



AN-180

Protege GX Cross Controller Operations

Application Note



The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2024. All rights reserved.

Last Published: 26-Apr-24 9:09 AM

Contents

Introduction	5
Software / Firmware Compatibility	5
Upgrading the Protege GX System	5
Networking Controllers	6
Establishing Links Between Controllers	8
Outputs	8
Inputs	9
Trouble Inputs	10
Keypads	11
Doors	12
Areas	13
Elevators	14
Services	15
Programmable Functions	16
Redundancy	17
Protege GX Records and Functions	18
Cross Controller Programming	20
Time Synchronization	20
Reporting Service and Reporting ID	20
Cross Controller Door Programming	20
Local / Global Door Programming	20
Door Inputs	21
Door Trouble Inputs	21
Global Antipassback	21
High Level Elevator Integration	21
Changes to the User Interface with Version 4	21
Keypad Display Options	21
Keypad Display Name	22
Changes to Groups	22
Record Groups	22
Menu Groups	22
User Area Groups	22
Central Station Reports	22
Treat User PIN Plus 1 as Duress	23

Introduction

Cross controller operations enable a set of controllers to operate as one system, in which all physically connected items on one controller are accessible and usable by various functions and records within Protege GX.

In Protege GX, sites generally contain multiple controllers that run independently of each other. Cross controller operations enable Protege GX controllers to operate as one system and share hardware resources. As an example, you can assign inputs from two different controllers to a single area and apply an output group to sirens connected to separate controllers.

Cross controller operations happen entirely behind the scenes. Controller communications are automatically established when assigning items from different controllers to the same record within Protege GX. The automated process reduces configuration and administration time.





Protege GX supports the linking of up to 64 controllers. If linking beyond this occurs, Protege GX generates a health status message stating which controllers are unable to communicate due to this limitation.

Software / Firmware Compatibility

In order to use these features, the following software and firmware versions are required.

Component	Software/Firmware Version	Notes
Protege GX software	4.0.128 or higher	
PRT-CTRL-DIN	2.08.583 or higher	All controllers must have the specified firmware version.
PRT-CTRL-DIN-ID		
PRT-GX-PCB	2.08.583 or higher	All controllers must have the specified firmware version.

If you are running an earlier version of the firmware, or if you are using an older PCB Controller (PRT-CTRL-GX), these features are not available. If you are running firmware version 2.08.583 or later with an earlier version of the software, it will result in unexpected operation.

	Firmware 2.08.499 and below	Firmware 2.08.583 and above
Below software version 4.0.128	 Cross controller operations and new features not available	 Software/Firmware versions incompatible. Controller will not accept programming downloads
Software version 4.0.128 and above	 Controller download will not be allowed if any cross controller links are made in programming. All new features will be ignored.	 Feature available

Upgrading the Protege GX System

For instructions on upgrading the Protege GX system, see the release notes for the latest version.

Networking Controllers

By default, each controller will attempt to communicate with another controller using the **IP Address** that is set in the software (**Sites | Controllers | General**). However, this is the address used by the Protege GX server to communicate with that controller, which may not be the same as the address that should be used by other controllers. For example, the controllers may be on a local network that is separate from the Protege GX server.

If a controller needs to use a different IP address to communicate with a second controller, add the following command in **Sites | Controllers | General**:

LocalIP = *,#

- Replace ***** with the serial number of the other controller
- Replace **#** with the internal IP address of the other controller

Do not type a space after the comma, as this will prevent the command from functioning.

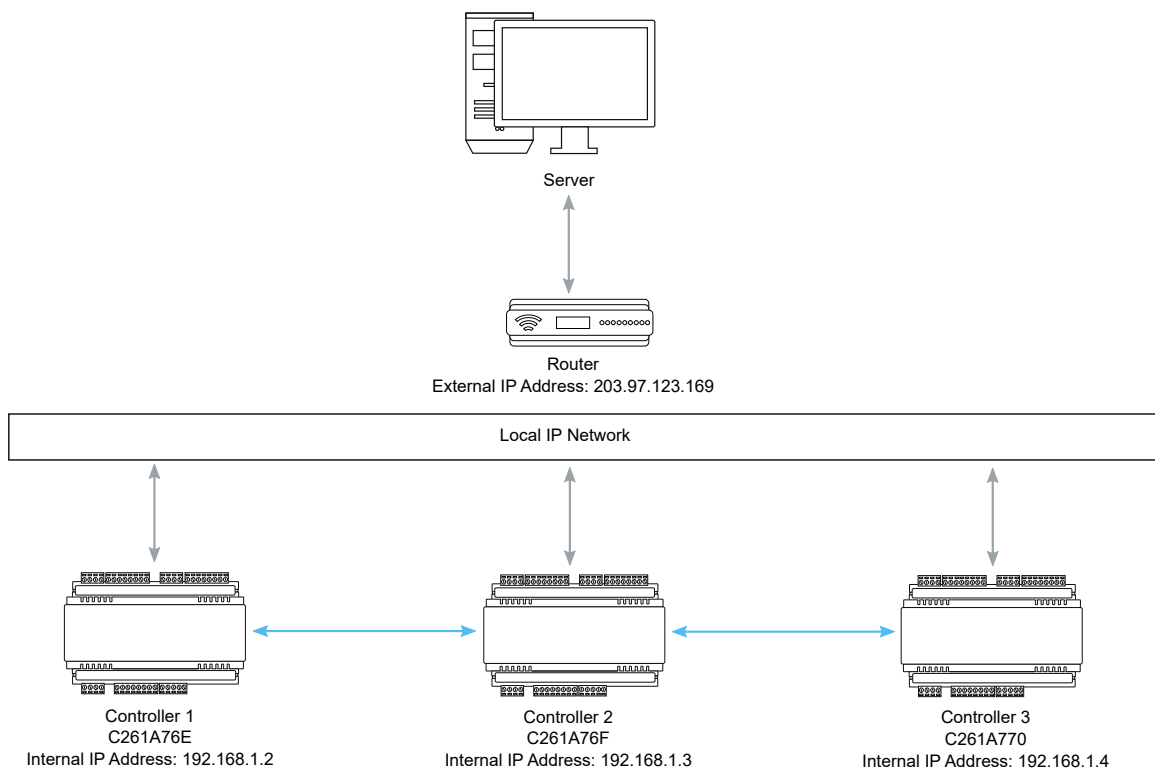
Enter one instance of this command for each other controller that this controller needs to communicate with, and repeat for all other controllers on the same local subnet. This ensures that each controller knows the local IP address of every other controller.

