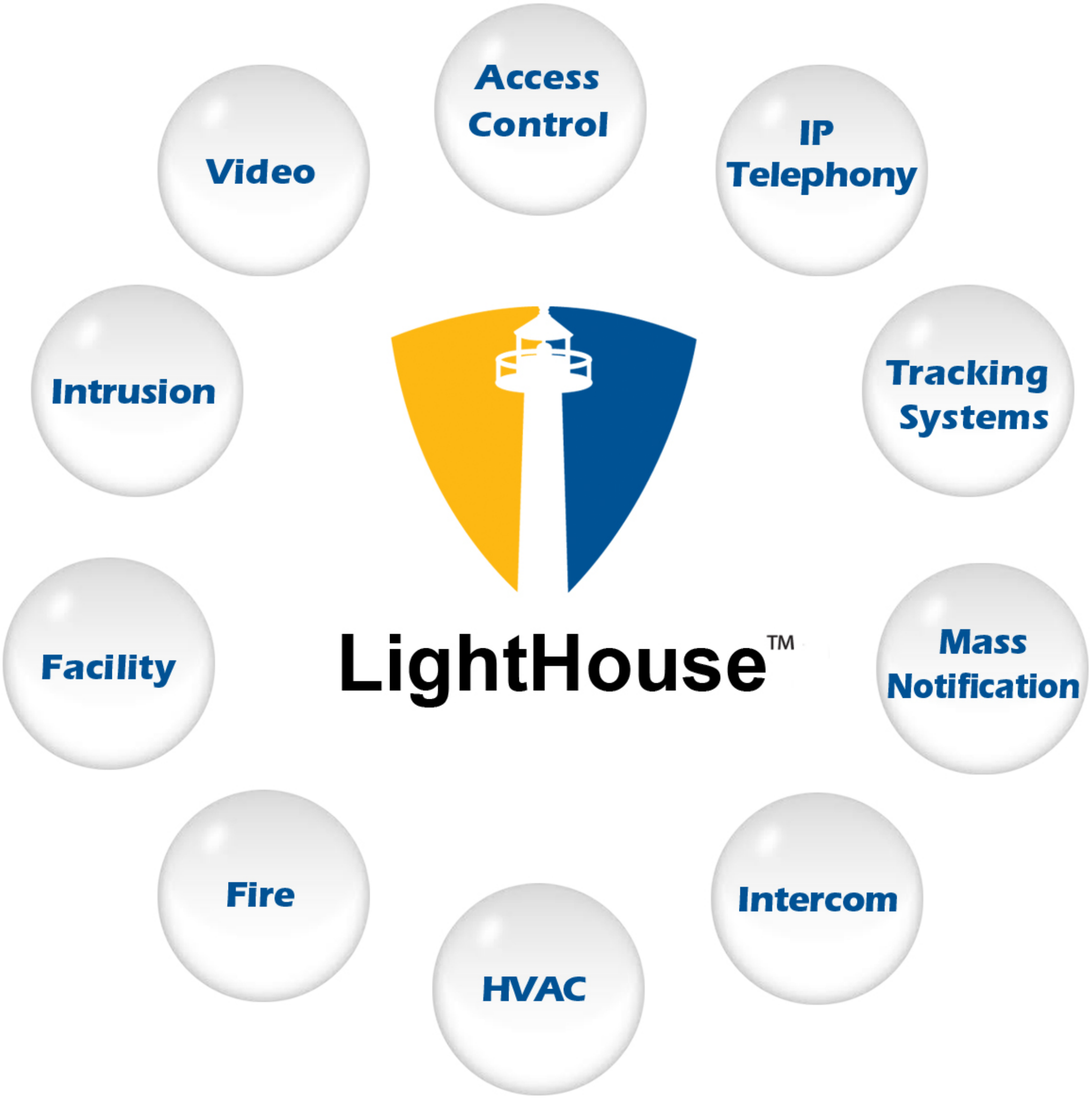
Network Harbor, inc.

