integriti
INTEGRATED SOLUTIONS

INTEGRITI

ALARM REPORTING COMMUNICATIONS TASK

INNER RANGE recommends that all Inner Range systems be installed & maintained by FACTORY CERTIFIED TECHNICIANS.

For a list of Accredited Dealers in your area refer to the Inner Range Website.
http://www.innerrange.com

ASIAL MEMBER
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED
GOLD MEMBER

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

Certified System
Quality
ISO 9001

Description of the Alarm Reporting Communications Task:

This document is correct as of Integriti Software Version 23.1.0 and Integriti Controller Firmware version 23.1.0.38985

This document should be read in conjunction with the Integriti Programming Reference Manual and any relevant Integriti Contact ID or SIA Reporting Map tables.

https://auth.innerrange.com/login?service=https://www.innerrange.com/login

Summary:

The purpose of the Alarm Reporting CT is to be able to report alarms via the selected alarm delivery device and/or communication protocol.

The currently supported communication protocols are:

- CSL DualCom (formerly WebWayOne)
- Trikdis
- IRIS
- SIA IP Reporting (UDP/TCP-2021)

Functionality:

The Alarm Reporting CT can perform the following operations:

1. Establish and maintain a connection with the alarm delivery device. *
2. Interact with the alarm delivery device by receiving and sending commands. *
3. Report alarms via the ContactID alarm reporting format.
4. Report alarms via the SIA alarm reporting format. †

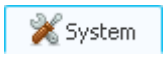
NOTES:

*1 SIA IP Reporting protocol communicates directly with the Central Monitoring Station Receiver via the Controller Ethernet connection and does not require a separate onsite alarm delivery device.

†2 SIA format is not available via the Trikdis alarm protocol.

Communications Task options programming overview

The following section will guide you through the creation of the communications task and the various options for each setting.

1. Click on the 

tab followed by 

.
2. Click 

to create a new communications task.
3. In the window that appears, enter a name for the communications task and enter any necessary notes in the notes field.
4. Under Comms Task Setup drop down the type list box and select “Alarm Reporting”.
5. Expand out the ‘Configuration’ section of the available Alarm Reporting programming.
6. Enter the designated client code for identifying the site to the monitoring installation.

> Information on how to create review filter stacks is available in the appendix of the System Configuration Handbook under the section titled ‘Filter Stacks’.

7. Expand out the ‘Settings’ section.
8. Optionally, set an input that will be used to reflect the status of the communications task.

> *Inputs C01:Z33-Z99 are ideal for this application. This input will go in to alarm if the communications task fails.*

9. Expand out the ‘Options’ section.
10. The review filter allows for the communications task to filter out the alarms that it will attempt to report to the alarm delivery device. There are a few tick box options and a timeout setting that control different aspects of when alarms will be reported, these are:
    - General Open/Close.
    - Xmit Historic.
    - Report Timeout Minutes.

11. Expand out the ‘Configurations’ section.

Change the Alarm Protocol to match the connecting equipment.
See the following section ‘

12. Specific Options for Alarm Protocol selection' for more detail on the following protocols:
    a. CSL DualCom
    b. Trikdis
    c. IRIS
    d. SIA IP Reporting
13. Configure EN50131 groups as required.
    Up to 8 Verify Groups can be configured. A group is enabled/checked when both the "All Path Fault" and the "Single Path Fault" inputs have been configured.
    When enabled, the "Verify Group" value of the comms task is tested against the "Verify Group" values that are configured in the areas.

    For details of other system programming required to implement these EN50131 operations, refer to the Document;
    Integriti_Application_Note-EN50131_Recommended_programming