The default port for cross controller communications is **9470**. You can configure the port by adding the following command to every controller in **Sites | Controllers | General**:

ICCPort = *

Replace ***** with the port to use for communication.

Programming Example



In the scenario shown above, the Protege GX server is communicating with all three remote controllers via the router. Therefore, to the server all controllers have the same external IP address: 203.97.123.169.

However, the controllers on the local network cannot use this external IP address to communicate with each other. Therefore, you must program the unique local IP address for each other controller.

In the **Commands** field in **Sites | Controllers | General**, add the following commands to establish cross controller communications:

- **Controller 1:**
LocalIP = C261A76F,192.168.1.3
LocalIP = C261A770,192.168.1.4
- **Controller 2:**
LocalIP = C261A76E, 192.168.1.2
LocalIP = C261A770,192.168.1.4
- **Controller 3:**
LocalIP = C261A76E, 192.168.1.2
LocalIP = C261A76F,192.168.1.3

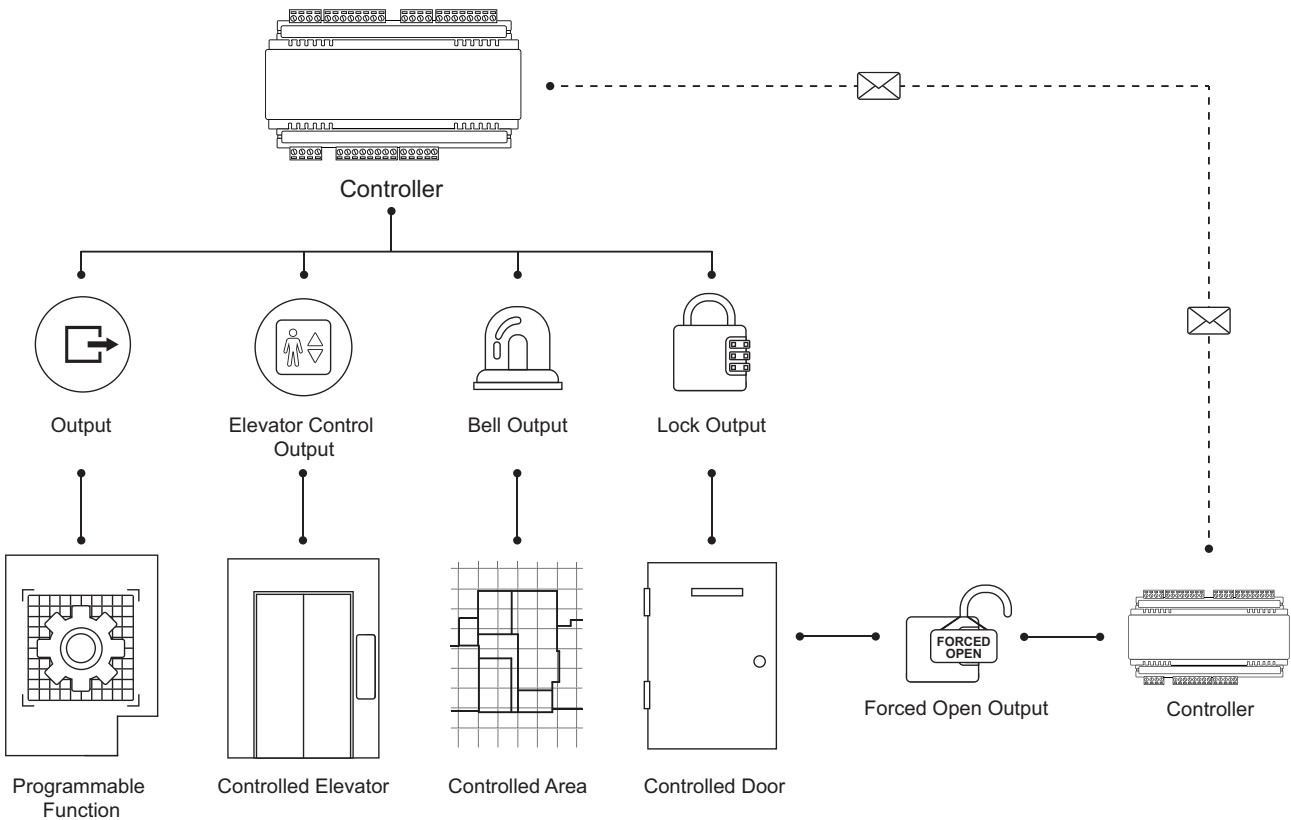
Establishing Links Between Controllers

The following section provides examples of how links are made within the Protege GX system and how different records function.

Outputs

Although outputs are connected to one specific controller, you can assign them to any function that can activate/deactivate an output.