LightHouse™

UNIFIED SECURITY MANAGEMENT PLATFORM



Access Control

IP Telephony

Video

Intrusion

Tracking Systems

LightHouse™

Facility

Mass Notification

Fire

Intercom

HVAC

The LightHouse™ system unifies every component of a user's security system in a seamless manner, providing comprehensive control within a single, intuitive interface. It supports virtually any component, sub-system or third-party security product on the market and has been successfully deployed in Federal, Military and Energy based installations as well as municipal and commercial sites.

System Overview

LightHouse™ unifies and manages the following functional areas:

- access control
- video and audio
- fire systems
- emergency management
- facility environmental monitoring
- mass notification
- work flow integrated process management

LightHouse capabilities include:

- Interoperability management
- Permission-based access, monitoring, control
- Encryption and authentication for server/client communications (FIPS 197 and FIPS 140-2)
- Advanced graphics for AutoCAD and raster based graphical maps and vector based icons
- Conditional behavior /policies
- Simple customizable operator/user layouts
- Multiple server /site connectivity
- Common repository for log/history
- Site and workstation lockout and permission based takeover
- Time zone management and reconciliation

Access Control
Mass Notification
CORE Capabilities
Workflow
Video
Audio

The LightHouse Unified Security Management Platform collects, analyzes, and unifies all available information from physical security devices and systems into a single comprehensive view for operator management and control. It provides situational awareness with video, audio (enabling listen-in capability), real-time device status, advanced incident management, and conditional behavior functionality. LightHouse is available as a software package only or pre-installed on server hardware. LightHouse is modular in nature, allowing ease of integration into additional systems in the future. It can support an unlimited number of unique layout views and dashboards for an unlimited number of users.

The LightHouse System Manager is the central server component for any LightHouse system. It securely manages user permissions, client connections, device/object linking, and timed events.

Portals are software components that provide the LightHouse System Manager with specific functionality and capabilities, such as the ability to control and monitor CCTV, intercom, and access control systems. Portals can be created to support virtually any type of electronic system, using any type of communication format including IP-based, serial, or proprietary protocols.

Core Capabilities

- Administrative rights
- User permissions and authentication
- Device management, control & monitoring schedules
- User & group profiles
- Flexible dashboard and display options
- Facility, location, and object mapping
- Encrypted communications
- Sub-system and communications interfaces
- Unlimited conditional behaviors
- Video wall management

Mass Notification
Access Control
CORE Capabilities
Workflow
Video
Audio

The LightHouse System Manager software supports a rich set of core capabilities which are augmented by portals and optional software modules.

The System Manager supervises administrator and user rights and permissions. For each user, one or more profiles are created encompassing screen layouts (dashboards), schedules, workstation permissions, and device interactions.

Client connections are authorized by assigning a client IP address to a user profile for which the user is prompted to select. All communications between clients and the system manager are authenticated and encrypted and support FIPS 140-2 compliance.

The System Manager supports both physical and/or virtual devices within the limitations of the systems integrated and associated hardware. Devices may be associated with other devices to form a device group, for purposes of monitoring and control. User groups may be created to enable the creation of common profiles, properties, rights, and privileges.

The System Manager has the ability to handle control-based and layout-based display synchronization across multiple clients via a common dashboard or layout. It supports facility, location, and object mapping, including display of situational awareness information on rendered drawings, complete with graphical objectification of each monitored component.

The system has the ability to support an unlimited number of conditional behaviors, including those defined by type (time or state based), associated macros, notifications, and override provisions. Macros are defined by the System Administrator.

Central to any system of this type is logging and reporting capability. LightHouse logs all system and user actions for later review. Reports are available for actions and states; devices; and incidents. They may be associated with video recordings and cardholder access.

Portals

- Augment core capabilities
- NERC compliance

The LightHouse System Manager's core capabilities are augmented by plug-in software modules. All plug-in components meet or exceed NERC standards.

Key plug-in modules are defined below.

