AN-317

# SIA L2 Reporting in Protege GX and Protege WX

Application Note

Last Published: 27-Sep-24 10:05 AM

# Contents

# Introduction

SIA Level Two is a reporting format defined by the Security Industry Association that is ideal for large scale integrated solutions such as the Protege system. This format is available for both IP and phone line reporting and provides many reporting features ideal for access control, automation and large burglary installations.

- All Protege controllers support SIA L2 reporting over an IP connection, using SIA DC-09 standard.
- Protege GX controllers with modem dialers support SIA L2 reporting over the phone line.

  Check the specifications of your controller model.

This application note provides basic instructions for programming SIA reporting, describes the SIA L2 format, and outlines the reporting codes and options available.

# Programming SIA L2 Reporting Services

The following basic instructions describe how to program an SIA L2 reporting service and assign it to areas. For more information about the options available for programming reporting services, see the **Programming | Services** section in the Protege GX Operator Reference Manual or Protege WX Programming Reference Manual.

There are two options for SIA L2 reporting:

- Phone line reporting using an SIA service.

  > This option is only available for Protege GX controllers with built-in modem dialers. Check your controller model for compatibility. Protege WX does not support this feature.

- IP reporting using a Report IP service.

## Programming an SIA (Phone Line) Reporting Service

> This option is only available in Protege GX.

1. In Protege GX, navigate to **Programming | Phone numbers**. Add one or more phone numbers that have been supplied by your monitoring station.
2. Navigate to **Programming | Services**. Set the **Controller** in the toolbar, and add a new service.
3. Set the **Service type** to SIA.
4. Set the **Service mode** to 1 - Start with controller OS to ensure that the service starts when the controller boots up.
5. In the **General** tab, enter the following settings and any others required for your site:
   - The **Client code** identifies the site in SIA messages, and is supplied by the monitoring station. This may be 4 or 6 digits.
   - Enter the phone numbers programmed above for the primary, secondary and backup connections to the monitoring station. You may also need a **PABX number** to allow the controller to dial out.
6. In the **Options** tab, enable the following options and any others required for your site:
   - Enable all of the reporting options to allow the service to report relevant events.
   - For setup and validation you can enable **Log modem events to event buffer**. To prevent large numbers of excess events, it is recommended that you disable this setting once the service has been validated.
   - Enable any required settings which allow variations to the SIA format (see page 7). These will depend on your site requirements and the capabilities of the central station receiver.
7. Click **Save**.
8. Wait for the record to be downloaded to the controller. Right click on the service and click **Start**.

## Programming an SIA Report IP Service

1. Navigate to **Programming | Services**.

   In Protege GX, select the relevant **Controller** from the toolbar.
2. Add a new reporting service.
3. Set the **Service type** to Report IP.
4. Set the **Service mode** to 1 - Start with controller OS to ensure that the service starts when the controller boots up.
5. In the **General** tab, enter the following settings and any others required for your site:
   - The **Client code** identifies the site in SIA messages, and is supplied by the monitoring station. This may be 4 or 6 digits.
   - Set the **Reporting protocol** to SIA over IP (DC09).

- If encryption is required, set the **Encryption level** and **Encryption key** provided by the monitoring station.
- It is recommended to configure a **Backup service** which provides a different path to the monitoring station. This may be a phone line or secondary IP connection.
- Enter the **Primary channel settings** and **Secondary channel settings** which are used to send messages to the receiver.

6. In the **Options** tab, enable the following settings and any others required for your site:
   - Enable all of the reporting options to allow the service to report relevant events.
   - For setup and validation, you can enable the logging settings. It is recommended that you disable these settings when the service has been validated to prevent large numbers of excess events.
7. Click **Save**.
8. Start the service.
   - **Protege GX**: Wait for the record to be downloaded to the controller. Right click on the service and click **Start**.
   - **Protege WX**: Navigate to **Monitoring | Services**. Click on the **Controls** button next to the new service and click **Start**.

## Assigning the Reporting Service to Areas

The reporting service must be assigned to one or more areas to allow it to report on arming, disarming and input events.

1. Navigate to **Programming | Areas**. Select one or more areas which will use this reporting service.
2. Navigate to **Reporting Services**.
   - **Protege GX**: In the **Configuration** tab, scroll down to **Reporting services**.
   - **Protege WX**: Select the **Reporting Services** tab.
3. Click **Add**, select the new SIA reporting service and click **OK**.
4. Click **Save**.