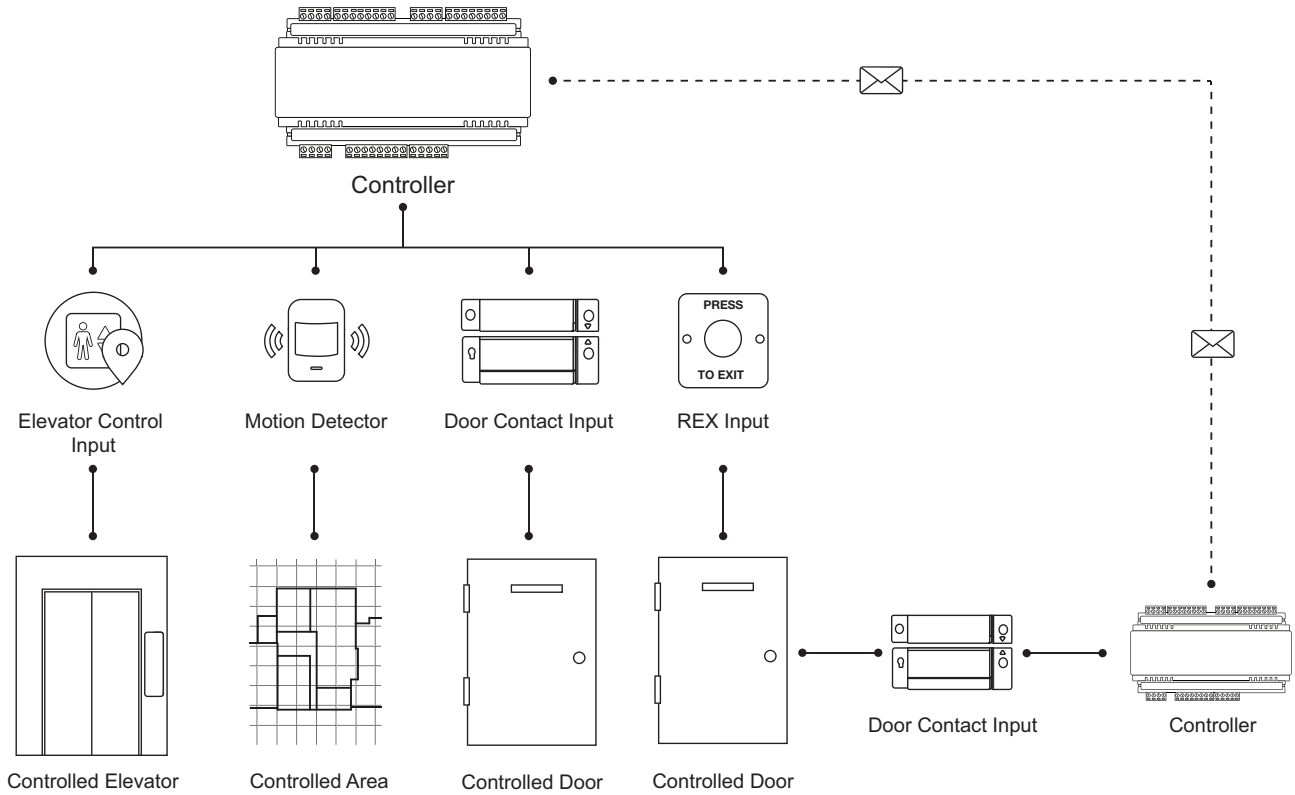
The following diagram shows some outputs assigned to one controller being used for various functions within Protege GX. It also shows another output from a different controller being used for the forced open function of a door. This creates a link between the two controllers.



Inputs

Although inputs are connected to one controller, you can assign them to any function that reacts to an input's state change.

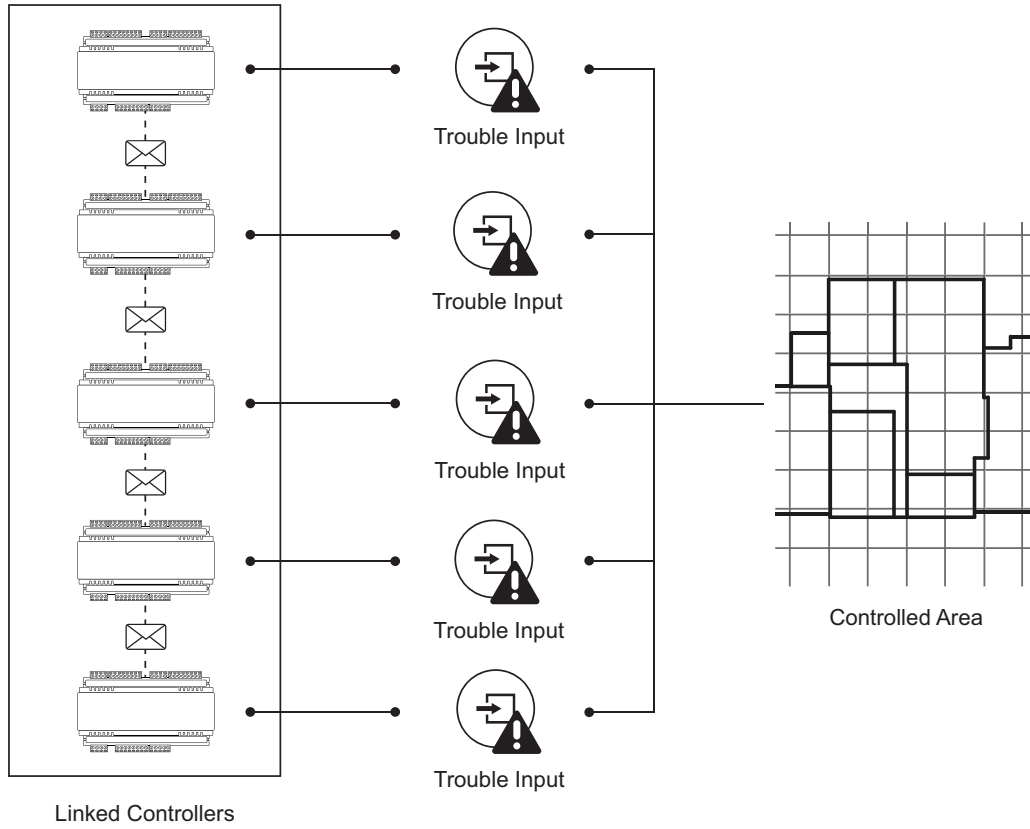
The following diagram shows some inputs assigned to one controller being used for various functions within Protege GX. It also shows another input from a different controller used for the door contact function of a door. This creates a link between the two controllers.



Trouble Inputs

Trouble inputs are linked to one specific controller, however you can assign them to any area.

The following diagram shows trouble inputs from multiple controllers assigned to one area. This creates a link between the controllers.



