AN-180

Protege GX Cross Controller Operations

Application Note

Last Published: 27-Nov-25 10:26 AM

Contents

Introduction

Normally in the Protege GX system each controller operates independently of other controllers, with its own network of expanders, inputs and outputs. Cross controller operations enable a group of controllers to communicate with each other, sharing hardware resources and tracking statuses across the system.

This allows you to:

- Assign inputs from two different controllers to a single area
- Create output groups that span multiple sections of the building
- Lock down all doors on site from a single panic button
- Use one reporting service for alarms from multiple controllers
- Maintain users' antipassback status across multiple controllers

Cross controller operations are managed through **cross controller groups**, which allow you to define which controllers need to communicate with each other. When two or more controllers are grouped together, they establish communications with each other and begin sharing resources.

Software / Firmware Compatibility

Component	Version	Notes
Protege GX software	4.0.128 or higher	If you are upgrading from Protege GX version 3 to version 4, contact ICT Technical Support for more information on the changes in version 4.
Protege GX Controller	2.08.583 or higher	All controllers must have the specified firmware version.
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), cross controller operations 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 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	Cross controller operations available

Programming Summary

The basic steps for enabling cross controller operations are as follows:

1. Plan which controllers need to communicate with each other (see page 6). Ensure that they are connected over the network.

2. Create cross controller groups. The process depends on what type of download server your site uses (see next page).
   - **Standard Download Server**: To create an implicit cross controller group, create programming links between at least two controllers. For example, assign an input from one controller to an area from another.

     To make the implicit controller groups more obvious, we recommend creating an output group that contains one group from each controller. Assign that output group to a dummy door.
   - **Enterprise Download Server**: Create explicit cross controller groups in **Sites | Cross controller groups** (see page 7).
3. In **Sites | Controllers**, synchronize the time between the controllers (see page 9). There are two options:
   - In the **Time update** tab for each controller, enable **Automatically synchronize with an internet time server** and program the same SNTP time server.
   - If there is no SNTP server available, disable **Automatically synchronize with an internet time server**. Right click on one controller and select **Set controller date time**.
4. If the controllers are on a different network from the server, you must tell them each other's local IP addresses (see page 10). In the **Commands** field, enter one instance for the following command for each other controller in the group:

   `LocalIP = *,#`
   - Replace ***** with the serial number of the other controller
   - Replace **#** with the internal IP address of the other controller

   Repeat for every controller in the group.

From then on as you program doors, areas and other types of records, you can use outputs and inputs from any controller within the same cross controller group. For more information, see Programming Records in Cross Controller Groups (page 14).

Cross Controller Groups

Cross controller groups are collections of controllers that can communicate with one another, allowing them to control and monitor inputs, outputs and other resources from any controller in the group.

Any controllers that are not in a cross controller group are standalone controllers, and can only use the inputs, outputs and other resources connected to that controller.

The programming rules for cross controller groups are:

- All controllers that use cross controller operations must be in a cross controller group.
- Controllers that do not use cross controller operations do not need to be in a cross controller group.
- Each controller can only be in one cross controller group.
- For best performance, we recommend a maximum of **48** controllers per cross controller group. There is a strict upper limit of 64 controllers per group.
- All controllers in the same group must be networked so they can communicate with each other. If the controllers cannot communicate, they will suffer performance issues.

In general, we recommend that cross controller groups should only be used when needed, as unnecessary cross controller operations can impact the performance of all controllers.

Protege GX will generate a health status message if more than 64 controllers are linked together.

Implicit and Explicit Cross Controller Groups

Protege GX forms cross controller groups in two different ways, depending on what type of download server your system uses.

Standard Protege GX Download Server—Implicit Cross Controller Groups

Most sites use the standard download server that is installed with the Protege GX software. Sites with standard download servers use **implicit cross controller groups** based on programming links.

For example, when you assign an input from one controller to a door on a different controller, you create a programming link between the two controllers. Protege GX will automatically create an implicit cross controller group containing all of the linked controllers.

While this is convenient, it can be difficult to understand which controllers are connected. The Protege GX user interface will not enforce the rules for cross controller groups (see above), so you are responsible for following these rules while programming the system.

We recommend planning out the cross controller groups before programming the whole system. A simple method is:

1. Create an output group containing one output from each controller.
2. Add a dummy door and assign the output group to it.

This forces the system to create the desired implicit cross controller group.

The single record download service is not affected by cross controller operations.

Enterprise Download Server—Explicit Cross Controller Groups

The enterprise download server is a separate application that is designed for enterprise-scale sites. If your site has the enterprise download server installed, you must set up **explicit cross controller groups** before you can program the site.

On enterprise download server sites, the user interface will only allow you to assign resources within the same cross controller group. For example, when you program a door, you can only select inputs, outputs and areas from controllers in the same group. This prevents you from selecting resources from controllers that cannot communicate with each other (e.g. controllers in different buildings). For more information, see Programming Records in Cross Controller Groups (page 14).

See Creating Explicit Cross Controller Groups for instructions for creating groups.

Guidelines for New Cross Controller Groups

When you are creating cross controller groups on new sites, consider the following guidelines:

- Controllers that do not need to share resources with other controllers should not be in a cross controller group (standalone controllers).
- Controllers that will share resources need to be in the same cross controller group. For example, some controllers in the same building may need to share control of doors, areas or reporting services.
- Controllers in completely separate locations (e.g. different cities) should not be in the same cross controller group, as they do not need to share resources.
- Cross controller groups should be as small as possible, as excessive cross controller operations can impact the performance of all controllers. We recommend keeping the group size below 48 controllers.

Creating Explicit Cross Controller Groups

In systems that use the enterprise download server, you can create explicit cross controller groups as follows:

1. Plan out the cross controller groups required for your system.
2. Navigate to **Sites | Cross controller groups**.
3. Add a new cross controller group with a descriptive name (e.g. Newmarket Apartments Common Areas).
4. Click **Add** and select the controllers that will be in this group.
5. Click **OK**.
6. Click **Save**. These controllers are now linked together.
7. Repeat to create additional groups as needed.