The relevant **Reporting options** must also be enabled in the areas (**Programming | Areas | Options (1)**) and input types (**Programming | Input types | Options (1)**).

# SIA L2 Message Format

By default, Protege controllers use the standard SIA L2 message format outlined below. When configuring the automation software at the monitoring station for the information coming from the receiver the following format should be used.

The standard SIA L2 message format is:

**#AAAA N ri GGG BA WXYZ**

Where:

| | |
|---|---|
| #AAAA | The account code block.<br>This may be prefixed by D# for a four-digit account code or F# for a six-digit account code.<br>This is set as the **Client code** in the service programming. |
| N | N signifies a new event. O signifies an existing event that is being reported again. |
| ri GGG | The area or partition that is being reported from 000 to 999.<br>This is the **Reporting ID** set in the area programming. |
| BA | A two-letter event code. There are a large number of event codes, which come in pairs indicating opening and closing events (for areas) or alarm and restore events (for inputs).<br>In this example the event code is BA for a burglary alarm. The corresponding restore code is BH. |
| WXYZ | The four-digit input or user number that generated the event code.<br>• Input numbers are based on the **Reporting ID** programmed in the input.<br>• User numbers are based on the user's Database ID. User number 9999 typically signifies the system user or a Protege operator. |

Reporting IDs and event codes are described further below.

IP reporting packets also include additional data, following the SIA DC-09 standard.

## Format Variations

The format of SIA messages can vary greatly depending on the configuration. Depending on the capabilities of the alarm receiver, it may be possible to extend the format to maximize the number of inputs, users and areas that can be reported by the service.

These format variations are only available for phone line reporting services. They are not available in Protege WX or with Protege GX IP reporting.

The following variation options are available in **Services | Options** when the **Service type** is set to SIA. Ensure that you discuss the configuration of the alarm receiver with your monitoring company prior to setting these options.

- **Send 4 digits client code**: When this option is enabled the SIA service will send a 4 digit client code instead of the standard 6 digits. This can be used with receivers that do not comply to the full SIA specification or software that cannot accept large point numbers.
- **Area client code will be 6 digits**: SIA Level 2 can accept client codes of either 4 or 6 digits. When this option is enabled, if the **Client code** set for an area (**Programming | Areas | Configuration**) is 4 digits long, it will be extended to 6 digits by adding 00. This option can be overridden by the **Send 4 digits client code** option.
- **Report 5 digit input numbers**: When this option is enabled the SIA service will send input identifiers as 5 digits instead of the standard 4. This allows larger input numbers to be specified.

  The SIA Level 2 format supports 5 digit input codes, but this may not be supported by all receivers.

- **Report user numbers in hexadecimal**: When this option is enabled the SIA service will send the user identifier as a 4 digit hexadecimal number. This option can override the **Report user number in 5 digits** option.
- **Report user number in 5 digits**: When this option is enabled the SIA service will send user identifiers as 5 digits instead of the standard 4. This allows larger user numbers to be specified.

  > The SIA Level 2 format supports 5 digit user codes, but this may not be supported by all receivers.

# Extended Data

SIA reporting over IP using the DC09 protocol supports extended data. This enables the controller to send the names of any inputs, trouble inputs, users and areas which are included in the report.

> This feature is supported in Protege GX controller firmware version 2.08.1334 or higher and Protege WX version 4.00.1358 or higher.

To enable extended data, navigate to **Sites | Controllers | General** in Protege GX or **System | Settings | General** in Protege WX and enter the following in the **Commands** field:

```
SIAExtendData = true
```

When this option is enabled, the names of the records will be included in each report after the standard SIA L2 message, according to the SIA DC09 format. For example, when a user disarms an area the report will be similar to the following:

```
#4837[Nri009OP0025][IReception Area][PJane Doe]
```

The characters before the record names indicate the type of information in this part of the message. `I` (alarm text) and **P** (programming data) are used for the record data.

## Record Names

The following name fields are used for different record types:

- For inputs, trouble inputs and areas, the service sends the **Keypad display name**.
- For users, the service sends the **Display name**.
- For operators, the service sends SYSTEM USER.

The maximum number of characters that can be sent is 32. Any additional characters will be ignored.

