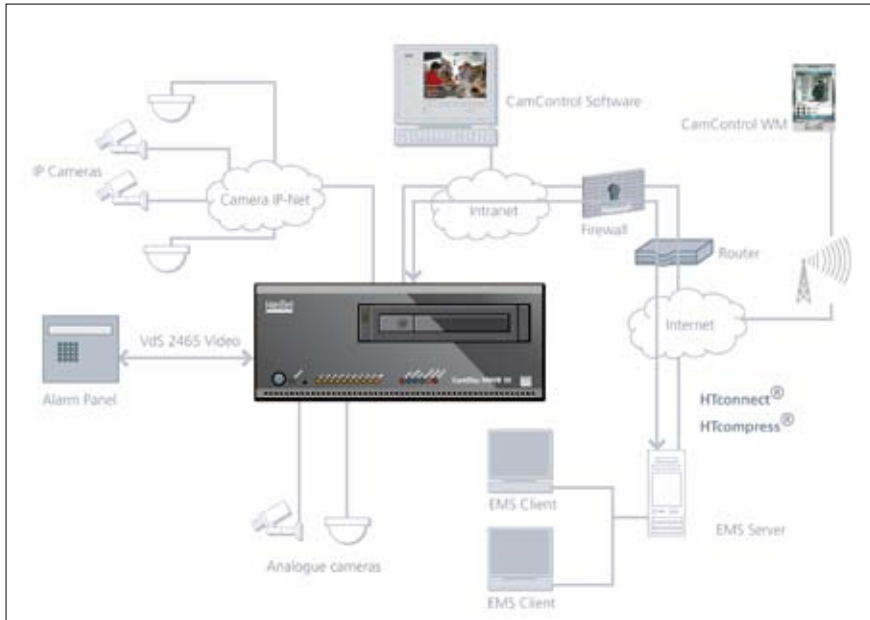


Competent project planning is crucial for quality

# Planning suggestions for digital video surveillance systems



*Schematic illustration of a video surveillance system.*



### About the author

Ulrich Schwieger, is technical director at HeiTel Digital, Stuthagen, Germany

**It is a well-known fact that a competent and qualified planning and project development is crucial for the quality of a video surveillance system.**

Author: Ulrich Schwieger

Planners and installers are particularly challenged since innovation cycles are extremely short in the sector of video surveillance technology, and the evolution in camera and communication technologies requires a high level of technical knowledge and expertise. On top of all that, it is nowadays vital to realise security solutions that allow for an integration of different technical features to form a comprehensive and coherent concept.

### From local recording and evaluation to networking of control rooms

In principle, it is necessary to take into account that the recording mode of modern video systems can be precisely adapted to suit different project-specific circumstances. In this context, permanent recording, event-based recording and permanent event-based recording modes can be distinguished.

In modern video surveil-

lance systems, purely permanent recording where the individual cameras of the video system are recording at a set rate of frames is the exception rather than the rule. What is needed are variable recording speeds resulting from the respective system status and object-specific conditions. For instance, to monitor an area that is not or little frequented by the public does not require permanent recording at a high frame rate. However, in case of deviations from a usual condition, e.g. when someone opens a door or window or when a person enters the detection area, the video system must be able to record what is happening at a higher frame rate as long as the unusual condition lasts. In addition, it might be necessary to establish a video connection with a local or decentralised control room depending on the deviation from normal status.

Modern video systems are equipped with appropriate detection mechanisms for motion

detection, which can be used for the situation described earlier. In addition, inputs and complex interfaces such as "VdS 2465 for Video" are available which are able to incorporate other features like burglar alarm or fire detection and alarm systems.

When a motion detector is activated or a burglar alarm system detects a door being opened, this can be directly transmitted to the video system, which in turn will initiate the appropriate functions, which may range from controlling the recording, establishing a connection to the control room to automatic control of PTZ systems, where the cameras are automatically positioned based on the data supplied by the burglar alarm system. The same applies when transmission of the frames to the control room is required.