When you add a new controller through the controller wizard you can select a **Cross controller group** to add it to or choose not to add it to a cross controller group.

Adding Explicit Cross Controller Groups to Existing Sites

When you install the enterprise download server on an existing site, you **must** create explicit cross controller groups to allow you to continue cross controller operations and program the site as expected.

The Protege GX database can generate a report on the implicit cross controller groups created by programming links between controllers. This report is generated by a stored procedure which is available in Protege GX version 4.3.386 and higher.

This allows you to create matching explicit cross controller groups that can be used by the enterprise download server.

The stored procedure can take up to a minute to run and may block some database tables during the process. We recommend you run this report during a period of low activity (e.g. immediately after upgrading the software). Alternatively, create a backup and restore it to a test machine to run the stored procedure on.

To run the stored procedure:

1. Run SQL Server Management Studio on the machine with the Protege GX databases installed.
2. Connect to the ProtegeGX server instance.
3. Expand the **Databases** node. Right click on the ProtegeGX database and select **New Query**.
4. Enter the following query:

```
SET TRANSACTION ISOLATION LEVEL READ UNCOMMITTED
EXEC ControllerGroupingReport
```

5. Click **Execute**.

The stored procedure will generate a report showing the following:

- **Section 1**: Number of implicit cross controller groups created by the download service based on programming links.
- **Section 2**: Number of explicit cross controller groups created by the operator.
- **Section 3**: List of the controllers in each implicit cross controller group.
- **Section 4**: List of the controllers in each explicit cross controller group.
- **Section 5**: List of the programming links between controllers, showing why two controllers are in the same implicit group.

  Please note that some programming links may not be relevant. For example, input types may show spurious programming links based on an incorrect Host Controller assignment. You can disregard these irrelevant links.

If the report does not show any implicit cross controller groups, you do not need to program any cross controller groups.

If the report does show cross controller programming, you have two options:

- Program explicit cross controller groups that match the existing implicit cross controller groups. Any controllers without programming links should be left as standalone.
- Remove the programming links (if they were unintentional or not required).

  Protege GX will not correct any existing programming that is not consistent with the new cross controller groups.

After programming cross controller groups, you can run the stored procedure again to make sure that each implicit cross controller group has an equivalent explicit cross controller group.

Time Synchronization

You must ensure that all controllers in a cross controller group keep their clocks synchronized so that schedules operate as expected.

We recommend setting all controllers in the group to use the **same** SNTP time server, with the correct time zone and daylight savings settings. SNTP settings are available under **Sites | Controllers | Time update**.

There may be a preferred time server that is used on the local network—discuss with the site's IT team. Alternatively, use the NTP Pool Project to find online time servers in your region.

If some controllers in the group do not have a time server programmed, they will automatically synchronize their clocks to match the controllers that do have a time server.

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.

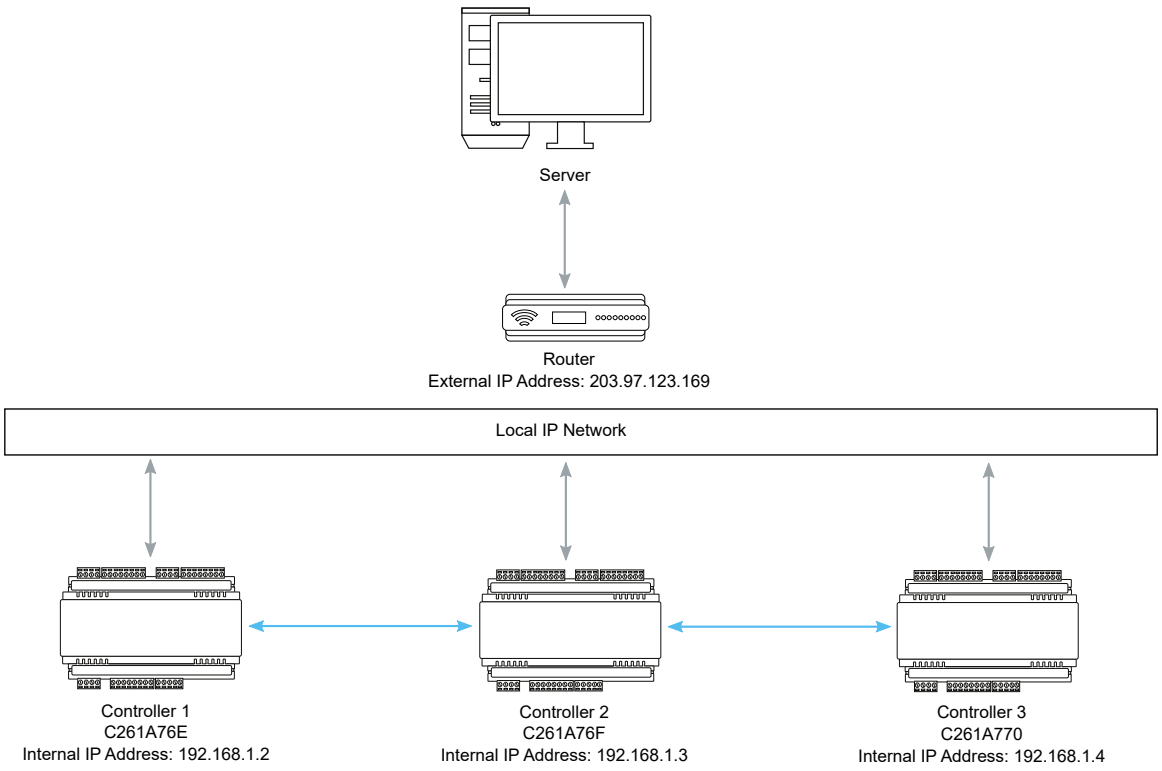
Enter one instance of this command for each other controller that this controller needs to communicate with, and repeat for all other controllers in the same cross controller group. This ensures that each controller knows the local IP address of every other controller in the group.