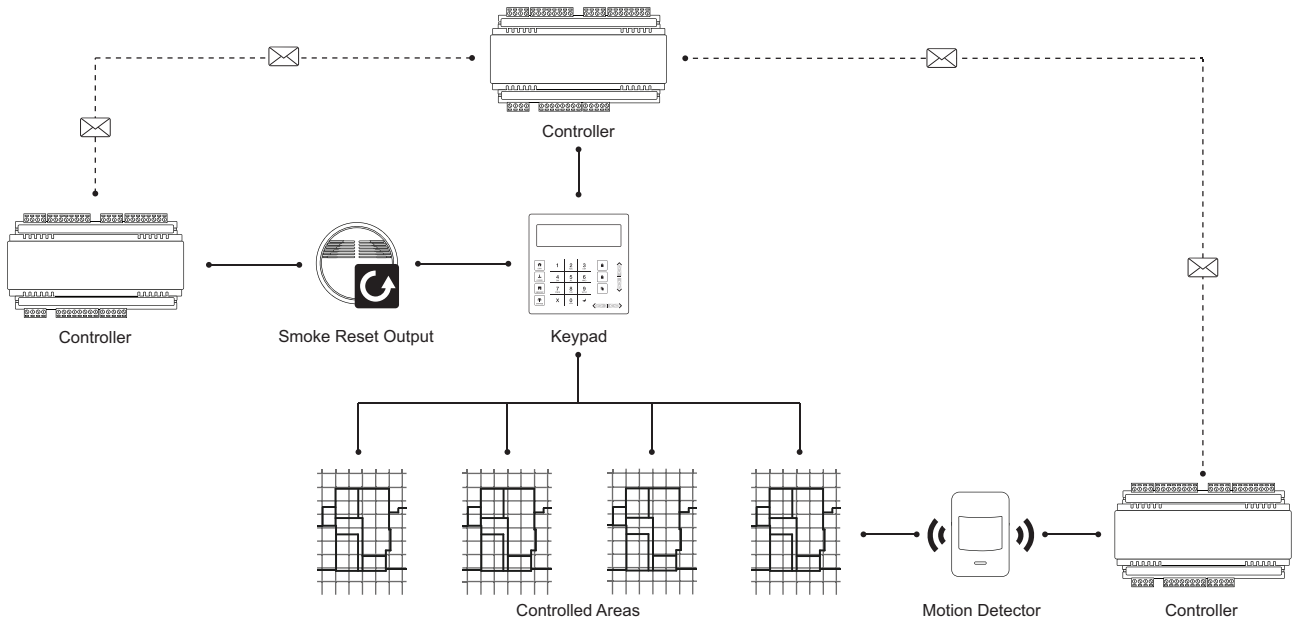
Keypads

Although keypads are connected to a specific controller, you can use them to view or control any area, bypass inputs, unlock doors, or view system information.

If you are using a keypad to control areas connected to different controllers (that are not linked by hardware items), you can assign an area group to the keypad to create links between controllers.

The following diagram shows:

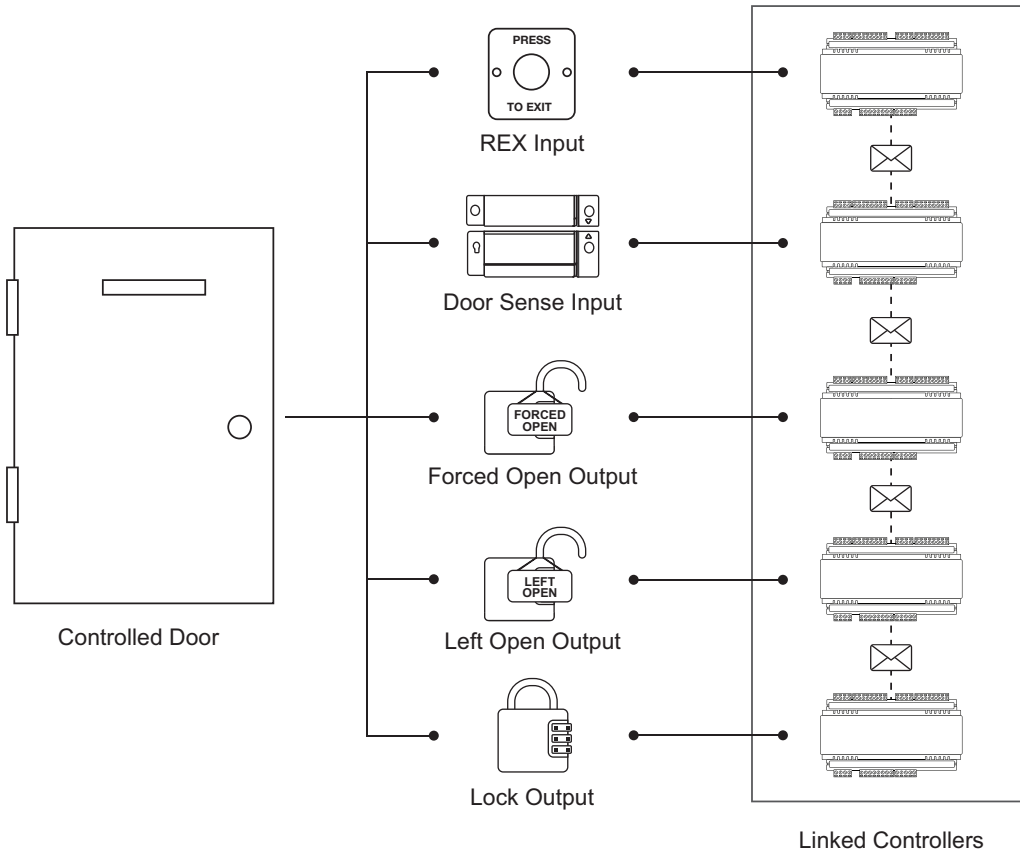
- A keypad connected to one controller and assigned four areas
- An output from a different controller used for the smoke reset output of the keypad
- An input from another controller used for the motion detector in one of the areas



Doors

You can assign inputs and outputs to a door from any controller on site. When you use multiple controllers to manage different functions of a door, the controllers communicate with each other to function as one unit.

