

Interfacing ISONAS Access Control to an IVC-controlled Video Surveillance System

To provide more flexibility and scalability for comprehensive security systems, more components are becoming IP enabled. This is true for video cameras, access control systems, perimeter security, and other key system components. This white paper explains how IP video camera systems from IVC and IP access control systems from ISONAS can be integrated to provide a more automated and complete solution.

The intended audience for the executive summary of this white paper is the information technology manager or facility security manager. For the detailed discussion, the intended audience is the network or security engineer responsible for facility security and personnel access control.

The integration between an IVC camera system and ISONAS access control system is designed to automate the recording of facility access by authorized and unauthorized personnel and record causes of tampering or fault alarms initiated by the access control system.

Executive Summary

Heightened security concerns at critical and remote facilities have created a need for more secure access control to these locations. Traditional gate and access control systems are no longer sufficient. Users now want video confirmation and event recording at these facility access points. Video confirmation adds a higher level of security and ensures that only authorized personnel are using the premises. It also provides the advantage of registering and viewing unauthorized access attempts.

IVC's video surveillance systems are comprised of cameras and camera management software. The primary functions of IVC's camera management software include the following:

- Provide single IP address access to large network of cameras.
- Provide web-based GUI for users to view video, control cameras, initiate recording, and playback recorded video.
- Serve video from the camera network to View Station or 3rd party clients.
- Provide a means for creating unlimited user-defined, multi-up, multi-monitor displays.
- Automate camera and system functions through the use of schedules.
- Manage alarms from cameras and other devices on the network.

IVC's software-based video surveillance systems provide tools for easy integration of IP-enabled security components. IVC's View Station Alarm Server provides the

mechanism for this integration. A true server application, the Alarm Server sits on the user's network and listens for alarms of varying types and from any source. IVC has recently modified its Alarm Server to recognize alarms from the ISONAS IP-based access control system.

ISONAS IP Door Reader-Controllers connect direct to the same network to which the camera system is connected. The panel-free system, featuring ISONAS Crystal Matrix Software™, places real-time control of enrollment, access, time & attendance and emergency response, in the hands of an authorized security administrator.

ISONAS PowerNet IP Readers are true network devices designed using IP standards and technology. Once installed, the reader-controllers use TCP/IP to open a dialogue with the ISONAS Crystal Matrix Software™ and respond to specific preprogrammed commands and parameters.

Alarm messages from the ISONAS system are initiated when the system determines the occurrence of an authorized or unauthorized access event or tampering of the card reader or keypad. Once an ISONAS alarm message is detected by the View Station Alarm Server and the alarm source and type is identified, any number of responses can be automatically initiated. These could include:

- Log the alarm for presentation in the View Station GUI
- Archive the alarm in an SQL database
- Present a visual cue to the security operator
- If PTZ camera at or near alarm source location, move and/or zoom camera
- Save video recording of activity at alarm source location
- Issue email notification to other parties (security personnel, first responders, etc)
- Issue commands to access control system (enable or disable access)
- Issue commands to other devices or software connected to the network

Key advantages of a fully integrated, IP-based video and access control system include:

Cost - Since an IP-based approach relies more on software and less on high-cost proprietary hardware, the installation costs per reader and per camera are significantly less than traditional analog approaches. Customers can realize additional cost savings by using existing network cabling and/or, where possible, power readers and cameras using Power over Ethernet technology. No specialized hardware is needed for storage of events and video; standard network-addressable storage is sufficient further reducing the cost of ownership. Since it is possible to remotely configure and troubleshoot these systems, installation and maintenance costs are also greatly reduced.

Ease of installation and maintenance - The physical installation of readers and cameras on a network is not much more complicated than installing a network printer. ISONAS and IVC systems are essentially software-based systems. Installation and

configuration, addition of new or custom features, system upgrades, and troubleshooting either by the customer or the vendor can be easily accomplished remotely. Factory-assisted installation and support ensures speedy installation and greater system up-time.

Operational Responsibilities

The network engineer responsible for managing devices on the security network must do some configuration work when the IVC Relay Server software, IVC View Station software, and ISONAS Crystal Matrix software are installed in the enterprise. The network engineer will also have to oversee the installation of cameras, readers, switches, midspans, and other network appliances required for a functional system

The facilities engineer or an electrician will be required to install camera and card reader hardware.