The transmission of frames should be targeted and selective. That is to say, the control room receives the frame of the camera attributed to the activation criterion of the burglary alarm system automatically. In general, several cameras are installed in the area to be surveyed. This is the reason why the frame of the respective alarm camera should be

transmitted to the control room automatically. Aside from live frames, the frames recorded at the time the alarm was triggered are also relevant.

Access to recorded video sequences and retrieval of frames from local archives are other important aspects of video systems. Modern systems offer a multitude of different options. Often, local and direct access are required as well as remote access and evaluation. Archives can generally be evaluated from any access point and through various communication networks. Special attention should be paid to an intelligent search algorithm that is able to automate direct access to the respective sequences. This would replace a time-consuming manual search. Event lists can be used to search for particular frame sequences; moreover, search functions can be realised by connecting any type of recorded data in parallel with the frames.

### Aspects of data protection

Data protection is of paramount importance in video surveillance systems. Video systems provide a number of features to ensure compliance with data protection regulations. Under certain conditions, individual areas of cameras may be masked, for instance, either for live and/or archive frames (private zones). Moreover, access to cameras and archives may be restricted



or banned for certain users. Access to individual archives or general access to archives may be controlled by a peer checking principle or by several people having to enter different passwords. When using IP networks, the devices can be restrictively shielded by firewalls to prevent unauthorised access via the public network. Nevertheless, thanks to intelligent communication technologies such as HTconnect®, access from decentralised control rooms and by authorised individuals via public networks is possible despite the firewall being activated.

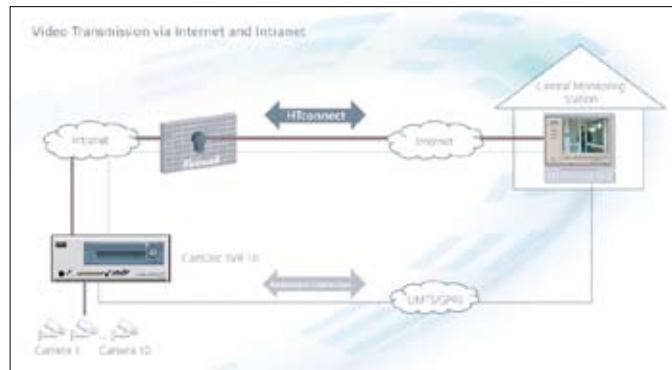
Hard disks with extremely large memories make it possible to archive the video sequences for long periods before they are automatically overwritten due to their ring memory structure. However, this may also pose problems. As to how long the recorded frames should be archived should be determined in advance. The video systems feature analogue functions that automatically delete the recorded frames after a specified period of time.

In addition, relevant provisions and data protection regulations need to be taken into account during the planning stage, in particular when it comes to the position and selection of cameras. This also applies to high resolution IP cameras. Consideration should always be given to the protection goal – does it really require the application of megapixel technology? In most cases, a camera with standard resolution would be adequate to monitor a public car park, for instance. A megapixel camera might be difficult as e.g. registration numbers or individuals can be identified.

Data protection may be an extremely complex matter, particularly in the case of video surveillance systems in areas with public access. In case of doubts about the video system's compliance with relevant regulations, it might be useful to consult a legal expert during the planning stage.

### Tamper resistance

Tamper resistance is a standard feature in burglar alarm systems, and a principal requirement. This applies to video systems only to some extent. Most video systems are able to detect camera failure



Video transmission via internet and intranet.

or disconnection by monitoring the video signals transmitted by individual cameras.

Only few manufacturers offer qualified camera monitoring beyond detection of signal failure. These video systems detect when a camera is being tampered so that it no longer serves its purpose.

Intelligent sabotage recognition algorithms are able to detect turning, readjusting, masking or defocusing of a camera. They are also able to detect conditions of inadequate lighting and illumination.

What matters, however, is that such system statuses are appropriately registered and reported. Error or sabotage messages are transmitted to alarm receiving and service centres.

