Technical Information Paper

Gallagher Command Centre Security System
Equipment Redundancy

Introduction

Gallagher Command Centre is a security management system consisting of a central server, multiple workstations and multiple sets of controller equipment, all using a standard network infrastructure to provide communication between the component parts of the system.

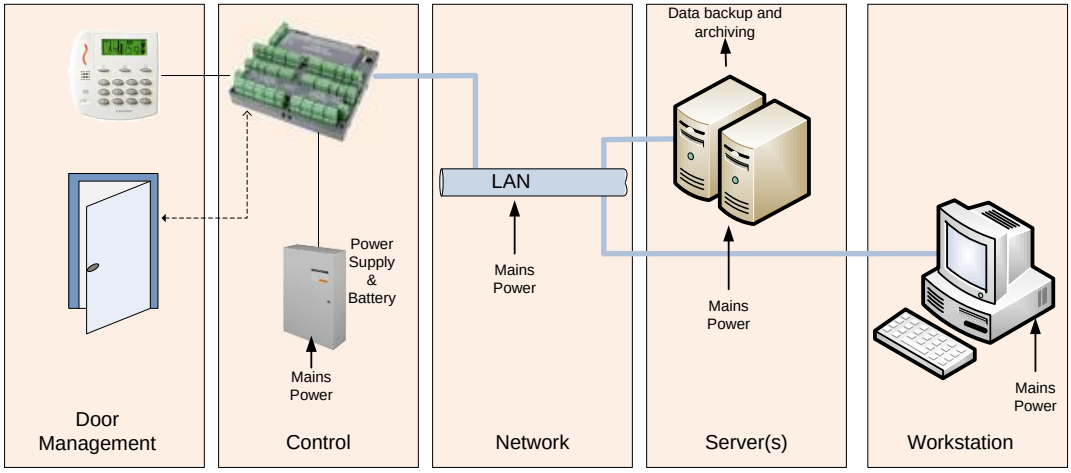
When the question about system recovery after a breakdown is asked, the immediate response is often “hot standby”. Hot standby is an option but comes with a cost. The cost may not be just the hot standby hardware solution; it may also be associated hardware such as power supply or LAN/WAN network infrastructure.

This paper describes options available and provides guidance to the best options for the customer, based on their specific requirements.

It is important to note that the Gallagher Multiserver provides cross-site operational cover and visibility. It is not a redundancy solution.

Throughout this Paper, although reference is made to the required power supplies, the actual power supply design will be covered in a separate Paper.

The infrastructure



A single site installation will typically consist of the parts as shown above. What needs to be considered is what will happen if any one or more parts of the system fail.

Door management

Doors are managed via the control equipment. Readers, door monitoring and door controls are connected to the Control equipment. The component parts are managed by a door module in the software. This means that the door management parts will interact with each other to provide the door management. It is difficult to provide duplication at the door level as the door itself is only a single item. If a component part of the door management fails, then the door access control will be compromised. Low voltage required to operate readers and door lock will generally be sourced from a low voltage power supply, associated with the control equipment.

Managing mains-powered automatic doors such as vehicle entry roller doors or pedestrian sliding doors require special attention. If these are essential access doors, a secondary mains power supply will be needed.

Control

A Gallagher Controller will support 10 doors requiring full card access control. If the controller fails, then up to 10 doors may also be compromised. To mitigate against this situation, for systems where a large number of people may be required to access a building, e.g. through a bank of turn-styles, it may be advisable to use two or more Controllers, distributing the turn-styles across the controllers. Then if one controller fails, access is still possible through turn-styles operating on the other controllers.

GBUS hardware requires a controller to operate. These devices have limited on-board stored functionality. The GBUS URI does have a fallback mode where if the controller fails, the GBUS URI will allow access for all cards having the common site facility code. Access restriction based on area, time or card activation is not supported.

