Teldat Group

IP Alarm System Resiliency on Disaster Recovery and ISP changes

A better alternative to DNS-based solutions

INDEX

Overview

Several IP Alarm providers have claimed for DNS-based[1] solutions as the unique means for overcoming the typical challenges identified in a commercial IP Alarm Monitoring service:

- In order to benefit from the most competitive rates, the CMS may need to change its Internet Service Provider to a new one. This change should be carried out with little effort in the CMS and should not imply manual reprogramming of the IP Communicator units.

- During disasters, the IP Communicators should switch to an alternative CMS automatically.

- IP Communicators on Alarm Panels should not be locked to a specific CMS. In other words, changing the IP Communicators to a new commercial CMS should not imply manual reprogramming of the units on the field.

Although the DNS gives an answer to these challenges, it suffers from severe limitations that may put the IP Alarm Monitoring Service into jeopardy. As such, the FireLite IP Alarm System uses an alternative approach which not only gives an answer to these challenges, but also does not suffer from the inherent limitations of the DNS service.

[1] **DNS**: **D**omain **N**ame **S**ystem. Among other services, the DNS public service translates the DNS name of a given IP machine into its IP address, so it can be contacted from any host on the Internet.

FireLite IP Alarm System description

FireLite IP Alarm System uses the Internet as the main communication path between the traditional Alarm Panel and the Central Monitoring Station (*CMS* from now on). As such, two new elements are added into the system:

- The **IPDACT** is FireLite's IP Communicator. This element is connected to the Fire Panel DACT[2]. The IPDACT formats the telephone alarm into IP and sends it over the Internet to the CMS.

- The **VisorALARM** is FireLite's IP Receiver. It is installed in the Network Server room, at the CMS private network, and it connects to the Automation Server over a serial line. The VisorALARM reformats the IP alarm received from the IPDACTs into a well known alarm format (Ademco-685, Sur-Gard and Radionics emulation) and retransmits it to the Automation Server.

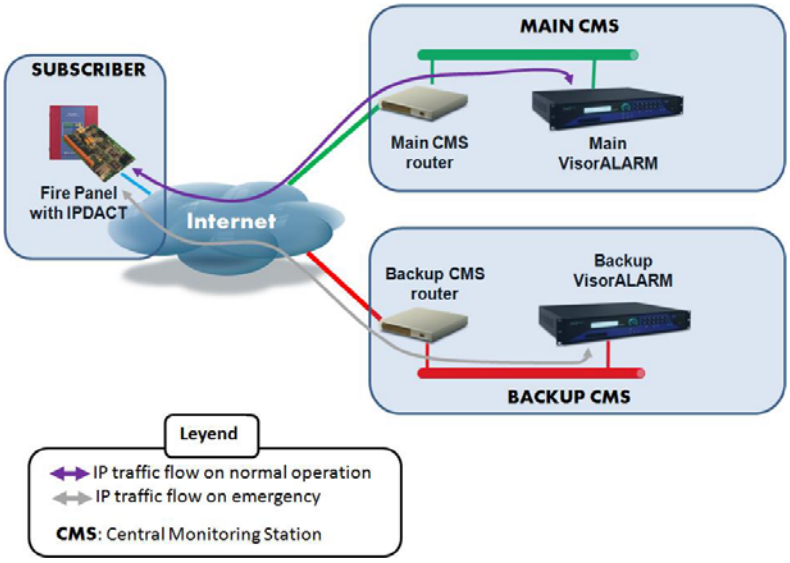

***Figure 1**. FireLite IP Alarm network diagram*

Figure 1 illustrates the basic IP Alarm System setup for Disaster Recovery. A secondary CMS takes over the Alarm Service when IPDACTs have lost the IP contact to their primary CMS. VisorALARM receivers can be clustered together leading to more complex architectures for Disaster Recovery. These architectures are out of the scope of this document, nor shown in the Figure.

The IP communication between IPDACTs and their Main and Backup VisorALARM is carried over the Teldat ARLY[3] protocol, which offers:

- Connectionless transmission through low size packets. This protocol is fully adapted to the Alarm Monitoring transmission pattern.

- Security: Through packet encryption and other advanced techniques for the system protection against replicas and against *man-in-the-middle* attacks.

- Reliability: Through IP packet sequencing and retransmissions.

[2] **DACT**: **D**igital **A**larm **C**ommunicator **T**ransmitter. It is the Alarm Panel module in charge of transmitting the alarms over the external telephone line.
[3] **ARLY**: **A**larm **R**e**L**a**Y**. It is the Teldat proprietary IP communication protocol for the Alarm Monitoring Service.