The following diagram shows a door's REX input, door sense input, forced open output, left open output, and its lock output, assigned from five separate controllers. This configuration groups these five controllers together with each one performing a different function.

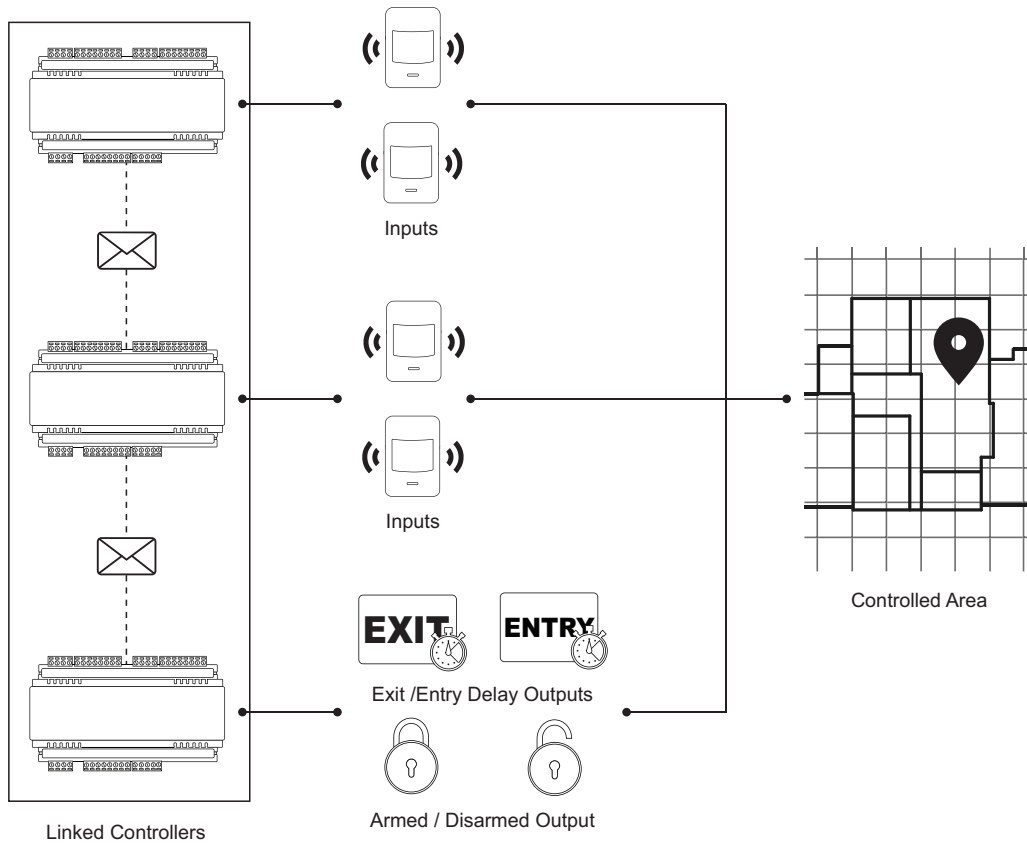


For information on how this operates when one of the controllers is offline, refer to the Redundancy section (see page 17).

Areas

You can assign inputs and outputs to an area from any controller on site. Multiple controllers managing and monitoring different components of an area communicate seamlessly and function as one unit.

The following diagram shows four inputs linked to two different controllers, as well as the exit delay output, entry delay output, armed output, and disarmed output, linked to a third controller. This configuration automatically links the three controllers together and enables each controller to carry out a specific function.

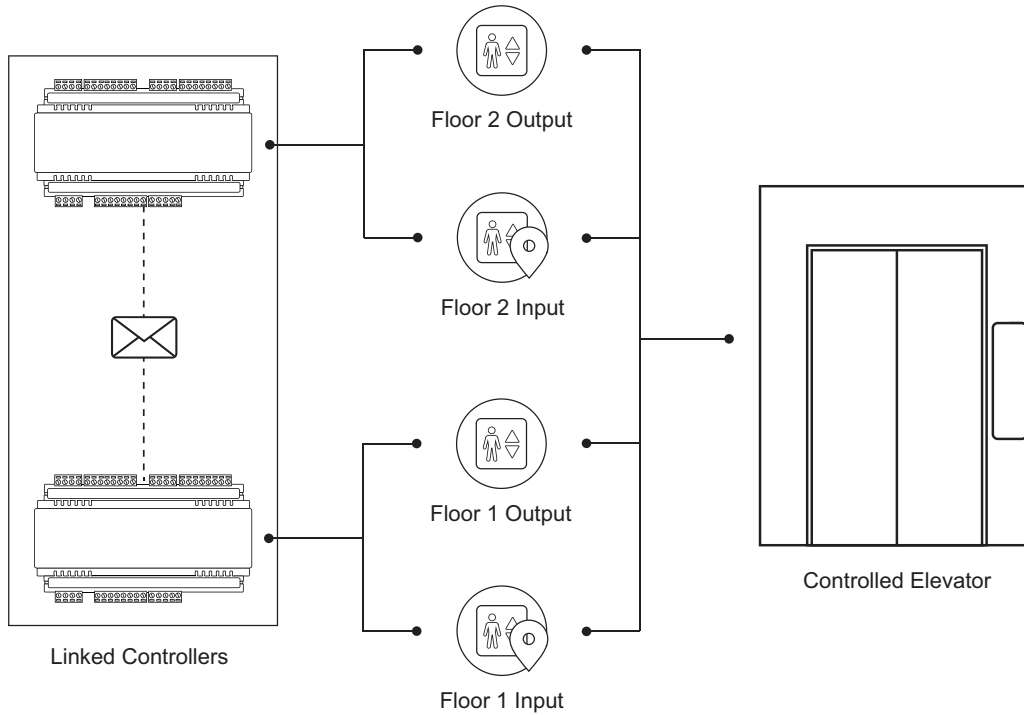


For information on how this operates when one of the controllers is offline, refer to the Redundancy section (see page 17).

