



Integrating Integriti controllers (peer to peer)

*Document created with reference to Controller firmware V3.2.1.19866
and Software version V3.2.0.7673*



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



© Copyright 2013

Inner Range Pty. Ltd.

Unauthorised copying of this document is prohibited

Integriti controller peer to peer communications

This feature uses multicast UDP networking and therefore requires the site networking infrastructure to support this. The simplest solution is to have the controllers on the same LAN segment. If this is not possible the options of using a VPN, or the possibly complicated solution of setting up forwarding of the required multicast UDP traffic can be implemented.

Integriti controllers can communicate directly with one another to perform three different functions. These functions are peer reporting, foreign entities and user locations. Integriti controllers use multicast for peer to peer communications.

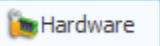
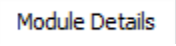
Integriti Professional software is required to configure peer to peer features and maintain controller time.

A Controller Hardware Smart Card Options license is required for each controller configured for peer to peer communications when using the Foreign Entities or User Locations features.

Each controller needs to be given a unique 'Peer-to-Peer ID'. This ID is required when configuring communications tasks. You will need to know the Peer-to-Peer ID of each controller when configuring communications tasks.

Controllers need to be on the same Ethernet LAN to use this feature.

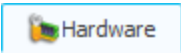
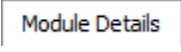
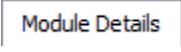
To allocate an ID to a controller...

1. Click on the  Hardware tab followed by  Control Module.
2. Double-click on a controller record.
3. The Editor Window for the controller should appear.
4. Under  Module Details, expand-out Peer-to-Peer.
5. Enter a unique number in to the 'Peer-to-Peer ID' field.
6. Close the editor window for the controller.
7. Repeat steps 1 – 7 for the remaining controllers that will be configured for peer to peer communications.

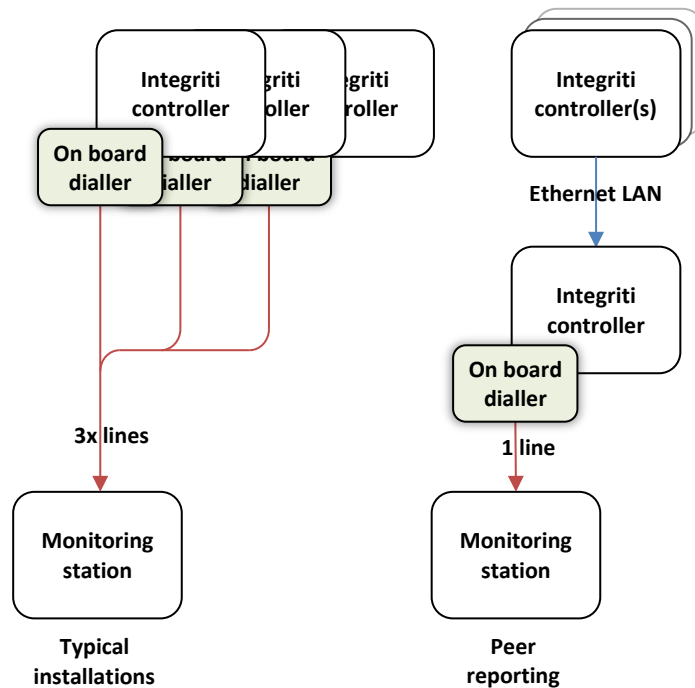
When used for peer to peer communications, Integrity controllers will require the following changes.

Configuring a controller for Peer to Peer...



1. Click on the  Hardware tab followed by .
2. Click on the  Module Details tab.
3. Expand out Peer-to-Peer.
4. Specify an encryption key. The encryption key is a total of 32 hexadecimal characters. The encryption key used must be identical on all controllers.
5. Tick the Receive Alarms option if the controller you are configuring will be used to receive review events.
6. Tick the Receive State option if the controller you are configuring is going to be used to monitor the state of an entity on another controller.
7. Tick the Send State option if the states of one or more entities on the controller you are configuring are to be monitored by one or more controllers.
8. Tick the Locations option if the controller you are configuring the system for global anti-passback.
9. Save and close the editor window for the Controller.
10. Repeat the above steps for the remaining controllers.

Peer Reporting



Peer reporting allows sending of alarms (and other reporting events) via other Integriti controllers. Integriti controllers can be configured to use the communication path(s) of another controller for reporting.

This feature can save on phone lines if required or can be used as a backup for other communications tasks.

Many controllers can be configured to communicate through the one controller.

When configuring alarm reporting, there is no restriction on the use of client codes. The controller can use its client code or an area client code, if present.

Client codes have 3 sources, which are prioritized in the following order:

1. Area client code in originating controller.
2. Communications task client code in the originating controller.
3. Communications task client code in the relaying controller.



Controllers sending reporting events will only send the abbreviated text ID's of the associated entities via SIA (text mode), IRFast (text mode) or SMS.

e.g. 'R01:Z06' instead of 'Cafeteria Door'

Peer reporting uses an extra communications task in the originating controller. The 'Peer Reporting' communications task can be used as a normal or backup communications task.

