

Quadrox' Storage Management Principles

Management summary

As video recording software, GuardNVR aims at making the best use of the available storage capacity. The system maximizes the relevance of the stored data by managing the data life cycle based on data age, image activity, alarm events, POS transaction data and other metadata parameters. At the same time, GuardNVR's disk management ensures that recording continues in all circumstances so that no important events are missed.

GuardNVR's data lifecycle management replaces risky and obsolete technologies like scheduling and purely alarm-based recording and instead provides 24/7 operability and optimized storage.

GuardNVR stores the video in a standard file format and uses standard codecs, to ensure the data's availability at all times by effectively making it independent of the Quadrox software. This does not inhibit performance or security of the system.

The next step in storage technology is to move to a distributed system, which is more performant as well as more robust and secure. Dedicated recording solutions like GuardNVR will continue to make sense in the future, and Quadrox remains committed to provide the state-of-the-art to the security industry.

Maximizing data relevance

The capacity of any video recording system is limited. The actual amount of video that can be stored on a digital video system depends on two factors: the hard disk's capacity and the configuration. Obviously, a high quality, high frame rate stream consumes more storage space than a low quality one. The actual storage time varies on most recorders from a day to several months.

This limit implies that the recorded video won't be available on the recorder forever, unless you stop recording when the disk is full, which is clearly not a bright idea. Storage management is an absolute necessity for each video recorder to continually make room for new movies.

Quadrox considers intelligent storage management its core business. In this white paper the principles used to optimize storage are put forward.

GuardNVR versus alarm based recorders

The GuardNVR system of using metadata and events from other systems to optimize the movie storage should be set apart from recording systems that are completely based on alarms. GuardNVR uses at its basis a continuous storage system that records everything that moves. This means that meaningful video is always recorded, regardless of any alerts. Alarm-based systems only record that which is denoted as an alert and base their search mechanism completely on this premise.

In an alarm-based system, there is always a sensitivity trade-off: the alert trigger has to be set sensitive enough so that video that may be deemed important (e.g. by visual verification) is at all recorded, yet it has to be discriminate enough to provide a meaningful search and prevent the user from being flooded with alarms. The former leads to a decrease in attentiveness of the guard that has to review the alarms, the latter leads to a high chance of missing an important recording over the lifetime of the system. This is a lose-lose situation.

GuardNVR doesn't suffer from this problem. Instead, it turns it to a win-win situation. It always starts with recording video. The activity detection mechanism is tuned to optimizing recording (not discriminating potentially important events), and is sensitive enough not to miss out on any real movement. Yet, when a real alert occurs (based on information from other systems or algorithms), it offers all the advantages in search and recording optimization that an alarm-based system has. Additionally, it has no problems with overlapping alarms (due to the labelling mechanism), annotations that are only added after the event, or even changes in severity afterwards.

The central idea behind GuardNVR's storage management is the maximization of data relevance. If we cannot store video eternally, the video that can be found on disk should be optimally meaningful for the user. There is no use in storing video of trivial events.

GuardNVR achieves this optimal storage by taking into account as much information as possible to determine which movies should be deleted first. In other words, by considering metadata (extra information about the video), the software manages the video data's life cycle from birth (capturing) to death (deletion). It continuously evaluates how meaningful the video is to the customer and when the time has come for some data to die, it deletes the least relevant first.

The first, most trivial parameter that defines relevance is age. The older a movie is, the less likely that important events haven't been noticed and consequently handled yet. Therefore, as a general rule, the oldest movies will be deleted first, just like old people are likely to die sooner than youngsters.

In case an important event does occur, the movie can be exported. Exported movies have eternal life, until they are deleted manually by the user; i.e. GuardNVR never makes an assumption on a movie that was important enough to be exported.

Exported movies are copied from the main storage. The original copy follows the same rules as other video, so after a while it will be deleted and it will not be available anymore through the normal application search. The exported copy is left to the mercy of the user.

Secondly, video that doesn't contain any events (as determined by the activity detection feature) is not stored at all¹, since allowing it a life would reduce the lifetime of other movies and video without action is with high probability irrelevant to the user.

Thirdly, the movie can be labelled with events from other systems, like alarm systems (dry contacts, OPC alarms, CAP alarms, video intelligence alerts, etc), ATM machines, POS terminals, etc. By labelling video, the user sets it apart from other recorded information, as such indicating that this recording has some special value to him. This makes it easier to search intelligently in the video, based on information other than time alone. More to the point, the chance that this video should be kept as long as possible is higher. The GuardNVR software allows the user to specify the concept "longer" by imposing a minimum event lifetime and/or a minimum number of events to keep.

Disk management – why we do not fill the disk completely

If you examine the disk usage of GuardNVR closely, you will notice that the system never uses the complete disk space. At all times, a buffer of about 12% of the disk is kept free. There are two important reasons for this.

First of all, this buffer ensures that the system can keep recording at all times. The movie management process responsible for deletion runs in the background and doesn't influence recording as such, but gathering information about the recorded movies does take some time. Also, it is only run at regular intervals. If the full disk would be used, the new recordings could potentially fill the disk in the periods between deletion moments, after which recording would stop. Now, new movies might fill up part of the buffer temporarily, but never fill the disk completely.

The second reason is more technical. The 12% value comes from a best practise as proscribed by Microsoft regarding its NTFS file system. Filling up the entire disk would cause fragmentation of the files, which would in turn reduce performance of the disk and ultimately the applications working with it. By keeping part of the disk unused, we prevent fragmentation and make sure that the disk can be overwritten almost infinite times before impacting the system's performance.

This buffer of empty disk space should be taken into account when specifying the hardware on which GuardNVR will run.