> Be aware that special characters in record names may not be decrypted correctly by Patriot receiver software. Patriot has confirmed that only ASCII characters are supported when using encryption.

# Reporting IDs

Reporting IDs are used to identify areas, inputs, trouble inputs and users in report messages. Typically you will need to supply a table of the IDs for each service to the monitoring station.

## Reporting IDs in Protege GX

Protege GX is capable of utilizing the entire range of Reporting IDs available in the SIA L2 format. This improves on the standard Contact ID formats by allowing 4 digit input and user codes, so that more records can be reported uniquely.

### Input and Trouble Input Reporting IDs

When each input and trouble input is added to the system it is assigned the next unique **Reporting ID**, and by default will report using that number. Reporting IDs assigned this way will be globally unique within the database. However, it is possible to customize the Reporting ID of each record, either manually or by applying a specific mapping.

By default SIA L2 allows a 4-digit ID for inputs and trouble inputs. However, it may be possible to extend this to a 6-digit ID (see page 7).

There are two options for customizing the Reporting IDs of inputs and trouble inputs:

- You can manually program the **Reporting ID** in **Programming | Inputs | General** or **Programming | Trouble inputs | General**.
- Reset the Reporting IDs for all inputs and trouble inputs by using the **Reset area, input and trouble input ID's** option in **Reports | Central station report** and selecting a **Report map type** (see next page). This will affect all inputs and trouble inputs assigned to an area which uses this reporting service.

  The recommended **Report map type** for use with the SIA format is None. This report map assigns sequential Reporting IDs to all inputs and trouble inputs. This is the most efficient mapping and allows the service to report on over 1000 inputs, which is not possible with the Standard and Large map types. The SIMS II report map is not available for SIA L2.

  When the None report map is used, inputs and trouble inputs will use the same range of Reporting IDs, starting from 1. These can be uniquely identified using the different event codes associated with inputs and trouble inputs (see page 12) and the different areas they are assigned to.

### Area Reporting IDs

The Reporting IDs for areas are 3 digits, and are configured in the same way as input and trouble input reporting IDs.

- You can manually program the **Reporting ID** in **Programming | Areas | Configuration**.
- Reset the Reporting IDs for all areas by using the **Reset area, input and trouble input ID's** option in **Reports | Central station report** (see next page). All of the areas which use this reporting service will be assigned a sequential Reporting ID (not affected by the **Report map type**).

### User Reporting IDs

In the SIA L2 format, user records are not identified using the programmed **Reporting ID**. Instead, the reporting service sends the unique **Database ID** to identify the user.

By default SIA L2 allows a 4-digit ID for users. However, it may be possible to extend this to a 6-digit or hexadecimal ID (see page 7).

The Database ID is displayed in the **Index** column of the central station report. Alternatively, you can run a user report to supply all relevant user records to the monitoring station.

# Central Station Reports in Protege GX

The report map generator in Protege GX is used to create central station reports. These allow you to view the reporting data for all of the inputs, trouble inputs, areas and users assigned to a particular reporting service. The report map is exported in CSV and HTML formats, which can be sent on to your monitoring station.

1. To generate a central station report, navigate to **Reports | Central station report**.
2. Select the **Reporting service** that you wish to create a report for.

   Only primary services are available (not backup services).

3. Enter an **Output directory** where the report will be saved. Click **Browse** to view your directories and create a new folder if required.

   When you run a report, Protege GX will create a subdirectory for each reporting service.

4. If you are using a reporting map, enable **Reset area, input and trouble input ID's** and select a **Report map type**. This will change the Reporting IDs of all areas, inputs and trouble inputs that are monitored by this service to follow the selected mapping table.

   This option will overwrite any custom Reporting IDs which have been entered.

5. Click **Generate**.
6. After a brief pause, a popup will inform you that the report export is complete. Click **OK**.
7. To view your report, click **Open**. This opens the output directory, which contains the report map in both CSV and HTML formats.

# Reporting IDs in Protege WX

## Input, Trouble Input and Area Reporting IDs

In Protege WX, Reporting IDs for areas, inputs and trouble inputs are set automatically when each record is added to the system. You can view and edit the Reporting IDs for each record in the following locations:

- For area records: **Programming | Areas | Configuration**.
- For input records: **Programming | Inputs | General**.
- For trouble input records: **Programming | Trouble Inputs | General**.