Review filtering on the 'Peer Reporting' communications task can be used to filter what events will be sent to the relaying controller.

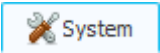
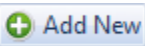


An incorrectly configured review filter could potentially block the wrong review events from being transmitted through to a monitoring station. A complete test should be carried out after the review filter has been created.

Peer reporting can be used as multiple communications tasks delivering to multiple controllers with reporting facilities (e.g. diallers).

Configuring Peer Reporting (Controller sending reports)...



1. Click on the  System tab followed by .
2. Click  Add New. The Editor Window for a new Communication Task should appear.
3. Give the Communications Task a name.
4. On the right-hand side under Comms Task Setup under Type, select Peer Reporting.
5. Expand-out Peer Reporting Programming.
 - a. Optionally enter a Client Code. If this field is left blank, the area client code is used instead.
 - b. Change the Destination Controller ID to the ID of the controller that will be receiving the report events.
 - c. Ticking the General Open/Close option will send
6. Save and close the editor window for the Communications Task.

Monitoring peer to peer connectivity

Peer to peer messages are sent between controllers using UDP multicast packets. Controllers configured to receive peer messages cannot determine if communications have failed. Therefore it is recommended that each controller configured for peer reporting should also be configured for test reports.

Test reports can be used to determine if peer reporting is operational.

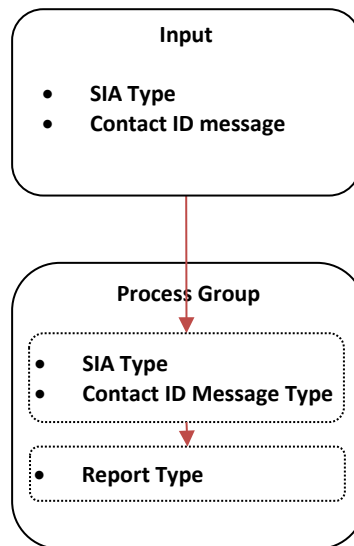
Configuring peer reporting for redundancy

In addition to test reports, the Peer Reporting communications task on the originating controller can have a Backup Task.

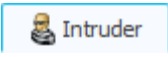
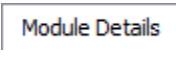
Report Type

If Peer reporting is enabled on a controller a Report Type should be defined in the Process Groups used.

Report ID hierarchy



If an input has a SIA Type or Contact ID Message, this will override settings in the Process Group for that input. If the Process Group has a SIA Type or Contact ID Message Type, this will override the Report Type.

1. Click on the  Intruder tab followed by .
2. Double-click on a controller record.
3. The Editor Window for the controller should appear.
4. Under , expand-out Peer-to-Peer.

Report Type	CID mapping	ID	SIA name	ID
Burglary	General Alarm Zone	140	General Alarm Zone	UAUR
Emergency	Burglary Zone	130	Burglary Zone	BABR
Fire	Fire Zone	110	Fire Zone	FAFR
Freezer	Duress User	121	Duress User	HAHR
Gas	Medical Zone	100	Medical Zone	MAMR
General	Panic Zone	120	Panic Zone	PAPR
Heat	Personal Emergency Zone	101	Personal Emergency Zone	QAQR
Holdup	Gas Detected Zone	151	Gas Detected Zone	GAGR
Medical	Heat Zone	114	Heat Zone	KAKR
Panic	Water Flow Zone	113	Water Flow Zone	SASR
Sprinkler	Expansion Module Tamper Zone	145	Expansion Module Tamper Zone	TATR
Tamper	Water Leakage Zone	154	Water Leakage Zone	WAWR
Water	Refrigeration Zone	152	Refrigeration Zone	ZAZR

Foreign Entities

The use of Foreign Entities allows a controller to see the state of entities on another controller. The state of a foreign entity can be used to control the state of a normal (local) entity. Whenever a controller sees that a foreign entity hosted within it (e.g. one of its zones, areas or doors) changes state, that controller broadcasts that change of state to all other controllers. Controllers that participate must be on the same subnet, although this may be on a VPN.

Configuring Foreign Entities...

- Foreign entities are automatically created by Integriti System Designer.
- States of foreign entities have a limited number of uses:
 - Combining into compound entries
 - Qualifiers
 - i. Area re-arm qualifiers
 - ii. BMS qualifiers
 - iii. Generic qualifiers (interlocks, user access, permission groups)
 - iv. Qualifiers for actions
 - v. Qualifiers for LCD messages
 - BMS mapped entities
 - Trigger entities for named actions
 - Sense entities for named actions
 - Ability to set a general variable to the state of the foreign entity
 - Aircon sense entities
 - Prisma idle display entity
 - Use in macros
- Click on the  Automation tab followed by  Foreign Entities to view the automatically configured foreign entities.

Foreign Entities should only be used with entities that have meaningful states. Foreign Entity states are reported as Boolean only (you can only tell if an entity is true or false). Refer to the following table to determine the state that will be reported.

