ideal
Create. Protect. Accelerate.

The Case for a Converged Network System in Building Construction

Introduction

Large, modern, construction projects rely on a high number of services for their day to day operation. HVAC, energy, lighting, CCTV, access control, intercom, digital signage, lifts and telephony are just some of the numerous systems that are implemented in building construction projects. The majority, if not all, of these systems comprise an endpoint of some description, such as a sensor, a phone or a camera, that all need to communicate back to a headend device that provides control, monitoring and alerting functions. The endpoints and associated headend device (typically a server of some sort) are connected to each other via the network deployed within the building.

Legacy network deployments and issues arising

The services previously mentioned are installed by different trades and historically (and even to this day to some extent) each trade would install its own network for their specific package of works. So, the security contractor may install their own network for the CCTV cameras and door access control along with associated headend equipment and they are solely responsible for it. They may even install a broadband connection so they can access their system remotely. Similarly, the BMS contractor will also install their own network for their sensors, servers and other associated equipment, again possibly with some external connection for remote access and/or monitoring. And this continues to happen throughout the different trades.

There are a number of issues with this approach. Firstly, there is a lot of waste with the backend network equipment. Having a separate network switch for the security systems means only a small portion of ports are used on a switch that has 24 or 48 ports of capacity. Next to it, in the same cabinet, you have another switch with three or four ports in use for the BMS sensors in that part of the building. Both switches are consuming power but are significantly under populated. Add to that all the other different trades that may require (or insist) on their own backend network infrastructure and the excess of equipment and power becomes significant. Not forgetting that each trade is also billing the client for their separate network infrastructure.

Secondly, there are the security implications of running multiple, independent networks with their own ingress points available over the internet. It is often unclear whether each contractor has the necessary expertise in cyber security to ensure their systems are safe from unauthorised access, or what governance is in place to ensure that all trades have secured their environments to an agreed standard.

Another consideration is interoperability. Should one service such as lighting control need to interact with the blind control system for whatever reason, how do these networks interconnect and who is responsible for this? What is their code of connection? Security, again, becomes a consideration as one trade could potentially compromise the previously secure standalone network of another trade.

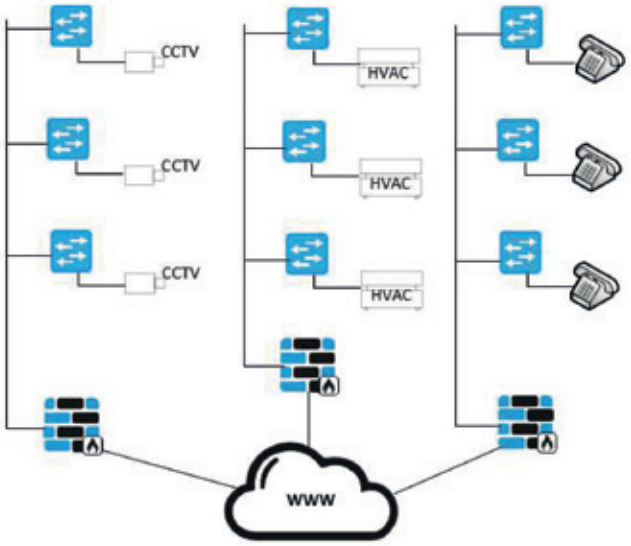


Diagram – Disparate Networks within a Single Building

There are numerous other considerations around monitoring, ongoing operational costs, management, etc. but for now let's explore the alternatives.

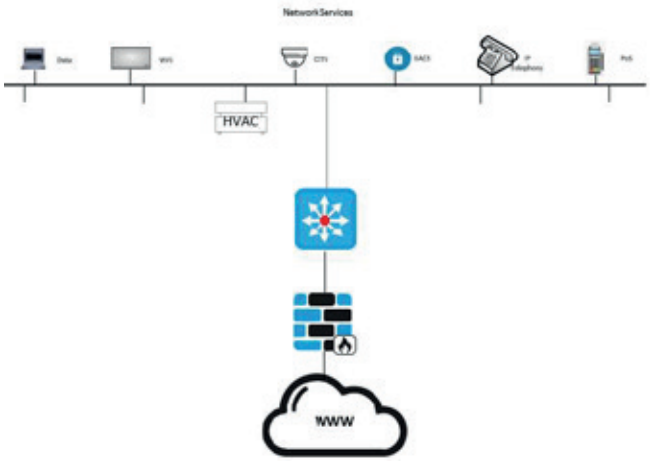
Converged Network System (CNS)

Having looked at legacy approaches to building networks, what are the alternatives? A new and somewhat obvious approach is to deploy a single network infrastructure that all trades can connect their equipment to, where a single contractor is responsible for providing said infrastructure. This is typically referred to as a Converged Network System (CNS).

