AN-362

CAN/ULC-S559 Fire Reporting in Protege Systems

Application Note

Last Published: 12-Jan-26 2:30 PM

Contents

Introduction

This application note describes how to program a Protege system to meet the requirements of CAN/ULC-S559 for fire reporting.

The applicable standards document is CAN/ULC-S559:2020 Standard for Equipment for Fire Signal Receiving Centres and Systems. This document should be read in conjunction with the standards document and the installation manuals for your Protege DIN rail products.

There are two types of communication systems used for reporting: active communication systems and passive communication systems. The key aspects of each system are outlined below.

Function	Active Communication Systems	Passive Communication Systems
Supported communication channel types	Report IP (ethernet or 4G)	Contact ID (phone line) Wireless alarm communicator module (cellular network)
Time to transmit alarm to fire signal receiving center	60 seconds (12.4)	
Time to transmit non-alarm status update to fire signal receiving center	90 seconds (12.5)	
Encryption level	128 bit (12.12)	-
Number of communication channels	One or more (14.1)	Two or more (15.1)
Time for primary channel communication failure to be detected by fire signal receiving center	<180 seconds (14.2a-1, 14.2b-2)	<6 hours (15.5)
Time for backup channel communication failure to be detected by fire signal receiving center	<24 hours when primary channel is functional (14.2b-3) <180 seconds when primary channel is not functional (14.2b-4)	<6 hours for MFVN or PSTN lines (15.5) <24 hours for other channels (15.5)
Time to start reporting on secondary channel in case of primary channel failure	-	<60 seconds (12.4, 15.5)
Time to report failure of one communication channel	-	<180 seconds (15.7)
Time to report primary power failure	<3 hours (5.3)	<3 hours (5.3)

The receiving software for IP communications must be ICT ArmorIP Version 3.

Active Communication Systems

Active communication systems may use:

1. One IP reporting service, or,
2. Two IP reporting services (primary and backup). It is recommended that these services use non-interdependent communication channels (e.g. ethernet and 4G).

Phone line reporting services do not meet the requirements for active communication systems.

Receiving Center Settings

The receiving center must use ICT ArmorIP V3 software with encrypted communication protocols. The required settings are:

- **Channel Type**: TCP/IP or UDP/IP
- **Poll Time**: 40 seconds
- **Poll Grace Time**: 20 seconds
- **Poll Offline**: 3
- **Encryption**: AES 256

With these settings, the receiving center will be notified when it does not receive any polls from the controller within at most 140 seconds.

For more information, see the ArmorIP Version 3 Internet Monitoring Application User Manual.

Programming the Primary Service

The recommended settings for the primary Report IP service are outlined below. With the suggested timings, when the controller attempts to report a signal and fails, it will fail over to the backup reporting service (if present) within 60 seconds.

Create the following service in **Programming | Services**.

Service type tab

- **Service type**: Report IP
- **Service mode**: 1 - Start with controller OS

General tab - Configuration

- **Client code**: Provided by fire signal receiving center.
- **Reporting protocol**: Armor IP (TCP) encrypted or Armor IP (UDP) encrypted.
- **Encryption level**: AES 256
- **Encryption key**: Provided by fire signal receiving center.
- **Poll time** (seconds): 40 seconds
- **Backup service**: Select the backup service after programming it (see below).
- **CID map settings**: If you are using a SIMS II input mapping, set this to SIMS II. If not, do not change this setting.
- **Time before backup** (seconds): 10 seconds is appropriate.

General tab - Primary channel settings

- **IP address / Host name, IP port number**: Provided by fire signal receiving center.
- **Adaptor**: Select Cable for ethernet, USB ethernet for a cellular modem.
- **Port open attempts**: 2 is appropriate.

- **Ack wait time** (seconds): 5 seconds (or as advised by your receiving center).
- **Report fail output / output group**: Select an output if required. This may be used for the COM Status Output which is connected to the fire panel (see page 11).
- **Enable offline polling**: If the communication system has a backup service, enable this option. This will enable the service to poll this channel while a secondary channel or backup service is in use.
- **Channel failed CID code/group/zone**: The event code, group number and zone number sent when the offline polling fails. Discuss with your signal receiving center.
- **Offline poll count**: 3
- **Offline test report time** (seconds): 240 seconds is appropriate (must be less than 24 hours).