All Gallagher Controllers have an on-board RJ45 network connector for connection into the network infrastructure. The supported network speeds are:

Controller	Speed
Gallagher Controller 3000	10 Mb/s
Gallagher Controller 5000GL	10 Mb/s
Gallagher Controller 6000	10 and 100 Mb/s
Gallagher Controller 6000HS	10, 100 and 1000 Mb/s

The Gallagher Controller 6000HS has dual Ethernet ports on board so that if the primary communication circuit fails, then the controller can be configured to automatically fail over to the secondary port. Note that the controller has a single network address configuration set for both ports.

If a Gallagher controller is off line from the server and associated operator workstations, the controller will continue to operate providing access control for the connected doors in accordance with the current controller stored configuration. Events are stored in controller memory and will automatically upload to the server on restoration of the controller to server connection.

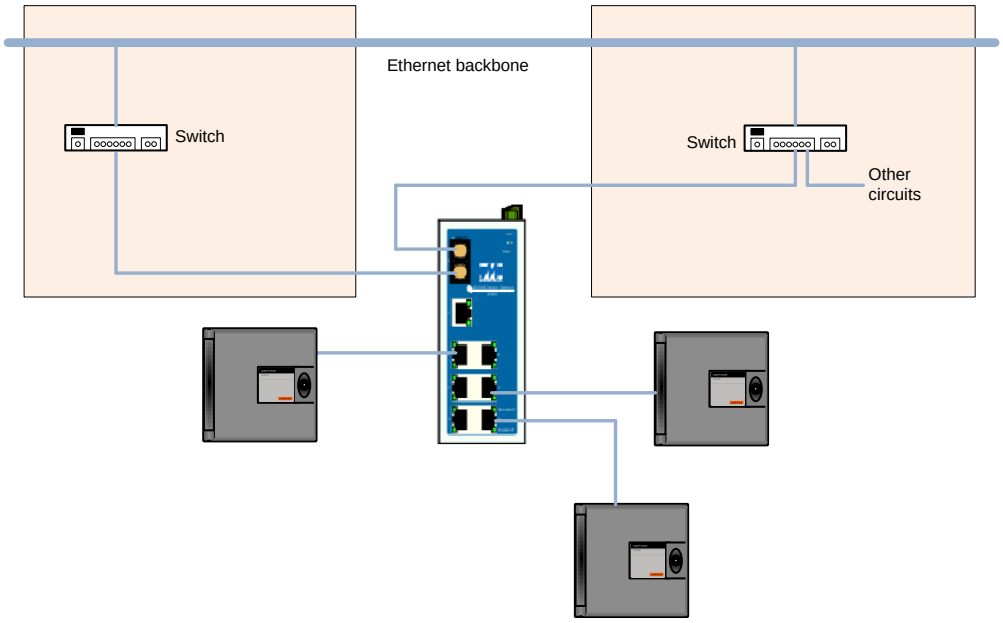
If the controller power fails, the Gallagher Controller 6000 will shut down in a controlled manner, storing all event data and configuration data ready for use when the controller restarts. In this situation, the Controller will not provide access control functionality

Network

The network infrastructure may be being provided by the customer's IT department. It is important that the security connectivity is clearly identified so that network cables are not inadvertently unplugged. The need for duplicate network circuits should be evaluated as a security requirement, not just a corporate network requirement.