It is not possible to automatically apply a report map to records in Protege WX.

A central station report contains all of the Reporting IDs for inputs, trouble inputs and areas using this reporting service. To generate this report, navigate to **Monitoring | Reporting | Central Station Report**. Select a service and click **Export** to generate the report and save it to your computer in CSV format.

## User Reporting IDs

In the SIA L2 format, user records are not identified using the programmed **Reporting ID**. Instead, the reporting service sends the unique **Database ID** to identify the user. This can be viewed in **Users | Users | General**.

# Area Event Codes

Area reporting codes are used to report the opening and closing of an area (arming and disarming) to the central station receiver. They generally come in pairs of arming code and disarming code.

The following codes are sent for area arming and disarming:

| Description | Arming Code | Disarming Code |
|---|---|---|
| **Area Arming/Disarming By User**<br>This is sent with the user ID that disarmed/armed the area. This is the code used for normal area arming and disarming. | CL | OP |
| **Area Group Arming/Disarming By User**<br>When a group of areas is controlled by a user, this code will be used for each area in the group. | CG | OG |
| **Automatic Area Arming/Disarming**<br>When an area arms/disarms in response to an event or action this code will be used. A user ID of 999 will be sent to identify that it is a system user. | CA | OA |
| **Cancel Area Arming**<br>The cancel arming code is used when a deferred area is prevented from completing the arming cycle. | - | OA |
| **Early Arming/Disarming**<br>Used to send an early open or close message when the area is armed or disarmed before it is due. | CK | OK |
| **Late Arming/Disarming**<br>This message is sent when the area is not armed or not disarmed before the scheduled time. | CT | OJ |
| **Remote Arming/Disarming**<br>Used to report area control functions that are actioned by a remote method, such as through the software. This uses a user code of 9999. | CQ | OQ |
| **Quick Arming/Disarming**<br>Used to report arming of the area without an exit delay. | CG | OP |
| **Key Switch Arming/Disarming**<br>Sent when an area is armed or disarmed from an input or programmable function. | CS | OS |
| **Stay Arming/Disarming**<br>Sent when the area is stay armed, indicating that only external inputs (inputs with the **Stay Input** option enabled) are armed. | CG | OP |
| **Partial Arming/Disarming**<br>Sent when the area is armed with bypassed inputs. | CG | OP |
| **Recent Arming**<br>Sent when the area has armed and an alarm has activated within the **Recent closing time**. | CR | OP |

# Input Event Codes

The event codes for inputs and trouble inputs indicate which type of condition is detected by the input. They generally come in pairs of alarm code and restore code.

Standard inputs typically report burglary alarm, tamper and bypass conditions. It is also possible to apply a custom event reporting code to any input using the input type, allowing them to report conditions such as medical alarms and smoke alerts.

In contrast, the trouble inputs for each module use specific event codes based on the type of trouble condition that they report. These are outlined in the relevant reporting tables for each module.

## Default Input Event Codes

The following event codes are used for standard intruder detection ('burglary') inputs.

| Event | Alarm Code | Restore Code |
|---|---|---|
| Alarm/Restore | BA | BH |
| Tamper/Restore | BT | BJ |
| Bypass/Unbypass | BB | BU |

## Verified Alarm Code

In some installations it is necessary to send a different code when an alarm has been confirmed by more than one input opening. This allows response centers to distinguish between unconfirmed and confirmed alarm reports.

| Event | Alarm Code | Restore Code |
|---|---|---|
| Burglary Verified Alarm/Restore | BV | BH |

To use this code the following two features must be enabled:

- Smart input mode
- Remote notify delay

For more information and programming instructions, see Application Note 312: Minimizing Offsite Reporting of False Alarms in Protege GX and Protege WX.

## Custom Input Event Codes

Custom reporting codes can be applied to inputs via the input type programming. Create an input type, set the **Custom reporting code**, and apply the input type to any number of inputs to cause them to report with the corresponding event codes.

