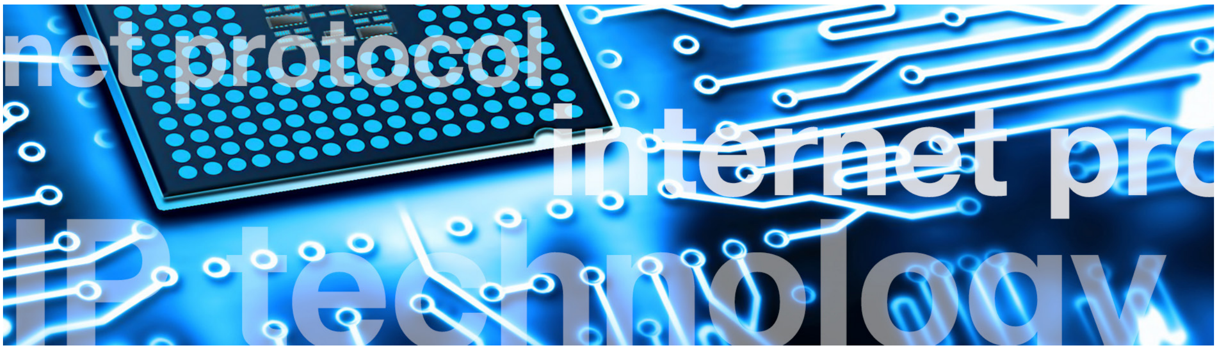
british security industry association

Installation of access control systems using IP technology – a guide



May 2017

For other information please contact:

British Security Industry Association
t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

Contents

The information and expression of opinions that are contained in this guide are not intended to be a comprehensive study, nor to provide specific advice and should not be treated as a substitute for obtaining such specific advice concerning individual situations.

The BSIA accepts no responsibility for any loss or liability which may arise from reliance on information or expressions of opinion that are contained in this guide. References to other sources of information are for information only and the BSIA takes no responsibility for any material found in them.

1. Introduction

It is now common practice for access control systems to utilise existing networks (LAN or WAN) for providing a communications path between the access controllers and the software. Associated with this is the need for a greater understanding of the network environment, taking into consideration the “rules” and practices used in the IT industry. These guidelines have therefore been prepared to provide guidance on what an access control system will require from an IP network.

2. Scope

This guide applies to systems combining access control functions with IP networks.

3. Terms, definitions and abbreviations

3.1 Abbreviations

IT – Information Technology
IP – Internet Protocol

3.2 Definitions

3.2.1 Bandwidth – the amount of data that can be transmitted in a fixed amount of time. Usually expressed in bits per second (bps) i.e. Kilo (Kbps), Mega (Mbps). This may be considered to be a synonym for capacity or ability of the network.

3.2.2 Infrastructure – for the purposes of this document taken to mean the hardware and software resources of an entire network that enable network connectivity, communication, operations and management.

3.2.3 Hosts – Devices or appliances that make use of an IP network to send digital data, each host on an IP network has a unique IP address.

3.2.4 Network – Common term used to describe a computer network whereby network enabled devices are able to exchange data using common communication protocols.

3.2.5 LAN – Local Area Network is a physical network sharing a common communications line or wireless link to a server covering a small geographical area e.g. office, school etc.

Note: A LAN may include wireless connections.

3.2.6 Virtual LAN – A VLAN is a group of computers or network enabled devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LANs. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

3.2.7 WAN – Wide Area Network is a telecommunications and / or computer network that extends over a large geographical area.

4. Components

4.1 Routers

Routers are used to forward data between IP networks, often used to link LANs via WANs using the internet or other telecommunication system. Data is forwarded from one part of the network to another through a router using a specific port and transmission method.

4.2 Firewalls

A firewall is a network security system, either hardware or software based, that controls incoming and outgoing data traffic based on a set of rules. Firewalls are used to protect the network and infrastructure from attack.

4.3 Hubs/switches

These are networking devices that connect computers or network enabled devices together and passes data between them.

- Hubs provide a means of connecting multiple network connections. The data is passed to all ports on the hub.
- Switches are devices that switch the data between specific ports, thus allowing bandwidth and redundancy control.

5. Transmission paths

When there is a requirement to transmit access control data from point A to point B a number of different technologies may be employed. These typically include wired and wireless systems such as: LAN, WAN, GSM, GPRS, 3G, 4G, Wi-Fi. Further explanation of these technologies can be found in BSIA Forms 210 and 211 – the installer's and user's guides to IP.

6. Considerations

6.1 Operational Requirements

The first consideration should be the level of access control, site location(s) and the communication method, alarm and reporting requirements and user requirements.

6.2 Site IT Considerations

The IP communications should be discussed and agreed with IT personnel responsible for the network. Consideration should be given to the extent to which the existing IP network will be used by the access control system.

6.3 Multiple Sites

When multiple sites are involved then consideration should be given to the communication paths between sites. Are the sites connected using a WAN or do they utilise the Internet through an ISP (Internet Service Provider)?

