User Settings (Ship Network IP)	System Automatic Actions	Management Address (Web UI Access IP)
Set the address to an IP outside of the 192.168.250.x band (e.g., 10.0.0.5)	No Change	192.168.250.1 (Default)
Set the address to an IP within the 192.168.250.x band (e.g., 192.168.250.20)	Management IP will be automatically changed upon IP Conflict Detection.	92.168.251.1 (Temporary Change)
Change the address back to an IP outside of the 192.168.250.x band.	Management IP will be automatically recovered upon conflict resolution.	192.168.250.1 (Default Revert)

14.4.2 Phone/PABX

No.	Item	Description
①	Phone/PABX	Sets the phone and Private Automatic Branch Exchange (PABX).
②	Extensions Management	Sets the extension number and details. • Edit(✎) button: To edit the registered extension, click the edit button. Then the pop-up window is opened. You can edit details. • Delete(🗑) button: To delete the registered extension, click the delete button. (Extension SDT have no delete button.) • Add(+) button: To create new extension numbers, click the plus icon. Then the pop-up window is opened. You can assign the new extension number. Click the Update button. The created extension numbers are displayed on the list. - Extension: Displays the registered extension. - Inbound Line: Each inbound line can be controlled and managed by individual selection through the blue indicator. Line 1 can only use SDT, so it cannot be set. - Outbound Line: Select the outbound line from the drop-down list. Line 1 can only use SDT, so it cannot be set. - Password: Displays the password.
③	Outbound Call Prefix	Sets the Outbound Call Prefix function by toggling the activation button (Activated/Deactivated). • Activated: You must start the phone numbers with "9". Enter '9 + Phone number' by using the keypad. (e.g. 9 1234 5678). • Deactivated: You can make outbound call without starting the "9". Click the Apply button to apply the settings to the system.

14.4.3 Data Limit

Data Limit

Data Limit

Postpaid

Daily Limit: Unlimited Data

Monthly Limit: Unlimited Data

Apply

SDF1

Daily Limit: Unlimited Data

Monthly Limit: Unlimited Data

Apply

SDF2

Daily Limit: Unlimited Data

Monthly Limit: Unlimited Data

Apply

SDF3

Daily Limit: Unlimited Data

Monthly Limit: Unlimited Data

Apply

SDF4

Daily Limit: Unlimited Data

Monthly Limit: Unlimited Data

Apply

No.	Item	Description
①	Data Limit	The data usage is limited for each provision type by setting the daily limit (from 00:00:00 to 23:59:59) and monthly limit (from the first day to the last day of the month).
②	Data Limit	Select the provision type of data use from the drop-down list. The data is set in megabit (MB) and the default value of the provision type is Unlimited Data. - No Data Permitted: The data connection is disabled when the No Data Permitted is selected in either the daily limit or monthly limit menu. - Unlimited Data: There is no limit to data use. - User Setting: Enter a maximum number of MB for the data connection. If the data usage reaches or exceeds the limit, an alert message pops up on the screen and the data service is restricted to use. To continue using the data services you must select the Unlimited Data provision type to start a new connection. Click the Apply button to apply the settings to the system.

14.4.4 Location

Location ①

②

Location

Position Mode

Automatic

Manual

Latitude

37.40183

Longitude

127.1125

Time of position

2025

/

6

/

30

:

5

:

50

:

59

Speed Over Ground

0

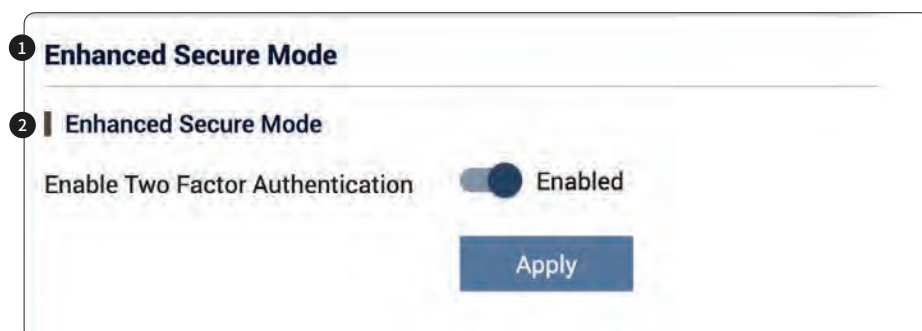
Course Over Ground

0

Apply

No.	Item	Description
①	Location	This feature allows you to manually specify a location. This feature is analogous to the manual position feature that can be configured in SDT. You can also verify the location selected in SDT’s manual position. (see section 5.4)
②	Location	Change the settings for the current location. • Position Mode: Select the settings for the location information (Automatic/ Manual). When set to Manual, you can enter the following parameters manually: - Latitude: Enter the latitude value. - Longitude: Enter the longitude value. - Speed Over Ground (SOG): Enter the SOG value. - Course Over Ground (COG): Enter the COG value.