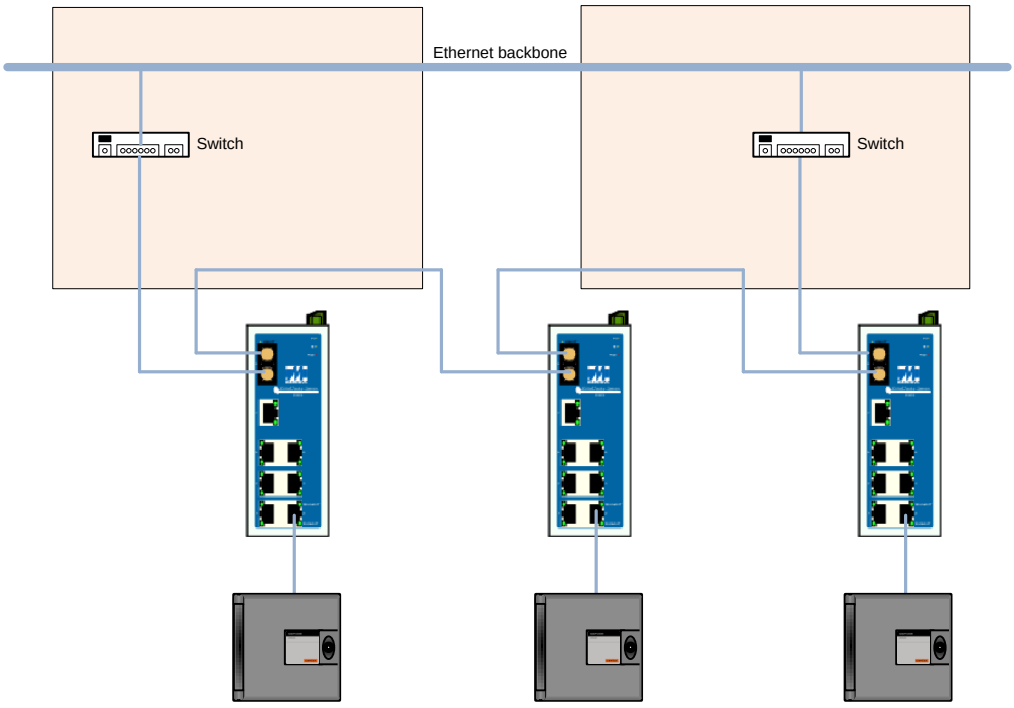
All network hardware will require backup power supply in accordance with the site needs for continuous operation. It may also be desirable to provide alternative network circuits to provide backup connectivity should a part of the network fail. An example is to use redundant network switches in the format shown below.

a. Single switch supporting multiple controllers



If one of the network connections from the redundant switch fails the alternative circuit will maintain communications.

b. Multiple switches supporting multiple controllers



The above configuration is ideally suited to a large campus or an extensive perimeter installation. If the network connection is cut anywhere on the network, there is an alternative path for all controllers to connect back to the controlling server.

Server

IMPORTANT NOTES

1. **Regular data backup and event archiving must be carried out so that should a server failure occur, there is valid data available to be recovered if required.**
2. **Gallagher Multiserver is NOT a solution for backup or standby requirements. It provides a means of linking 2 or more sites from an operational perspective.**
3. **A server is very much dependant on the network being operational. Multiple server installations require a stable network to operate.**

Gallagher has configuration options for backups and archiving. System administrators should take full advantage of this functionality.

The Gallagher Server provides:

- Operator workstation access to the system;
- Hardware configuration (downloaded to controllers);
- Event storage; and
- Specific control functionality not normally applicable to controller functionality.

Note that the controllers do not need to be on-line to the server to operate.

Redundancy at the server level may be provided in many formats. One must bear in mind that the faster and more seamless the changeover, the more expensive the solution will be. Another matter to consider are should the changeover be an automatic or a manual operation. An automatic changeover take place immediately the primary server appears to have failed or should the changeover be a manual process where the secondary server is only started after a period of several minutes.

Restoring back to the primary server after a period of secondary server operation should always be a manual operation, to ensure the operating environment is stable before changeover.

The customer's IT department should be consulted before implementing any standby solution to ensure that the proposed solution does fit within the company corporate policy.

If the server is off-line operators cannot see any events occurring in real-time and cannot make any changes to the system configuration. This includes adding, editing or removing cardholder records. Access control at doors will still be operating and events will still be stored in the controller pending upload to the server on restoral of the server. Although alarm events will not be available at a workstation, if a controller has a dialler installed for connection to a monitoring station, alarms will be transmitted from the controller as normal.

