BOSCH
Invented for life

Building Reliability into Bosch Video over IP

Technical Brief

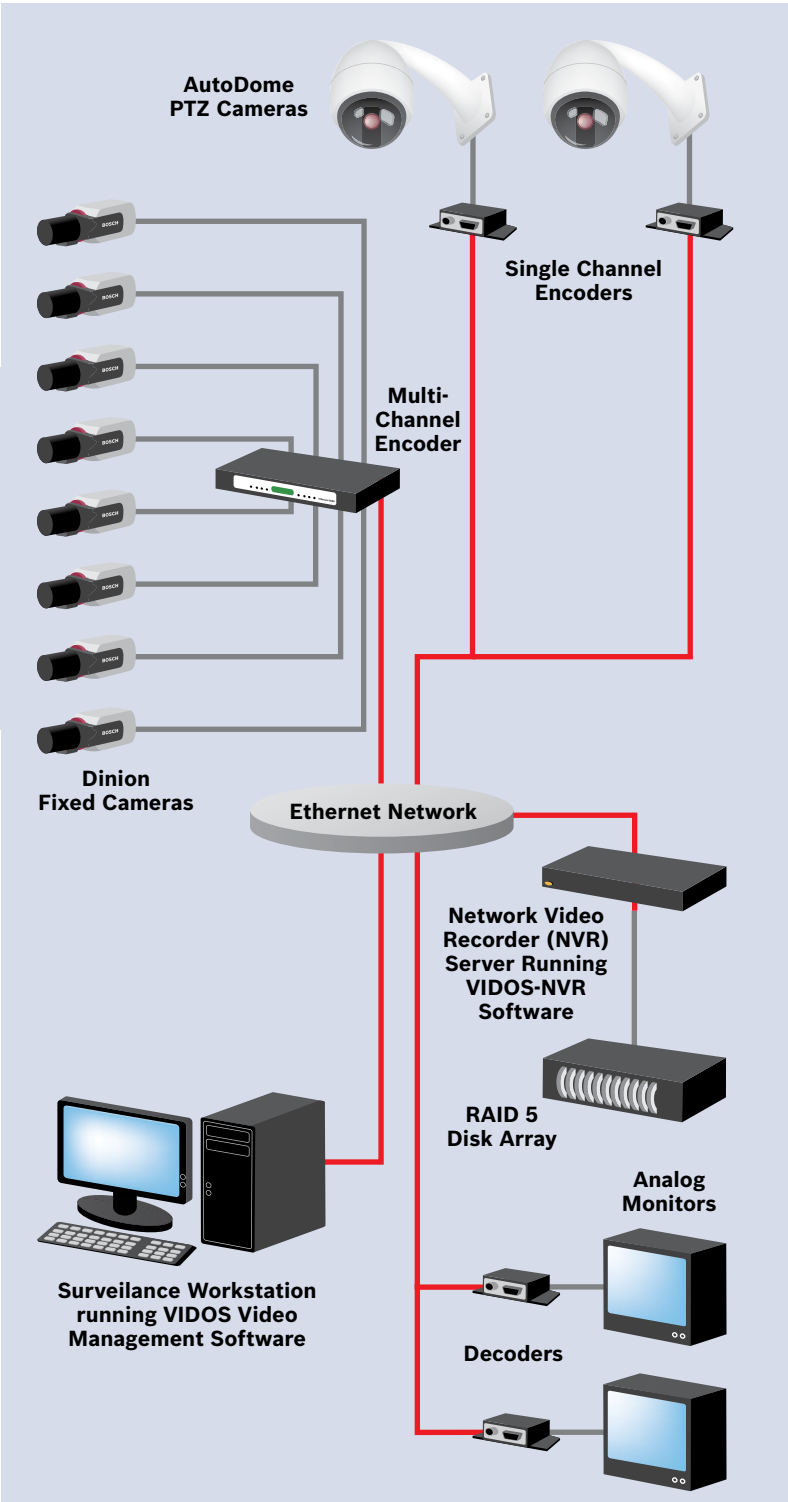
What is Reliable IP-Based CCTV?