Custom reporting codes are only used for input opening/closing. For tamper and bypass events the default event codes are used.

| Reporting Code | Description | Alarm Code | Restore Code |
|---|---|---|---|
| 0 | Medical Alarm | MA | MH |
| 1 | Pendant Transmitter | QA | QH |
| 2 | Fail to Report In | YC | YK |

| Reporting Code | Description | Alarm Code | Restore Code |
|---|---|---|---|
| 3 | Fire Alarm | FA | FH |
| 4 | Smoke Alarm | FA | FH |
| 5 | Combustion | FA | FH |
| 6 | Water Flow | WA | WH |
| 7 | Heat | KA | KH |
| 8 | Pull Station | FA | FH |
| 9 | Duct | FA | FH |
| 10 | Flame | FA | FH |
| 11 | Near Flame | FA | FH |
| 12 | Panic Alarm | PA | PH |
| 13 | Duress | HA | HH |
| 14 | Silent | PA | PH |
| 15 | Audible | PA | PH |
| 16 | Burglary | BA | BH |
| 17 | Perimeter | BA | BH |
| 18 | Interior | BA | BH |
| 19 | 24 Hour | TA | TH |
| 20 | Entry/Exit | BA | BH |
| 21 | Day/Night | BA | BH |
| 22 | Outdoor | BA | BH |
| 23 | Tamper | TA | TH |
| 24 | Near Alarm | UA | UH |
| 25 | 24 Hour Non Burglary | UA | UH |
| 26 | Gas Detected | GA | GH |
| 27 | Refrigeration | ZA | ZH |
| 28 | Loss of Heat | KA | KH |
| 29 | Water Leakage | WA | WH |
| 30 | Foil Break | UA | UH |
| 31 | Day Trouble | UA | UH |

## Additional Custom Input Event Codes

In addition to the list of codes available in the user interface, a larger range of custom event codes is available for inputs and trouble inputs using command programming. This allows you to report a larger number of unique event types to the monitoring station.

This feature is only available for SIA DC09 reporting over IP. It is supported in Protege GX controller firmware version 2.08.1334 or higher and Protege WX version 4.00.1358 or higher.

To use one of the event codes from the table below, select or create an input type in **Programming | Input types | General** and enter the following command:

```
SIACode = X
```

Where **X** is a number from 32-210 corresponding to the desired reporting code from the table below. This input type can then be assigned to the relevant inputs or trouble inputs.

| Reporting Code | Description | Alarm Code | Restore Code |
|---|---|---|---|
| 32 | Alarm Panel Substitution | AA | AA |
| 33 | Abort | AB | UJ |
| 34 | Analog Service | AS | AN |
| 35 | AC Fail | AT | AR |
| 36 | Burglary Alarm | BA | BH |
| 37 | Burglary Bypass | BB | BU |
| 38 | Burglary Cancel | BC | BR |
| 39 | Swinger Trouble | BD | BE |
| 40 | Unverified Burglary | BG | BH |
| 41 | Burglary Alarm Cross Point | BM | BH |
| 42 | Burglary Supervisory | BS | BJ |
| 43 | Burglary Trouble | BT | BJ |
| 44 | Burglary Verified | BV | BR |
| 45 | Burglary Test | BX | BR |
| 46 | Missing Supervision | BZ | BJ |
| 47 | Automatic Closing | CA | OA |
| 48 | Closing Delinquent | CD | CL |
| 49 | Closing Extend | CE | CL |
| 50 | Forced Closing | CF | OP |
| 51 | Close Area | CG | CL |
| 52 | Fail to close | CI | CL |
| 53 | Late to Close | CJ | CL |
| 54 | Early to Close | CK | CL |
| 55 | Closing Report | CL | OP |
| 56 | Missing Alarm - Recent Closing | CM | UJ |
| 57 | Command Sent | CO | CO |
| 58 | Automatic Closing | CP | OA |
| 59 | Remote Closing | CQ | OQ |
| 60 | Recent Closing | CR | OR |
| 61 | Closing Keyswitch | CS | OS |
| 62 | Late to Open | CT | OP |