Elevators

Elevators use outputs to establish and break contact between the elevator car panel and the lift controller. For low level integrations, outputs are needed for each elevator car button used to select a floor. Destination reporting also uses inputs to monitor which floor buttons a user selects.

The following diagram shows the elevator's inputs and outputs linked to two different controllers. This configuration automatically links the controllers together.

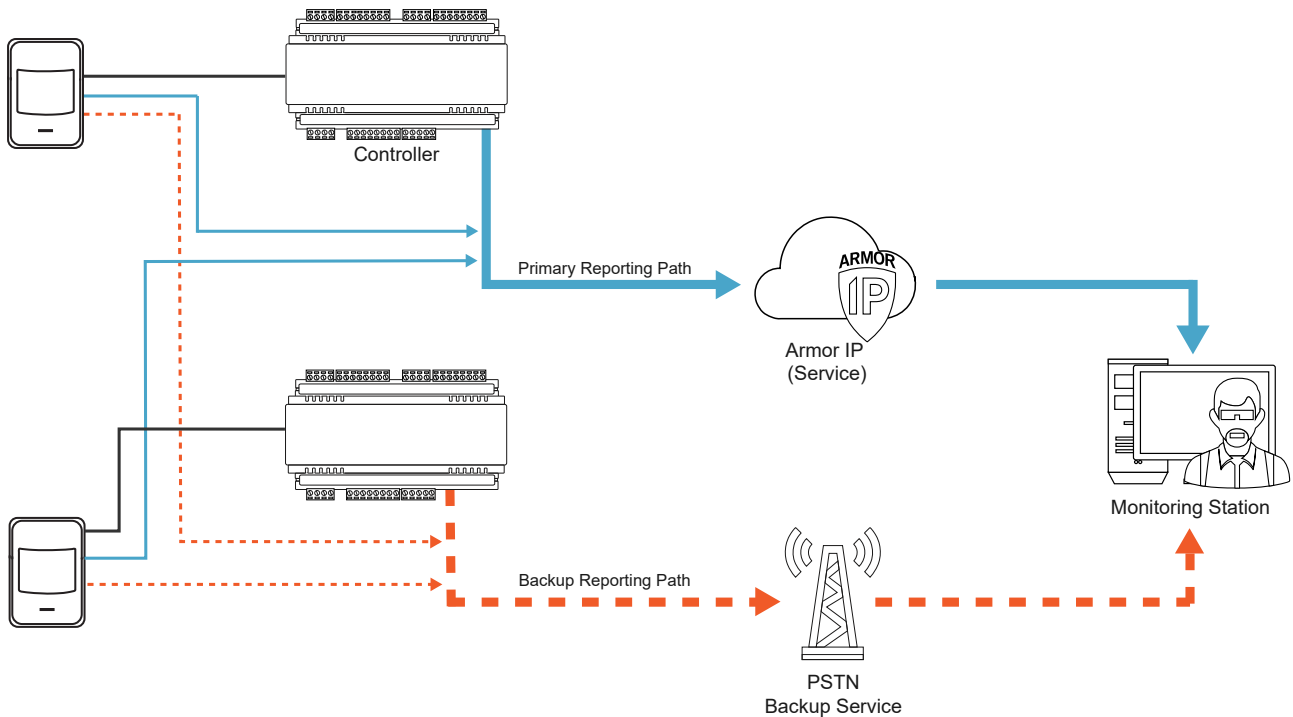


For information on how this operates in the event of one of the controllers dropping offline, refer to the Redundancy section (see page 17).

Services

Services (including the reporting services) operate exclusively on their assigned controller. However, reporting services are still able to report events from multiple controllers.

Reporting services are able to back up to another service running on another controller. For example, ReportIP can back up to a controller running ContactID (connected to a PSTN).

