IP Alarm Service High Availability

VisorALARM IP Redundancy

APPLICATION DOCUMENT	
Product : VisorALARM & mIP / IPDACT **Summary:** VisorALARM architecture for High Availability **Date :** November 2007	**Product version :** ---- **Document version :** 1.0

INDEX

Introduction

The Alarm Monitoring Service, as any other mission critical service, has tight restrictions on its availability. As any mission critical service, any loss of performance or service failure can derive into a high loss of revenue, customer dissatisfaction and, what it is worse, it can lead to loss of human lives.

Disaster Recovery Plans spans over all service elements, coordinating them together in in seek of the highest availability. There are diverse ways to implement Disaster Recovery Plans for Alarm Monitoring Services. However, all of them have something in common: they must be supported over the most robust communications paths.

This important challenge becomes a big concern in IP-based alarm systems, hence the need for an intelligent platforms that can automatically react to network service breakdowns to keep the Alarm Service running without losing any performance.

The Teldat IP Alarm system adds the IP Communication path to the traditional Alarm System. The high over the telephone network elements achieve this goal by delivering line redundancy to the Fire Panel side, as well as to the Central Monitoring Station (CMS). The line redundancy in the CMS can be combined with equipment redundancy – the VisorALARM's are grouped in clusters[1].

This document describes Teldat's IP line redundancy in the CMS network. The backup process is detailed and all the system elements are listed. In the next section, the Teldat IPDACT and VisorALARM text configuration parameters required for the IP backup are explained. Finally, a detailed explanation on the Teldat IP Alarm System troubleshooting is given.