Questions for the system owner are:

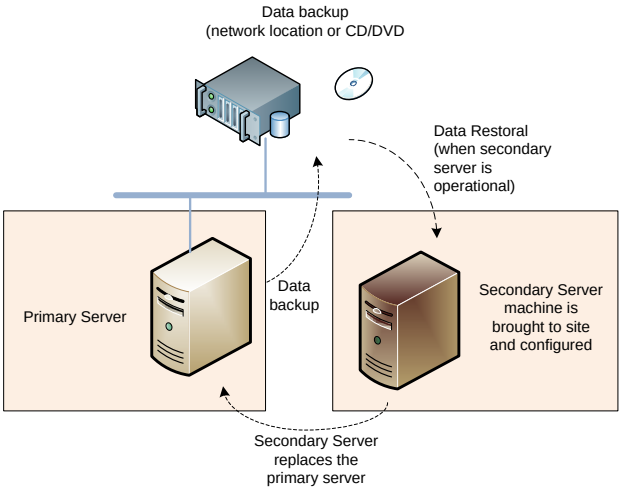
(i) How long is it acceptable to lose communication between the server and workstations and Controllers?

(ii) Is the intent to protect against equipment failure, building disaster, or both?

These questions are covered in the options described below.

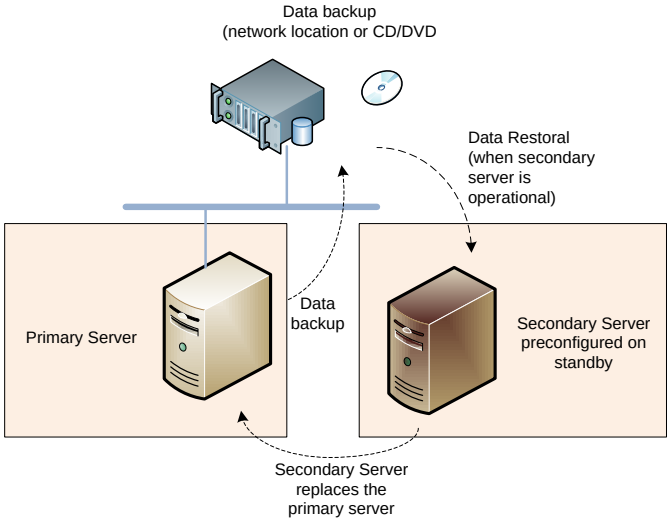
a. If the above scenario is acceptable for more than 4-6 hours, then a replacement server can be configured and made operational within this time frame. The replacement (secondary) server must be configured with the same machine name / IP address as the primary server. It can be installed at either a local or remote location. Data is recovered from the central data storage location or backup media such as a CD / DVD into the secondary server. Services need to be started on the secondary machine. This may take 2 – 3 minutes. Controllers will need to be reinitialised as there will be data mismatches between the current data on the controllers and the old data recovered from the central

storage location. Configuration changes and card record changes implemented since the backup was generated until the primary server failed, must now be re-entered.



b. If the above scenario only is acceptable for up to 30 minutes, then there are several options available:

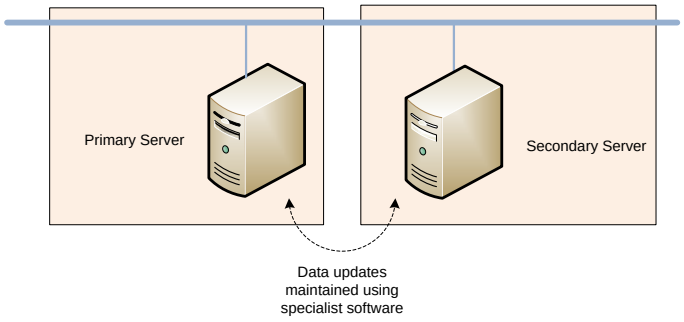
   i. A "cold standby" server may be applicable. For this configuration, data is backed up to a network location at regular intervals. Should the primary server fail, the secondary server, having the same name as the primary server is started and the backed up data is restored from the central network location or CD/DVD, to the secondary server. This is essentially the same as option 1 above but the secondary server is on site and pre-configured, ready to operate. Services need to be started on the secondary machine. This may take 2 – 3 minutes.