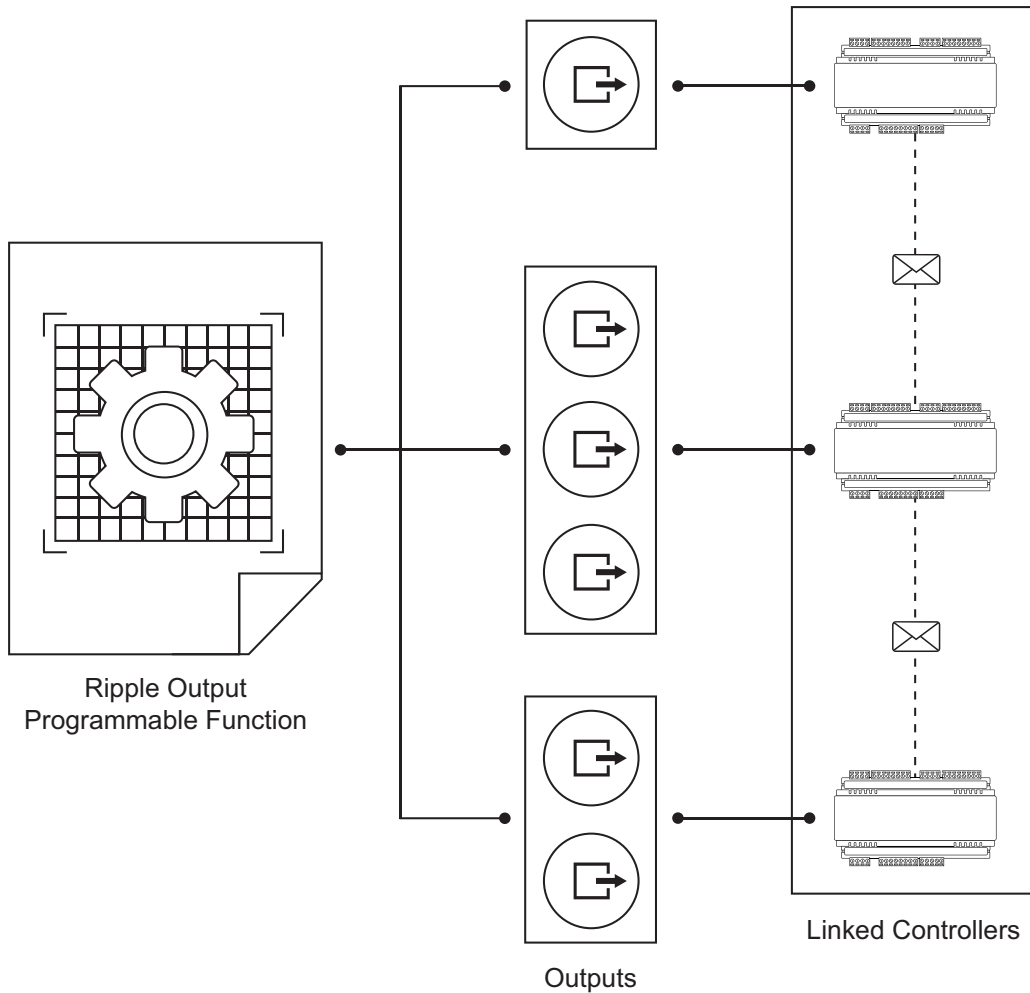


For more information, see [Reporting Service and Reporting ID](#) (page 20).

Programmable Functions

Programmable functions are not linked to a specific controller, enabling you to use a mixture of inputs, outputs and data values from within the site.

The following diagram shows a ripple output function controlling six outputs spread across three controllers.



For information on how this operates when one of the controllers is offline, refer to the Redundancy section (see next page).

Redundancy

Although cross controller operations enable controllers to share hardware resources across a site, some types of records must have a host controller associated with them.

To facilitate this, the Protege GX software makes intelligent decisions to determine which controller is hosting the record. This decision is based on the physical devices linked to the record. This means that the controller with the most inputs, trouble inputs and outputs associated with a particular record takes primary control of the record.

The primary controller associated with a record is displayed in the second column of the record list by default. This field cannot be edited manually, but is useful for on-site troubleshooting as it indicates which global records an offline controller may impact.

In terms of redundancy this means that:

- When a controller physically connected to a card reader and a door lock loses communication with its linked controllers, it can still respond to card reads and unlock the door. During the downtime, the controller stores events locally until it comes back online and can send events to the server database.
- If an area's host controller is online, but the other linked controllers are offline, the area is still able to arm by bypassing any inputs located on the offline controllers.
- If a controller needs to activate a group of outputs, some of which are inaccessible, the controller will still activate as many outputs in the group as it can.

Protege GX Records and Functions

The table below outlines how various records and functions within Protege GX interact with cross controller programming, with a brief description of each record's capabilities. Some differences between version 4.0.128 and earlier versions have been noted.

Record	Description
Schedules	Schedules are not specific to any hardware and can be freely used in any record programming.
Holiday Groups	Holiday groups are not specific to any hardware and can be freely used in any schedule.
Users	Users are not linked to a specific controller. Protege GX determines which controllers need to know about which users based on their access levels.
Access Levels	Access levels are not linked to a specific controller. They can contain records and groups from any controller in the site as needed by a specific user.
Doors	Doors are global but are processed by a host controller. Doors are downloaded to the controllers that are linked to them via the inputs and outputs assigned to the doors. Inputs and outputs can be from any controller in the site. For more information, see Doors (page 12).
Inputs	Inputs are linked to one specific controller. However, they can be assigned to any function within a site that can utilize them. For more information, see Inputs (page 9).
Outputs	Outputs are linked to one specific controller. However, you can assign them to any function within a site that can activate/deactivate an output. For more information, see Outputs (page 8).
Trouble Inputs	Trouble inputs are linked to one specific controller. However, you can assign them to any area within the site. For more information, see Trouble Inputs (page 10). All door related trouble inputs have been removed from the Reader Expander programming and are now assigned directly to the door. For more information, see Door Trouble Inputs (page 21).
Door Types	Door types are not associated with a specific controller. A door type is added to the site and can be used by any door.
Input Types	Input types are not associated with a specific controller. An input type is added to the site and can be used by any input.
Areas	Areas are global but are processed by a host controller. You can assign inputs and outputs to an area from any controller on site. Any doors can be linked to an area. For more information, see Areas (page 13).
Elevator Cars	Elevator cars are global but are processed by a host controller. You can assign inputs and outputs to an elevator car from any controller on site. For more information, see Elevators (page 14).
Floors	Floors are not programmed on a specific controller and can be assigned to any elevator car.
Daylight savings	Daylight savings records must be assigned to a specific controller.
Phone Numbers	Phone numbers are not specific to any hardware and can be freely used in any record programming.
Services	All services must have a controller specified when they are programmed. For more information, see Services (page 15).
Door Groups	Door groups apply to the entire site. The All Doors option no longer exists. For more information, see Changes to Groups (page 22).

Record	Description
Area Groups	Area groups apply to the entire site. The All Areas option no longer exists. For more information, see Changes to Groups (page 22).
Keypad Groups	Keypad groups apply to the entire site.
Menu Groups	Menu groups apply to the entire site.
Output Groups	Output groups apply to the entire site.
Elevator Groups	Elevator groups apply to the entire site. The All Elevators option no longer exists. For more information, see Changes to Groups (page 22).
Floor Groups	Floor groups apply to the entire site. The All Floors option no longer exists. For more information, see Changes to Groups (page 22).
Keypads	Keypads must be associated with a specific controller. A keypad can be configured to control any area, bypass inputs, unlock doors, etc. anywhere in the site. For more information, see Keypads (page 11).
Analog Expanders Input Expanders Output Expanders Reader Expanders	Expanders are physical hardware and must be associated with a specific controller. The inputs, outputs and data values on an expander can be used in any record in the site.
Smart Readers	Smart readers are physically connected to a controller and only communicate with that controller. The door and function outputs can be assigned from any controller.
Automation	Automations are associated with a C-Bus service which is hosted on a specified controller. However, the automation can be linked to any input or output within the site.
Programmable Functions	Programmable functions are not specific to a controller. For more information, see Programmable Functions (page 16).
Data Values	Data values are not specific to a controller. They may take their input from any analog expander and be used by any programmable function.