The operation of the system is transparent to end-users, who simply supply their standard access credentials to obtain entry or exit from the facility.

System responses to authorized or unauthorized entry are fully programmable and will vary from application to application. However, in most cases, these are likely to be automatic and require little or no intervention by security personnel. View Station will have to be set up to present the operator necessary views and direction to react to specific events. Security and executive management will need to develop policies and procedures incorporating the tools provided by this solution in order to provide required levels of security.

ISONAS IP Access Control System

All ISONAS IP Door Reader-Controllers connect directly to the data network via existing LAN wiring. This panel-free system, featuring ISONAS Crystal Matrix Software™, places real-time control of enrollment, access, time & attendance and emergency response, in the hands of authorized security administrators. ISONAS PowerNet IP Readers are “true network devices” designed using IP standards and technology. Once installed, the reader-controllers use TCP/IP to open a dialogue with the ISONAS Crystal Matrix Software™ and await specific commands and parameters. This “plug and play” configuration is easier to install than traditional panel-based systems. The streamlining of installation, maintenance and integration results in significant cost-savings.

The ISONAS Crystal Matrix software package is a fully featured Access Control software system. It provides fine-detailed level control of all access security related issues. Reports are available for all system activity, as well as real time reporting on who is currently in the facility.

Real-time monitoring of the system’s activity includes the display of card holder images and floor plans, as well as Operator Override operations such as lock-downs and manual door operations. The system also supports display of configurable alarm conditions.

The Crystal Matrix Software can initiate automatic actions, such as the scheduled unlocking and locking of doors, through its scheduling features, or the execution of user-configurable custom action-sets through its scripting features.

When installing the software, the user has the option of installing several components. For integration with the IVC video management system, the following Crystal Matrix Software components must be installed:

Crystal Access Administrator

This is the administrative application (ISONAS.exe). It provides all of the facilities used to define the system and how it should operate, including the definition of people, assignment of badges, definition of doors and shifts and definition of permissions. It is only necessary for this program to be run when defining or revising this information. If the access control system is installed on a computer which is connected to a network, there can be many different computers in the network that are used from time to time to update the database that defines the system and how it operates.

Crystal Access Monitor

This is the Monitor and Operations application (crystal.exe). It displays the current state and ongoing activity of the door controllers. If operations are enabled, it will allow the operator to manually unlatch a door, LOCK or UNLOCK a door, clear ALARMS or remove people from the “IN” list which is used to prevent “Passback” of badges so that multiple entries to the facility can be done with the same badge credential. It is not necessary for the Monitor and Operations program to be running for the access control

system to be operating. In a network installation, there may be many copies of the Crystal.exe program running at the same time.

Controller Supervisor

The Controller Supervisor (CSUP) program is the application that is actively communicating with the door controllers. In a complex system there may be multiple servers defined, and each server may have multiple connections. There must be one copy of the CUSP running for each different server in the system. If the CUSP is not running, the controllers attached to it will drop into “standalone” mode and make decisions locally about whether or not to allow access for a given badge.

Interfaces – INRServ (ISONAS Notification Request Server)

The INRServ program provides easy access to ISONAS supported interfaces including SNMP, ISOAscii, and TCP/IP as well as a testing environment for IADI. The INRServ creates and sends reader alarm messages via TCP/IP onto the network. As the diagram below illustrates, the IVC Alarm Server will read and parse these messages to determine the source of the alarm and then initiate programmed responses specific to the alarm type and source. Responses may include commands to the IVC camera management software or to other device or software on the network.