Automatic Disaster Recovery

During disasters when the CMS staff must evacuate its facility or when the CMS IP Service goes down, Internet Service Providers are usually unable to forward the IP address space on their Internet connection to another location. In these circumstances, prior to falling back to a phone line communication, the IPDACT automatically switches the IP to its secondary CMS.

In compliance with the NFPA-72[4] signaling standard for OT-PSDN[5], the CMS notices the IP communication failure of a subscriber account within 90 seconds. IPDACTs send polling request packets every 90 seconds to the Main CMS and wait for the receiver response within that time interval (two-way polling). If the IP polling fails, the system goes on backup, so that:

- The main receiver triggers a Communication Loss alarm on that account.
- The IPDACT switches to its backup receiver, keeping the complete Alarm Monitoring service.

The IPDACT will switch back to the main receiver on a normal operation as soon as the main IP communication has been recovered.

Changing the CMS location or IP Service Provider

Instead of relying on the IP Alarm Monitoring Service on an external DNS service, IPDACTs make use of IP tracking mechanisms offered by the ARLY communication protocol; so that they can be reprogrammed with the new CMS IP addresses (backup and main) with very little effort from the CMS administrator and no manual reprogramming in each Fire Panel location. Furthermore, during the CMS IP address space modification, the Alarm Monitoring Service will not be disrupted.

During the Fire Panel installation, the VisorALARM downloads into the IPDACT the IP addresses of the Main and Backup CMSs. The VisorALARM picks the IP addresses from the appropriate IPDACT programming pattern in its Data Base. On the other hand, the VisorALARM keeps track of the IPDACTs contact IP address since it caches it during the last polling interval.

When the IP address space of the CMS is modified, the IPDACTs are reprogrammed without disrupting the Alarm Monitoring Service, following these steps:

1. The new IP address space is activated into the Main CMS. All the IPDACTs in the field switch to the Backup CMS, as the IPDACTs haven't been informed yet on how to reach the Main CMS in the new address.

2. The new IP address from the Main CMS is edited into the appropriate programming pattern of the Backup VisorALARM Data Base. With a one-click operation into the VisorALARM Manager Application[6], the IPDACTs are batched reprogrammed.

3. Once the batch reprogramming is completed, all the IPDACTs in the field will then reconnect to the Main CMS at the new address.

[4] **NFPA**: **N**ational **F**ire **P**rotection **A**ssociation
[5] **OT-PSDN**: **O**ther **T**ransmission technologies – **P**acket **S**witched **D**ata **N**etworks. This standard details the features required for an IP Communicator device so it does not need to fallback to a telephone alarm transmission in case that the IP Communication goes down.
[6] The VisorALARM Manager Application is the Windows based tool used for configuring and monitoring the VisorALARM and the registered IPDACT accounts from the CMS dependencies.

Why DNS-based solutions are not a good idea?

The DNS approach implies a deeper coordination with the CMS IT administrators, since they will be responsible of maintaining the new DNS domain and the new DNS hostname assigned to each receiver. The DNS approach hence forces the IP Alarm System to rely on an external DNS service, adding another point of failure in the system that is not 100% controlled by the Alarm Monitoring Service responsible. As the reader have learned in the previous sections of this document, the FireLite IP Alarm System offers high resilience capabilities without the need for DNS.

The DNS lookup is the procedure used by the IP Communicators to learn the contact IP address of their CMSs in a DNS-based solution. This procedure can slow down communication if DNS servers are slow to respond, or even block the IP communication if the DNS is not working (problems in the subscriber's DNS service, problems on the public DNS Service or even problems on the DNS Service in the CMS). In FireLite's approach, these problems will never arise.

When the CMS contact IP address is changed in a DNS-based solution, the IP Communicator will try to communicate with a bad IP address before it looks up the new IP address. If a dealer changes to a new CMS the IP Communicator will never change to the new IP address if the old CMS is still answering on the old IP address. As the reader can derive, on changing to another CMS, the Alarm System runs into a transition period (i.e. communicators pointing to the old CMS) for an uncertain time. The FireLite system does not suffer from this problem.

On the other hand, the DNS Denial of Service attacks are very popular (i.e. the response to an IP Communicator DNS lookup comes with a faked IP address for the CMS) and will cause the system to malfunction. In fact, if the public DNS service is down, not only the IP alarm service will be inoperative (even when the IP link is working fine), but also the time uncertainty on the DNS system recovery in these circumstances may be unaffordable.