A CNS negates all the risks and disadvantages of the legacy approach. Immediately an economy of scale can be realised by providing sufficient port capacity for all trades in all areas of the building, where it is required and scaled as growth demands.

This eliminates wastage around unused port capacity and power draw. The contractor responsible for deploying the CNS also has much greater buying power sourcing from a single vendor as opposed to say, five trades all buying ten switches from their preferred vendors - all at the client's expense.

Diagram – CNS High Level Diagram



These economies can be translated into resilience within the network design to provide multiple network paths and redundant components to achieve optimum uptime for all trades.

Cyber Security for the entire environment can be centralised in that it becomes the responsibility of the CNS contractor. They then define how different trades (or IP Partners) will communicate with each other (if at all) and they ensure each IP partner's environment is secure and that there is a separation of traffic. Preventing unauthorised access and attack mitigation is now the focus of a single, experienced contractor.

A CNS offers a single domain for managing the network estate. All switches, routers, firewalls, wireless access points, etc. that make up the entire communications network for the CNS are under a single monitoring system and the CNS contractor (or building management team) can take immediate action in the event of being alerted to a network issue.

The Prime contractor can eliminate interoperability issues between IP Partners by standardising on best of breed vendors for the CNS components at design stage.

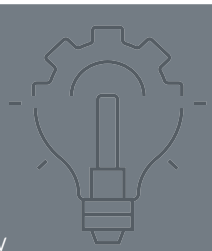
Perhaps one of the more interesting aspects of deploying a CNS is that it provides the building blocks for Smart Building Technology. The ability for multiple systems within a building to communicate with each other, gather and analyse information and make automatic decisions based on that data can bring benefits around productivity, energy consumption, operational savings and user experience.

This ultimately makes the building more desirable to tenants, helping to increase its letting ability. A further benefit is the lessened requirements for network engineers onsite due to off-site build.

Granted, you can build any network off-site, but the CNS only requires one team of installation engineers when it comes to on-site commissioning whereas a building with several networks under different packages will all have teams vying for space and time to install. As well as the reduction in the number of network engineering teams, there are other benefits realised such as reductions in Health & Safety costs, supervision, and carbon footprint of the build. All of these can directly translate into a cost saving for the client.

It also simplifies the model for the client post completion. With a CNS to manage, there is only a single service provider to onboard, and that has both cost and operational benefits. In this environment, a service provider can bring greater value to the building by influencing operations such as Cyber Security beyond the original build specifications were likely to have allowed for.

Conclusion



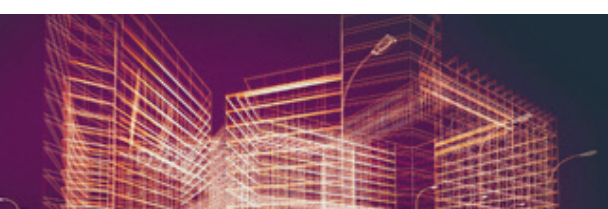
To summarise, a CNS can offer a number of core benefits:

1. Reduced power waste
2. Increased buying power
3. Increased and simplified overall security
4. A single source of responsibility and management
5. Opportunity for off-site construction

About Ideal:

Ideal is a UK-based managed service provider to the construction industry. We architect, commission and support high-performance, resilient, complex network infrastructures for many contractors including Skanska, Mace and TClarke. Partnering with industry-leading technology vendors such as Cisco we build high-availability, robust and flexible networks for buildings such as Twickenham Stadium, Westfield Shopping Centre, Battersea Power Station and 22 Bishopsgate.

www.ideal.co.uk/construction-services



Intelligent Technology, Real Performance