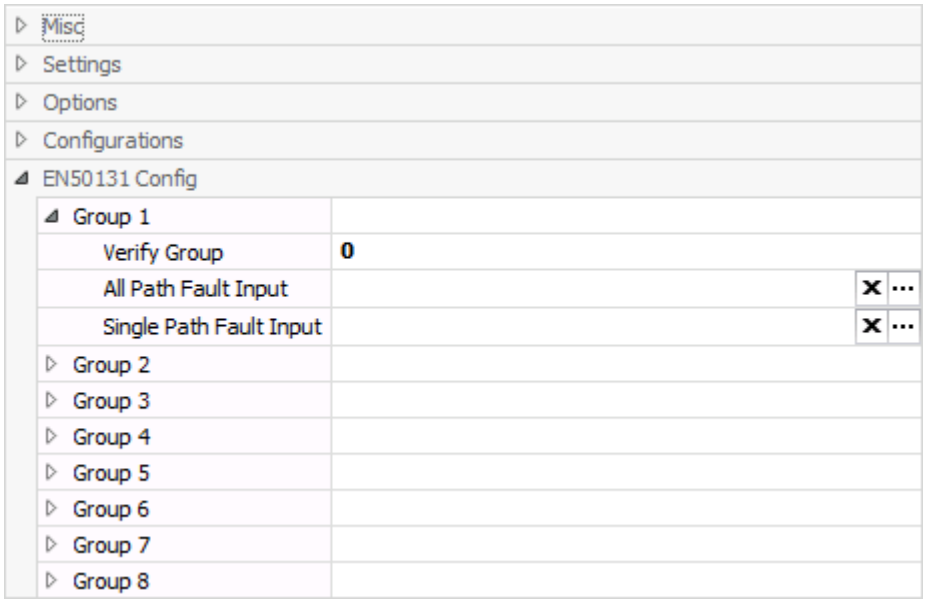


Figure 1: Comms task EN50131 configuration

14. Click the  button and close the dialog.

Specific Options for Alarm Protocol selection

This section expands upon the Alarm Protocol selection from step 12.

CSL DualCom Protocol Options

Communication Port

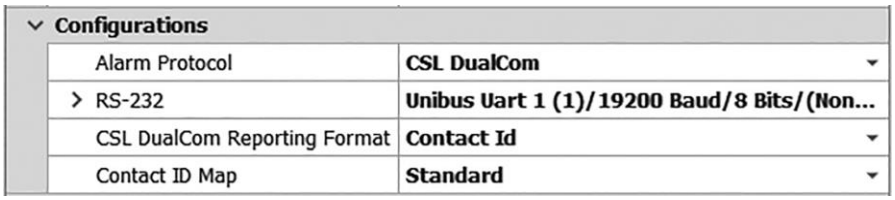
The CSL DualCom device connects to the Integriti controller via a serial RS232 interface. Any RS232 serial port of the Integriti controller can be chosen. The default port settings are 19200, 8, N, 1.

Alarm Format:

The alarm event format can be chosen to be either:

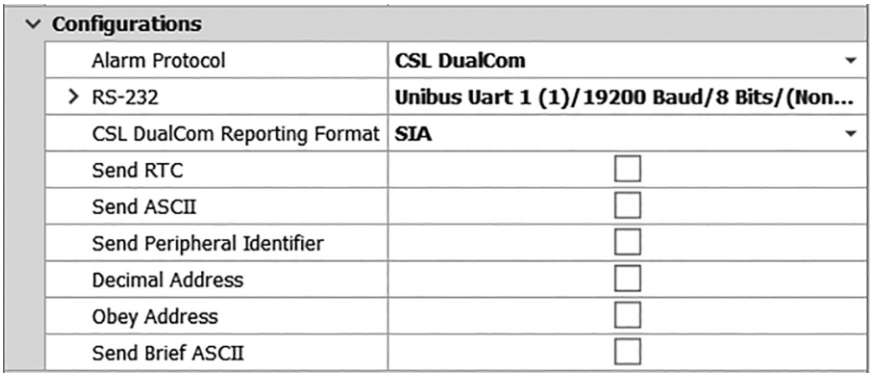
- ContactID
- SIA

ContactID Format Configuration



When the ContactID format is chosen the ContactID map can be selected

SIA Format Configuration:



When the SIA format is chosen the following settings can be configured:

Send time:

When set the time of the event will be sent in the SIA alarm data

Send ASCII:

When set the review text of the event will be sent in the SIA alarm data

Send peripheral identifier:

When set an additional identifier is sent in the SIA alarm data

Decimal address:

When set the address of input are set as decimal instead of hexadecimal in the SIA alarm data

Obey address:

When set some system input events do not have an identifier sent for them (E.g. AC fail, System power up etc.)