No Protege GX server based operations and records are affected by these changes. This includes integrations with Salto, Cencon and Suprema, as they communicate directly with the Protege GX software services.

Cross Controller Programming

This section contains some important notes on programming a system using cross controller operations. It also provides further detail about the changes to the Protege GX user interface between versions 3 and 4 of the software.

Time Synchronization

In order for schedules to operate as expected when controllers are linked in a cross controller configuration, you must ensure that the clocks on the controllers are synchronized.

- The recommended method of time synchronization is to use SNTP (Simple Network Time Protocol). If you configure SNTP on one controller, you should also configure SNTP on all other linked controllers. If some controllers are located in different time zones, using SNTP enables each controller to have its time zone configured individually.

SNTP Settings are available under **Sites | Controllers | Time Update**.

- If you prefer to synchronize the time manually (if an SNTP server is not available from the network) and all relevant controllers are in the same time zone, then all controllers should have SNTP disabled. When the time is set on one controller, it is automatically updated and synchronized for all linked controllers.

The controller time can be set manually by right-clicking on the controller record, editing the time displayed, and clicking **Set Controller Date Time**.

- If a time server is not available but there are controllers in different time zones that need to communicate with each other, enable SNTP for all controllers and configure the time zones as required. Even though a time server is unreachable in this case, a manual time update is able to synchronize the time between the controllers using the configured time zones.

Reporting Service and Reporting ID

As it is not always clear which controllers are linked together, all areas, inputs and trouble inputs **must** have a **Reporting Service** assigned.

If the primary reporting service is configured with another service as a backup, you only need to specify the primary service for the input, trouble input or area.

In addition to this, all areas, inputs and trouble inputs must have a **Reporting ID** assigned. When an area, input or trouble input is assigned to a reporting service and does not have a Reporting ID assigned, the lowest available Reporting ID is automatically assigned. You can manually edit this as required.

Cross Controller Door Programming

Local / Global Door Programming

A **Programming Mode** option is available in the toolbar in **Programming | Doors**. This option allows you to select either **Local** or **Global** programming mode.

- Using **Local** mode limits the inputs, outputs and areas available to be assigned to the door to those connected to the same controller.
- **Global** mode makes all inputs, outputs and areas on the site available to be assigned to the door, with the controller's name appended to the record name.

Door Inputs

Cross controller operations allows you to assign any input within the system to a door for the REX, REN, door sense, bond sense and beam sense functions. Door inputs are defined from the **Inputs** tab of the **Programming | Doors** menu.

The original settings located in the **Expanders | Reader Expanders** menu are now ignored during normal operation. These options are only relevant for the offline operation of the reader expander. If a reader expander's inputs are used for these door functions, and the reader expander goes offline, you may notice unexpected behavior if the default inputs are not applied.

Door Trouble Inputs

The following trouble inputs are assigned directly to the door:

Input	Code	Description
1	423	Door forced open
2	426	Door left open
3	145	Smart reader tamper
4	302	Smart reader low battery
5	140	Smart reader RF failure
6	143	Smart reader comms failure
7	140	Reserved
8	140	Reserved

You can select the **Door (DR)** option from the **Module Type** drop-down (**Programming | Trouble Inputs | General**). When this option is selected, the module address field allows you to select the door that the trouble input is associated with.

If a controller is running older firmware, the door trouble inputs are mapped back to the reader expander trouble inputs during a download to the controller. This ensures that the trouble inputs are processed correctly if the controller has not gone through the firmware update process.

Global Antipassback

When several controllers are operating together, Antipassback will function globally across a site. This means that a user can enter an area through one door and still be allowed to access an exit door even if it is connected to a different controller.

The settings for resetting Antipassback on schedule or after a defined time are located in the **Programming | Doors | Advanced Options** menu.

High Level Elevator Integration

As doors are not associated with a specific controller, you are required to manually define a controller for doors used for elevator HLI integrations (under **Programming | Doors | General | Elevator HLI**).

Changes to the User Interface with Version 4

Keypad Display Options

The **Display** options for keypads have been moved from **Sites | Controllers | General** to **Expanders | Keypads | General**.

Keypad Display Name

Although it is useful to have long and descriptive record names in your programming, it is not practical when the name is also displayed on a 16 character keypad display. To accommodate both long names in the software and shorter names for keypad display, a new **Keypad Display Name** field has been introduced.

This field applies to the following records:

- Doors
- Inputs
- Areas
- Trouble inputs
- Automation

Changes to Groups

Due to the globalization of door, area, elevator and floor records, the **Include All** options have been removed from the door, area, floor and elevator groups menus. This option can now be selected within the access level.

Record Groups

Due to the globalization of certain records within Protege GX, record group filtering has been implemented for:

- Doors
- Areas
- Schedules
- Menu groups
- Door type
- Input types
- Phone numbers
- Floors
- Elevator cars

Menu Groups

A **Keypad Groups** section has been added to the menu groups page. This allows you to filter menu groups based on the keypad group assigned to them. This also prevents the downloading of multiple menu groups per access level for legacy firmware. If the keypad groups section is left blank the menu group is valid on all keypads.

User Area Groups

The user's area group option has moved from **Users | Users | General** to a new **Area Groups** tab.

Central Station Reports

The CID map options have been made obsolete for the ReportIP and the ContactID services. In their place, central station reports have been implemented. Central station reports provide a report map for the Contact ID and Report IP services that you can supply to the monitoring station. This report map can be generated from **Reports | Central Station Report**.

The map settings remain configurable from the **Services** menu for ReportIP and ContactID. This allows backwards compatibility for older firmware. These options are ignored by cross controller aware firmware versions.

Treat User PIN Plus 1 as Duress

The **Treat User PIN Plus 1 as Duress** option can now be configured on an individual user level from **Users | Users | Options**.

If you are using a PCB controller with version 4.0 software or higher, enabling this option for one user enables it globally for all users.

Version 3 Options

A **Version 3 Settings** section has been added to **Sites | Controllers | Configuration**. This section is read-only and refers to the options that previously applied globally to a controller. This is only relevant to PCB controllers.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2024. All rights reserved.

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.