Within the context of this Technical Brief, reliable IP-based CCTV means:

- The system's key components are engineered to fail as infrequently as possible.
- If a key component does fail, its status can be quickly detected and reported for rapid corrective action.
- If key components fail, "stand-by" components can be brought in immediately (to offer fault-tolerance).

The key components of an IP-based CCTV system are:

- IP network
- RAID storage
- NVR server
- Encoders and decoders
- Cameras
- VIDOS workstations



The IP Network

The network itself holds the key components together, so it is a critical point of failure. You can find highly reliable architectures (which usually carry a high cost), but there are some simple precautions you can take to engineer reliability into your IP-based CCTV system – without focusing exclusively on the switch's physical reliability.

Common failure scenarios

- Excess traffic: Bandwidth overload can cause performance degradation.Peak traffic can occur if too many people try to view video simultaneously, or if there is a massive surge in PTZ activity while the network was already running close to maximum.
- Switch failure.
- Cables: A simple yet significant issue can be faulty Ethernet cables and/or poor connectors. This usually results in one camera's failure, but if the uplink cable connecting two switches is affected, then every camera will be lost.

Designing for reliability

When designing your system, carefully consider "worst-case" scenarios, depending on the specific deployment. You may simply have fixed cameras live streaming to a monitoring center. Or you may have live streaming to multiple recipients, centralized network video recording (NVR) storage, and Automatic Network Replenishment (ANR) – assuming you have adopted Recording at the Edge technology. (Recording at the Edge means that in the event of a network interruption, the encoders buffer video and then when the network is up again, both live video and the buffered video are sent.) If you combine this with exceptional PTZ activity and users trying to download clips from the encoders, your network will be highly stressed.

Although very rare among good quality commercial switches, switch failure rates are significantly higher for low-cost retail switches (e.g., an $80-dollar 16-port switch). Failure rates are also much higher if the switch is frequently moved, or cables are frequently plugged and unplugged.

CAT-5e has rapidly surpassed CAT-5 in popularity, due in part to its improved performance characteristics and its reliability.

A good way to tackle the issue of scalability (many users viewing the same video) is to use the multicast capability of the Bosch Video over IP encoders and the network.

Detecting issues

Network monitoring tools are standard tools for every IT department – both at the high-end and low-end. They are used to monitor SNMP traps, such as those generated by all BVIP encoders and decoders. The failure of any CODEC, just like any other network-based asset, triggers a centralized alarm.

Physical fault tolerance in the switch

The most fault-tolerant network in the world is the Internet. Designed to withstand multiple attacks on various paths, it has the ability to re-route network traffic to its intended destination. The IEEE developed the 802.1D standard, which was implemented by companies such as Cisco (with the Spanning-Tree Protocol). This ensures that there is one and only one active path for data to take when passing through a network of switches and bridges from its source to its destination – even if that path is interrupted, immediately re-routed, and eventually rebuilt.

Recording at the Edge and ANR

Recording at the Edge is the concept of taking audio/video from a camera, and storing it at the edge of the Ethernet network instead of transporting it across the network to a centralized recording facility (e.g., an NVR).

Recording at the Edge is a distributed (or decentralized) approach to storage: video is spread across a number of edge-storage devices, as opposed to centralized on one.

Reliability through network independence: Recording at the Edge is more reliable because recording is independent of the network's status and amount of traffic. Even if the network grinds to a halt, recording continues unaffected.

Network fault tolerance: One of the concerns about IP-based CCTV is its dependence on the network. With Recording at the Edge, this is not an issue because a network outage only impacts live video. Conversely, in a centralized storage model, both live video and the ability to record are lost. Bosch's patent-pending Automatic Network Replenishment (ANR) combines the buffering qualities of Recording at the Edge with an intelligent central NVR that tracks any recording gaps due to network interruptions, and then automatically fills (or replenishes) those gaps.

