

## Central Monitoring Stations:

### Video management over IP networks – Secure Access using HTconnect

By Ulrich Schwieger and Daniel Krönke

Two clearly evident trends in safety technology and engineering are forcing operators of central monitoring stations to face new challenges: The ongoing fusion between video technology and intruder alarm technology and the massive migration from older transmission mediums such as ISDN or X.25, to IP networks.

It follows that only those managers of monitoring centres that come to terms with the new infrastructure requirements at an early stage are able to secure competitive advantages.

Managers of monitoring centres will therefore opt for intelligent and flexible solutions for operator station and video management that allow them to react to the highly varied, project-specific customer requirements they face. In the future it will not be necessary to integrate the classical single trades of burglar alarm technology, access control and video technology, but also to incorporate existing public and private communication infrastructures. Central monitoring stations are therefore more and more being required to assume the task of system integration.

#### Problems with IP and UMTS (3G) networks

IP networks are of special significance with regard to system integration because they have now established themselves as „the number one communication platform“, even – and increasingly – in the field of safety technology.

However, modern IP networks also throw up several imponderables: In contrast to the singular use of „old“ transmission paths, customers using a control centre today want to incorporate their existing IP infrastructure and to use it cost-effectively. This is understandable. However, the interfaces are no longer clearly demarcated and do not end at the DSL connection of the provider. The simple reason for this is that DSL connections are used for multifunctional access to the Internet, e.g. email, Internet access FTP etc. Particularly in the case of companies divided into branches, network access is a vital component for their business activities.

There are special requirements to be met to ensure the availability of IP data networks, especially for video applications.

Normally, there is a DSL connection serving as the interface between the customer's local network (Intranet) and the public IP network (Internet). Intranet and Internet must be viewed as independent IP networks. The Intranet is usually protected by a firewall against unauthorised access from the public network. However, this security rule becomes a problem when the monitoring centre wants to access the video transmitter located within the customers Intranet.

These are unfortunately not within the protective firewall and an appropriate port must be opened permanently for external access. Every system administrator will object to this solution for obvious reasons.

The widespread use of dynamic IP addresses is also problematic when operating monitoring centres. Dynamic addressing is used by the Internet Service Provider for network access by DSL, but is also used within many Local Area Networks (LANs). The principle of alternating addresses for each new connection prevents direct access to the

## Central Monitoring Stations:

### Video management over IP networks – Secure Access using HTconnect

By Ulrich Schwieger and Daniel Krönke

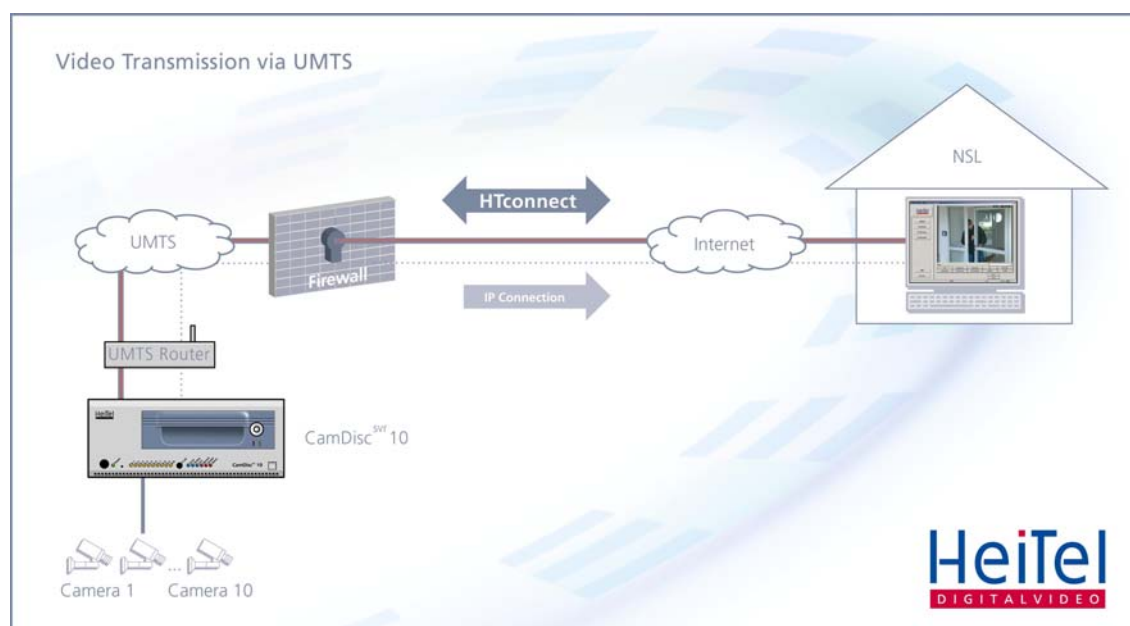
video transmitter for the rather simple reason that the IP address is not known at the control station end.

You can work around this problem by using DynDNS services from third-parties. However, the use of DynDNS (Dynamic Domain Name System) for safety-relevant jobs is controversial because use of such services are not normally covered by basic contractual principles, the update intervals are not guaranteed and there are no binding statements on availability.