| Reporting Code | Description | Alarm Code | Restore Code |
|---|---|---|---|
| 63 | Force Armed | CW | OP |
| 64 | Custom Function Executed | CX | CX |
| 65 | Point Closing | CZ | OZ |
| 66 | Card Assigned/Deleted | DA | DB |
| 67 | Access Closed | DC | DO |
| 68 | Access Denied/Granted | DD | DG |
| 69 | Request to Enter | DE | DG |
| 70 | Door Forced Alarm | DF | DR |
| 71 | Access Denied - Passback | DI | DG |
| 72 | Door Forced Trouble | DJ | DR |
| 73 | Access Lockout | DK | DR |
| 74 | Door Left Open Alarm | DL | DH |
| 75 | Door Left Open Trouble | DM | DH |
| 76 | Access Denied - Unauthorized Time | DP | DG |
| 77 | Access Denied - Unauthorized Arm State | DQ | DG |
| 78 | Door Station | DS | DR |
| 79 | Dealer ID | DU | UR |
| 80 | Access Denied - Unauthorized Entry Level | DV | DG |
| 81 | Access Denied - Interlock | DW | DG |
| 82 | Request to Exit | DX | DG |
| 83 | Door Locked | DY | DR |
| 84 | Access Denied - Door Secured | DZ | DG |
| 85 | Exit Alarm | EA | UR |
| 86 | Exit Error | EE | UJ |
| 87 | Expansion Device Missing | EN | ER |
| 88 | Expansion Device Tamper | ES | EJ |
| 89 | Expansion Trouble | ET | ER |
| 90 | External Device Condition | EX | UJ |
| 91 | Missing Alarm - Exit Error | EZ | UJ |
| 92 | Fire Alarm | FA | FH |
| 93 | Fire Bypass | FB | FU |
| 94 | Fire Cancel | FC | FJ |
| 95 | Unverified Event - Fire | FG | FH |
| 96 | Fire Test Begin/End | FI | FK |
| 97 | Fire Alarm Silenced | FL | FR |

| Reporting Code | Description | Alarm Code | Restore Code |
|---|---|---|---|
| 98 | Fire Supervisory | FS | FV |
| 99 | Fire Trouble | FT | FJ |
| 100 | Fire Supervisory Trouble | FW | FQ |
| 101 | Fire Test | FX | FR |
| 102 | Missing Fire Trouble | FY | FJ |
| 103 | Missing Fire Supervision | FZ | FQ |
| 104 | Gas Alarm | GA | GH |
| 105 | Gas Bypass | GB | GU |
| 106 | Gas Supervisory | GS | GR |
| 107 | Gas Trouble | GT | GJ |
| 108 | Gas Test | GX | GR |
| 109 | Hold Up Alarm | HA | HH |
| 110 | Hold Up Bypass | HB | HU |
| 111 | Hold up supervisory | HS | HR |
| 112 | Hold up trouble | HT | HJ |
| 113 | Equipment Failure Condition | IA | IR |
| 114 | User Code Tamper | JA | UJ |
| 115 | Date Changed | JD | UJ |
| 116 | Holiday Changed | JH | UJ |
| 117 | Latchkey Alert | JK | UJ |
| 118 | User On Premises | JP | UJ |
| 119 | Schedule execute | JR | UJ |
| 120 | Schedule change | JS | UJ |
| 121 | Time Changed | JT | UJ |
| 122 | User code change | JV | UJ |
| 123 | User Code Deleted | JX | UJ |
| 124 | User Code Added | JY | UJ |
| 125 | User Level Set | JZ | UJ |
| 126 | Heat Alarm | KA | KH |
| 127 | Heat Bypass | KB | KU |
| 128 | Heat supervisory | KS | KJ |
| 129 | Heat Trouble | KT | KJ |
| 130 | Phone Line Trouble | LT | LR |
| 131 | Medical Alarm | MA | MH |
| 132 | Medical Bypass | MB | MU |