14.4.5 Enhanced Secure Mode

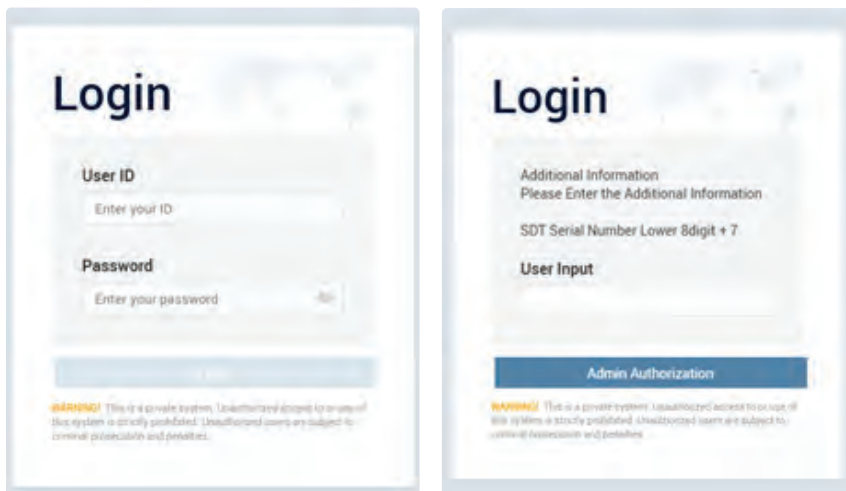


① Enhanced Secure Mode

② Enhanced Secure Mode

Enable Two Factor Authentication ☒ Enabled

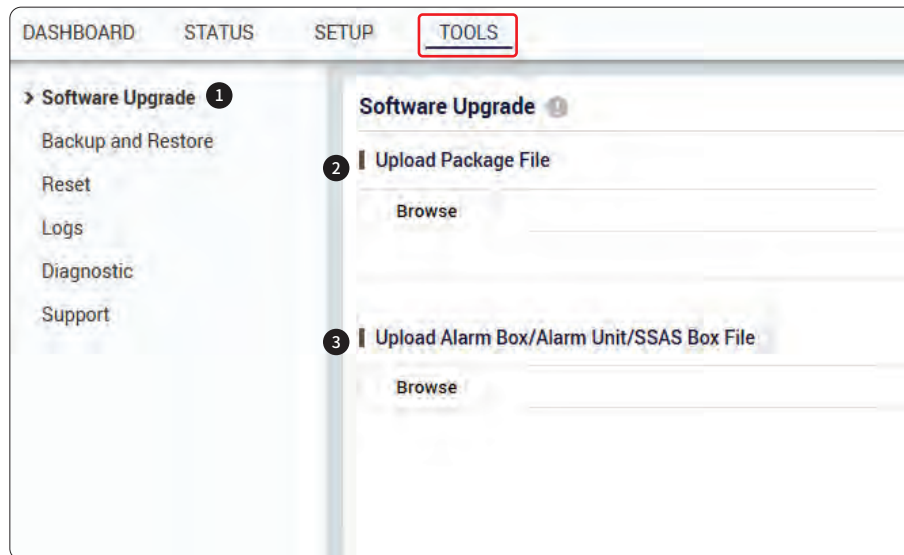
Apply

No.	Item	Description
①	Enhanced Secure Mode	Enhanced Secure Mode allows you to configure settings for enhanced security.
②	Enable Two Factor Authentication	If you enable this feature, two-step verification using the last 8 digits of the SDT serial number will be performed during account login via the web UI.  For example, if the SDT serial number is GSĐT12341234 and the two-step verification prompts you to add 7 to the lower 8 digits of the SDT serial number, you would enter 12341241 (12341234 + 7). This feature will take effect starting with your next login.

14.5 Tools

This menu provides various tools, including software upgrades, backup and restore configurations, initialization, log storage, and diagnostics.

14.5.1 Software Upgrade

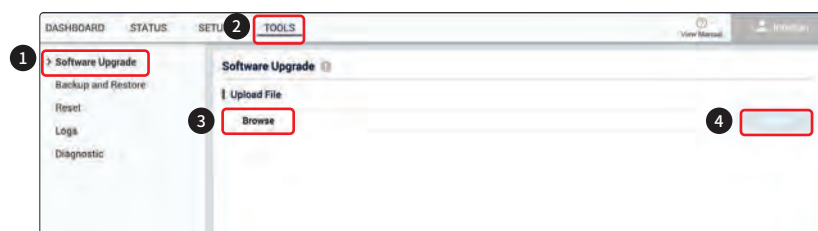


No.	Item	Description
①	Software Upgrade	Upgrades antenna software firmware.
②	Upload Package File	Upgrade the software for the C200M/C700 GMDSS.
③	Upload Alarm Box / Alarm Unit / SSAS Box File	Upgrade the firmware for accessories such as the Alarm Box, Alarm Unit, and SSAS Box.

Software Upgrade on AptusLX

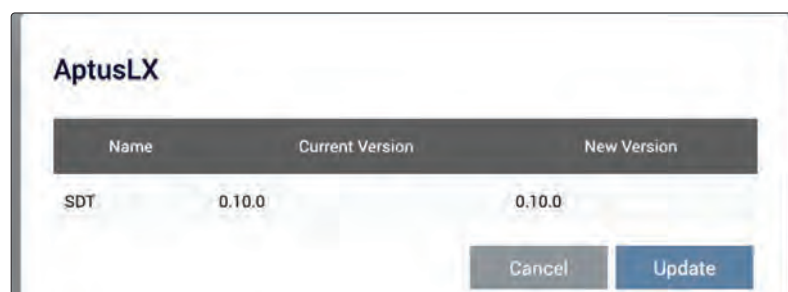
The C200M/C700 GMDSS software can be upgraded via the web UI. If the SDT and BDU are connected, both can be upgraded using the unified binary file. Additionally, using the SDT standalone binary file allows upgrading only the SDT. (see section 13.1 for detailed upgrade instructions.)

1. After accessing AptusLX, go to **TOOLS** → **Software Upgrade**.
2. **Browse** and select the upgrade package file to upload.
3. Click the **Upload** button to transfer the software upgrade file (*.bin) to the SDT and/or BDU module.