Access Control Portals

- Complete status and control of access control devices, including door control, arming/disarming alarm points and intrusion zones, and relay activation
- Integrate 3rd party access platforms
- Retrieve cardholder information
- Allow multiple manufacturers in the same view
- Display alarm instructions including image
- Permit logging of user actions
- Provide event history
- Auto-populate feature
- Common look and feel
- Customizable layouts
- Secure communications
- Permission-based controls
- Advanced incident management
- Unlimited schedules
- Allow unlimited device scaling*

* Subject to system hardware limitations

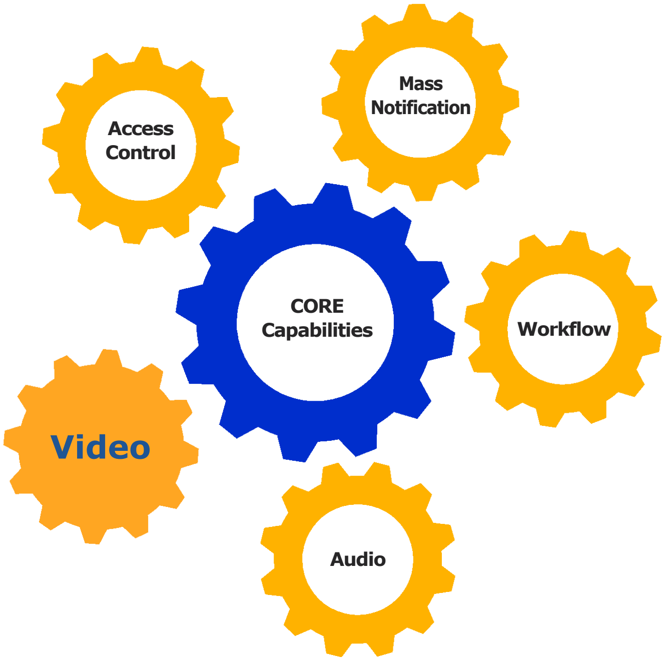
Access Control
Mass Notification
CORE Capabilities
Workflow
Video
Audio

Access Control portals provide real-time status and control of access control system devices, both LightHouse - specific and those connected through third party systems. LightHouse adds features and additional alarm states often not supported by the access control system, such as letting the administrator determine whether to treat supervision or offline states as alarms and whether to treat rejected or noticed cards as alarms. Alarm instructions can be provided by the access control system for display to LightHouse users or instructions can be created specific to LightHouse. All LightHouse user actions affecting access control system devices can be logged by the access control system (if supported by the access control system) and are also logged in LightHouse system logs. Audio and video associated with the alarms are also referenced in the LightHouse logs and can be retrieved while reviewing the logs. LightHouse adds advanced incident management functionality to access control systems that lack it. LightHouse allows seamless user control of multiple access control systems (and multiple independent systems from the same manufacturer) to be monitored and controlled from the same LightHouse client workstation. LightHouse provides a common control method and common look and feel to allow users to become familiar and skilled with one master interface. Most access control systems allow auto-population of LightHouse devices. That means access control devices require little (often no) setup within LightHouse. As devices are added, removed, or reconfigured on the access control system, they are automatically updated in LightHouse. Secure communications is provided with FIPS 197 and FIPS 140-2 compliance for encryption and authentication for all server/client communications

Video Portals

- Integrate 3rd party video platforms
- Allow unlimited video scaling*
- Common user interface
- User, event, or schedule triggered recording
- Receives alarms from video platform
- Automatic map display
- Presets & sequences
- Display control & customization