General tab - Secondary channel settings

If your fire signal receiving center has an alternative IP address for receiving messages, enter the settings here. Program the same settings as for the primary channel, with the following exceptions:

- **IP address / Host name, IP port number**: Alternative address provided by fire signal receiving center.
- **Enable offline polling**: Enabled.
- **Channel failed CID code/group/zone**: Set different codes for the secondary channel.

This is not considered an alternative communication path as it uses the same communication method as the first channel.

Options tab

- **Switch secondary IP immediately**: Disabled
- **Report open**: Enabled
- **Report close**: Enabled
- **Report alarms**: Enabled
- **Report tampers**: Enabled
- **Report restore**: Enabled
- **Report bypass**: Enabled
- **Log acknowledge response**: Disabled
- **Log polling message**: Disabled
- **Log message retries**: Disabled
- **Log reporting failure**: Disabled
- **Service operates as backup**: Disabled

Programming the Backup Service

In an active communication system, the backup service has the same requirements as the primary service but uses a different communication method. Program an additional Report IP service with the same settings as the primary service, apart from the following exceptions:

- **Backup service**: <Not set>
- **Enable offline polling**: Enabled for both the primary and secondary channels.
- **Adaptor**: Select a different adaptor from the primary service.
- **Channel failed CID code/group/zone**: Must be different from the codes used for the primary service.
- **Service operates as backup**: Enabled.

Save and return to the primary service. In the **General** tab, select the **Backup service**.

Passive Communication Systems

Passive communications require two non-interdependent communication channels. This is a achieved by connecting a wireless alarm communicator module to the phone line within the building. When the phone line has a fault or communication failure, the alarm communicator sends fault and fire messages over the cellular network (3G or 4G).

You must use a DAYR7-listed cellular alarm communicator such as the DSC LE4010. Follow all instructions in the product manuals for setting up a backup communicator for CAN/ULC-S559 (Commercial Fire Monitoring) installations, as well as any instructions related to general UL installations.

The alarm communicator must perform the following functions:

- Monitor the phone line for integrity. Report a failure on the phone line within 180 seconds of detection.
- If reporting fails on the phone line, transfer the call to the cellular network and report any pending messages to the monitoring center within 60 seconds.
- Test the cellular network connection at least every 24 hours.
- If the cellular connection fails, report the fault on the phone line within 180 seconds.

Only controllers with onboard modems support phone line reporting. Ensure that you order the correct controller model.

Programming the Contact ID Service

Create the following Contact ID service in **Programming | Services**.

Service type tab

- **Service type**: ContactID
- **Service mode**: 1 - Start with controller OS

Configuration tab

- **Client code**: Provided by fire signal receiving center.
- Select the **PABX number** (if required) and the alternative phone numbers for the fire signal receiving center. The service will attempt to use **Phone number 1**, then **Phone backup**, then **Phone number 2**.

  Click the ellipsis **[...]** to open the phone number programming window.

Options tab

- **Use alternate dialing method**: When disabled, the service will try **Phone number 1** multiple times before switching to **Phone backup**. When enabled, the service will alternate between phone numbers. Discuss the appropriate method with your receiving center.
- **Report open**: Enabled
- **Report close**: Enabled
- **Report alarms**: Enabled
- **Report tampers**: Enabled
- **Report restore**: Enabled
- **Report bypass**: Enabled
- **Service operates as backup**: Disabled
- **Log modem events to event buffer**: Disabled

Settings tab - Settings

- **Cid mapping**: If you are using a SIMS II input mapping, set this to SIMS II. If not, do not change this setting.
- **Dial attempts**: Must be between 5-10 for a phone line.

- **Port attempts**: 8 is appropriate.
- **Report count**: Must be set to 0 to allow the service to send all pending messages in one call.
- **Handshake time** (seconds): Length of time the controller will wait to receive a handshake from the receiving center. You may wish to reduce this time to prevent the controller from waiting on an inactive line for too long before failing over to the backup phone number. Discuss the appropriate value with your receiving center.
- **Dial time** (seconds): Length of time the controller will wait between failed dialing attempts. The minimum is 10 seconds. Discuss the appropriate value with your receiving center.
- **Off hook output / output group**: If required, program an output or output group that will be activated while the Contact ID service is reporting.
- **Report OK output / output group**: If required, program an output or output group that will be activated when the service makes a successful report. You must program the Report OK output or group with a timer to deactivate it (otherwise it will remain on indefinitely). Click the ellipsis **[...]** to open the output or output group programming, then set the **Activation time** / **Output time**. Click **Save**.