Trikdis Protocol Options

Communication Port

The Trikdis G16 device connects to the Integriti controller via a serial TTL interface. Any TTL serial port of the Integriti controller can be chosen. The default port settings are 19200, 8, N, 1.

ContactID Format Configuration

Select from one of three ContactID map options:

- Standard
- Access
- Sims II

IRIS Protocol Options

Communication Port

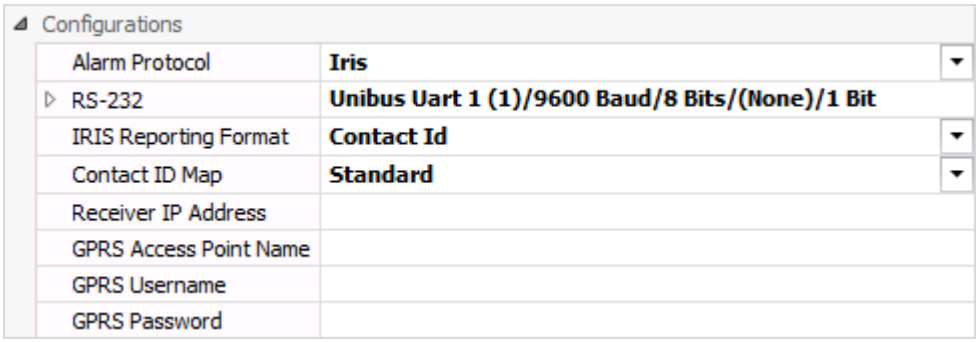
The Chiron IRIS Touch device connects to the Integriti controller via a serial RS232 interface. Any RS232 serial port of the Integriti controller can be chosen. The default port settings are 9600, 8, N, 1.

Alarm Format:

The alarm event format can be chosen to be either:

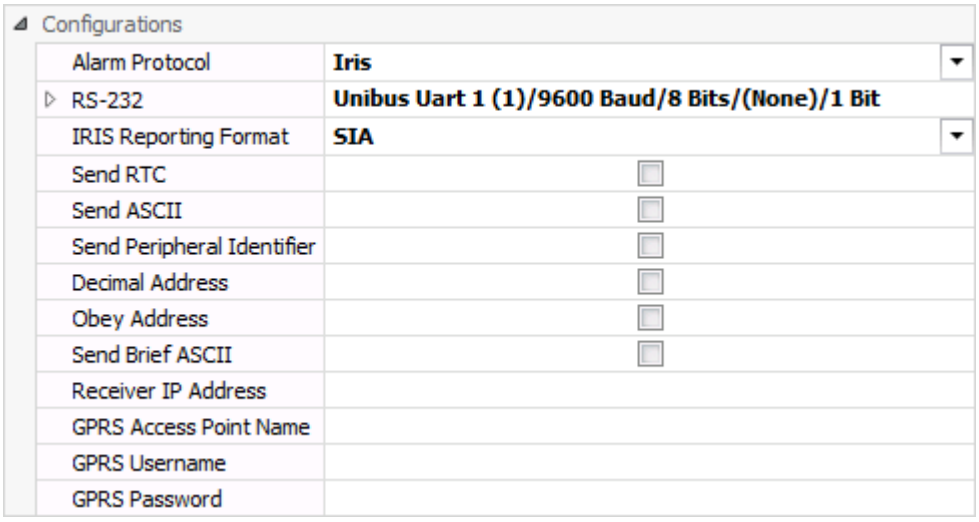
- ContactID
- SIA

ContactID Format Configuration



When the ContactID format is chosen the ContactID map can be selected.

SIA Format Configuration:



When the SIA format is chosen the following settings can be configured:

Send time

When set the time of the event will be sent in the SIA alarm data

Send ASCII

When set the review text of the event will be sent in the SIA alarm data

Send peripheral identifier

When set an additional identifier is sent in the SIA alarm data

Decimal address

When set the address of input are set as decimal instead of hexadecimal in the SIA alarm data

Obey address

When set some system input events do not have an identifier sent for them (E.g. AC fail, System power up etc.)