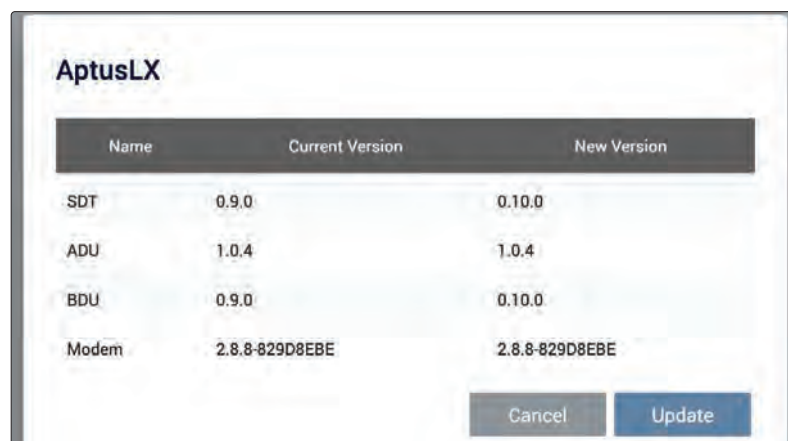


4. A pop-up window will display the software status. Check both the current and new version details:

For SDT standalone binary file

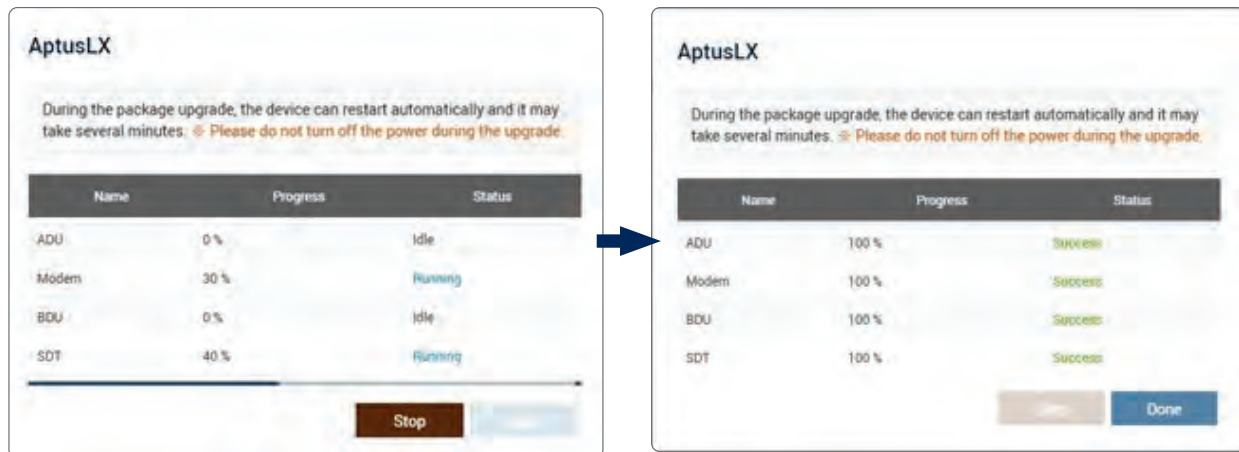


For unified binary file

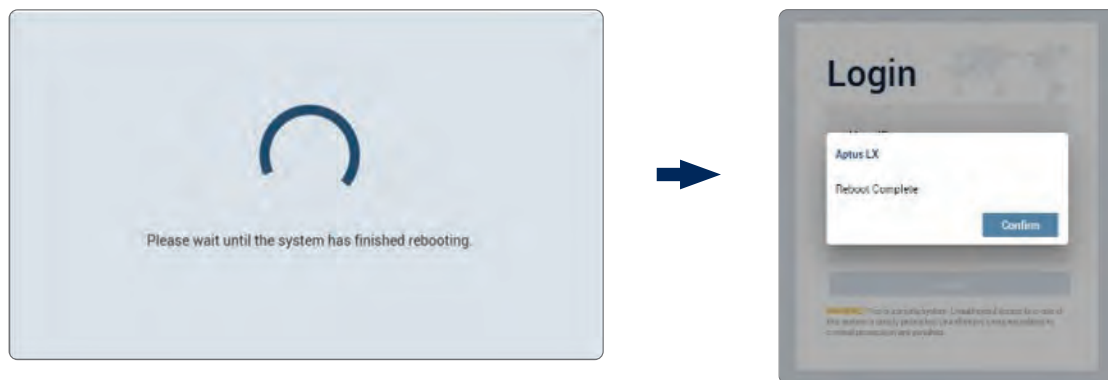


5. Click the **Upgrade** button.

During the upgrade, the window will display progress and status.



- If the firmware upgrade is successful, “Success” will appear in the Status column, and the system will reboot automatically.
- If the upgrade fails, ‘Upgrade Fail’ will appear in the Status column. Try to upgrade again or use a different upgrade file.



6. Click the Done button to close the pop-up window.

**NOTE**

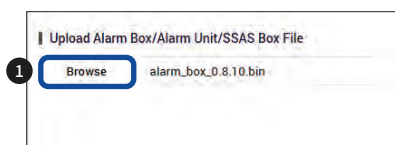
- When upgrading the software package that includes both the SDT and BDU modules, ensure that neither the SDT nor the BDU is disconnected.
- To verify the applied upgrade status, go to **Menu** → **System Settings** → **Product Information** → **Terminal Information**. User can find the software versions for the SDT, BDU, ADU, and Modem.
- Firmware upgrade files can be downloaded from the Intellian Partner Portal.

**WARNING**

Do not turn off the equipment power during the upgrade.

Accessory Package Update Procedure

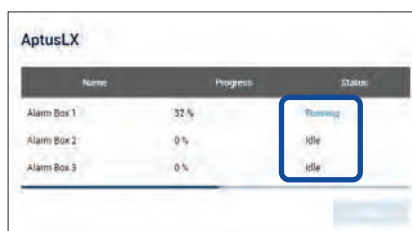
1. Browse and select the accessory upgrade package file to upload.
2. Click the **Upload** button to upload the firmware package file (*.bin). The firmware state will appear in the pop-up window.



3. Check that the firmware is correctly connected to all related accessories. Click the **Update** button.



During the upgrade process, the window will display the progress and status.



If the firmware is successfully upgraded, "Success" will be displayed in the Status column.
If the upgrade fails, 'Upgrade Fail' will appear in the Status column. Try to upgrade again or use a different upgrade file.