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
  ```

Protege GX Records and Functions

The table below outlines how various records and functions within Protege GX interact with cross controller programming.

Record	Description
Schedules	Most schedules are not specific to any controller and can be freely used in any record programming. If the schedule has a **Qualify output**, the schedule may only be assigned to records in the same cross controller group as the output. Use caution when assigning these schedules to records that are not normally associated with a specific controller, such as door types and input types.
Holiday Groups	Holiday groups are not specific to any hardware and can be freely used in any schedule.
Credential Types	All credential types are downloaded to all controllers.
Card Profiles	Card profiles are downloaded to all controllers with wireless locks enabled.
Function Codes	Function codes may be assigned to any door within the same cross controller group as the doors, outputs and areas that the function code controls.
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	Most access levels are not linked to a specific controller. They can contain records and groups from any controller in the site. If the access level has outputs or output groups assigned, all records assigned to it (e.g. doors, areas) must be from the same cross controller group.
Doors	Each door has a host controller that controls its operation. It can be assigned any inputs, outputs and areas in the same cross controller group. The exception is offline wireless locks, which do not have a host controller as they are not physically connected to the system. If a reader expander goes offline from its controller, it will revert to using its own inputs and outputs based on the settings in the **Expanders | Reader expanders | Reader 1/2 options** tab. Each user's antipassback status is maintained between all doors in the same cross controller group.
Inputs	Inputs are connected to one specific controller but can be assigned to any record within the cross controller group.
Outputs	Outputs are connected to one specific controller but can be assigned to any record within the cross controller group.
Trouble Inputs	Trouble inputs are linked to one specific controller but can be assigned to any record within the cross controller group.