Entity	True	False
None	Always True	
Compound entity¹	Evaluates to True	Evaluates to False
Holiday	Valid	Invalid
Comms Task	Running	Not Running
Compare	Value between thresholds	Value outside thresholds
Procedure	Macro is running	Macro is not running
Constant	Non zero	Equal to Zero
Aircon	State is on	State is off
Alog	Analog Value is non-zero	Analog value is zero
Area	Armed	Disarmed
Area List¹	All areas armed	One or more areas disarmed
Aux	On	Off
Aux List¹	All auxiliaries are on	One or more auxiliaries are off
Count	Count is non-zero	Count is zero
Door	Locked, tongue and reed sealed	Unlocked or tongue or reed unsealed
Door List¹	All doors TRUE	One or more doors FALSE
General Variable	Value >= Test value	Value < Test value
Gtimer	Expiry time has elapsed	Expiry time has not yet elapsed
Input	Sealed	Not sealed
Interlock¹	Interlocked	Not interlocked
Lift	Button timer running	Button timer not running
Module	Present on LAN	Not present on LAN

¹ This entity can be inverted by setting the reverse flag.

Entity	True	False
Paction	Sense entity 1 TRUE	Sense entity 1 FALSE
Schedule	Valid	Not valid
Siren	Sounding	Not sounding
Time Period	Valid	Not valid
Timer	Timer is running	Timer is not running
User	User exists in controller	User does not exist in controller

- Missing Entities (e.g. Process Group, Reader, Floor, Card Format, etc) are always false. Notable amongst these are Floor and Floor list.
- System Designer will set foreign entities up automatically if you program something using an entity from another controller.
- Using foreign Entities does not allow you to control the state of an entity on another controller (arm and area, lock a door, etc).
 - This can be achieved via a named action on the target controller that is triggered by a foreign entity. E.g. Controller 2 has a named action that unlocks a door based on the state of a zone input on Controller 1.
- Foreign Entities are state (not edge) based and so can miss quick transitions.
- For certain limited functions, the value of a foreign entity is used instead of its state. These functions are limited to:
 - Expression evaluation in a macro
 - Setting a general variable to the value of the foreign entity via an action
 - Comparisons
 - Temperature sense for Aircon.

Only the following foreign entities also have a value:

Foreign Entity	Value
Input	Input state bit map
Count	Input count
Alog	Input calibrated analog value
Aux	Analog Auxiliary calibrated value
General Variable	Current value of Gvar
Gtimer	Elapsed time so far (100ms ticks)
Constant	Value of Constant

User Locations

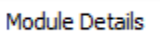
User Locations allows global anti-passback across multiple controllers.

When enabled, each controller holds the location of all users. Every time a user changes locations, the controller at which the user has badged broadcasts the user's new location.

User Locations has not been designed to work with AURM. If User Locations has been enabled, AURM must be disabled to ensure the Integrity controllers will continue to function correctly.

When using User Location, location based access control is required instead of area based.

To enable User Locations...

5. Click on the  **Hardware** tab followed by  **Control Module**.
6. Double-click on a controller record.
7. The Editor Window for the controller should appear.
8. Under  **Module Details**, expand-out Peer-to-Peer.
9. Select the Locations option.
10. Close the editor window for the controller.

Troubleshooting

If peer to peer is not functioning it may be due to a number of factors.

- Controllers configured for peer to peer communications that do not have a license will have the following review message:
Peer 2 Peer: Error: Not licensed
- Controllers should be on the same Ethernet LAN as one another.
- Integrity controllers that were upgraded to make use of this feature may not have the correct default programming. After a controller has been upgraded, check the following fields and ensure the defaults are correct.

These fields are found in the Controller editor under Module Details, Peer-to-Peer.

Field	Default value
Multicast IP Address	239.255.43.97
Port	69
Time Window (secs)	60

- Controllers with an incorrect encryption key will log the following message to review.

Peer 2 Peer: Error: Received invalid CRC

- If the time settings on controllers are not in sync, the following message will be logged to review.

Peer 2 Peer: Error: Time shifted

1. Check the Time/Date settings between the two controllers and ensure the Time Window (secs) option is set to a reasonable value (default is 60).
2. Controllers using peer to peer should be connected to Integrity Professional software.

- If a controller has sent a peer reporting alarm message to another controller and no acknowledgement has been received, the following message will be logged to review.

Comms Task xx (Peer Reporting) Alarm transmission failed

The Integrity controller will try three times before logging a failure to review.

Comms Task xx (Peer Reporting) Alarm transmission timeout

1. Check the configuration of the receiving controller. Ensure both controllers have the same multicast address and port.
 2. Check network connectivity between the two controllers.
- Each controller must have its own unique non-zero Peer-to-Peer ID.
The Integrity system designer software attempts to program an available Peer-to-Peer ID to an Integrity controller on enrolment.
There are a few cases where this ID may not be allocated correctly (due to importing or restoring panels, software downgrades etc.).
If the IDs are not all unique and non-zero, the operator will need to manually re-allocate Peer-to-Peer IDs to correct this situation.