In case you configure GuardNVR to use less than the full disk space, the buffer will be calculated based on the amount of space you have allocated for movies.

¹ We could store all video and delete non-activity video first, but this would put more load on the hard disk, reducing its lifetime. Because of this, we don't do this by default.

If there isn't enough space on the storage medium to keep all the events as requested, there is a risk that new, recent movies will be "smothered" by labelled movies and deleted almost immediately. A safety mechanism is in place that ensures that at least 12 hours of non-labelled movies will be recorded, if needed at the cost of the user-imposed lower limits above.

To continue our "survival of the fittest" analogy, we can say that smart movies will generally live to a ripe old age, but the young movie children are protected from them in case it comes to a fight.

Sometimes the system has to decide between several labelled and non-labelled movies which are all old enough to be deleted. In that case, a prioritization mechanism kicks in that sorts the movies according to importance (e.g. severity of the alarm) and deletes those that are least important first, until enough space has been freed. This occurs mostly when ample storage space is available. Since this is a relative criterion, it introduces a statistical element into the equation, making it difficult to predict how long labelled and non-labelled movies will survive exactly.

Note that the movies are labelled, not copied. This implies that there is no dedicated storage space reserved for event-labelled movies, and that no information is doubled in size, like is the case with exported movies.

Apart from maximizing the amount of relevant data on the disk, also some limits can be imposed. The user can choose to use only part of the disk, e.g. because he doesn't want the video system to interfere with other applications in an integrated scenario. Additionally, there is the possibility to put an upper lifetime on movies. In that case, movies older than the specified date will be immediately deleted (one might say executed), regardless of their relevance. This option is used when legal rules apply that forbid long-time recording of data.

Sometimes disaster strikes and a situation presents itself in which the previous procedures can no longer be applied. For example, the disk is completely filled by a data flood from another application, preventing GuardNVR to continue recording. The GuardNVR might not have enough resources to properly prioritize all the movies and delete the least relevant ones. In such case, emergency procedures kick in that will delete the oldest movies to free space to continue the recording process. This might mean that labelled movies are deleted indiscriminately and important information is lost. If this happens, GuardNVR can be configured to send a notification and will always log a message in the event log describing the situation.

If specific information is so important that loss is unacceptable in all cases, it should be exported and kept on a separate storage. This can be done automatically in case of alarm, using FTP upload.

In some exceptional cases, GuardNVR might temporarily stop recording during critical situations. It will start again as soon as the situation normalises.

Scheduling is obsolete

A lot of older video recording systems in the market, and some new ones, use scheduling to optimize storage. The idea is to not record video when it is assumed that nothing is happening, or that a person is present anyway to handle the situation.

This method introduces an enormous risk of missing events that happen outside of the schedule time, or right on the edge of the schedule. The assumption that nothing will happen during non-scheduled often proves to be false, and when it does there are no recordings for the authorities to forensically analyse the situation. The same is true

when the customer relies on personal handling of security issues.

This contrasts with the expectation of the customer, who thinks that he is buying a security system that is operational 24/7. Often “optimizing recordings” seems a good idea at the start, until they find out that vital recordings are missing. Scheduling effectively turns the system off during some times of the day, which is not acceptable in modern day security.

Additionally, scheduling required a lot of maintenance to keep office hours up to date, add data about public and other holidays, etc. It is not a one time configuration. Instead it requires someone to adjust the configuration regularly, which is expensive for the customer and adds substantially to the total cost of ownership of the system.

When something has to be done regularly, it runs the risk of being done badly. If scheduling is already fundamentally risky business, the potential for misconfiguration and negligence adds even more to that risk, with a very high probability of missing vital recordings as the result.

With modern recording systems like GuardNVR, there is no reason to run these risks as a user, or to add scheduling costs to the customer’s bill. The data relevance optimization outlined in this paper ensures maximum data usefulness without any user intervention so that the customer’s expectation is perfectly matched. With the increase of hard disk size in recent years, the user doesn’t have to worry about recording time either. Scheduling is obsolete technology.

Ensuring data availability

Contrary to its name, the purpose of a video recording system is not to record data. It is to make (historical) information available to its users. GuardNVR ensures constant data availability by recording in standard formats. We use the standard file format ASF, and standard codecs like JPEG, MPEG-4 and WMV.

Using standards prevents customer lock-in to our software. In fact, you don’t need GuardNVR at all to play the movies that it recorded. The original recordings (not only exports) can always be visually verified by the user or the authorities using most 3rd party media players. If needed, the movies can easily be archived on other storage media like CDs. The customer can rest assured that the movies will still be playable in the far future.

There are no disadvantages to using standard recording formats. The use of cache files prevents that the file system becomes a bottleneck and makes the system as performant as database-based systems.

Although the files are playable by any media player, the security of the data remains guaranteed by preventing attacks on the level of the operating system (Windows provides a fail-safe login and user rights mechanism) and the network. Some claim that their system is more secure because they use a proprietary format. This type of statement is mocked in cryptographic circles. GuardNVR provides electronic security through tried and tested cryptography-based standard mechanisms, while always allowing legitimate user access to data.



About Quadrox:

Quadrox is a leading provider of digital video security solutions. Its standards-based WebCCTV™ product family provides an efficient and reliable infrastructure by which companies can distribute, update and manage video sources and content over corporate intranets, extranets and the Internet. Quadrox European offices are located in Belgium. Quadrox US offices are located in Henderson, Nevada.

For additional information, please, contact:

Svitlana Tanasiychuk

Quadrox NV, Duigemhofstraat 101, 3020 Herent, Belgium

Tel: +32 (016) 58 25 85

Fax: +32 (016) 58 25 86

E-mail: info@quadrox.be

Website: www.quadrox.com