Door Types	Most door types are not specific to any controller and can be used by any door on site. If the door type has a schedule with a **Qualify output** it can only be used for doors in the same cross controller group as the output.
Input Types	Most input types are not specific to any controller and can be used by any input on site. If the input type has a **Control output / output group** or a schedule with a **Qualify output** it can only be used for inputs in the same cross controller group as the output(s).

Record	Description
Areas	Each area has a host controller that controls its operation. It can be assigned any inputs and outputs from the same cross controller group. Each user's antipassback status is maintained between all areas in the same cross controller group.
Elevator Cars	Each elevator car has a host controller that controls its operation. It can be assigned any inputs, outputs and areas in the same cross controller group.
Floors	Floors are not programmed on a specific controller and can be assigned to any elevator car.
Daylight savings	Daylight savings records are assigned to one specific controller, or can be shared between all controllers.
Phone Numbers	Phone numbers are not specific to any controller and can be freely used in any service programming.
Services	Services are managed by one specific controller but can be assigned to areas within the same cross controller group. Only outputs from the same cross controller group may be assigned to the service.
Door Groups	Door groups can contain doors from any controller when used in access levels. When the door group will be used to control doors (e.g. in a programmable function), ensure that only doors from the same cross controller group are included.
Area Groups	Area groups can contain areas from any controller when used in access levels. When the area group will be used to control areas (e.g. in a programmable function or keypad), ensure that only areas from the same cross controller group are included.
Keypad Groups	Keypad groups can contain keypads from any controller.
Menu Groups	Menu groups apply to the entire site. You can restrict them to specific keypads using the **Keypad groups** setting.