4. Click the **Done** button to close the pop-up window.



NOTE

- Alarm boxes, alarm units, and SSAS boxes can all be upgraded using the same method.
- Firmware upgrade files can be downloaded from the Intellian Partner Portal.



WARNING

Do not turn off the equipment power during the upgrade.

14.5.2 Backup & Restore



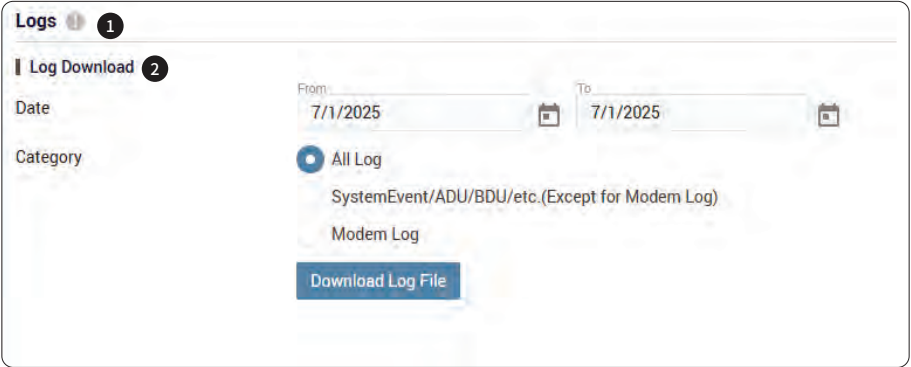
No.	Item	Description
①	Backup and Restore	Backs up and restores configuration files for the C200M/C700 GMDSS.
②	Backup	Saves configuration files for the C200M/C700 GMDSS to a PC. Click the Backup button to save the settings to your PC.
③	Restore	Restores backed-up configuration files. Browse and select the package restore file to upload, then click the Upload button. Then the system will automatically reboot and apply the setting values.

14.5.3 Reset



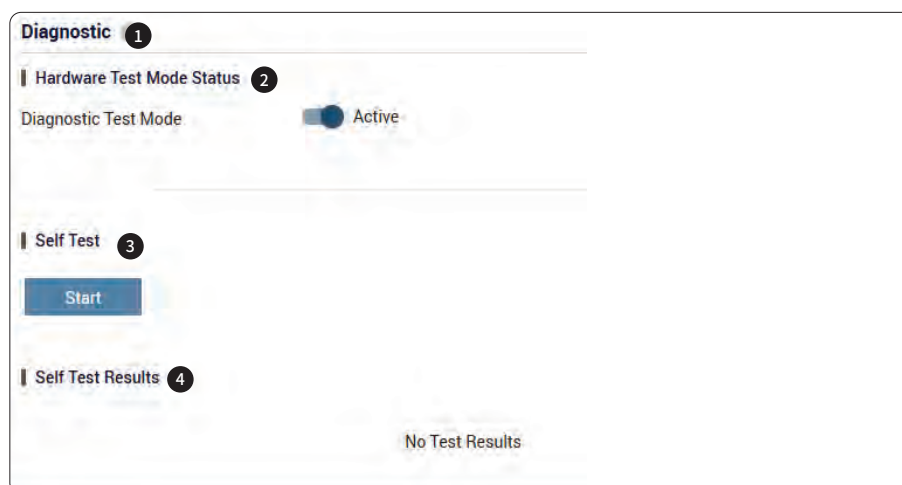
No.	Item	Description
①	Reset	Resets the systems, user data and factory reset.
②	Reboot	Click the Reboot button to reset the SDT, BDU and antenna.
③	User Data Reset	Resets all configurations, including call and data history, for the SDT.
④	Factory Reset	Click the Factory Reset button to initialize the antenna system. The user configuration is initialized.

14.5.4 Logs



No.	Item	Description
①	Logs	Downloads the antenna log data.
②	Log Download	Displays the antenna log list. Any log data (.gz) within a month can be downloaded. Select the desired category and click the Download Log File button. • Date: Sets the date range for which you want to download files. Any log data up to a month old can be downloaded. • Category: Select the desired category. - All Log: Downloads all log files, including SDT, ADU, BDU and modem logs. - System Event/ADU/BDU/etc. (Expect for Modem Log): Downloads antenna log files along with log files for SDT/ADU/BDU, excluding modem log files. - Modem Log: Downloads only modem log files.

14.5.5 Diagnostic



No.	Item	Description
①	Diagnostic	Executes antenna diagnosis test to check the antenna status.
②	Hardware Test Mode Status	Sets the hardware test function by toggling the activation button (Active/Inactive).
③	Self Test	The activation button must be selected to the "Active" in the previous step. Click the Start button to run the self-test.
④	Self Test Result	Displays the self-test result.

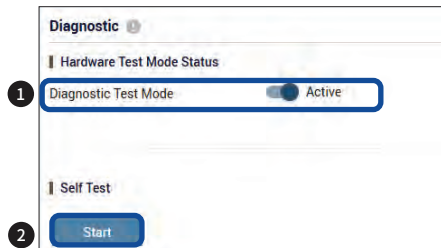
**WARNING**

While selecting the **Active** button in the H/W Test Mode Activate menu, the system is in the hardware test mode. All satellite connections are interrupted during test mode. Select the **Inactive** button for normal operation.