- Most ISPs do not provide a service level agreement and do not guarantee the availability of the transmission path(s). Therefore, the system design needs to consider what effect any downtime would have on the operation (or security) of the system.

6.4 Ports

Access control systems will communicate using either a proprietary or open protocol. The data that is transmitted between the access control computer and the controllers/readers will use a specific port on the associated IP address.

The usage, and blocking, of ports is usually configured by IT personnel and can be configured in both the firewall and routers. It is crucial that the port information is made available and discussed with the appropriate IT personnel to ensure any changes do not affect the operation of the access control system.

Often IT security updates or the introduction of additional equipment/software on the network can result in changes to port usage and availability. This could have an impact on the operation of the access control system. Consideration should be given as to how future IT security updates will be applied minimising any adverse effects on the access control system.

6.5 Remote Access

Off-site communications with the access control system either instigated by the system itself or by a remote user is common place. Remote access is typically provided for monitoring, management and maintenance of the system. The security of this remote access is key to the security of the whole access control system and must be agreed upon at an early stage.

6.6 Network design

Key to any IP system is the design of the network infrastructure.

6.6.1 Network topography

When the location of the various system components are known, the layout of the network can be evaluated and decisions made as to where any existing cabling can be used or where new cabling needs to be installed.

6.6.2 Network usage/bandwidth

Unlike Video Surveillance system (VSS), access control systems use very little network bandwidth. The access control manufacturer will be able to provide typical bandwidth usage for the system. It is likely that an access control system can share an existing network.

7. Network security

A risk assessment to assess the possible vulnerabilities of a network installation should be performed. Appropriate actions should be taken to protect the network and hosts from physical and electronic attack, this should include stored or transmitted data.

8. Network Integrity

[Considered part of ‘security’ by IT] The design of the network should ensure not only a level of service suitable to the access control application but also a level of robustness (or availability) suitable to the system. This is also referred to as ‘quality of service’ whereby a predetermined bandwidth and percentage availability will be specified.

Consideration should also be given to the concept of network available resources where additional capability is provided by a non-security source for the access control system. An example of this may be networked storage (or cloud services) or operator workstations.

Where there is a reliance on IT equipment (e.g. hubs/switches) then this equipment should be supplied with the same level of standby power and security as the rest of the access control system.

9. Management of the network

An IP access control system may be considered more flexible than conventional access control systems in that they may use the same network infrastructure as other business systems. The loading on that infrastructure may consequently be more variable. In systems where the service level is not guaranteed, consideration should be given to managing that network to monitor the performance and ensure prompt corrective action where required.

10. WAN/VLAN links

Where event data is to be sent via a WAN link, the appropriate link should be supplied. VLANs are typically used to segregate the access control system from other systems minimising any interference from other services/systems on the same network. As a result, bandwidth may be limited or reduced. The bandwidth requirements for the access control system should be discussed and agreed with the IT department to ensure the correct VLAN setting.

11. Maintenance

IP access control systems will most likely be a hybrid of security and IT equipment and may therefore use different engineering resources for maintenance or repair. Any maintenance and/or Service Level Agreements (SLAs) should take this into account, to ensure that all aspects of the access control system have the appropriate level of cover. Where access control systems use an existing (or shared) network, consideration should be given to the level of service and maintenance on the network infrastructure itself to ensure that the access control system remains fully functional.

12. Training

IP access control systems may require additional skills to that of the provision of conventional access control services, and may therefore require additional training to familiarise engineers, administrators and users in the installation, configuration, usage and maintenance/service of the system.

13. Documentation and records

The system design proposal and as-fitted documentation should include the following information:

- Use of fixed IP addresses, either manually allocated or assigned by automated method (DHCP).
- User names and passwords.
- Contact and policy details for the providers of the SLAs of all equipment.

14. Document references

BSIA Form 210 – An Installers Guide to IP in the Security Industry.
BSIA Form 211 – A User Guide to the Use of IP in the Security Industry.

15. Further Reading

BSIA Form 132 – A Specifier's Guide to Access Control Systems.
BSIA Form 151 – A Users' Basic Guide to Access Control.
BSIA Form 152 – An Installer's Basic Guide to Access Control.
BSIA Form 234 – Installation of IP-based Secure Signalling Systems for I&HAS – An industry guide.
BSIA Form 235 – Installation of CCTV systems Using IP Technology – A guide.
BSIA Form 236 – A Guide to Internet Protocol for ARCs and RVRCs.

This document was created by the technical groups and committees of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

In order to provide guidance and simplification in the complex area of IP access control systems, the BSIA is very active in the European & International standards arenas and also develops its own guides and codes of practice where currently standards do not exist.

The technical groups and committees encourage debate on new developments and concerns within the security industry. In doing so it seeks to ensure that all stakeholder interests are represented including: security companies, users, the police, inspectorates and insurers.

As a security company, BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, end users, specifiers, standards and legislative bodies. For more information contact the BSIA.

BSIA Ltd
Kirkham House
John Comyn Drive
Worcester
WR3 7NS

t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

@thebsia

bsia
british security industry association