Simplicity: You can implement Recording at the Edge by deploying PC-based DVRs at the edge; however, with vulnerable operating systems, these are more challenging to maintain than a simple purpose-built embedded appliance. Products like the Bosch VideoJet 8008 and embedded DVRs are better suited to this role – since conventional DVRs traditionally focus on recording, searching, and playback rather than scalable live streaming over the network, which is a primary function of an IP-based CCTV architecture.

Fault tolerance: Recording at the Edge is more fault tolerant because if one edge recorder fails, only those cameras connected to that unit stop recording. In a centralized approach, all cameras cease recording.

Network bandwidth optimization: Recording at the Edge is a network bandwidth-friendly approach because it does not use any network bandwidth to record video – the network is only used to play back audio/video from the edge at a review station.

Pre-alarm recording: To add security, centralized storage is frequently used to record alarm video for easy alarm verification and long-term, secure storage. Pre-alarm recording is offered by introducing a buffer in the encoder so that the seconds (or minutes, hours, or days) of video before and after an alarm can be automatically transmitted to the centralized storage location.

In those instances where the pre-alarm video is not long enough, it is comforting to know that the original, complete video is still available, since it was recorded at the edge.

Dual streaming: In situations where network bandwidth is severely limited, Recording at the Edge is ideal for high-quality recorded video, but it does not solve the challenge of viewing live video over a restricted network. Bosch encoders support dual streaming, which enables the encoder to deliver two totally independent streams of video, separately configured for different frame rates and image resolutions. For limited bandwidth networks, one high-quality stream is typically used for local recording, and a lower-quality (lower bit rate) video is used for live viewing. Conversely, for high- bandwidth networks, the same stream is used to record locally and centrally, and ANR is used to fill any gaps in centralized recording due to network interruptions.

Economies of scale: A major justification for centralized storage is that we can use enormous RAID disk arrays, reducing the cost per terabyte. These cost savings must be balanced against the advantages of Recording at the Edge. The best solution is to seamlessly combine both approaches: when network bandwidth is available and reliable, then use it, but when it is severely limited or intermittent, then use Recording at the Edge.

System management: Another significant benefit of centralized systems is the relative simplicity of system management, because everything is located in one room or data center rather than dispersed across hundreds or thousands of miles. For Recording at the Edge to be a pragmatic solution, it is critical to include centralized network performance monitoring and associated system management utilities. These include SNMP compatibility with network management systems such as Tivoli and HP OpenView, and the ability to reconfigure and upgrade multiple units simultaneously.

RAID Storage

Fortunately, just about every industry records critical information digitally on hard drives, and CCTV is no different. This means that the cost and reliability of massive storage are very favorable. RAID (Redundant Array of Independent Disks) systems are the most popular high-capacity digital video storage format, and are typically installed with redundant power supplies.

Designing for reliability

A typical RAID device has a number of hard drives, and depending on the configuration, it can be set up to use sharing or data replication to deliver higher data integrity, fault tolerance, and throughput than using a single hard drive.

RAID 0 (also known as striped set) is technically not a RAID, because there is no redundancy. It exists to spread the data evenly across all the disks (improving performance) and to create large virtual drives from many smaller physical ones. Warning: since the file system is spread across multiple drives, the RAID's reliability equals the average reliability of each drive (MTBF) divided by the number of drives. So a 4-drive RAID 0 system has a total MTBF of one-quarter of an individual drive.

JBOD (Just a Bunch of Disks) represents concatenation, the reverse of partitioning. It creates one large virtual drive from many smaller physical ones. It differs from RAID 0 in that if a drive fails, then all the data on that drive alone is lost – but not the others. Because the data is not evenly spread across the drives, it does not have the same performance characteristics as RAID 0; however, it is an effective way to combine many small hard drives of varying capacities.