In principle, comprehensive protection concepts should apply the VdS interface "VdS 2465 for Video" since it helps alarm systems to detect such system statuses. The alarm system's operating panels and display screens are then able to show the system's status in plain text. Any system interferences or sabotage conditions of the video system may

thus be included in the alarm system's "Zwangsläufigkeit".

### Camera selection

In many cases the FAQ whether analogue network cameras should be used can easily be answered. Network cameras have to be applied when a resolution greater than 720 x 576 pixels (PAL format) is required since there are no limitations to the possible maximum number of pixels which is typical of PAL.

Moreover, the application of network cameras might be useful when existing network structures should be used as much as possible to reduce installation expense. When megapixel cameras are used, a number of issues need to be considered in advance.

Logically, high-resolution cameras are equipped with image recorders that feature pixel counts that match their resolution. As the recorder's chip size is the same in most cases – in CCTV systems, a recorder size of 1/3 inch has become common – the size of the individual pixel decreases reciprocally to the total number of pixels.

In general, the pixel size has to

be reduced since the sensors' size remains the same. Problem: the amount of light per pixel decreases pro rata. As a result, megapixel cameras with identical sensor size are less sensitive to light compared with standard resolution cameras.

Though manufacturers are trying to compensate for the reduced light sensitivity of megapixel cameras by design improvements such as better surface structure of sensors or using more light-sensitive lenses, they have not been able to achieve a marked improvement. This is why greater signal amplification and longer exposures are used in most cases.

The bigger the individual pixel, the greater, in general, the signal strength and the (signal-to) noise ratio. The signal strength becomes weaker with decreasing pixels, and the (signal-to) noise ratio deteriorates. The greater signal amplification required because of the weak signal strength also amplifies some of the noise due to the poorer signal to noise ratio. As a result, the quality of the frames deteriorates, the images become grainy.

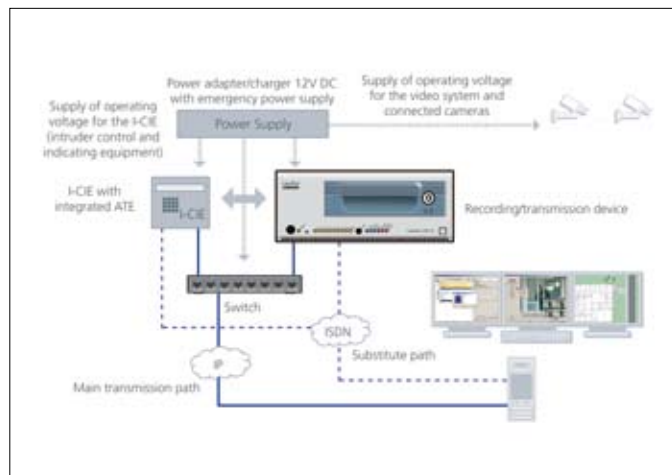
Longer exposures are also problematic since movements or parts in motion cause the image to be out of focus.

In many cases, cameras with a lower resolution are able to generate better results than megapixel cameras.

In principle, the features and quality of megapixel cameras should not be judged on the basis of static frames as the quality of an IP camera is primarily influenced by frame content and movement.

When applying megapixel cameras, special attention must be given to selecting the right lens. Lenses for fixed cameras are generally not suitable for megapixel cameras.

Another aspect that has to be considered when megapixel cameras are applied is the data volume generated by them, which increases relative to the resolution. Hence, the frame of a 2 megapixel camera contains five times the data volume of a standard resolution camera at the same compression factor. This factor needs to be taken into account for planning and network integration. The memory cards and hard disc capacity must be designed accordingly.



System configuration video surveillance and burglar alarm system.



## Embedding IP cameras into existing communication infrastructures

In any case, one should not succumb to the misapprehension that IP cameras can generally be easily integrated into existing IP networks since the network structures available are generally Intranets that have primarily operational functions. Megapixel cameras tend to generate heavy network loads; they may tax such network structures considerably and may severely obstruct the intended function.

