Software-based Alarm Receiver Enhances Central Station Efficiency and Performance

SCS-VR Virtual Receiver from Digital Monitoring Products breaks new ground

For decades central station alarm receivers have used a combination of hardware and software. Dedicated hardware was required because the receiver needed to accept alarm signals sent over traditional telephone lines. But as the security industry has shifted more heavily toward alternative forms of alarm communications based on network, Internet and cellular alarm communications, it has become technically possible to create a software-based or virtual receiver that runs on one or more standard servers and receives alarm communications over a data network connection.

This is the approach used on the SCS-VR virtual receiver from DMP. The SCS-VR works with panels that use DMP network alarm messaging and with a range of automation software. The SCS-VR works with the Microsoft SQL Server 2005 or SQL Server 2008, and has the ability to run on more than one server from the same database. The SCS-VR software accepts alarms from network, Internet or cellular communicators and is UL listed to the UL 1610 Central Station Alarm Standard Receivers and UL 1076 for Proprietary Alarm Receivers.

The SCS-VR offers a wide range of benefits for alarm dealers and central station operators, including:

- Scalability

- The wide area network inputs monitor the status and condition of one another and back each other up, enhancing panels' ability to reach the receiver and supporting redundant communications service providers on a single receiver

- Software can be deployed on multiple servers to support a geographically distributed approach with path protection and minimize nuisance supervision failure messages for high-security applications

- Greater processing power for extensive diagnostics

- Group capability enables a single receiver to function as multiple separate receivers, each with its own unique programming

- Support for automatic software updates

- Power and space savings

- Critical UL listings

In this white paper, we explore these benefits and how the SCS-VR achieves them.

Scalability

Central stations can purchase SCS-VR licenses for as few as 500 or as many as 20,000 panels. (Support for more than 20,000 panels is available upon request.) At any time, users can purchase a license for additional capacity, enabling them to quickly expand their monitoring capacity without additional hardware.

The wide area network inputs monitor the status and condition of one another and back each other up, enhancing panels' ability to reach the receiver and supporting redundant communications service providers on a single receiver.

Whether a panel uses a cellular, Internet or other IP data network connection to the central station, the link to the central station receiver is through an IP network. The SCS-VR can be licensed to support from one to a virtually unlimited number of wide area IP network connections.

If the central station operator chooses at least two IP network connections, which can be from two different service providers, the ability of customer panels to reach the receiver will be enhanced. The reason is that IP communications use a destination data address—in this case the data address of the central station receiver. Unlike with traditional phone line communications, which use a fixed pre-established path to the central station, an IP communicator can take multiple paths through the IP network to reach the central station.
This means that if one of the redundant paths into the receiver is blocked, the communication signals will seek an alternate route, as long as they can get to the service provider network. But that functionality is only possible with a receiver such as the SCS-VR that supports IP communications over multiple wide area network connections.

It's important to recognize that if there is only a single wide area network connection at the customer end of the connection and that link experiences a communication problem, alarm signals would fail to go through to either a traditional or software-based receiver. It's worth noting, though, that often these outages are temporary and the communication gets through on a subsequent attempt.

To maximize the likelihood that alarm communications will get through, both the customer location and the central station receiver should have redundant wide area network connections—an option that is easily supported with a software-based receiver approach. Redundant wide area network connections to a central station and to the customer site are a key requirement for high-security applications such as jewelry stores.

SCS-VR software can be deployed on multiple servers to support a geographically distributed approach with path protection—and minimize nuisance supervision failure messages for high-security applications.

To further enhance the communications link to customers, the SCS-VR software can be deployed on multiple servers in different geographic locations. This can help ensure that alarm communications get through even in the case of a disaster or major network outage affecting an entire geographic area.

Although geographic redundancy was an option in the past, each geographic location had its own central station receiver—and because most central station automation software systems can accept a connection from only a single receiver, the central station operator had to manage and maintain two separate customer databases.

The SCS-VR eliminates this requirement because the geographically dispersed servers continue to operate as a single logical system. Servers have the ability to communicate with each other and each server backs up the other servers in the system. The system also can be set up to automatically balance the workload among all of the servers.

This approach also minimizes supervision failure messages. The reason is that if there is congestion or a problem in the portion of the network between where a high-security business customer connects to its service provider and one of the central station locations, the communications will be routed to another central station without sending a supervision failure or path-down message. If, instead, two hardware-based central stations were involved, communications would switch over to the second central station, but the automation system would still register a supervision failure or path-down message from the first receiver, potentially entailing the expense of sending a runner to the customer location.

When used with DMP panel models XR500N, XR500E, and XR100N, the SCS-VR also can minimize the need for a runner when a communications problem occurs on the link between the customer site and the customer's service

provider. These panels are UL-approved for high-security installations using an IP network connection as the primary communications link with cellular backup--and they support a unique capability called "Adaptive Technology", that adds supervision to the cellular backup link if the primary IP link experiences a supervision failure, thereby eliminating the need for a runner.

Extensive diagnostics
The SCS-VR has more processing power than a typical hardware-based receiver, which enables it to provide more sophisticated diagnostic capabilities, including:

- Panels currently in substitution failure

- Panels not currently checking in

- Average bandwidth per panel

- Recent bandwidth per panel

- Average bandwidth per group of panels

- Show panels that use excessive bandwidth

- Time of last check-in message received per panel

- Time of last message received per panel, plus the text of the message

- IP address of each panel

- Show which panels use encryption and which do not

- Show when the IP address of a panel has changed

Group capability
Group capability in the SCS-VR enables central station operators to essentially divide a single receiver into multiple receivers, each with its own unique programming. This capability lets the central station establish different message handling rules for each group on a receiver. It's particularly useful for wholesale central station operators as a means of establishing different default procedures for different dealers, streamlining the process of setting up new accounts.

Automatic software updates
By leveraging the SCS-VR's network connectivity, DMP is able to provide automatic software updates in a totally transparent manner. Central stations can use an optional network upgrade sharing service to automatically distribute updates to all nodes attached to the current database.

Power and space savings
A software-based virtual receiver consumes less power and requires less space in the central station than a hardware-based counterpart.

UL listings

The SCS-VR software-based virtual receiver has ANSI/UL 1610 approval for Central Station Alarm Receivers and ANSI/UL 1076 approval for Proprietary Alarm Receivers. The 1610 standard applies to components intended for use in a burglar alarm system in which the operations of electrical protection circuits and devices are transmitted automatically to, recorded in, maintained from, and supervised from a central-station that employs trained operators and alarm investigators who are in attendance at all times. The 1076 standard applies to a system in which the central supervising station is located at the protected property and intended for operation by personnel responsible to the owner of the protected property, which may consist of a single property or of noncontiguous properties under a single ownership.

In meeting the requirements of the ANSI/UL 1610 and ANSI/UL 1076 standards, the SCS-VR supports critical capabilities such as compromise testing, supervision for high-line security, and AES encryption. Underwriters Laboratories has created a new listing category for software-based receivers with the designation UZSA.

DMP is a privately held independent manufacturer of innovative intrusion, fire, access control, network and cellular communication products that are designed and made in the United States of America. DMP is the recognized leader in alarm communication over data networks, with products that are available through professional electronic security companies. For more information visit www.dmp.com.

DMP Digital Monitoring Products

800-641-4282	INTRUSION • FIRE • ACCESS • NETWORKS
www.dmp.com	2500 N. Partnership Boulevard
Made in the USA	Springfield, Missouri 65803-8877

MADE IN U.S.A.