| Reporting Code | Description | Alarm Code | Restore Code |
|---|---|---|---|
| 133 | Message | MI | MI |
| 134 | Medical Supervisory | MS | MR |
| 135 | Medical Trouble | MT | MJ |
| 136 | No Activity | NA | NS |
| 137 | Network Condition | NC | NR |
| 138 | Forced Perimeter Arm | NF | CL |
| 139 | Perimeter Armed | NL | OP |
| 140 | Network Failure | NT | NR |
| 141 | Automatic Opening | OA | CA |
| 142 | Cancel Report | OC | UH |
| 143 | Open Area | OG | OP |
| 144 | Early to Open from Alarm | OH | OP |
| 145 | Fail to Open | OI | OP |
| 146 | Late Open | OJ | OP |
| 147 | Early Open | OK | OP |
| 148 | Late to Open from Alarm | OL | OP |
| 149 | Opening/Closing Report | OP | CL |
| 150 | Remote Opening | OQ | OP |
| 151 | Disarm from Alarm | OR | UJ |
| 152 | Late to Close | OT | CL |
| 153 | Point Opening | OZ | CZ |
| 154 | Panic Alarm | PA | PH |
| 155 | Panic Bypass | PB | PU |
| 156 | Panic Supervisory | PS | PR |
| 157 | Panic Trouble | PT | PJ |
| 158 | Emergency Alarm | QA | QH |
| 159 | Emergency Bypass | QB | QU |
| 160 | Emergency Supervisory | QS | QR |
| 161 | Emergency Trouble | QT | QJ |
| 162 | Relay Close | RC | RO |
| 163 | Relay Open | RO | RC |
| 164 | Data Lost | RT | UJ |
| 165 | Test Off Normal | RY | UJ |
| 166 | Sprinkler Alarm | SA | SH |
| 167 | Sprinkler Bypass | SB | SH |

| Reporting Code | Description | Alarm Code | Restore Code |
|---|---|---|---|
| 168 | Change Of State | SC | SC |
| 169 | Sprinkler Supervisory | SS | SR |
| 170 | Sprinkler Trouble | ST | SJ |
| 171 | Tamper Alarm | TA | TR |
| 172 | Tamper Bypass | TB | TU |
| 173 | Walk Test Point | TP | TP |
| 174 | Tamper Trouble | TT | TJ |
| 175 | Untyped Zone Alarm | UA | UH |
| 176 | Untyped Zone Bypass | UB | UU |
| 177 | Unverified Event - Untyped | UG | UH |
| 178 | Untyped Zone Supervisory | US | UR |
| 179 | Untyped Zone Trouble | UT | UJ |
| 180 | Untyped Missing Trouble | UY | UJ |
| 181 | Untyped Missing Alarm | UZ | UH |
| 182 | Printer Paper In/Out | VO | VI |
| 183 | Printer Trouble | VT | VR |
| 184 | Printer Test | VX | VR |
| 185 | Water Alarm | WA | WH |
| 186 | Water Bypass | WB | WU |
| 187 | Water Supervisory | WS | WR |
| 188 | Water Trouble | WT | WJ |
| 189 | Extra Point | XE | UR |
| 190 | Extra RF Point | XF | UR |
| 191 | Sensor Reset | XI | UR |
| 192 | Low Received Signal Strength | XL | XJ |
| 193 | Missing Alarm - Cross Point | XM | UJ |
| 194 | RF Interference | XQ | XH |
| 195 | RF Receiver Tamper | XS | XJ |
| 196 | TX Battery Trouble | XT | XR |
| 197 | Forced Point | XW | UR |
| 198 | Bell Fault | YA | YH |
| 199 | Busy Seconds | YB | UJ |
| 200 | RX Line card Trouble | YD | YE |
| 201 | Overcurrent Trouble | YI | YJ |
| 202 | Power Supply Trouble | YP | YQ |

| Reporting Code | Description | Alarm Code | Restore Code |
|---|---|---|---|
| 203 | Communication Trouble | YS | UJ |
| 204 | System Battery Trouble | YT | YR |
| 205 | Diagnostic Error | YU | UJ |
| 206 | Service Completed | YZ | UJ |
| 207 | Freeze Alarm | ZA | ZH |
| 208 | Freeze Bypass | ZB | ZU |
| 209 | Freeze Supervisory | ZS | ZR |
| 210 | Freeze Trouble | ZT | ZJ |

# Trouble Input Event Codes

Below are the default event codes for the trouble inputs on each module. You can override these using an input type with the custom event codes described above (see page 12).

Trouble inputs send the same event codes regardless of whether they are programmed to generate 24hr alarms or regular area alarms.

