Technical Information Paper

Controller Peer to Peer Direct Communications

Introduction

Many security systems have a requirement for functionality to be shared across two of more controllers. For example, an input is activated on one controller, causing an output to operate on a second controller. This is referred to as peer to peer communication.

How this is achieved?

When considering peer to peer communication, it is important to differentiate between peer to peer via a central server and direct peer to peer where controllers talk to each other with requiring a server to be on line.

Gallagher employs direct peer to peer communication via the Gallagher Controller network connection. Remote Controllers may be located anywhere in the system network (LAN, WAN or wireless). An input on a Controller in one city could activate a relay on a Controller in another city.

Gallagher Command Centre automatically manages this connection during site configuration. When an output is associated with an input and each are on different controllers, Command Centre automatically associated the two controllers transparently to the user. The result is a direct link between the two Controllers. The security server does not form part of the communication path. This means that even if the security server is off-line, providing there is a network connection between the two Controllers, the peer to peer function will continue to operate.

Systems requiring the server to manage the connection are more vulnerable in that:

- The server must always be on line
- Communication delays may result due to the additional equipment involved

What may be achieved?

Any Gallagher Command Centre item may be spanned across multiple controllers.

Some practical examples of where peer to peer provides efficient system operation are;

- A single intruder alarm siren at one location, which is triggered by alarmed detectors through a building or campus.
- Elevator control where large multi-story, multilevel elevator group requires more than one controller to manage the elevator groups. Peer to peer allows instant communication between the controllers
- A single alarm dialler for communicating alarms to a monitoring company can transmit alarms from any controller on the network. Separate diallers per controller are not required.
- A Remote Arming Terminal monitoring and controlling many alarm zones over many Controllers. The remote Arming terminal is connected to a single Controller.
- Anti-passback and anti-tailgating management where a cardholder is “flagged” as entering a zone. This is passed to other Controllers that need to know that the flag has been set, to restrict double entry into the one access area.
- Interlocking of functions such as carpark entry/exit control.

Examples or where peer to peer can be used but should not be relied on are areas where multiple parts (inputs, outputs, alarm zones etc) contribute to a single function and network latency could disrupt expected activity. Examples are:

- A door is configured with an access reader on one controller, inputs monitored on a second controller and the door control relay on a third controller.
- A less obvious example not recommended is an alarm zone spanning many controllers. A failure of the alarm zone controller could result in unexpected performance elsewhere in the system.
- Mantrap (sallyport) doors where it would be possible for two people (one at each door) could compromise the mantrap should network latency cause transmission delays.

Where Gallagher 6000HS Controllers are used, should the primary network path fail, the controller automatically shifts to the secondary network connection, maintaining the peer to peer communication automatically.

Data security

All peer to peer command messages are initiated using SSL encrypted data, authenticated sessions using RSA1024 bit keys and message encryption uses 256 bit AES encryption.

Peer to peer capacity

Each Gallagher Controller 6000 can support up to 60 concurrent peer to peer connections to other controllers on the system. If more than 60 are assigned to a single controller, then the connections are queued should the maximum of 60 be reached. When connections are completed, remaining connections are made.

Controller monitoring

A special form of peer to peer communication is a feature known as “off-line monitoring”. One controller may be configured to check that other controllers are on line. The time between checks is configurable, as may be required for each system.

GALLAGHER GROUP LIMITED

181 Kahikatea Drive, Hamilton 3206, New Zealand.
Private Bag 3026, Hamilton 3240, New Zealand.

TEL +64 7 838 9800
FAX +64 7 838 9801

EMAIL info@security.gallagher.co
www.security.gallagher.co

Disclaimer

Whilst every effort has been made to ensure accuracy, neither Gallagher Group Limited nor any employee of the company, shall be liable on any ground whatsoever to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the Gallagher policy of continuing development, design and specifications are subject to change without notice. Developed and manufactured by Gallagher Group Ltd, an ISO 9001.2008 Certified Supplier. Gallagher is a registered trademark of Gallagher Group Ltd. Gallagher Security Management Systems is a division of the Gallagher Group Ltd.

Copyright © Gallagher Group Ltd 2012. All rights reserved