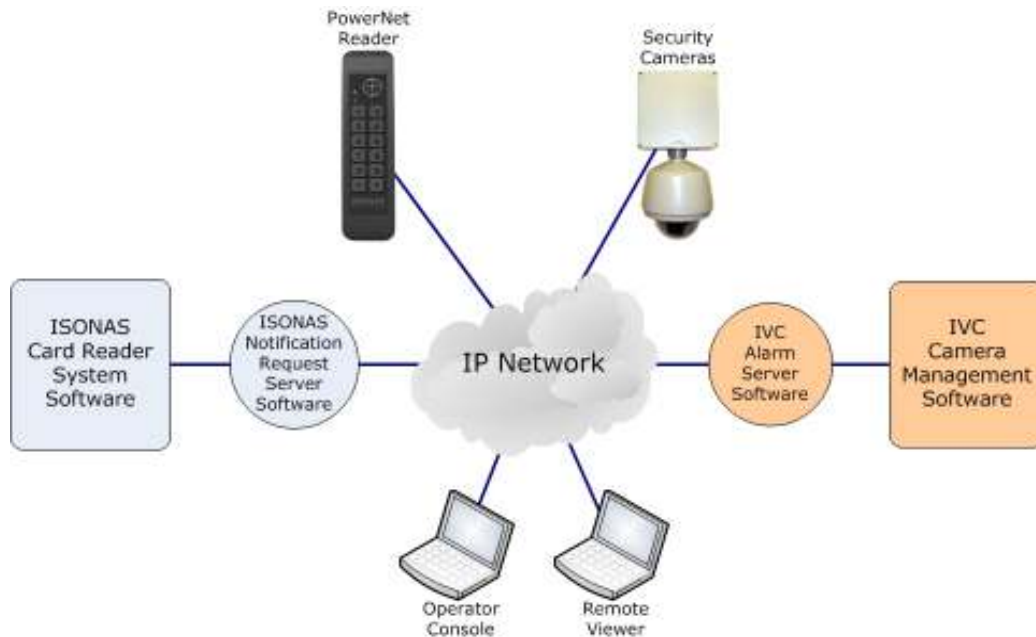


Fig. 1

IVC Camera Management System

IVC's integrated video management solution incorporates IVC's Relay Server, Alarm Server, Tour Server, and View Station software products. IVC's Relay Server software is the central component of this state-of-the-art software suite. The IVC system architecture is built on modularized component services that provide an extendable platform for building sophisticated features and functionalities:

| | |
|-------------------------|---|
| Core Services: | Relay Server, Tour Server, and Alarm Server |
| Integration Components: | ivc_ax , IVC Player, URL API |
| Interface for Viewing: | View Station |

These software components work seamlessly together to become a complete, coherent solution or an extensible part of an integrated solution.

IVC software is a standards-based, state-of-the-art solution for surveillance-related applications. The system architecture is built on modularized component services that provide an extensible platform for building sophisticated features and functionalities. The Relay Server, Tour Server and Alarm Server provide the core services. The ivc_ax and IVC Player components allow easy integration of video surveillance applications.

At the heart of the IVC Camera Management Software Suite is the core service, Relay Server. The IVC Relay Server is a scalable and complete camera management solution. Because of its standard browser interface, the surveillance experience begins from a standard web browser such as Microsoft's Internet Explorer. All of the camera video and controls are unified under the Relay Server software. A comprehensive HTTP URL API provides the View Station client program, third party software and other system devices access to the cameras. The supported digital media for the audio and video is also standards-based. For video media, M-JPEG, MPEG4, and H.264 are supported. Additional functions of the Relay Server software include:

- Video storage management
- Video network bandwidth management
- User authentication

Regardless of the complexity of the surveillance system, the solution is powerful but also easy to implement and use. Any TCP/IP network backbone is sufficient for wired and/or wireless installations.

Any LAN, WAN and VPN client that have proper access rights can perform live monitoring and control. Multiple streams can be accessed simultaneously from the

View Station, browsers and third party software. The live media is delivered as soon as it is captured, and stored media is available for instant playback.

The IVC Relay Server camera management software is designed to be scalable to grow along with the number of cameras on the network. Multiple servers can be deployed as peers to distribute the load, or they can be arranged in a hierarchy with server-to-server functionality. One to hundreds of cameras can easily be managed anywhere on the network from a simple web browser and/or a feature-rich client application. Figure 2 illustrates how a distributed video network may be deployed using IVC software.