Output Groups	Output groups must contain only outputs from the same cross controller group.
Elevator Groups	Elevator groups can contain elevator cars from any controller when used in access levels. When the elevator group will be used to control elevator cars (e.g. in a programmable function), ensure that only elevator cars from the same cross controller group are included.
Floor Groups	Floor groups can contain any floors.
Keypads	Keypads are physically connected to a specific controller. A keypad can be used to view and control resources from other controllers in the same cross controller group.
Analog Expanders Input Expanders Output Expanders Reader Expanders	Expanders are physically connected to a specific controller. The inputs, outputs and data values on an expander can be used in any record in the same cross controller group.
Smart Readers	Smart readers are physically connected to a specific controller. The door and function outputs can be assigned from any controller in the same cross controller group.
Automation	Automations are managed by a specific controller (and may be associated with a C-Bus service on that controller). They can be linked to inputs and outputs in the same cross controller group.

Record	Description
Programmable Functions	Each programmable function has a host controller that controls its operation. It can be assigned inputs, outputs and other resources from the same cross controller group.
Data Values	Data values are managed by a specific controller based on the analog expander they are assigned to.

Host Controllers and Redundancy

Some types of records, such as doors, areas and programmable functions, have a **host controller** associated with them. The host controller is responsible for the primary operation of the record, such as processing access requests for a door.

To facilitate this, Protege GX makes intelligent decisions to determine which controller is hosting the record, based on the physical devices linked to it. For example, the controller with the most inputs, trouble inputs and outputs associated with an area is takes primary control of that area.

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