## Controller Trouble Inputs

| Trouble Input Address | Description | Alarm Code | Restore Code |
|---|---|---|---|
| **CP001:01** | Reserved | - | - |
| **CP001:02** | 12V Supply Failure (DIN rail controllers) | AT | AR |
| | AC Failure (PCB controllers) | AT | AR |
| **CP001:03** | Reserved | - | - |
| **CP001:04** | Real Time Clock Not Set | | |
| **CP001:05** | Service Report Test | TX | UJ |
| **CP001:06** | Service Report Failure to Communicate | YC | UH |
| **CP001:07** | Phone Line Fault (modem model only) | LT | LR |
| **CP001:08** | Auxiliary Failure | YP | YQ |
| **CP001:09** | Bell Cut/Tamper | YA | YH |
| **CP001:10** | Reserved | - | - |
| **CP001:11** | Bell Current Overload | YA | YH |
| **CP001:12** | Reserved | - | - |
| **CP001:13** | Module Communication | YA | YH |
| **CP001:14** | Module Network Security | ET | ER |
| **CP001:15-19** | Reserved | - | - |
| **CP001:20** | Report IP Reporting Failure | UA | UH |
| **CP001:21** | Reserved | - | - |
| **CP001:22** | ModBUS Communication Fault | UA | UH |
| **CP001:23** | Protege System Remote Access | UA | UH |
| **CP001:24** | Installer Logged In | UA | UH |
| **CP001:25-8** | Reserved | - | - |
| **CP001:29** | System restarted | YC | YK |
| **CP001:30** | PoE Connection Lost (PoE model only) | YC | YK |
| **CP001:31** | Output Over-Current Failure (PoE model only) | YC | YK |
| **CP001:32** | 3G Modem Link Lost (legacy 3G modem model only) | UA | UH |
| **CP001:33** | Controller Group Link Lost | UA | UH |
| **CP001:34-64** | Reserved | - | - |

## Keypad Trouble Inputs

| Trouble Input Address | Description | Alarm Code | Restore Code |
|---|---|---|---|
| **KPxxx:01** | Module Tamper | TA | TH |
| **KPxxx:02** | Reserved | - | - |
| **KPxxx:03** | Panic (keys 1 + 3) | PA | PH |
| **KPxxx:04** | Duress (user duress code entered) | HA | HH |
| **KPxxx:05-6** | Reserved | - | - |
| **KPxxx:07** | Too Many Incorrect Codes | JA | UJ |
| **KPxxx:08** | Module Offline | EM | EN |

## Input Expander Trouble Inputs

| Input Address | Description | Alarm Code | Restore Code |
|---|---|---|---|
| **ZXxxx:01-15** | Reserved | - | - |
| **ZXxxx:16** | Module Offline | EM | EN |

## Reader Expander Trouble Inputs

| Trouble Input Address | Description | Alarm Code | Restore Code |
|---|---|---|---|
| **RDxxx:01-11** | Reserved | - | - |
| **RDxxx:12** | Reader 1 Tamper | TT | TJ |
| **RDxxx:13** | Reader 2 Tamper | TT | TJ |
| **RDxxx:14** | Door 1 Too Many Access Attempts | JA | UJ |
| **RDxxx:15** | Door 2 Too Many Access Attempts | JA | UJ |
| **RDxxx:16** | Module Offline | EM | EN |

The reader expander also monitors trouble inputs associated with connected doors.

| Trouble Input Address | Description | Alarm Code | Restore Code |
|---|---|---|---|
| **RDxxx:DR1:01** | Door Forced | DF | DR |
| **RDxxx:DR2:01** | Door Forced | DF | DR |
| **RDxxx:DR1:02** | Door Left Open | DM | DH |
| **RDxxx:DR2:02** | Door Left Open | DM | DH |
| **RDxxx:DR1:08** | Door Duress | HA | HH |
| **RDxxx:DR2:08** | Door Duress | HA | HH |

## Output Expander Trouble Inputs

| Trouble Input Address | Description | Alarm Code | Restore Code |
|---|---|---|---|
| **PXxxx:01-7** | Reserved | - | - |
| **PXxxx:08** | Module Offline | EM | EN |

## Analog Expander Trouble Inputs

| Trouble Input Address | Description | Alarm Code | Restore Code |
|---|---|---|---|
| **AExxx:01** | Module Tamper | TA | TH |
| **AExxx:02** | Mains Failure | AT | AR |
| **AExxx:03** | Low Battery/Battery Failure | YT | YR |
| **AExxx:04** | Output Voltage Low | MA | MH |
| **AExxx:05** | Output Over-Current Failure | MA | MH |
| **AExxx:06** | Core Temperature Over-Temp Failure | MA | MH |
| **AExxx:07** | Reserved | - | - |
| **AExxx:08** | Module Offline | EM | EN |

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.