This is why only video systems (DVR, NVR, video recording and transmission systems) with decoupled physical and functional network connections should be applied. This ensures integration into an existing network with less resource input and does not obstruct the system's intended operational function.

On the one hand, such system structures prevent the network from being unnecessarily taxed by the camera technology, and on the other hand, access to the video archives and live frames is possible at any time through the existing network structures.

The application of network cameras poses yet another problem: the different and proprietary transmission and log formats of different vendors. Consequently, the network recorder used must support the selected cameras. From the perspective of "good value for money", the video system applied should be able to adapt to



Complex video management systems can be accessed via mobile channels like wireless UMTS networks or standard internet connections.

changing customer requirements. It is necessary to ensure that additional network cameras can be integrated at a later stage, bearing in mind that these might be cameras that were not yet available on the market at the time the video system was installed.

Practical applications often boast hybrid systems, using both analogue and network cameras. The recording and transmission systems must be designed accordingly; they must be able to process data from both network and analogue cameras.

### Integration of video systems in private and public IP networks

Connecting video technology to decentralised superordinate management systems and alarm receiving and service centres has meanwhile become an established central and indispensable feature.

In addition, operators in particular those in enterprises with a branch structure, want to be able to access video systems in selected branches via a central access point and different network structures.

The technical options are manifold and range from PDAs or smart phones to laptops with appropriate software and complex video management systems. The system can be accessed via mobile channels like wireless UMTS networks or standard internet connections.

In this context, the integration of video technology into the existing communication infrastructure may pose problems since the ADSL connections that connect local customer networks with the Internet often feature dynamic IP addresses.

In order to access systems connected in this way over the Internet, special services such as

DynDNS need to be used. Another problem occurs: availability of these network services is not guaranteed and complex settings have to be done on the customer network's router.

When smart communication technologies such as HTconnect® are used, there is no need for complex settings or additional network services. This implies additional benefits: there is no need for otherwise obligatory router configuration in terms of NAT (Network Address Translation) or port forwarding, the firewall does not need to be opened, and availability of the entire transmission path between the video system and the control room is monitored permanently. Thus, the control room will immediately detect interferences in the connection or failures of network components.

### Conclusion

The performance features of modern video systems are manifold and give planners and installers the opportunity to realise security systems that can be customised for the user's requirements. When it comes to the practical application, however, users often do not make full use of the systems' features. Planners and installers who are familiar with the multitude of performance features certainly have a competitive edge. Associations like VdS Schadenverhütung and BHE as well as the manufacturers of video systems offer training classes and seminars to provide the necessary expertise. ■

# Business & Product News Every Day!

- The Global Security News Portal -



[www.SecurityWorldHotel.com](http://www.SecurityWorldHotel.com)

Full international coverage



[www.SecurityWorldHotel.com/na](http://www.SecurityWorldHotel.com/na)

News dedicated to the North American market



[www.SecurityWorldHotel.com/se](http://www.SecurityWorldHotel.com/se)

News dedicated to the Swedish market



[www.SecurityWorldHotel.com/me](http://www.SecurityWorldHotel.com/me)

News dedicated to the Middle Eastern market



[www.SecurityWorldHotel.com/no](http://www.SecurityWorldHotel.com/no)

News dedicated to the Norwegian market



[www.SecurityWorldHotel.com/uk](http://www.SecurityWorldHotel.com/uk)

News dedicated to the UK market



[www.SecurityWorldHotel.com/dk](http://www.SecurityWorldHotel.com/dk)

News dedicated to the Danish market

**armedia**

- CONNECTING SECURITY BUYERS AND SUPPLIERS -

AR Media International AB • Västberga Allé 32 • SE 126 30 HÄGERSTEN • Sweden • Tel +46 8 556 306 80 • Fax +46 8 19 10 11 • E-mail: [info@armedia.se](mailto:info@armedia.se) • [www.armedia.se](http://www.armedia.se)

security news every day - [www.securityworldhotel.com](http://www.securityworldhotel.com)