If the network goes down or a controller drops offline, the host controller manages as many functions of the record as it can. 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. However, it will not be able to detect issues such as a forced door if the door position input is on another controller.
- If linked controllers are offline, you can still arm an area from a keypad connected to the host controller. The area can bypass 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.

When programming sites with cross controller operations, always consider how the system will function if the controllers can no longer communicate with each other.

Programming Records in Cross Controller Groups

In systems that use the standard download server, programming is not restricted by cross controller groups. You can always assign any record in the system to any other record, even if the controllers that host those records cannot communicate with each other. You must take care to follow the rules of programming cross controller groups (see page 6).

When the enterprise download server is installed, the user interface restricts programming based on explicitly-defined cross controller groups. This makes it easier for installers to set up cross controller operations without error.

The following rules apply in the user interface:

- When you create a type of record that uses inputs or outputs (e.g. a door or area), initially you will be able to select any input or output from the site.
- Once you select an input or output, the record will be linked to a host controller. From then on, you can only select inputs and outputs that are accessible from that host controller.
  - For controllers that are not in a cross controller group, you can only select inputs/outputs from the same controller.
  - For controllers that are in a cross controller group, you can select inputs/outputs from any controller in that group.
- The toolbar displays the **Cross controller group** that the record belongs to.

- You can select the **Local** checkbox in the toolbar to restrict programming to only inputs/outputs on that controller. This replaces the **Programming mode** dropdown from previous software versions.

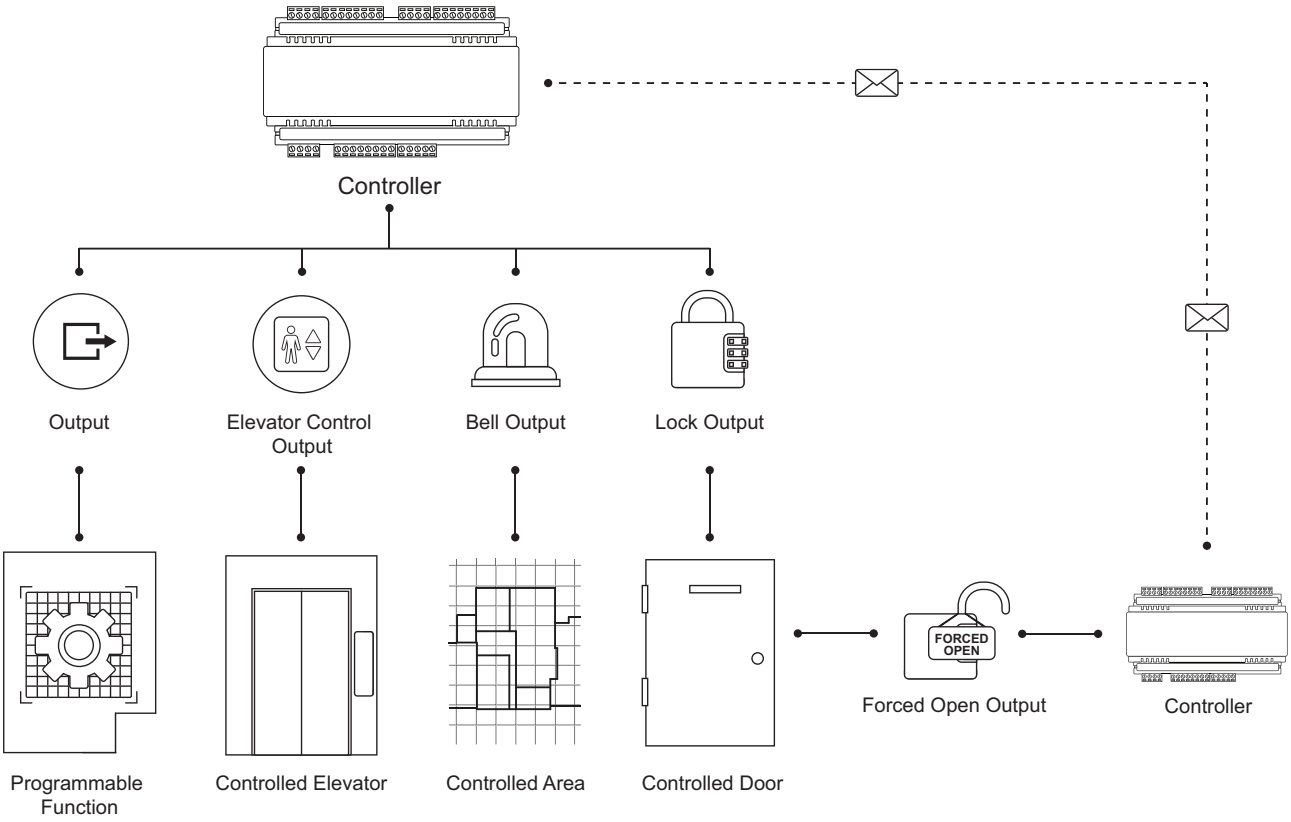
Examples of Cross Controller Operations

This section explains how cross controller operations work in practice and gives examples of use for different resources.

Outputs