Fig. 2

IVC View Station Software

IVC's View Station software component is a full-feature front-end for the IVC camera system. It will allow any single View Station location to manage and view 100s of cameras as if they were on a single physical Relay Server. Any system camera can be accessed through the View Station's intuitive user interface. View Station is a client program that presents video and data from potentially multiple instances of Relay Server, Tour Server and Alarm Server to customizable displays. View Station's customizable layout feature permits the tailoring of displays to meet the special requirements of the site. Live video, camera control, playback, custom command buttons, tour statuses, and alarm notification windows can be mixed and matched in any combination to give a bulls-eye view of the monitoring operation. Multiple views can be running simultaneously and multiple screens are supported. Live video feeds can be displayed full screen or rotating through multiple-feed scans.

For alarm handling, the View Station software integrates seamlessly with the Alarm Server component (described below). Audible and visual alerts are provided to the corresponding camera video window to alert the operator to the alarm condition. Video relating to the alarm event can be instantly replayed. All of these rich features make the IVC surveillance solution complete and coherent.

Alarm Server Component

The core service, Alarm Server, is a flexible software component designed to react to a variety input triggers and generate output events to pre-defined destinations. As Figure 3 indicates, input trigger sources may include, but are not limited to, camera in-video motion detection, intelligent video object detection, access control devices, discrete sensors, and process monitoring. The drawing also shows that the Alarm Server offers similar flexibility in response definition.

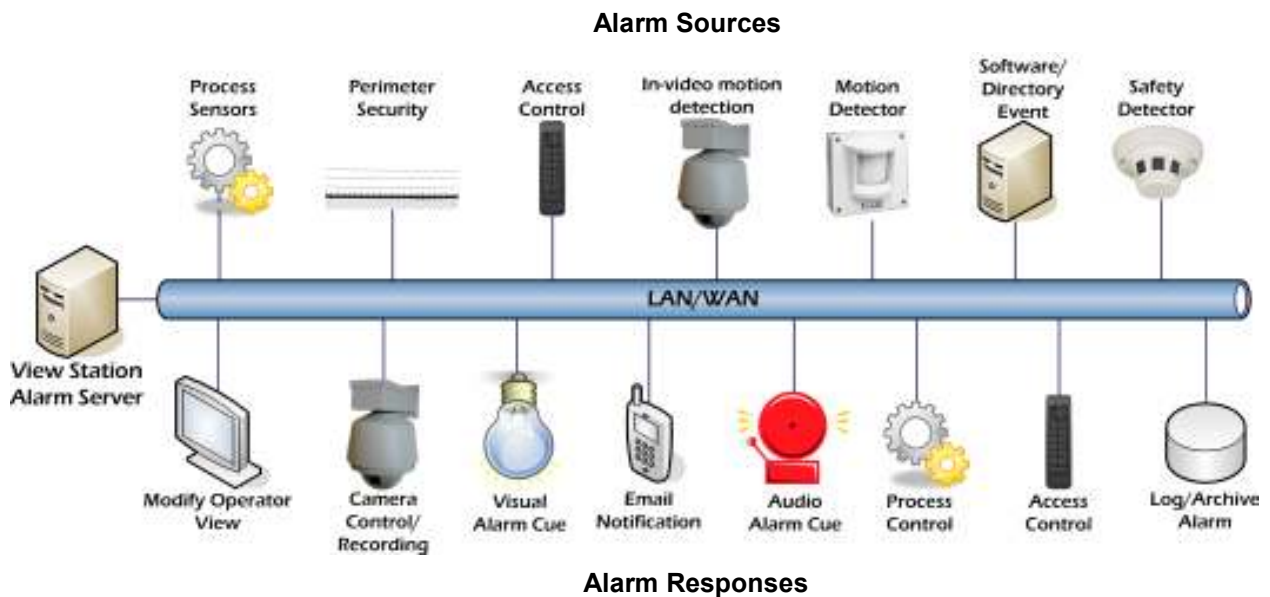


Fig. 3

As designed, the Alarm Server acts as an integration tool, providing the means to integrate other security or system components with the video system. It is this mechanism that is used to integrate ISONAS access control systems with an IVC video system.

Integration of ISONAS and IVC systems

To facilitate integration of ISONAS IP access control systems and IVC video systems, IVC has added specific support of the ISONAS system to its Alarm Server.