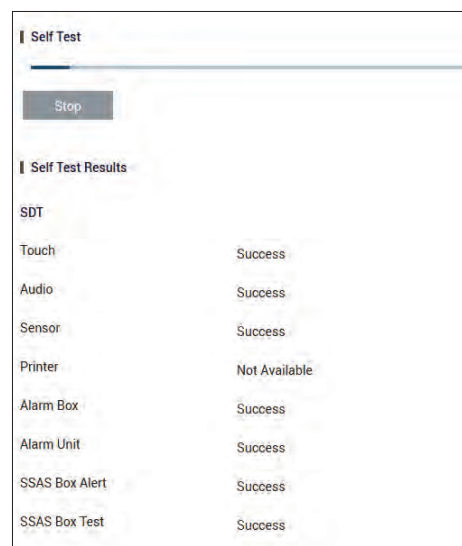
Diagnostic Procedures:

The diagnostic functions available on the WebUI automatically execute items that can be detected from the SDT, excluding those requiring user interaction.

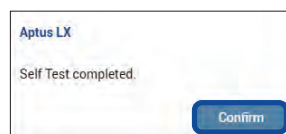
1. Set the Diagnostic Test Mode to Active and click the **Start** button.



Once the diagnostic test starts, the SDT items will complete first, and the antenna items will take a few minutes to complete the test.



2. After the diagnostic test is completed, the system will display a pop-up window. Click the **Confirm** button.



3. Verify the complete success, including the antenna items.

Antenna	
MoCA	Success
SLIC	Success
Wi-Fi	Success
PoE	Success
Ethernet Switch	Success
SIM	Success
Modem	Success
ADU	Success
RFU	Success

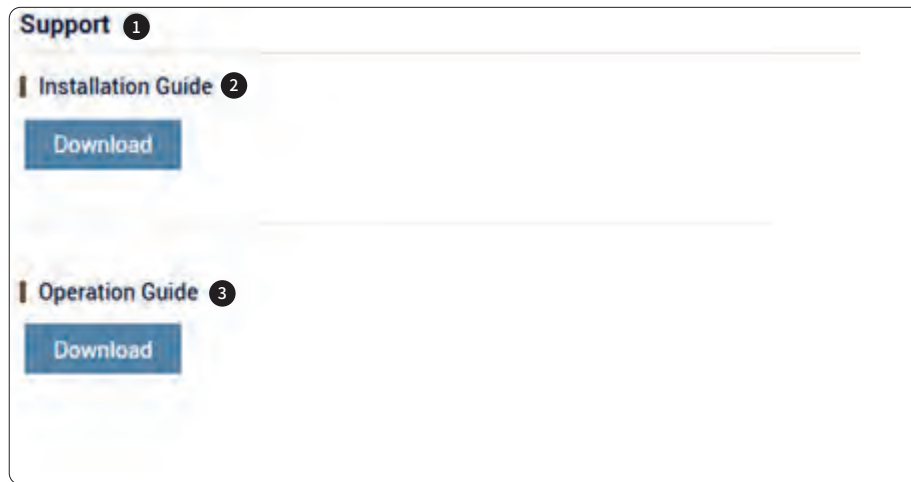
4. Set the Diagnostic Test Mode to Inactive.

Diagnostic

Hardware Test Mode Status

Diagnostic Test Mode ☐ Inactive

14.5.6 Support



No.	Item	Description
①	Support	Downloads the installation guide and operation guide files.
②	Installation Guide	The installation guide file (.pdf) can be downloaded. Click the Download button.
③	Operation Guide	The operation guide file (.pdf) can be downloaded. Click the Download button.

Chapter 15. Appendix

15.1 Specification

Interface	
Item	Specification
Display	- Resolution: 1024 X 600 Pixels - Pixel Arrangement: RGB vertical Stripe - Response time: Typ. 30ms
LAN	100BASE-TX (RJ-45, IEEE 802.3u (IEC 61162-450)) / IGMP Version 3
Switch	Not supported.
Hub	Not supported.
Datagram	UdPbC
Network function	SF, NF (ONF is not supported.)
Transmission group	MISC, BAM1, BAM2, NETA
Multicast address	239.192.0.1, 239.192.0.17, 239.192.0.18, 239.192.0.56, 239.192.0.254
Destination port	60001, 60017, 60018, 60056, 514
Input	ACN(CRP), HBT, SRP(SBM)
Output	ALC, ALF(MSM), ARC(CRP), SM1, SM2, SM3, SM4, SMB, SMV, SRP (SBM)

15.2 BAM Sentences

This appendix provides detailed information about the Bridge Alert Management (BAM) sentences supported by the C200M/C700 GMDSS System, according to IEC 62923-1 and IEC 62923-2. For further details, refer to the relevant sections on BAM configuration and operation within this manual. The table below lists all BAM sentences the C200M/C700 GMDSS System can transmit (as a talker):

Sentence Formatter	Function Description	Transmission Interval	Data Latency
ALC	Cyclic alert list	30s	n/a
ALF	Alert sentence	n/a	n/a
ARC	Alert command refused	n/a	n/a

The table below lists all BAM sentences the C200M/C700 GMDSS System can transmit (as a talker):

Sentence Formatter	Function Description	Presence
ACN	Alert command	Optional
HBT	Heartbeat supervision sentence	Optional

BAM Talker Sentence Formats

ALC	Cyclic Alert List: \$--ALC,xx,xx,xx,x.x,aaa,x.x,x.x,x.x,.....,aaa,x.x,x.x,x.x*hh<CR><LF>
ALF	Alert Sentence: \$--ALF,x,x,x,hmmss.ss,a,a,aaa,x.x,x.x,x.x,x,c---c*hh<CR><LF>
ARC	Alert Command Refused: \$--ARC,hmmss.ss,aaa,x.x,x.x,c*hh<CR><LF>

BAM Listener Sentence Formats

ACN	Alert Command: \$--ACN,hmmss.ss,aaa,x.x,x.x,c,a*hh<CR><LF>
HBT	Heartbeat Supervision Sentence: \$--HBT,x.x,A,x*hh<CR><LF>

SRP Sentence Formats

SRP	\s:ccxxx*hh\\$--SRP,x,hhhhhhhhhhh,c-c*hh<CR><LF>
-----	--



NOTE

Unused fields are set to null. Null fields are used to clearly indicate that no data is being transmitted, and use the symbols “,” or “*”.