[1] VisorALARM clusters are not considered in this document

1. System topology and operation

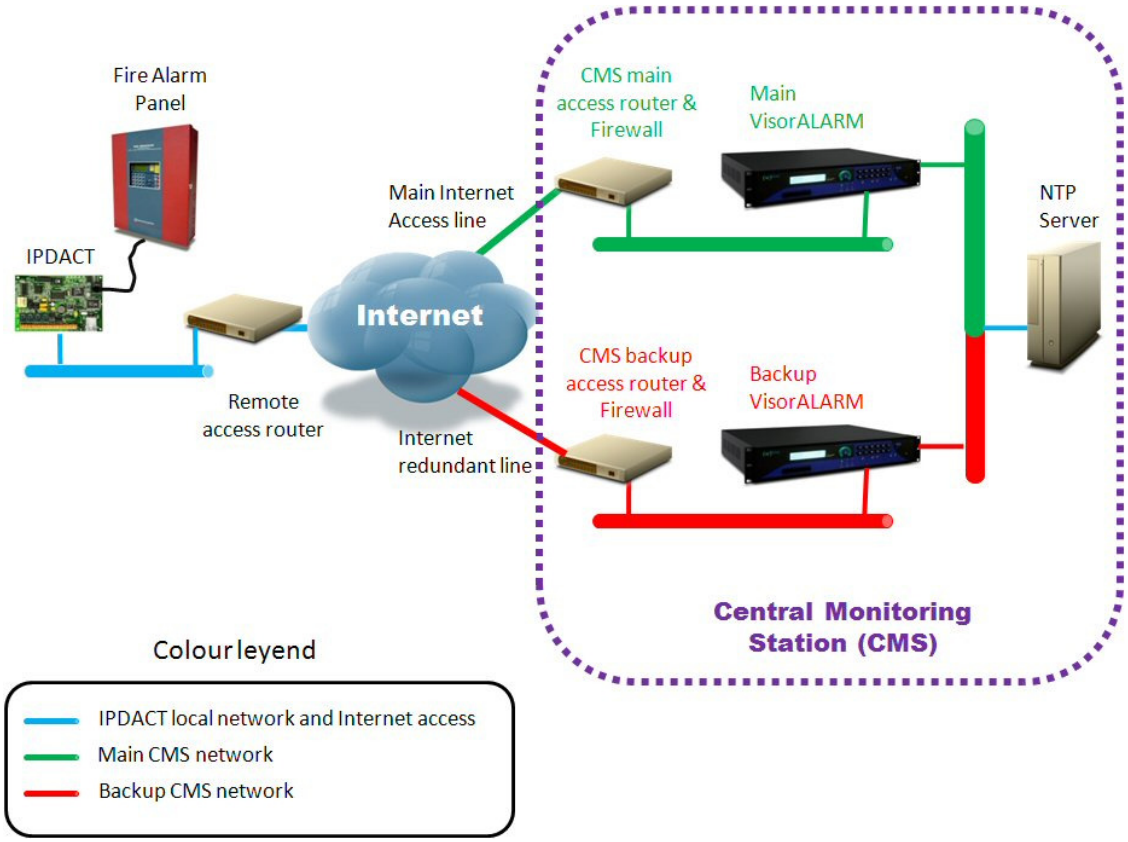

Figure 1. IP network diagram for CMS High Availability

Normal operation

The IPDACT only communicates with the Main VisorALARM receiver over the main CMS line. The main VisorALARM hence deals with the three IP traffic flows - registration, alarm transmission and supervision – delivered by all IPDACT's on field. The main Communication path of this IP traffic in the CMS network is depicted in green in the above Figure.

Operation in Emergency

Upon a main link failure the IPDACT switches the transmission over the backup CMS line to the backup VisorALARM. The backup VisorALARM is taking the roll of a main VisorALARM, serving all IPDACT's on field just as if it was the main one. The backup Communication path is red coloured in Figure 1. On the other hand, the IPDACT keeps

supervising the link to the main VisorALARM receiver so it can switch back to Normal Operation as soon as the main link is recovered.

The backup switching, as well as the main link recovery process are automated, so no user interaction is required.

VisorALARM Data Base synchronization

Since each VisorALARM keeps its own Data Base with the IPDACT accounts on field, the main VisorALARM and the backup Data Bases must be synchronized at all times, so the backup VisorALARM can keep the update of new IPDACT's and then serve them in emergency conditions.

The Data Base update process is sensitive to the internal time clocks of each VisorALARM receiver. In fact, both VisorALARM units must synchronize their clocks with a Network Time Protocol Server – NTP server. This clock server can be of private use, as shown in Figure 1 or can be a public server located in the Internet.

The Data Base synchronization is carried out periodically and involves two additional communication flows between both receivers:

- Polling: The backup VisorALARM polls the main one periodically for Data Base updates.
- Update: If there has been any change between the two Data Bases, they are synchronized.

2. The traffic pattern charts

The CMS network depicted in Figure 1 has been simplified for a better understanding of the system backup performance. In real scenarios, the CMS network can be of diverse complexity and will, of course, include Firewalls to increase the security.

As defined in the previous section, there are different communication flows that must be allowed along the IP network for the backup system to work properly.

2.1 IP traffic flows between the IPDACT and the VisorALARM's

All the communication flows between the IPDACT and the currently active VisorALARM – either the main or the backup one – is of type UDP and they have the following pattern:

Pair of units involved	Direction	Type	Dst. Port (default)[2]	Connection starts at
IPDACT / VisorALARM	Two-way	UDP	80	IPDACT

Chart 1. IPDACT – VisorALARM traffic pattern

The default Destination Port value can be modified in the IPDACT and VisorALARM configuration.

2.2 VisorALARM clock synchronization

Both the main and the backup VisorALARM synchronize their internal clocks with an external IP server in compliance with the Network Time Protocol Standard, type UDP.

Pair of units involved	Direction	Type	Dst. Port (default)	Connection starts at
VisorALARM / NTP Server	Two-way	UDP	123	VisorALARM

Chart 2. VisorALARM – NTP Svr clock synchronization

2.3 VisorALARM query for Data Base update

Pair of units involved	Direction	Type	Dst. Port (default)	Connection starts at
Main VisorALARM / Backup VisorALARM	Two-way	UDP	80	Backup VisorALARM

Chart 3. VisorALARM queries for the DDBB update

2.3 VisorALARM Data Base synchronization

Pair of units involved	Direction	Type	Dst. Port (default)	Connection starts at
Main VisorALARM / Backup VisorALARM	Two-way	TCP	35001	Backup VisorALARM

Chart 3. VisorALARM DDBB synchronization

[2] The Dst. Port value shown in the Chart corresponds to the Destination Port. Although the IPDACT fixes the Source Port the same value, this one is usually changed to a random value in the IPDACT Internet access router (NAPT translation).