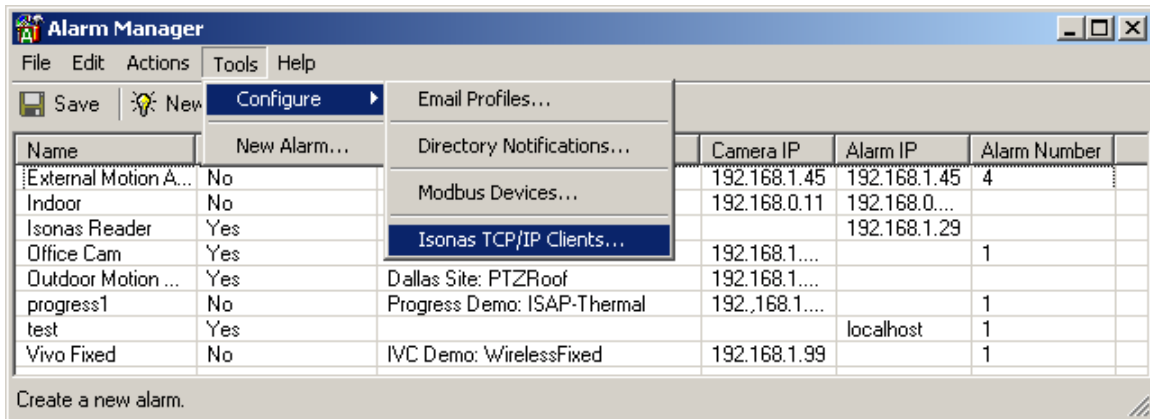


Fig. 4

Using dialogs designed for the ISONAS system, users identify the IP address and port number of the ISONAS Notification Request Server (INRServ) connected to the reader for which the user wishes to create an alarm and corresponding response definitions. Once the IVC Alarm Server is aware of an INRServ, the user may then create specific reader alarms.

In general, to specify an alarm from specific reader, the user must:

1. Name the alarm
2. Identify the alarm source
3. Specify alarm responses

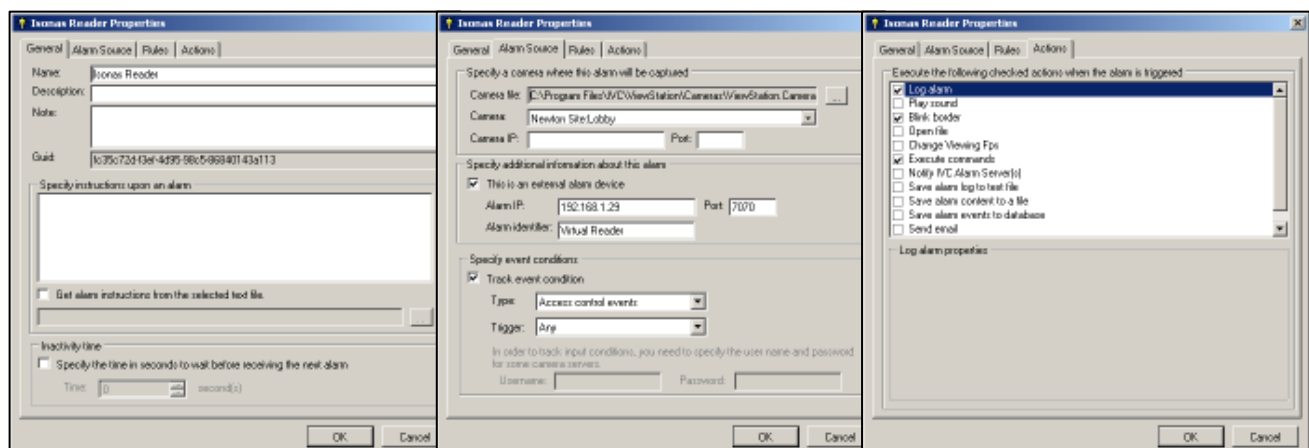


Fig. 5

It is important to note that the IVC alarm system provides the ability to generate multiple alarm types for each reader. To simplify the interface, IVC grouped all possible alarms generated by an ISONAS reader into one of five categories. As shown in Figure 6, the user chooses one of these categories in step 2 of the alarm definition process.