Settings tab - Background monitoring

The phone connection to the monitoring center must be tested at least every 6 hours. One option for this is using background monitoring, which sends a specific Contact ID code as a test report.

Alternatively, you can use the Service Report Test trouble input as described below.

- **Enable background monitoring**: Enabled
- **Background poll time when OK** (seconds): Must be less than 6 hours. 3600 seconds (1 hour) is an appropriate value, but discuss with your receiving center.
- **Background poll time when known failure**: As above.
- **Test report CID code / group / zone**: The Contact ID event code, group number and zone number that the controller will send for the background monitoring test report.
- **Phone 1 failed CID code / group / zone**: The Contact ID event code, group number and zone number that the controller will use to report failed communication with **Phone number 1**.
- **Phone 2 failed CID code / group / zone**: The Contact ID event code, group number and zone number that the controller will use to report failed communication with **Phone number 2**.
- **Backup phone failed CID code / group / zone**: The Contact ID event code, group number and zone number that the controller will use to report failed communication with the **Phone backup**.

Programming the Test Report Trouble Input

If you are not using background monitoring, you must program the Service Report Test trouble input to test the line once every 6 hours.

1. **Protege GX**: Navigate to **Sites | Controllers**.
   Protege WX: Navigate to **System | Settings**.
2. In the **Configuration** tab, set the **Test report time** to 06:00 (6 hours) or less.
3. In the **Options** tab, enable **Test report time is periodic**.
4. Click **Save**.

Now the test report trouble input will open every 6 hours to test the reporting service.

Programming Fire Area and Inputs

We must create an area to monitor the inputs from the fire alarm control panel (inputs 1-3 on the controller or input expander). This area must be dedicated to fire monitoring and may not be used for burglary inputs.

1. Navigate to **Programming | Areas**.
2. Add a new area with a descriptive name (e.g. Fire Area).
3. In the **Configuration** tab, adjust the timing settings as required.
4. **In Protege GX**: Under **Reporting services**, add the primary reporting service.
   In Protege WX: In the **Reporting Services** tab, add the primary reporting service.
5. Click **Save**.
6. Navigate to **Programming | Inputs**.
7. Select the inputs outlined below. In the **Areas and input types** tab, program them as follows:

Input Address	Input Name	Area 1	Input Type 1
1	Fire	Fire Area	Fire
2	Supervisory	Fire Area	24 Hour Alarm
3	Trouble	Fire Area	24 Hour Alarm

8. Click **Save**.
9. Navigate to **Programming | Trouble inputs**.
10. Click **Save**.
11. **In Protege GX**: Return to **Programming | Areas**. Right click on the fire area and click **Arm**.
    In Protege WX: Navigate to **Monitoring | Areas**. Arm the fire area.
12. Finally, start the reporting services.
    In Protege GX: Navigate to **Programming | Services**. Right click on the primary reporting service and click **Start**.
    In Protege WX: Navigate to **Monitoring | Services**. Start the primary reporting service.

Programming Trouble Inputs

As usual, trouble inputs are programmed in a system area. The following trouble inputs must be monitored for fire reporting:

Trouble Input Address	System Type	Trouble Input Name	Area 1	Input Type 1
CP1.5	Passive	Service Report Test	System Area	Trouble Silent
CP1.6	Passive	ContactID Reporting Failure	System Area	Trouble Silent
CP1.20	Active	ReportIP Reporting Failure	System Area	Trouble Silent
AExxx.2	Both	Mains Failure	System Area	Trouble Silent

In addition, assign your primary reporting service to the system area and ensure that the system area is always armed.

CAN/ULC-S559:2020, section 5.3 specifies that audible/visual indication of primary power failure is not required at the signal transmitting unit as long as a signal is sent to the receiving center. This is provided by the Mains Failure trouble input above.

Indicating Reporting Failures

Section 15.8 of CAN/ULC-S559:2020 requires an on-site indication should reporting fail on both channels within 180 seconds. This is required for passive reporting systems but also recommended for active reporting systems.

There are two methods for achieving this:

- Sites with keypads can display the trouble message on the keypad.
- If the fire alarm control panel has an COM Status input, it may be connected to any available dry relay contact on the controller or output expander. When there is a reporting failure, the relay will turn on to activate the COM Status indicator on the fire alarm control panel.