UMTS (Universal Mobile Telecommunications System) is rapidly increasing in significance as the 3rd generation (3G) mobile telephone standard, as significantly higher data transmission rates are possible with 3G than when using the GSM standard. But even here, the devil is in the detail: A connection to the Internet from 3G networks can be established without any problem, but there are no contingencies for the reverse direction. An IP connection from a landline Internet connection to a 3G subscriber is prevented by the 3G network operators for technical and contractual reasons. The single 3G networks are shielded by a firewall from „the rest of the world“ and only allow for outgoing connections to the Internet or to connections within the Internet. On top of this, dynamic IP addresses are also used within 3G networks. The addresses can therefore not be resolved by DynDNS.

### Direct access using HTconnect

The HTconnect method just developed by HeiTel Digital Video GmbH overcomes the problems described above without negating the protection from the firewall! HTConnect makes it possible for the monitoring centre to connect to video transmitters located behind firewall-protected Intranets and located to the 3G phone network! HTconnect additionally permanently checks the availability of the system because both the video transmitter and the networks used for transmission are subjected to a constant functional check. The auto-diagnosis integrated into the HeiTel systems (i.e. auto-ping) allows the monitoring centre operator to isolate the network error that occurs to the public Internet or to the customer's own Intranet.



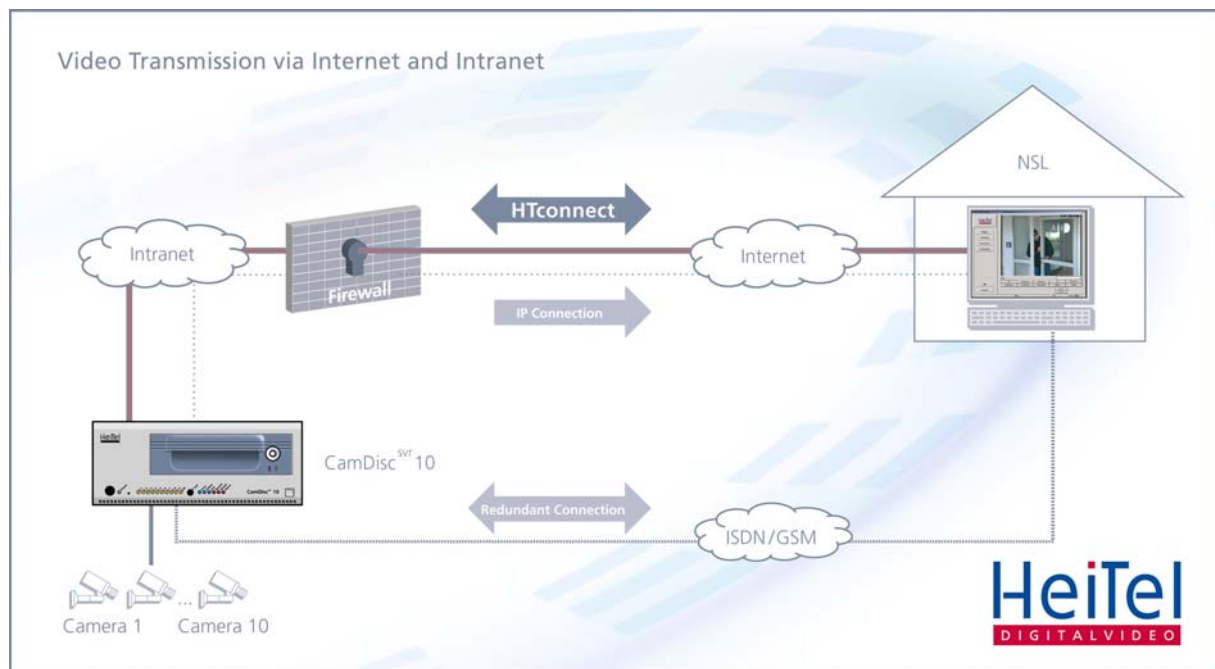
## Central Monitoring Stations:

### Video management over IP networks – Secure Access using HTconnect

By Ulrich Schwieger and Daniel Krönke

#### Redundant transmission provides additional security

Even the most stable IP connection is not immune to temporary failure. For safety-relevant applications, an additional transmission path should therefore always be planned in for use as back-up in case of the failure of the IP network. ISDN for landline transmission or GSM for radio telephony transmission would be ideal here. Both the receiving end (monitoring centre) and the transmission end (video system) must be equipped accordingly. This remains possible without reservation for all HeiTel devices.



#### Summary

With the HTconnect system, HeiTel has developed a method that allows for unlimited but secure access to video systems using combined Internet/Intranet IP networks without cancelling the protection of the local network's firewall or having to pass on DynIP addressing.

Additionally, HTconnect permanently checks the integrity and availability of the complete system comprised of the public network, the private network and the video transmitters.

Ulrich Schwieger, Head of Product Management  
 Daniel Krönke, Head of Marketing Communications  
 HeiTel Digital Video GmbH, June 2008  
[www.heitel.com](http://www.heitel.com)