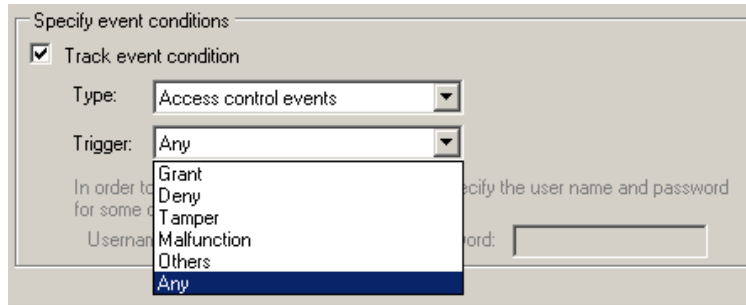


Fig.6

The chart below lists how the ISONAS event conditions are mapped to these groups.

| ISONAS Event Notification | IVC Access Control Event Trigger |
|---------------------------|----------------------------------|
| REJECT | Deny |
| ADMIT | Grant |
| UNAUTHORIZED OPEN | Malfunction |
| TAMPER | Tamper |
| AUX | Others |
| REX | Others |
| EXTENDED OPEN | Others |
| CONTROLLER FAILURE | Malfunction |
| LOCKDOWN | Others |
| UNLOCKED | Others |
| NORMAL RESET | Others |
| REJECT PASSBACK | Deny |
| REJECT EXPIRED | Deny |
| REJECT OVER LIMIT | Deny |
| REJECT TAMPER | Deny |
| OPERATIONS ADMIT | Others |
| OPENED | Grant |
| CLOSED | Others |
| CLEAR ALARM | Others |
| LOCAL RESET | Others |
| ARM DUAL AUTHORIZATION | Others |
| INPUT POINT TRUE | Others |
| INPUT POINT FALSE | Others |
| OUTPUT POINT TRUE | Others |
| OUTPUT POINT FALSE | Others |

Given that the complete system is IP-based, alarm responses are not limited to camera operations. In addition to moving cameras and recording video, an alarm response may include one or more of the following:

- Log the alarm so it is listed in the Alarm Log window in a View Station screen
- Provide an audio cue to the operator
- Provide a visual cue to the operator
 - Automatically change operators monitor view (e.g. switch to full screen view of associated camera video)
 - Blink border of related camera video window
 - Actuate discreet visual device, such as a warning light
- Change the viewing frame rate of all live video windows within the current view
- Execute commands for one or more of the following:
 - Commands to the IVC Relay Server to control cameras, initiate recording
 - Alarm Server commands to enable/disable alarms
 - URL commands to other devices and software on the network, such as the ISONAS reader
 - Windows commands
 - Special commands added by IVC to support custom applications
- Notify other Alarm Servers running on the network
- Save the Alarm in a database
- Send an email notification

The IVC Alarm Server is architected in such a way that it is relatively easy to add support for other alarm protocols and to add component specific response capabilities.

A typical response to an access control alarm generated by an ISONAS reader might be to log the alarm, unlock the door or lift the gate, move the camera, and record the person causing the alarm. The IVC Alarm Server certainly provides the capability to generate this type of response. However, as illustrated above, the response to this alarm can be much more. For most benign alarms, such as authorized entry, no other response may be required. For an attempted unauthorized access or tampering alarm, however, the user may want to include additional response activities, such as alerting security personnel or off-property authorities.

Conclusion

In the Executive summary of this paper, the advantages of an IP-based system, such as the one described here, were enumerated. These advantages can apply to almost any IP-based system. Clearly the trend in the security products market is moving to IP.

However, at some point, someone has to make all the various components required for a comprehensive security system work together. IVC and ISONAS have worked independently to engineer high-quality products with open, well-documented interfaces. These companies have also cooperated to add features and interfaces to their products, making it easier for customers to install these distinct systems and build highly integrated, cohesive security systems.

For customers that require access control with video surveillance, the solution described here will provide users a system that is highly cost-effective and easy to use, maintain, and expand.

For more information contact:

Industrial Video & Control
617-359-4617
info@ivcco.com
www.ivcco.com

ISONAS
800/581-0083
sales@isonas.com
www.isonas.com