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

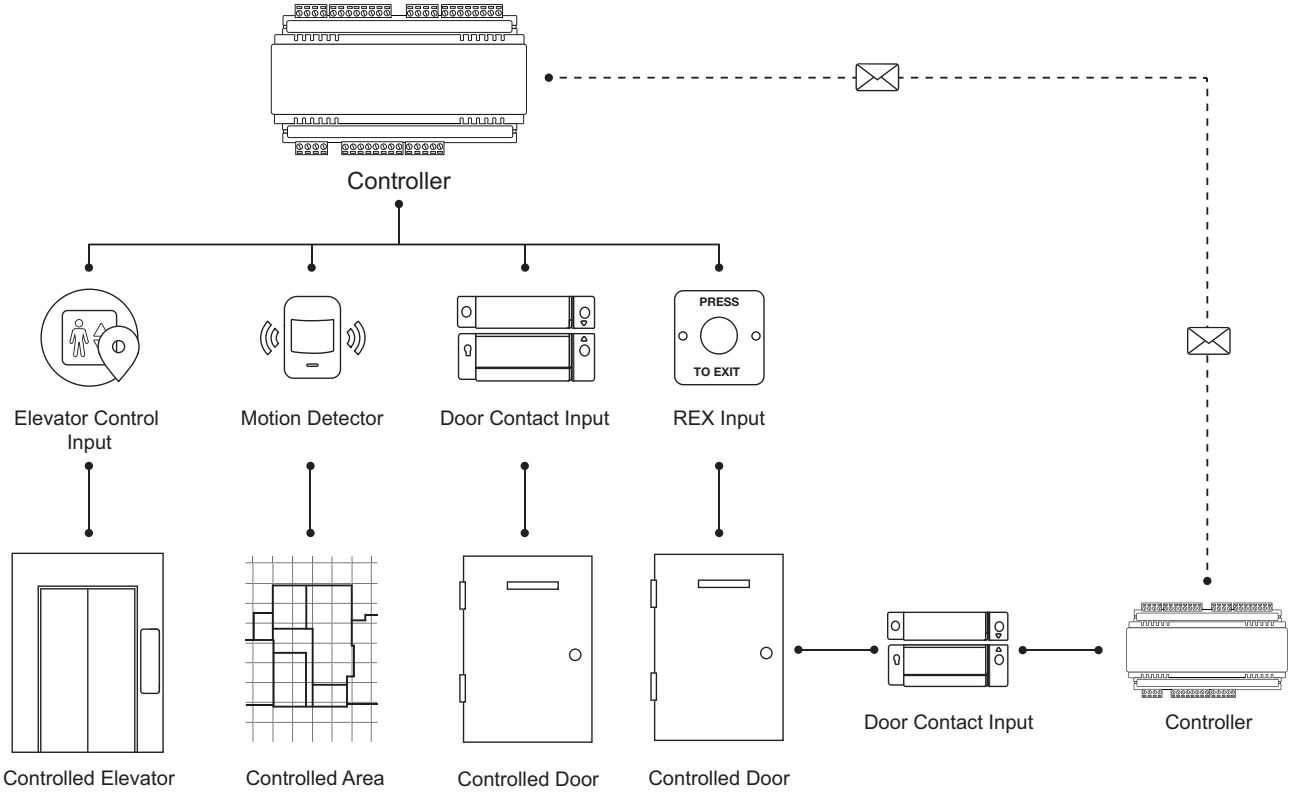
This diagram shows how outputs from multiple controllers can be used to control different functions of a single door.



Inputs

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

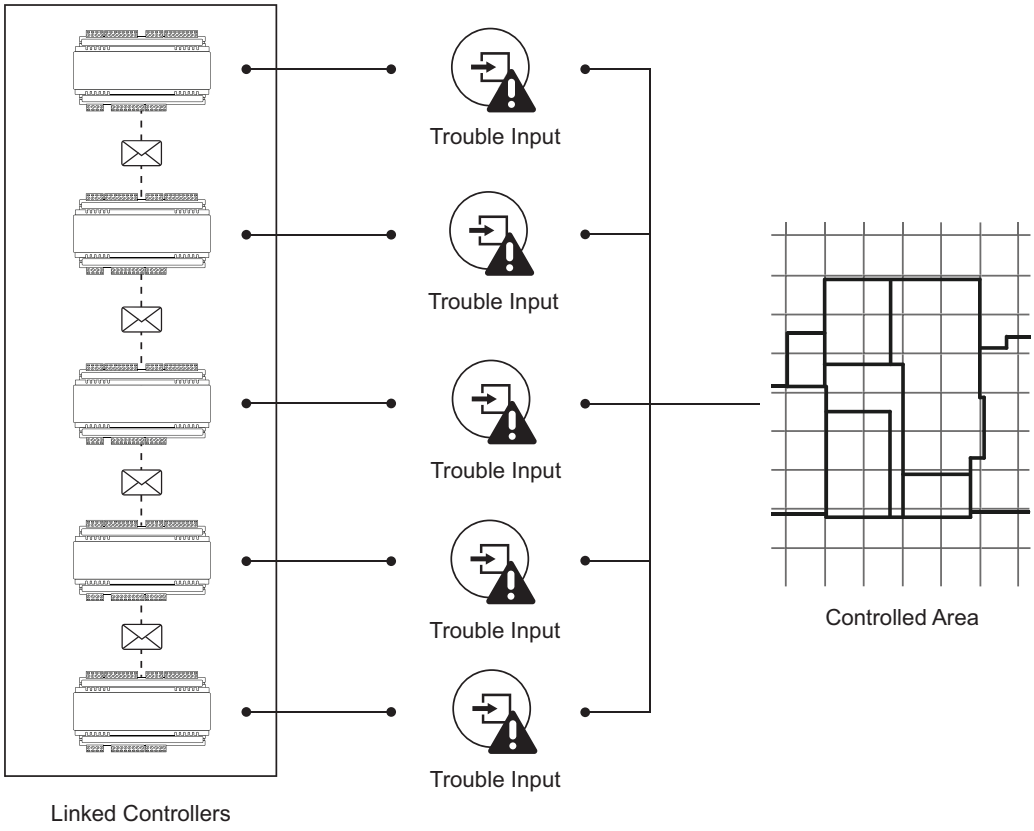
This diagram shows how inputs from two different controllers can be used to monitor a single door.



Trouble Inputs

Trouble inputs are linked to one specific controller. However, you can assign them to any area within the cross controller group.

This diagram shows trouble inputs from multiple controllers assigned to one area.



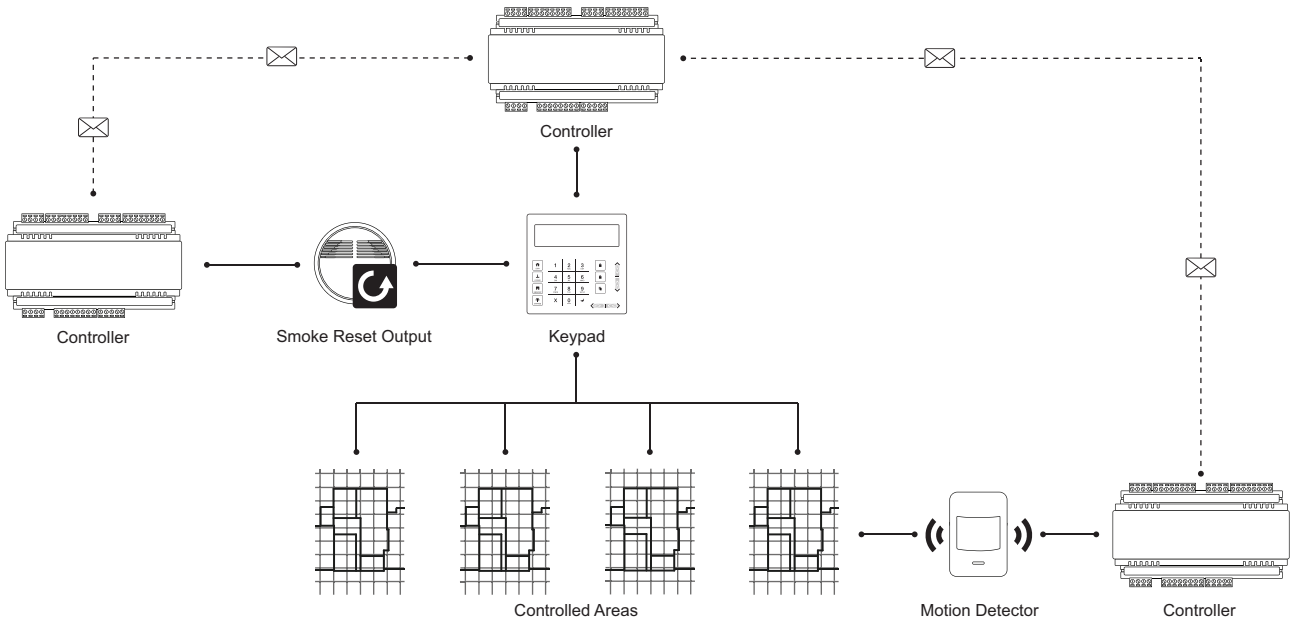
Keypads

Although keypads are connected to a specific controller, you can use them to view or control areas, bypass inputs or unlock doors from other controllers in the same cross controller group.

By default, each keypad will give users access to arm and disarm all areas within the cross controller group. You can narrow this down by assigning an area group to the keypad.

This diagram shows:

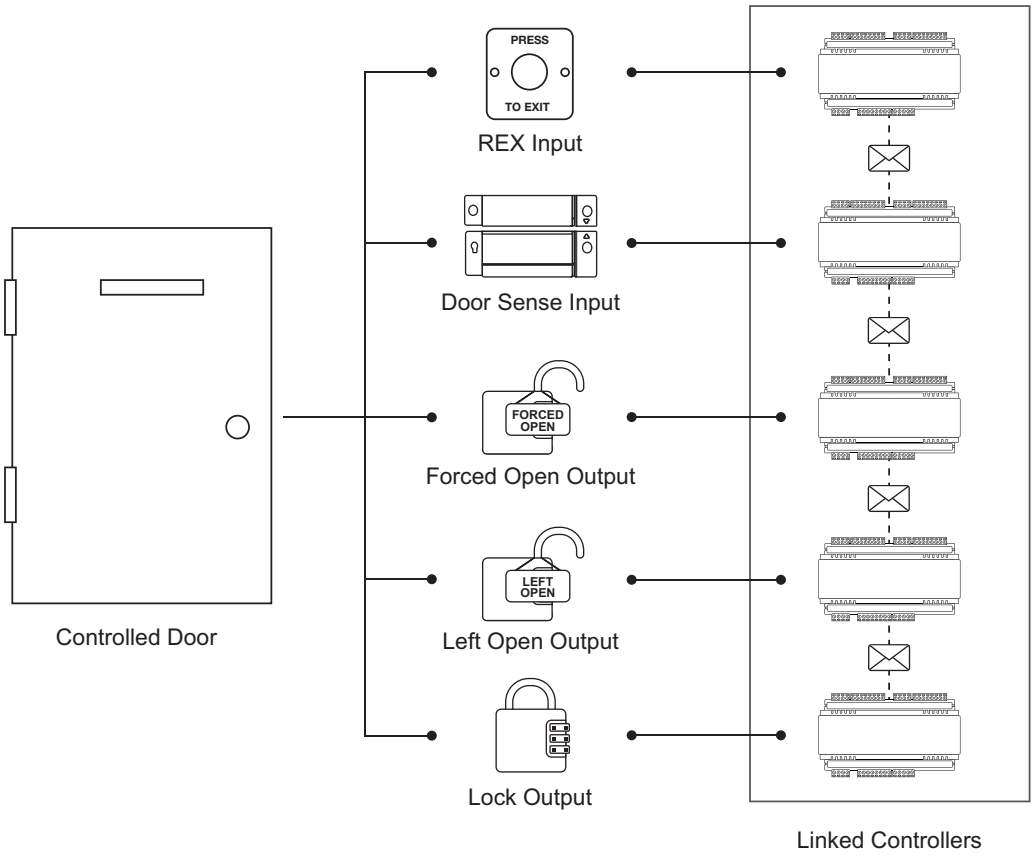
- A keypad connected to one controller and assigned four areas
- An output from a different controller used for the smoke reset output of the keypad
- An input from another controller used for the motion detector in one of the areas



Doors

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

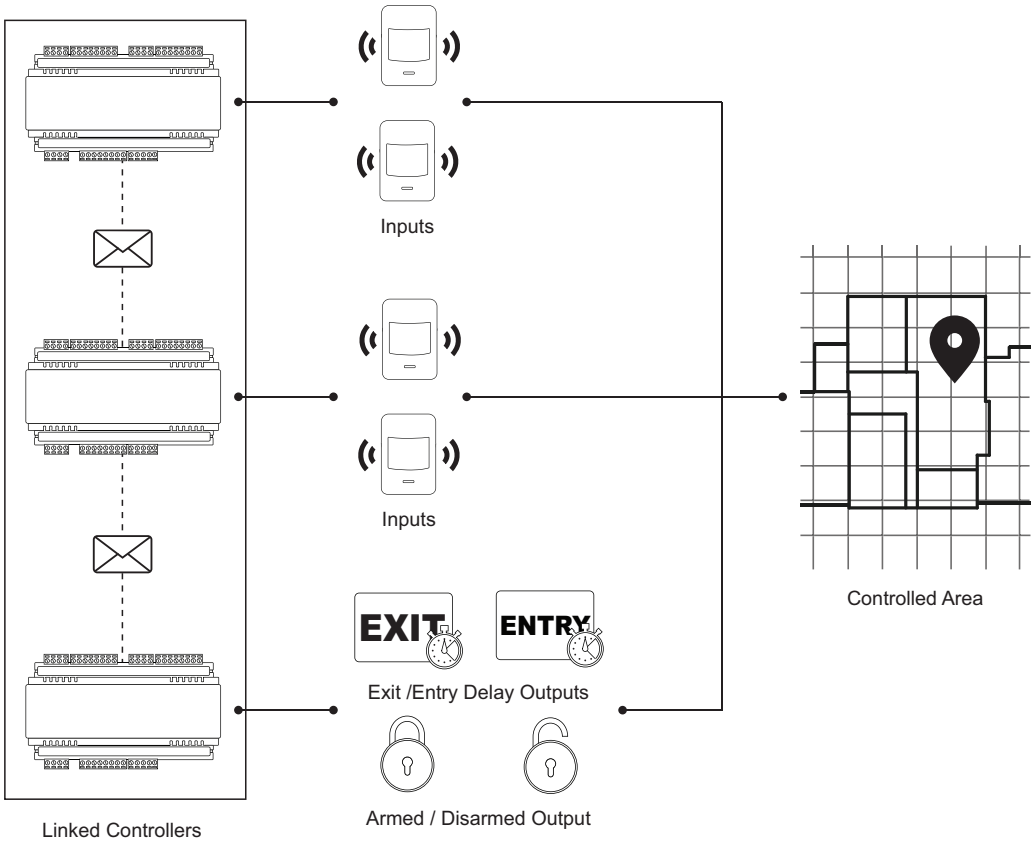
This diagram shows a door's REX input, door sense input, forced open output, left open output, and lock output, assigned from five separate controllers.



Areas

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

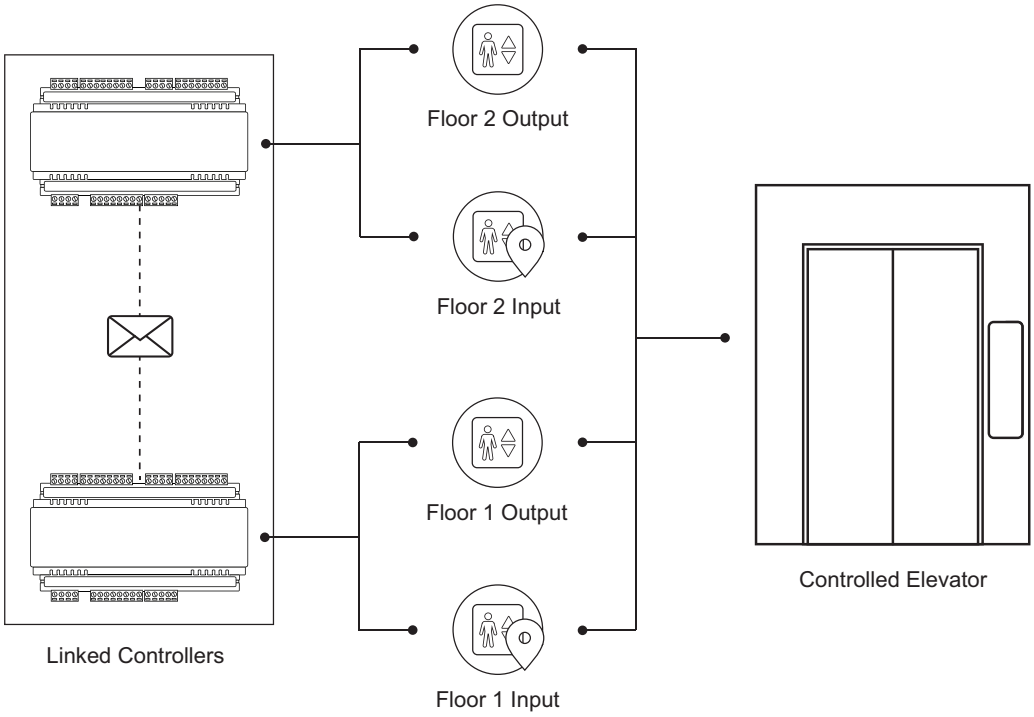
This diagram shows four inputs linked to two different controllers, as well as several outputs linked to a third controller.



Elevator Cars

Elevators cars using low level integration can use outputs and inputs from any controller in the same group.

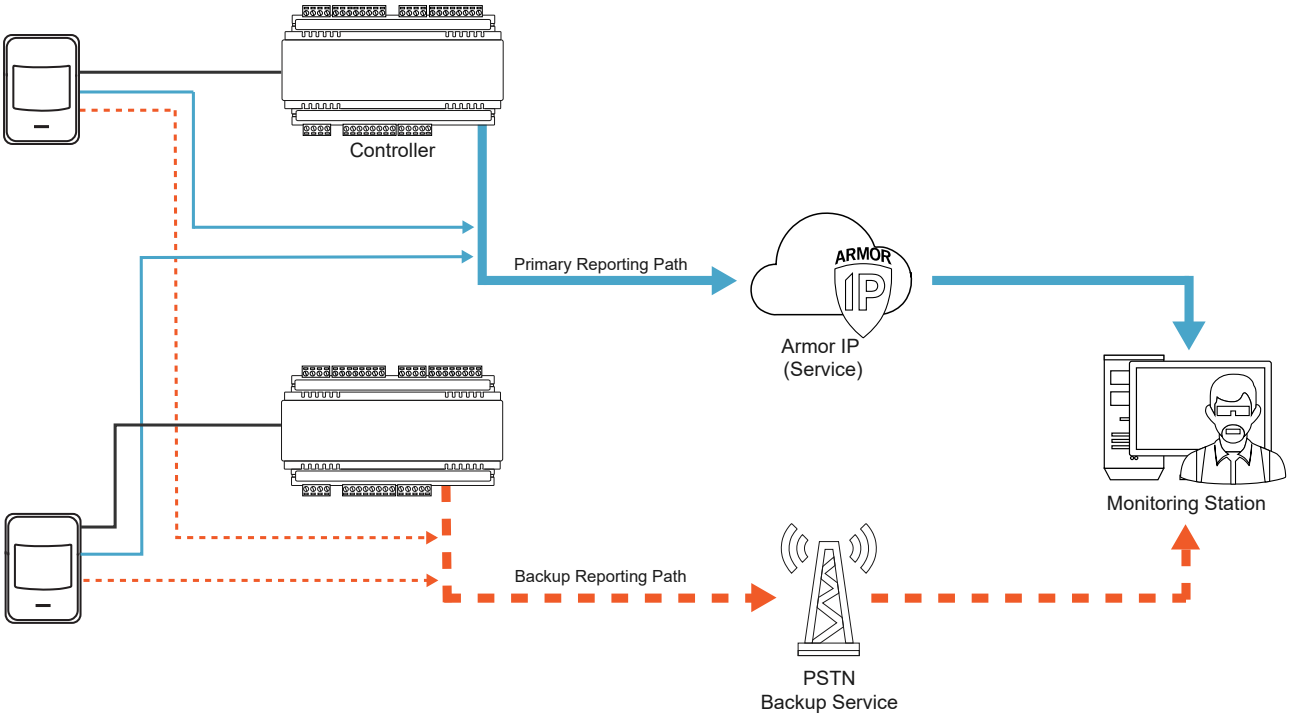
This diagram shows the elevator's inputs and outputs linked to two different controllers.



Services

Services (including reporting services) operate exclusively on their assigned controller. However, reporting services can be assigned to areas from any controller within the cross controller group.