* Subject to system hardware limitations

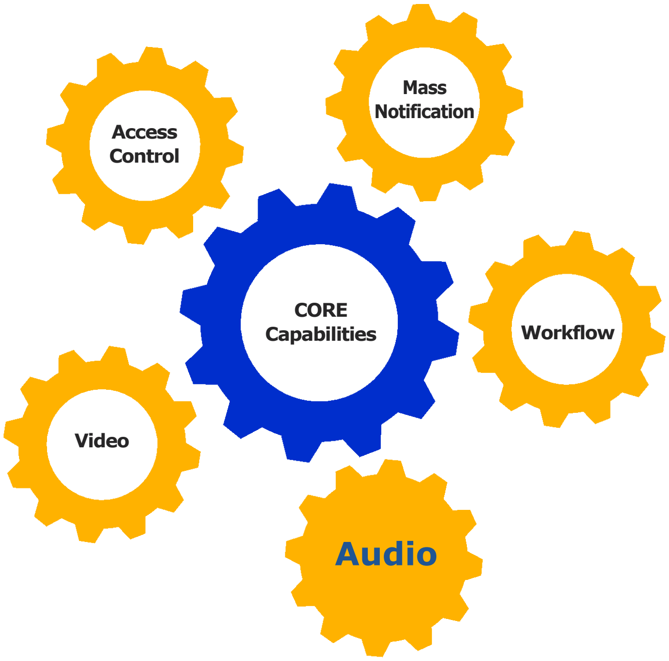


Video portals serve as integration components for 3rd party bringing their capabilities into the LightHouse environment. This means that devices connected to the system can trigger video recording, live displays and notifications. Alarms from the video system , e.g., from an analytic routine, may be associated with actions programmed in the core platform. In short, the full functionality of the external video management system is preserved while its ultimate functionality is magnified by LightHouse. The Video Management System integrates third-party products such as IP-based cameras, NVR systems, DVR systems, and analog matrix CCTV switchers using portals specifically designed for each system. These portals include components that reside on the LightHouse Server and most have components, such as setup forms, that are streamed to the clients as necessary. This architecture allows connection to multiple manufacturers' products concurrently. All camera devices thus become part of the system and can be displayed in mix and match fashion.

Audio Portals

- Integrate 3rd party audio platforms
- Support multiple manufacturers concurrently
- Secure managed audio
- Allow unlimited audio scaling*
- Common user interface
- Intercom control
- Audio recording and play
- Automatic map display
- SIP and RTP support
- Device status display
- Support for legacy serial/analog systems

* Subject to system hardware limitations

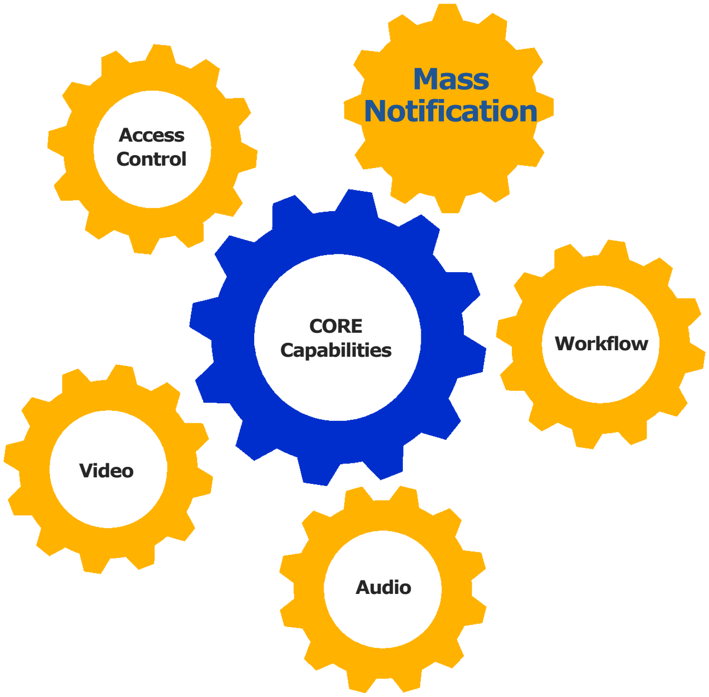


The Audio portals module serves as the integration component for 3rd party audio platforms, bringing their capabilities into the LightHouse environment. The system will obtain and display state information from devices on the audio platform, perform scripted functions on integration platform devices based upon time and audio platform device state, and place audio calls from the integration platform client. It will associate in logs the relationship between actions causing or caused by an intercom call, from either incident management or scripted functions. It allows search and playback of recorded and pre-recorded audio. Further, the plug-in provides a rich set of intercom management functions, both from Network Harbor's own intercom devices or 3rd party. It supports 3rd party SIP servers.