15.3 List of BAM Alert

Doubtful pos (ID: 3013)	
Priority	Caution
Category	B
Alert Description	GMDSS update manual position
Decision Support	Update the manual position as described in Position Settings.
Raise/Rectify Conditions	Raise: Occurs 4 hours after the user sets Manual Position
	Rectify: On manual position update/cancel or when mode set to Auto. Rectify sent if Auto on boot.
Escalation Properties	Not Applicable
Permitted Exceptions / Other	Raised in manual position mode if set position > 4 hours old.

Lost position (ID: 3016)	
Priority	Caution
Category	B
Alert Description	Check GMDSS terminal for lost position
Decision Support	Change to manual position mode as described in Position Settings.
Raise/Rectify Conditions	Raise: Occurs after 10 minutes of no GNSS information.
	Rectify: When manual position is set or GNSS information is received again. Rectify sent if Manual on boot.
Escalation Properties	Not Applicable
Permitted Exceptions / Other	Raised in auto (GNSS) mode if position lost > 10 min. Cleared to Normal if mode set to manual.

System fault (ID: 3062)	
Priority	Warning
Category	B
Alert Description	Reverted to the factory image due to system error
Decision Support	Please contact technical support in Intellian.
Raise/Rectify Conditions	Raise: Occurs when the application image is a factory partition
	Rectify: Power-cycle the system. If that does not help, contact technical support in Intellian.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

Printer fault (ID: 3062)	
Priority	Warning
Category	B
Alert Description	Check GMDSS printer
Decision Support	Check printer online/selected. Bring back online/reselect if needed. Consult printer manual if unresolved.
Raise/Rectify Conditions	Raise: Printer disconnected, or unspecified printer error detected, or printer offline/deselected for 60s or more.
	Rectify: Connection reestablished.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

Paper low (ID: 3079)	
Priority	Caution
Category	B
Alert Description	Check GMDSS printer paper
Decision Support	Replace /refill printer paper.
Raise/Rectify Conditions	Raise: Printer out of paper.
	Rectify: Paper refilled.
Escalation Properties	Not Applicable
Permitted Exceptions / Other	-

Lost connection (ID: 3116)	
Priority	Caution
Category	B
Alert Description	Check GMDSS satellite terminal
Decision Support	Verify Antenna Unit has free line of sight to the sky. Remove obstructions.
Raise/Rectify Conditions	Raise: The terminal has been unable to detect or otherwise contact the satellites of the Iridium satellite system for a period of one minute or more.
	Rectify: Iridium satellite system detected.
Escalation Properties	Not Applicable
Permitted Exceptions / Other	-

Distress Rx (ID: 3122)	
Priority	Warning
Category	A
Alert Description	Incoming distress. Check GMDSS display
Decision Support	Read the received Distress Alert Relay (see Maritime Safety Information (MSI)).
Raise/Rectify Conditions	Raise: Distress Alert Relay message (MSI of Distress priority) received.
	Rectify: All Distress Alert Relay messages read.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	Only one alert raised for multiple messages. Ack'able=N (CAM must send ARC if ACN received).

Urgency Rx (ID: 3122)	
Priority	Warning
Category	A
Alert Description	Incoming urgency warning. Check GMDSS display
Decision Support	Read the received urgency MSI message or urgency priority message (see Maritime Safety Information (MSI) and Safety Messaging).
Raise/Rectify Conditions	Raise: Urgency MSI message or urgency priority message received.
	Rectify: All urgency priority messages read. (MSI or Safety msg)
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	Only one alert raised for multiple messages. Ack'able=N (CAM must send ARC if ACN received).

Distress missed (ID: 3122)	
Priority	Warning
Category	A
Alert Description	Missed distress call. Check GMDSS display
Decision Support	Open the Call History to see the details on the missed call.
Raise/Rectify Conditions	Raise: Incoming distress priority voice call not answered.
	Rectify: Call History accessed.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	Only one alert raised for multiple missed calls. Ack'able=N (CAM must send ARC if ACN received).

Urgency missed (ID: 3122)	
Priority	Warning
Category	A
Alert Description	Missed urgency call. Check GMDSS display
Decision Support	Open the Call History to see the details on the missed call.
Raise/Rectify Conditions	Raise: Incoming urgency priority voice call not answered.
	Rectify: Call History accessed.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	Only one alert raised for multiple missed calls. Ack'able=N (CAM must send ARC if ACN received).

MSI Rx (ID: 3123)	
Priority	Caution
Category	B
Alert Description	Check new received maritime safety information
Decision Support	Read the received MSI message (see Maritime Safety Information (MSI)).
Raise/Rectify Conditions	Raise: Safety priority MSI message received.
	Rectify: All safety priority MSI messages read.
Escalation Properties	Not Applicable
Permitted Exceptions / Other	Only one alert raised for multiple safety messages.

Safety Rx (ID: 3123)	
Priority	Caution
Category	B
Alert Description	Check new received safety message
Decision Support	Read the received safety message (see Safety Messaging).
Raise/Rectify Conditions	Raise: Safety message received (Safety priority).
	Rectify: All safety messages read.
Escalation Properties	Not Applicable
Permitted Exceptions / Other	Only one alert raised for multiple safety messages.

Safety missed (ID: 3123)	
Priority	Caution
Category	B
Alert Description	Missed safety call. Check GMDSS display
Decision Support	Open the Call History to see the details on the missed call.
Raise/Rectify Conditions	Raise: Incoming safety priority voice call not answered.
	Rectify: Call History accessed.
Escalation Properties	Not Applicable
Permitted Exceptions / Other	Only one alert raised for multiple missed calls.