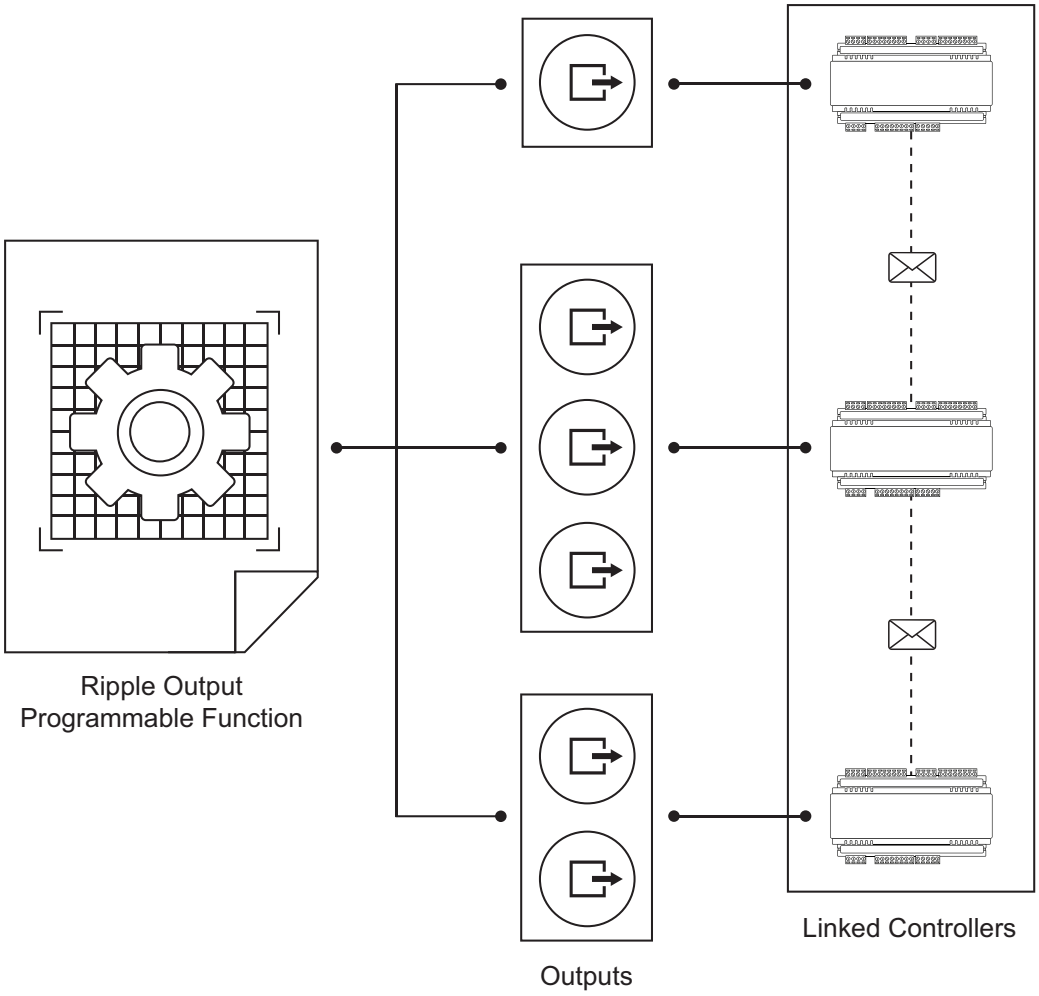
Reporting services are able to back up to another service running on another controller. For example, ReportIP can back up to a controller running ContactID (connected to a PSTN).



Programmable Functions

Programmable functions can use a mixture of inputs, outputs and data values from within the cross controller group.

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



Connecting more than 64 Controllers

Each cross controller group can only include up to 64 controllers, and it is not possible to add a controller to more than one group. However, sometimes it is necessary to connect more than 64 controllers together to achieve a specific requirement for a large site.

For example, the following scenarios might require many controllers to coordinate with each other:

- When anyone presses a panic button, lock down the entire university campus.
- When a fire alarm is activated, unlock every door in the high-rise building.
- When an alarm occurs anywhere in the airport, activate a siren in the control center.

In these instances, you must connect multiple cross controller groups together. There are two methods to achieve this:

1. **I/O Wiring**: Physically wire an output from Cross Controller Group A to an input from Cross Controller Group B. When that output is activated (e.g. by an alarm or programmable function in Cross Controller Group A), the input is opened. That input can then trigger an alarm or activate an output in Cross Controller Group B.
2. **Link Me Service**: The Link Me service enables you to mirror one or more outputs between two controllers. When the primary controller activates or deactivates specific outputs, the secondary controller updates its own outputs to match. This allows Cross Controller Group B to control a programmable function, schedule or virtual input based on the status of the outputs in Cross Controller Group A.

The best method for each site will depend on the number of outputs that need to be shared, the physical wiring situation and the network configuration.

We recommend keeping the controller group size below 48. It is better to create multiple smaller cross controller groups than a few large groups.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.