Receiver IP Configuration:

The IRIS communicator needs to be configured with the IP address endpoint that it will communicate with.

GPRS Authentication Configuration:

If the GPRS network authentication credentials are required then the APN, username and password can be configured.

SIA IP Reporting Protocol Options

Introduction

The SIA IP Reporting protocol allows an Integriti Security Controller (ISC) or Integriti Access Controller (IAC) to report events from the protected premises to a central monitoring station using Internet protocol (IP) to transfer the event data.
The Integriti Controller Ethernet connection is used and a separate onsite alarm reporting device is not required.

The SIA IP Reporting Protocol is defined in the SIA Standard;
SIA DC-09-2021. SIA Digital Communication Standard (DCS) – Internet Protocol Event Reporting.

Supported SIA IP Features.

The following SIA IP features are supported:

- TCP (Only supports connections that remain open, when socket is not closed after a message transmission)
- UDP
- 128 Bit AES-CBC Encryption
- SIA Alarm Reporting Format. SIA-DCS-DC03. (SIA Digital Communication Standard - “SIA Format” Protocol for Alarm System Communications)
- Contact ID Alarm Reporting Format. ADM-CID - DC05. (Digital Communication Standard - “Contact ID” Protocol for Alarm System Communications)
- Link Supervision (Supervision Message), with programmable period from 10 seconds to 18 hours
- Static IP Programming for Central Station Receiver (CSR)
- DNS Programming for CSR (Installations using this feature will not comply to SIA DC-09-2021)

Unupported SIA IP Features.

The following SIA IP features are not supported:

- Optional Extended Data.
- RSP (Message response). Handled the same as DUH (Unable to process) response.
- Timestamp only supported on encrypted messages.

Supported Alarm Identifier Tokens (Reporting formats)

The following alarm reporting formats are supported:

- SIA-DCS
- ADM-CID

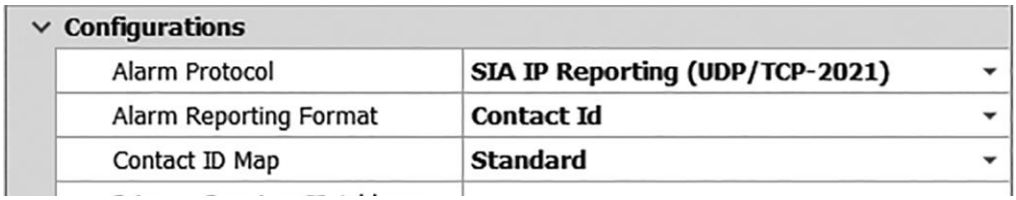
Configuration

Alarm Reporting Format:

The alarm event format can be chosen to be either:

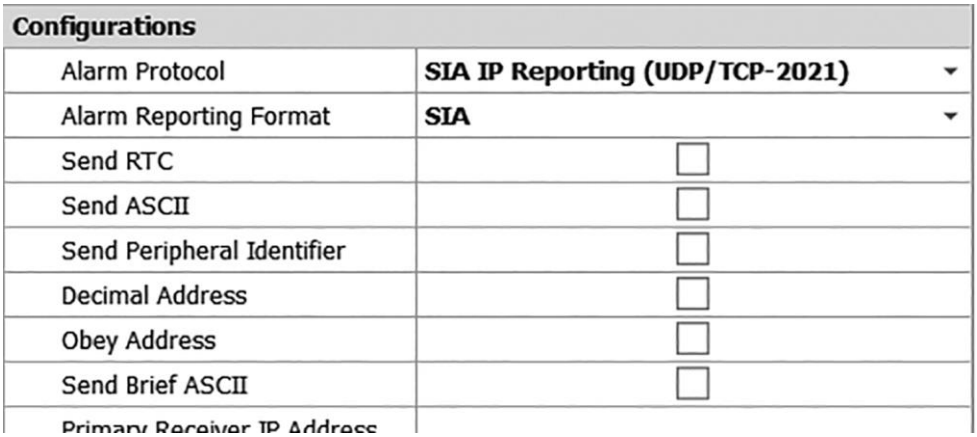
- ContactID
- SIA

ContactID Format Configuration



When the ContactID format is chosen, the Contact ID Map must be selected. The ContactID Map determines which Inputs (Zones & System Inputs) are uniquely reported.