Storage low (ID: 3079)	
Priority	Caution
Category	B
Alert Description	Check GMDSS message storage medium
Decision Support	If the system uses more than 80% of the storage space, it automatically deletes the logs in order, starting with the oldest logs, until the storage space is below 80%.
Raise/Rectify Conditions	Raise: Storage space insufficient (e.g., up to 80% used).
	Rectify: Storage space below threshold (e.g., below 80%).
Escalation Properties	Not Applicable
Permitted Exceptions / Other	-

Invalid antenna (ID: 12001)	
Priority	Warning
Category	B
Alert Description	GMDSS unavailable. Incompatible antenna
Decision Support	If the combination of SDT-1 and BDU/ADU is not connected correctly.
Raise/Rectify Conditions	Raise: Control Unit detects incompatible Antenna Unit revision (e.g., C700 BDU/ADU on C200M SDT-1)
	Rectify: Control Unit detected compatible Antenna Unit
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

Lost handset (ID: 12002)	
Priority	Warning
Category	B
Alert Description	Voice calls unavailable. Check handset cable.
Decision Support	Check the cable between the handset and the Control Unit.
Raise/Rectify Conditions	Raise: Analog handset not connected or becomes disconnected (poor/intentional). (Control Unit loses connection with Handset).
	Rectify: Connection reestablished.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

Lost antenna ADU (ID: 12002)	
Priority	Warning
Category	B
Alert Description	GMDSS unavailable. Check BDU/ADU cable in antenna.
Decision Support	Check the cable between the BDU and the ADU.
Raise/Rectify Conditions	Raise: SDT connected to BDU, but ADU not connected to or becomes disconnect. (Control Unit loses connection with Antenna Unit).
	Rectify: Connection reestablished.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	Not raised if SDT-BDU connection lost.

Lost antenna BDU (ID: 12002)	
Priority	Warning
Category	B
Alert Description	GMDSS unavailable. Check ethernet cable between SDT and BDU.
Decision Support	Check the ethernet cable connection between SDT and BDU.
Raise/Rectify Conditions	Raise: BDU not connected or SDT-BDU connection disconnected (ethernet cable issue).
	Rectify: Connection reestablished.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	If this alert "Lost antenna BDU/ADU" is active, This Alert is not raised.

Lost alarm box (ID: 12002)	
Priority	Warning
Category	B
Alert Description	Alarm box lost. Check alarm box cable.
Decision Support	Check the cable between the Junction box and the Alarm box(s).
Raise/Rectify Conditions	Raise: Not connected to alarm box (from boot) or connection lost (intentional/ CAN failure). (Interface Unit loses connection with Alarm panel).
	Rectify: Connection reestablished.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	Only one alert raised for multiple lost Alarm Panels.

Lost alarm unit (ID: 12002)	
Priority	Warning
Category	B
Alert Description	Alarm unit lost. Check alarm unit cable.
Decision Support	Check the cable between the Junction box and the Alarm unit.
Raise/Rectify Conditions	Raise: Not connected to alarm unit (from boot) or connection lost (intentional/ CAN failure).
	Rectify: Connection reestablished.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

Lost SSAS box (ID: 12002)	
Priority	Warning
Category	B
Alert Description	SSAS box lost. Check SSAS box cable.
Decision Support	Check the cable between the Junction box and the SSAS box(s).
Raise/Rectify Conditions	Raise: Not connected to SSAS box (from boot) or connection lost (intentional/ CAN failure).
	Rectify: Connection reestablished.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

Invalid SIM card (ID: 12201)	
Priority	Warning
Category	B
Alert Description	GMDSS unavailable. Check SIM subscription information
Decision Support	Check if the SIM supports the GMDSS feature.
Raise/Rectify Conditions	Raise: SIM that does not support GMDSS is inserted.
	Rectify: Insert a SIM that supports GMDSS.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

Lost SIM card (ID: 12202)	
Priority	Warning
Category	B
Alert Description	GMDSS unavailable. Check SIM card slot
Decision Support	Verify the SIM card is properly inserted.
Raise/Rectify Conditions	Raise: SIM not inserted or cannot be detected.
	Rectify: SIM card detected.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

GMDSS fault (ID: 21002)	
Priority	Warning
Category	B
Alert Description	GMDSS service blocked (SIM locked)
Decision Support	Contact your service provider.
Raise/Rectify Conditions	Raise: GMDSS System is unavailable by Iridium network.
	Rectify: None specified. Contact your service provider.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

GMDSS fault (ID: 21002)	
Priority	Warning
Category	B
Alert Description	GMDSS service blocked (Unlock device)
Decision Support	Contact your service provider.
Raise/Rectify Conditions	Raise: GMDSS System is unavailable by Iridium network.
	Rectify: None specified. Contact your service provider.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

GMDSS fault (ID: 21002)	
Priority	Warning
Category	B
Alert Description	GMDSS service blocked (IMSI invalid)
Decision Support	Contact your service provider.
Raise/Rectify Conditions	Raise: GMDSS System is unavailable by Iridium network.
	Rectify: None specified. Contact your service provider.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

GMDSS fault (ID: 21002)	
Priority	Warning
Category	B
Alert Description	GMDSS service blocked (IMEI blacklisted)
Decision Support	Contact your service provider.
Raise/Rectify Conditions	Raise: GMDSS System is unavailable by Iridium network.
	Rectify: None specified. Contact your service provider.
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	-