Indicating on a Keypad

1. Navigate to **Expanders | Keypads**.
2. Select the keypad that you need to display the indication.
3. In the **Options 1** tab, enable **Display trouble message**.
4. Click **Save**.

When there is a trouble in the system such as a reporting failure, the keypad will beep once and display the message, "Trouble fault check system".

End users can investigate the trouble by logging in the keypad and navigating to **Menu > 5. View > 2. Trouble View**.

Indicating with a COM Status Output

The COM status output connected to the fire panel must turn on when there is a reporting failure and off when communication is re-established.

- For IP reporting, use the **Report fail output** to control the COM status output.
- For Contact ID reporting, this can be achieved by using a dummy area to monitor the Contact ID Reporting Failure trouble input. The recommended method is to use an area that is **disarmed** at all times, where the **Ready output** for the area controls the COM Status output. The output must be inverted so that when the trouble input opens, the COM status output turns on, and vice versa.

The following instructions outline how to use a **Ready output** to control the COM status output:

1. Navigate to **Programming | Outputs**.
2. Select the output that will control the COM status output.
3. In the **Options** tab, enable **Invert output**.
4. Click **Save**.

   If the output is not on the controller, you must module update the expander the output is connected to.

5. Navigate to **Programming | Areas**.
6. Add a new area with a descriptive name, e.g. Contact ID Failure Monitoring (Do not arm).
7. In the **Outputs** tab, set the **Ready output** to the COM status output.
8. Click **Save**.
9. Navigate to **Programming | Trouble inputs**.
10. Select the ContactID Reporting Failure trouble input.
11. In the **Areas and input types** tab, set **Area 2** to the new area and **Input type 2** to Trouble Silent.

Optionally, click the ellipsis **[...]** button to open the input types page. Create a new input type with no settings enabled and assign it to this trouble input. This will prevent the trouble input activation from raising an alarm in this area.

12. Click **Save**.
13. **In Protege GX**: Return to **Programming | Areas**. Right click on the new area and click **Arm 24hrs**.

    In Protege WX: Navigate to **Monitoring | Areas**. Arm the 24hr portion of the new area.

    Do not arm the main portion of the area.

In normal operation, the area is ready to arm so the ready output is on (COM status output is off). When reporting fails the trouble input opens, causing the area to turn the ready output off so the COM status output turns on. This transmits the communication fault signal to the fire panel.

To prevent end users from arming this area, do not include it in any access levels.

Delaying the COM Status Output

Section 15.8 allows for the on-site indication to be delayed for up to 15 minutes to give time for the issue to resolve itself. If desired, you can program this using a ripple function.

1. Program and validate the COM status output with the instructions above.
2. Create a virtual output:
   - Navigate to **Programming | Outputs** and click **Add**.
   - Give the output a descriptive name, e.g. Contact ID Monitoring Ready Output (Virtual).
   - Set the **Module type** to Output (PX).
   - Set the **Module address** to any available address not used by any physical modules, or alternatively create a virtual output expander to assign the virtual output to.
   - Set the **Module output** to any available number.
   - It is recommended to disable event logging for virtual outputs to reduce their impact on event storage. In the **Options** tab, disable the **Log output events** option.
   - Click **Save**.
3. Navigate to **Programming | Areas** and select the Contact ID monitoring area programmed above.
4. In the **Outputs** tab, set the **Ready output** to the new virtual output.
5. Click **Save**.
6. Navigate to **Automation | Programmable functions**.
7. **In Protege GX**: Select the **Controller** in the toolbar.
8. Add a new programmable function with a descriptive name, e.g. Contact ID Monitoring Ripple Function.
9. Set **Type** to Ripple output.
10. In the **Ripple output** tab, set the following:
    - **Output to enable this function**: Ready virtual output
    - **Stage 1 output**: COM status output (inverted as usual)
    - **Stage 2 output**: Ready virtual output
    - **Inter stage on ripple time**: 0
    - **Inter stage off ripple time**: Up to 900 seconds (15 minutes).
11. Click **Save**.
12. **In Protege GX**: Right click on the programmable function and click **Start**.

    In Protege WX: Navigate to **Monitoring | Programmable Functions**. Start the programmable function.

Now, when the trouble input opens, the ready virtual output turns off. After a delay of up to 15 minutes, the COM status output activates, sending the signal to the fire panel. If the trouble input closes during this delay, the COM status output will not activate.

When the trouble input closes, the COM status output will deactivate immediately.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.