RAID 5 is the most common configuration for high reliability. One of the hard drives is used to record redundant data so that any one of the hard drives can fail without any loss of data. While the drive is out of service, the overall performance hardly changes; but a second hard drive failure at this stage results in a total loss of data. This is why most RAID manufacturers try to keep the number of hard drives to a reasonable maximum of approximately 14. And be sure to remember that you have less usable storage than you think because one of the drives holds redundant data. For example, on an 8- drive RAID 5 system containing 250 GB drives, you lose 250 GB, leaving you with 7 x 250 GB or 1.75 TB of usable space.

The NVR Server

The NVR server is the equipment that runs the NVR software, which manages information flowing into and out of directly attached RAID devices. The NVR server is a commercial-class PC, so it is specially designed to run non-stop (24x7). It includes a redundant power supply and runs Windows 2003 Server, a commercial-class Operating System. Windows 2003 Server is much more expensive than an OS such as Windows XP because of its inherent stability and reliability. Each NVR can be responsible for up to 64 incoming video streams and up to 36 TB of storage, and failure is rare.

In the unlikely event of an NVR server failure, a PC on the same network running Bosch VIDOS video management software can be configured to automatically redirect all the video streams to a standby NVR server. This is known as N+1 server redundancy.

Encoders and Decoders

In the majority of CCTV systems, cameras are connected to encoders, and monitors to decoders, which explains why there are many more encoders in a system. Coupled with the fact that decoders are all solid-state devices with external power supplies, they are statistically less likely to fail than encoders.

Solid-state encoders have no moving parts and are consequently extremely reliable. Encoders with internal storage (such as hard drives) are a critical component of the most important reliability feature: fault tolerance during a network outage – a relatively frequent event compared to hardware failures. ANR enables this feature.

If encoders or decoders go offline, they show up in the VIDOS video management system because it supports centralized status monitoring. Both encoders and decoders are also SNMP-ready.

Decoders also spread the viewing load, because you can have an unlimited number on the network. Each decoder independently handles one to four streams of video and is not limited by the PC's processing power. Such decoders can drive analog and VGA monitors, as well as projection screens and monitor walls (such as those provided by Barco). Driven by the unceasing commoditization of PCs with upgraded video cards, they are being used as software decoders, presenting multiple windows of video on an array of PC monitors. Referred to as a "video wall," it is an attractive and flexible alternative to using dedicated decoders because the windows (or cameos) can be arranged in complex patterns to best suit your application's need.

The Camera

The most common camera reliability issue is video loss caused by a break in the connection or internal mechanism. This is automatically detected in the encoder, which immediately notifies VIDOS to trigger an alarm.

The most common malicious cause is uniform picture caused by masking (spray-painting) or hooding (covering the camera with a bag). Video content analysis algorithms embedded into the encoders detect these situations and trigger specific alarms.

Other common malicious issues fall into the following categories:

- Blinding caused by shining a bright light into the lens and saturating the image
- Diverting the camera so that is does not observe the area of interest
- Defocusing the image

The VIDOS Workstation

The VIDOS video management system is not used just for video surveillance. Technical support and field engineers also use it to alert them to problems with the network and devices.

Because encoders and decoders have field-upgradeable firmware, Bosch periodically releases improved and higher performance firmware. The units can be selected into a group and remotely upgraded in a single stroke.

VIDOS uses Maps and a variety of configuration files, and it is very common for these to be shared on a single drive – one that is backed up by IT on a regular basis.

Summary

Video over IP opens up new horizons, particularly around connectivity over long distances. However, with that enormous benefit come risks that must be mitigated by the informed selection of security hardware and software – as well as a trusted IP networking infrastructure and technical support.

It is easy to think that Video over IP implies that all the video must traverse the network, but with Bosch, you have the option to record at the edge, like the prevalent DVR. This means that video can be recorded at high quality and 24x7 without ever touching the network – until someone needs to play back the video.

Smart Video over IP CCTV installations use the network when its needed, not continuously. Excessive use of the IP network is the single biggest contributor to reliability performance degradation, and only Bosch has the answer: Recording at the Edge.