As for (a) above, controllers will need to be reinitialised as there will be data mismatches between the current data on the controllers and the old data recovered from the central storage location. Configuration changes and card record changes implemented since the backup was generated until the primary server failed, must now be re-entered.

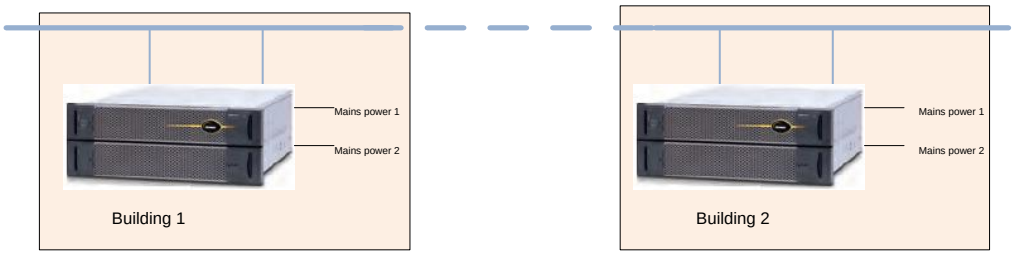
ii. A warm standby solution will provide changeover in less than 30 minutes and will not require intervention by the user. The changeover is automatic. Under this scenario, both the primary and secondary servers are operational and the data is maintained between servers using a specialist product such as HP Doubletake ® or Arcserve® (formally CA XOSoft). If the two servers are connected to the same subnet, changeover can occur in a few minutes, the time to restart services. If the servers are in different subnets, it may take up to 20 minutes to changeover.

It is recommended that an engineer specialising in the preferred software be employed to configure the software to ensure correct operation.



c. If the change from primary server to secondary server must be maintained without any break, then a product such as a Stratus® high availability server is recommended. Stratus advise that this solution provides 99.9999% uptime. The Stratus Server has multiple disk drives in RAID configuration, dual network connectivity, dual motherboards, and dual power supplies down to mains power connections. Although it is a dual machine, a Stratus server appears as a single IP address to the network.

d. Should the site requirements dictate that total protection against both equipment failure and building disaster, then a combination of options 2b(ii) and (c) will provide this level of redundancy.



e. Virtual Machine (VM) Solutions are becoming more popular as operating environments in today's IT world. A VM environment can be configured to provide a seamless changeover. The duplication of the Gallagher Server installation is managed within the VM system. The corporate IT provider would normally manage the VM environment.

Automatic or manual changeover?

Should the changeover from a primary server to a secondary server be an automatic or a manual function? If this situation is not covered by existing company IT policies, then the options need careful consideration. It is important to note that the automatic process will not necessarily know about other site conditions when making the decision to changeover. For example in the case of a managed outage for a very short interval, it may be desirable to not changeover to a secondary server but wait until the outage is cleared, remaining with the primary server.

When reverting from a secondary server back to the primary server it is recommended that the changeover is manually initiated, to ensure that the primary environment is stable before reverting.

A mode of operation commonly adopted is:

Primary to secondary changeover – automatic, without operator intervention.

Secondary to primary changeover – automatic but initiated by an operator.

Summary of server options

Option	Changeover method	Server restoration time	Equipment failure protection	Building disaster protection
(a) Standby machine requires new installation.	Manual	4 – 6 hours	Yes	Yes
(b) (i) Standby machine already installed ready to run	Manual	<30 minutes	Yes	Yes
(b) (ii) Standby machine already installed.	Automatic	<30 minutes	Yes	Yes
(c) Single high availability server	Automatic	Instant	Yes	No
(d) Dual high availability servers	Automatic	Instant (LAN) <30 min. (WAN)	Yes	Yes
(e) Virtual machine	Automatic	Instant	Yes	Yes

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