SIA Format Configuration:



When the SIA format is chosen the following settings can be configured:

Send RTC (time)

When set the time of the event will be sent in the SIA alarm data.

Send ASCII

When set the review text of the event will be sent in the SIA alarm data.

Send Peripheral Identifier

When set an additional identifier is sent in the SIA alarm data.

Decimal Address

When set the address of inputs are set as decimal instead of hexadecimal in the SIA alarm data.

Obey Address

When set some system input events do not have an identifier sent for them (e.g. AC fail, System power up, etc.)

Send Brief ASCII

When set an abbreviated version of the review text of the event will be sent.

Receiver IP Communications Configuration:

Configurations	
Alarm Protocol	SIA IP Reporting (UDP/TCP-2021)
Alarm Reporting Format	Contact Id
Contact ID Map	Standard
Primary Receiver IP Address	
Primary Receiver Port	0
Primary Domain Name	
Primary SIA Protocol	UDP-2021
Secondary Receiver IP Address	
Secondary Receiver Port	0
Secondary Domain Name	
Secondary SIA Protocol	UDP-2021
Account Prefix	0
Receiver Number	0
Supervise Connection	☐
Supervision Period	00 hours 00 minutes 00 seconds
Enable Encryption	☐
Encryption Key	

The SIA IP Communications Task needs to be configured with the primary and optional secondary IP connection details, account details, supervisory settings and encryption settings for communications with the central station receiver.

The data and settings for these options and details of which optional settings are required is normally supplied by the central monitoring station.

Primary Receiver IP Address

The IP address of the primary central station receiver.

Primary Receiver Port

The central station receiver port to connect to.

Primary Domain name (Optional)

The domain name of the central station receiver to use for a DNS lookup. Note: The Installation will no longer be compliant with “SIA IP Reporting (UDP/TCP-2021)” if this option is used. This option is an alternative for “Primary Receiver IP Address”.

Primary SIA Protocol

The layer 4 protocol to use to connect to the central station receiver. The options are “UDP-2021” or “TCP-2021”.

Secondary Receiver IP Address (Optional)

The IP address of the secondary central station receiver.

Secondary Receiver Port (Optional)

The secondary central station receiver port to connect to.

Secondary Domain name (Optional)

The domain name of the secondary central station receiver to use for a DNS lookup. Note: The Installation will no longer be compliant with "SIA IP Reporting (UDP/TCP-2021)" if this option is used. This option is an alternative for "Secondary Receiver IP Address".

Secondary SIA Protocol (Optional)

The layer 4 protocol to use to connect to the secondary central station receiver.

Client Code (Required)

Also known as the account number - Main form of identification. Limited to 3-8 Hex Characters

Account Prefix (Optional)

The account prefix for this equipment.

Receiver number (Optional)

Identification to further extend the identification for the receiving equipment.

Supervise Connection

Enables supervision of the connection between this equipment and the central station receiver. When enabled this device will periodically check if it can still communicate with the central station receiver.

Supervision Period

The period of time to wait before testing the connection when supervise connection is enabled. Must be in the range of 10 seconds to 18 hours. Note: For values greater than 3600 seconds, the nearest hour will be used. Only required when "supervise connection" is enabled.

Encryption

Enables AES 128 bit encryption between this device and the central station receiver.

Encryption Key

The private key to be used for encryption between this device and central station receiver. Only required when encryption is enabled.

Inputs

There are three inputs that can be controlled by the Alarm Reporting CT, these are:

Input Name	Sealed State	Unsealed State
Online	The protocol is considered to be online/polling/working.	The protocol is considered to be offline/not working.
Fail	An alarm was reported successfully.	An alarm failed to be reported.
Backup	The backup communications task is not executing.	Backup communications task is delivering alarms on behalf of the Alarm Reporting communications task.

Appendix 1: Wiring Trikdis G16 TTL connection