



Mesh Freedom White Paper

“Freedom is never voluntarily given by the oppressor; it must be demanded by the oppressed.” Martin Luther King

Executive Summary

This white paper is intended to educate end users and integrators about the benefits of using IT enabled card access and physical security systems to eliminate the problems and costs associated with proprietary control panels. The issue with access control hardware is not IP. Many panels and reader suppliers are developing IP interfaces. The real issue is that control panels and IP readers are designed using C+ or other code that precludes the ability to properly deploy access control on IT platforms.

Control panels are based on proprietary software that must be matched to PC programming software. Each new panel software version or PC programming version sows the seeds of obsolescence of previous versions. Panels are proprietary and are not interoperable between suppliers. End users, having selected a system and having deployed masses of control panels often feel trapped and compelled to continue with the same system. IT departments see little logic to this hardware based architecture and are often at odds with security departments over the management of security software.

MESH Freedom Bridges

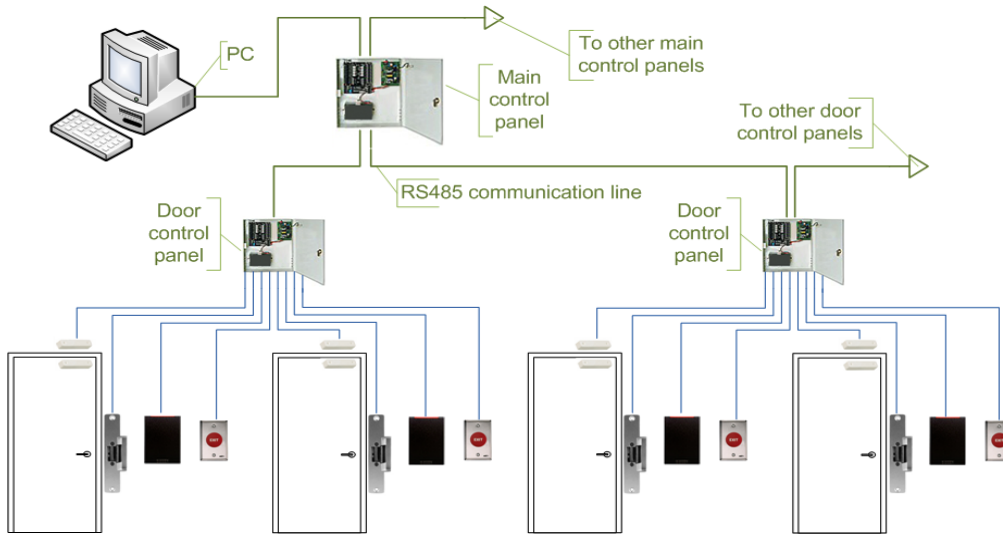
Instead of control panels and door interface modules that are programmed from a PC, the new architecture allows users to connect any standard reader type (wiegand, smart, FIPs etc.) directly to a network through inexpensive IP bridges.

The software component of MESH Freedom is the MESH web browser security operating platform. Unlike control panels, the user database and the door control software is written in IT language located on a server(s), thereby future proofing systems from the traditional issue of proprietary hardware version obsolescence and improving scalability by eliminating the need for additional hardware every time a reader is added to a system.

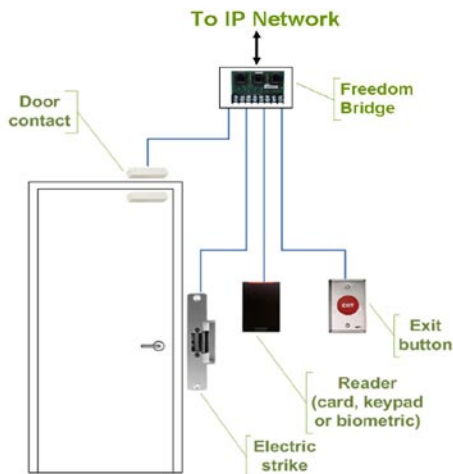
The MESH Version 8 platform includes the functionality of the most sophisticated access control systems. Additional components include visitor management and badging, incident reporting, facility maps, touch screen intercom systems, and package tracking.

In addition, access control applets can be loaded onto existing third party IT hardware, including servers, routers and possibly even IP cameras thereby eliminating the need for separate access control hardware.

Typical Control Panel Architecture



Typical Freedom Architecture



MESH Freedom Hardware

VSI is in the process of releasing a series of bridges to accommodate a full array of field requirements. Each bridge is essentially an IP switch that includes specialized card access components including reader inputs and ports to manage inputs and door outputs. When a card is presented at a reader, the reader sends a message to the bridge that encrypts the message. The message is sent to local or remote IT hardware for validation and a message is then sent to the bridge to enable door control.

VSI expects the most common objection to the architecture to be concerns about the stability of networks and the concern that a lost connection to a server will affect door control. Each Freedom bridge is designed with fault tolerant software that will allow the bridge to connect to any synchronized server on a network. For example, if a server in facility A fails, the bridge will simply contact other servers B thru X within the Enterprise to find an open path for door control.

A. Wired Bridges

Each wired switch comes with 4 supervised inputs and 2 outputs per reader. All wired switches are POE enabled with a power input where necessary.

One and two reader bridges are designed to connect to existing card readers to the network either at the door or at the termination point of the existing card reader cabling.

Four and eight reader bridges are designed for replacing existing control hardware at the connection point of the existing hardware or to make more efficient use of existing routers.

B. Wireless WiFi Bridges

VSI is initially limiting WiFi switches to one and two readers only since the expectation is that wireless switches will primarily be used at remote doors where cabling is expensive or difficult. The wireless switches will be fault tolerant enabled for MESHNET applications.

C. I/O switches

VSI is releasing a series of specialized switches to provide additional security functions. These functions include elevator control and input bridges for applications requiring supplemental control over sensors, door contacts, and request to exit devices.

Additional Benefits

A. IT Convergence. As a single database, MESH simplifies the integration of physical and logical security databases. VSI is also developing a modified platform in which door control applets can operate independently of the user database, thereby allowing users to use their existing logical security database as the defacto physical security system.

B. SaaS and the Cloud. As a web based architecture MESH Freedom is inherently designed for SaaS and Cloud applications. In addition, fault tolerant bridges combined with multiple synchronized site or remote servers allow a more stable architecture than is often perceived of Cloud arrays.

C. US Government HSPD-12. When the FIPS-201 standard was set by the US Government, proper deployments were almost predicated on an IT server model. The current control panel model is being found to be extremely expensive, difficult to implement, and not very secure. MESH Freedom bypasses the need for hardware, provides for larger and secure data formats and a more seamless approach to PKI requirements.

D. Cost. Up to 80% of the cost of traditional systems involves the installation of control panels. MESH Freedom eliminates that cost along with reducing service costs, cabling costs and system integration costs.

Summary

VSI sees the future of physical security as one in which card readers and sensors will simply be managed devices within an IT platform and user databases will be managed within the framework of existing logical security databases. This is simply not possible with today's proprietary control panels. For end users, this represents a more sensible and much more affordable approach to physical security.

This new architecture represents a severe technological disruption to the business model of control panel suppliers. However, for major IT suppliers this represents an excellent opportunity to enter an otherwise closed market due to the presence of control panels by providing physical security as a software application using their existing IT architecture and within their existing market channels.

VSI – Freeing the world from the oppression of proprietary hardware

Prepared By:

Stephen Pineau
President and CEO
Viscount Systems Inc.
May 2010