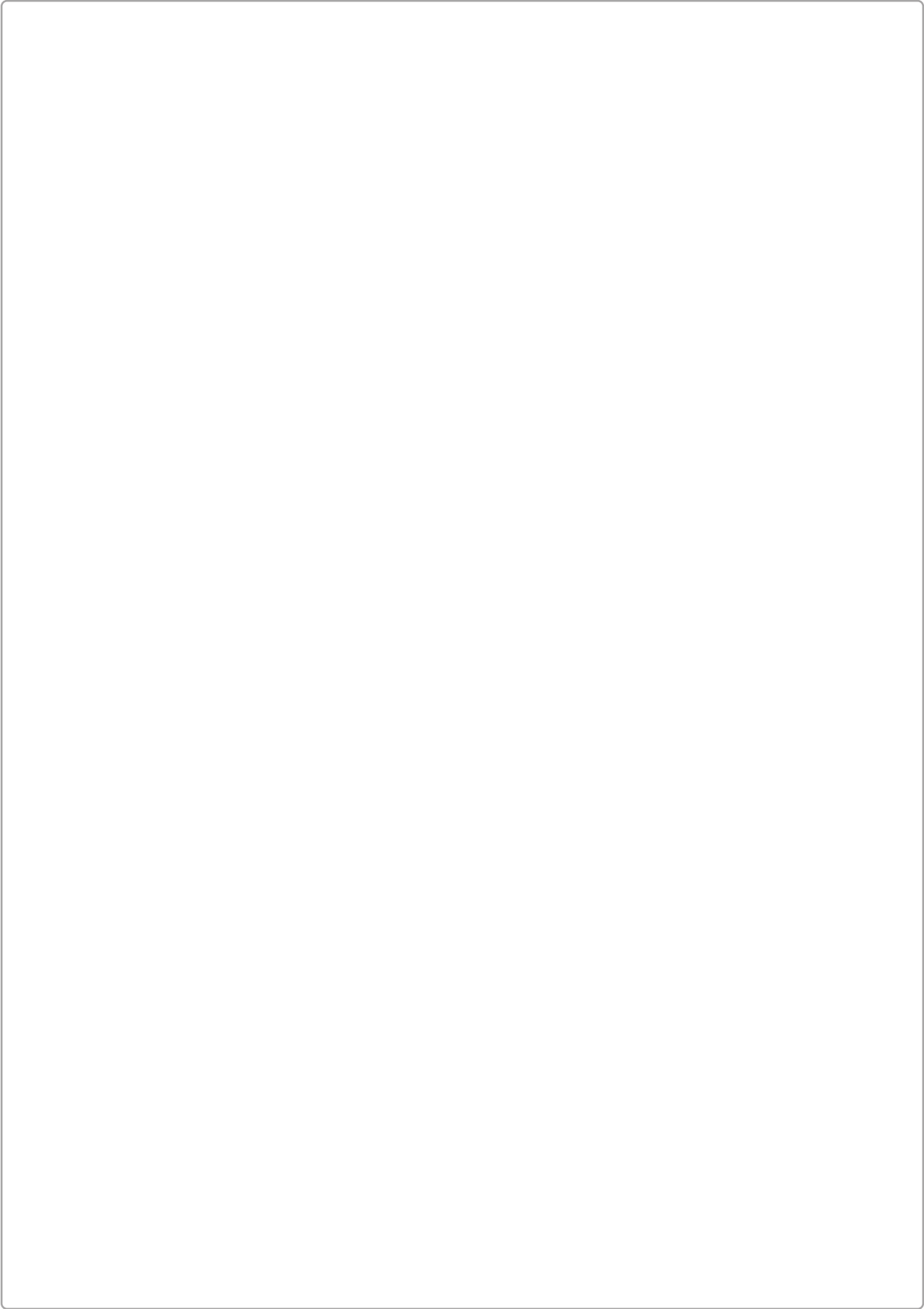
Safety Tx fail (ID: 22002)	
Priority	Warning
Category	B
Alert Description	Failed to send safety message.
Decision Support	Verify Antenna Unit line of sight. Remove obstructions. Initiate resending (see Safety Messaging).
Raise/Rectify Conditions	Raise: No messages were sent to the Iridium server for 5 minutes after the safety message was sent.
	Rectify: User Acknowledged message transmission failure (transitory alert).
Escalation Properties	Repeated as a warning after 90 seconds.
Permitted Exceptions / Other	Only one alert raised for multiple failed safety message transmissions.

15.4 Abbreviation / Acronym

Abbreviation / Acronym	Meaning
A	
ACK	Acknowledgment
ADU	Above Deck Unit
B	
BAM	Bridge Alert Management
BDU	Below Deck Unit
C	
COG	Course Over Ground
CSO	Chief Security Officer
CWA	Coastal Warning Area
D	
DAR	Distress Alert Relay
DTMF	Dual-Tone Multi-Frequency
E	
EIRP	Effective Isotropic Radiated Power
G	
G/T	Gain-to-Noise-Temperature Ratio
GEO	Geostationary Orbit
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
I	
IC	Integrated Circuit
IGS	Iridium GMDSS System
IME	Input Method Editor
IMO	International Maritime Organization
IP	Internet Protocol
L	
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LEO	Low Earth Orbit
M	
MB	Megabit
MET	Meteorological Area
MMSI	Maritime Mobile Service Identity
MoCA	Multimedia over Coax Alliance
MSI	Maritime Safety Information
N	
NAV	Navigation
O	
OTA	Over-the-Air
P	
PABX	Private Automatic Branch Exchange
PBX	Private Branch Exchange
PSU	Power Supply Unit

Abbreviation / Acronym	Meaning
R	
RCC	Responsible Rescue Coordination Center
RF	Radio Frequency
RX	Receive
S	
SAR	Search and Rescue
SDT	Safety Display Terminal
SES	Ship Earth Station
SFA	Safety Function Assessment
SIM	Subscriber Identity Module
SMS	Short Message Service
SOG	Speed Over Ground
SOLAS	Safety of Life at Sea
SSAS	Ship Security Alert System
T	
TNC	Threaded Neill-Concelman
TX	Transmit
U	
UHF	Ultra High Frequency
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
V	
VBUS	USB Power Bus
VBW	Vessel Speed Relative to Water
VDC	Volts Direct Current
VHF	Very High Frequency
VHW	Speed Through Water
VTG	Course Over Ground and Ground Speed
W	
WAN	Wide Area Network

Note



Note