Mass Notification Portals

- Integrate 3rd party mass notification and emergency communication platforms
- Bridge devices, events, and policies to the notification system
- Provide communication status to operators

Mass Notification portals allows LightHouse to send event notifications to third party mass notification systems to trigger the appropriate outbound communication. Data acquisition, system logic, and policy enforcement are handled by LightHouse while the task of communication to appropriate parties is handled by the third party mass notification system.



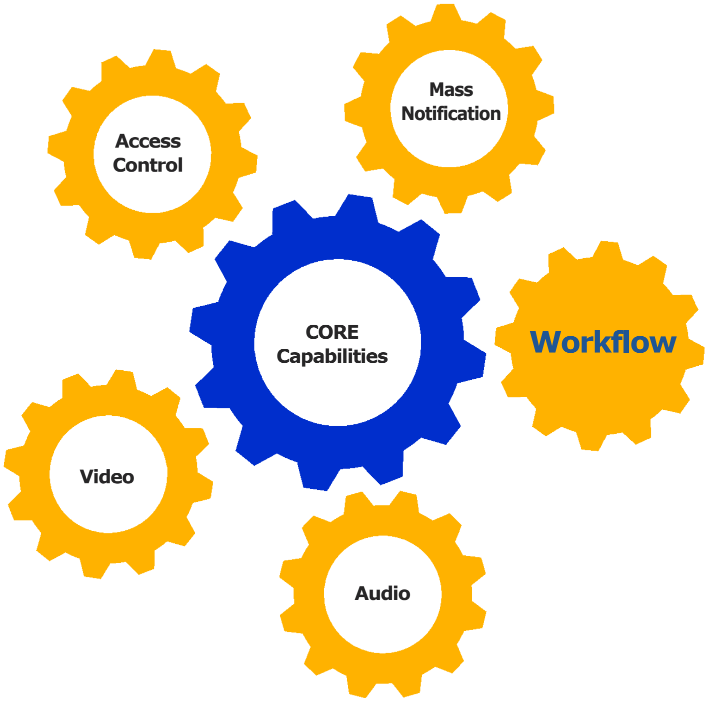
Alerts generated by the Portal and sent to the notification system honor that system's user preferences regarding delivery method and priority. Through the portal, LightHouse will attempt to deliver messaging to desktop pop-ups, mobile phones, work phones, SMS/text messaging, and work e-mail devices. LightHouse operators will receive status of notifications and which recipients have not acknowledged.

Workflow Portals

- Customize user and system actions
- Create action triggers based on device states, external actions, and user intervention
- Allow unlimited process scaling*
- Real time workflow display, including current state
- Workflow step printout capability
- Logging and reporting

* Subject to system hardware limitations

Workflow portals extends the conditional behavior and policy support embedded in the system's core capabilities to true workflow and task management. LightHouse presents an architectural model that provides for virtually unlimited extensibility allowing new input triggers, output actions, and decision steps to be created. The Workflow portal serves as the task manager and system director connecting physical events to initiate a workflow process. It assigns and tracks tasks; provides e-mail notification of tasks assigned and query results; assigns time frames and contingent actions; and more.



System Specifications

System Manager Functions

- Audio management via SIP and RTP
- Scalability
- Multi-site capability
- Location based monitoring and control
- Rights and permissions
    - Admin
    - Users
- Profiles
    - Establishment of characteristics
    - User Dashboard configurations
    - User and monitor access
    - Schedules
    - Map Access
- Dashboard Layout Options
    - 1 x 1 to 4 x 4
    - User information
    - Interaction controls
    - Placed information
    - Dynamic resizing of grid elements
- Client connection management
- Portals (function-specific software components)
    - Support for unlimited number
- Devices
    - Support for physical and virtual devices
    - Graphical icon representation
    - Support for device groups
    - Support for device linkage
    - User privileges
- Mapping
    - Native rendering and user directed scaling of vector-based drawings (including direct display of AutoCAD™ .DWG file drawings)
    - Native rendering of raster-based drawings, or bitmaps
    - Situational awareness information with component graphical objects
- Schedules
    - Format definition
    - Automatic time zone reconciliation
- Macro Definitions
    - Command Type - timed wait, single device, multiple device/device groups, timed reciprocating device, transmit system message, transmit non-system message
    - Priority value
- Actions
    - Support unlimited conditional behaviors
    - Classifications - type, associated macro, notifications, override provisions
- Logs and Reports
    - All system and user actions
    - Actions and states - date/time, command identification, devices commanded, initiating entity
    - Devices - device ID, state entered
    - Report export
    - Information association - video recording, audio recording, cardholder access
- Displays
    - Video wall support
    - Command and control wall support

Portals

- Access Control
- Video
- Audio
- Mass Notification
- Workflow Management
- Real-time location systems

Software Plug-Ins

- Active Directory
- Real-time Locating System
- Timed and Linked Events
- External Web-hosted Content
- Basic Challenge Logon

Additional Network Harbor System Options

- Personnel record and identity management
- Visitor management
- GIS

Specifications

Server Software

Operating Systems (Microsoft)

Windows Server 2003 or 2008
Windows 7 Professional

Framework	.NET

Database

Software	Microsoft SQL Server 2012
Data Structure	XML

Hardware Requirements

Server

Processor	Quad core
RAM	16 GB
Storage	3 TB usable minimum RAID 5 minimum
Power Supplies	Redundant Hot Swappable

Client PC

Operating System
Windows 7 (or later) or
Windows Server 2002 (or later)

RAM 16 GB

Video Outputs - as required to support local requirement

Command/control Wall or
Video Wall Application Host

Operating System
Windows 7 (or later) or
Windows Server 2002 (or later)

RAM 16 GB

Video Outputs required to support wall requirements

Server - Client Communications

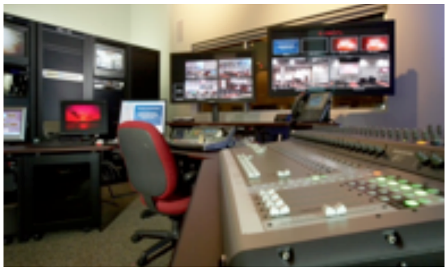
Encryption

Initialization	RSA-2048
Messaging	AES-256
Authentication	SHA-2
Compliance	FIPS 140-2 FIPS 197

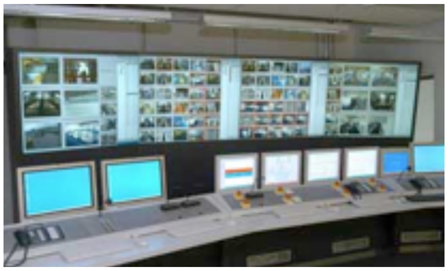
Server - Portal Communications

IP networks	Supported protocols include IPv4, IPv6, TCP, UDP, DHCP. DNS. FTP. SMTP, SNMP, HTTP, HTTPS
Serial networks	RS-232, RS-422, RS-485
Proprietary	consult factory

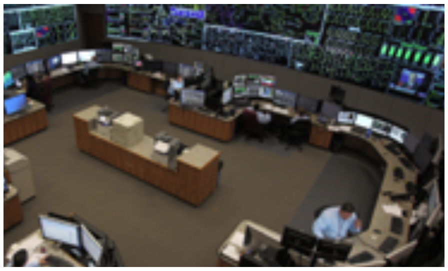
Markets



Military



Airports



Utilities

Universities

About Network Harbor, Inc.

Founded in 2005, Network Harbor, Inc. is a privately held company based in Bartonville, IL. Network Harbor executive management and development staff have over 20 years in security integration development.