



TECH TIP

Designing a video surveillance
system for reliability

Redundancy

Introduction

Providing a reliable video surveillance system is essential when it comes to mission-critical enterprises, where any system failure can lead to unpredictable losses. As a result, a video surveillance system should always be designed in a way that follows best practices to maximize reliability and minimize downtime.

A redundancy plan is necessary, but it may be providing a false sense of security if single points of failure (which create weak links in the system) have not been considered and eliminated. The more parallel elements that exist in a system, the less risk of catastrophic failure once one of them fails. The operation is still guaranteed by the other elements and this usually provides enough time to repair the failure before resulting in a complete system outage. To summarize, when designing a video system for reliability:

- A system interconnected in daisy chain will fail when its weakest element will fail. i.e. it's important to design each element as reliable as possible.
- Designing a redundant path for each critical functionality will permit the system to sustain a branch failure while keeping the whole system operational.
- It's critical to perform a real-time system health monitoring and failure audit; the goal is to be able to repair any reported failure with minimum latency.

The system will be more predictable and require less urgent onsite interventions to solve critical failures. Overall, this will also result in a satisfied customer, which is the main goal of any large-scale deployment.

The remainder of this document will describe how such concepts have been incorporated into March Networks' video surveillance solutions.

Design for reliability: March Networks' approach to video surveillance

Reliability starts with the building blocks

A video surveillance system can be split into:

1. Onsite elements.

Cameras connected to a local recorder, which is then routed to a corporate network for local/remote access.

2. Central services.

Typically installed in the corporate data center, these services offer a unified platform to users of all different categories (investigators, administrators, guards, etc.) for the supervision, management, monitoring and data aggregation of all the sites resources.



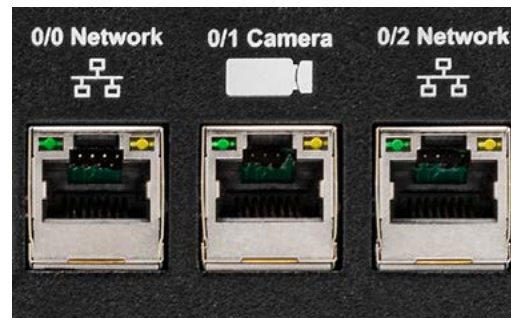
Let's discuss the various elements individually.

NVRs

March Networks designs and oversees the manufacturing of all our embedded recorder platforms. Our goal is to provide reliable building blocks which rarely fail, thus reducing onsite maintenance activities. For instance, our X-Series Hybrid Recorder family offers an astonishing Mean Time Between Failures (MTBF) of more than 268,000 hours (approximately 30 years)! This represents one of the highest (if not the highest) MTBF available on the market. In addition, the following features can further extend reliability:

- Redundant power supply (available for select recorder families)
- Redundant fans
- Redundant network interfaces (available for select recorder families)
- Internal battery to ensure graceful shutdown preventing file corruptions in case of power outages
- RAID configuration for the storage
- The Operating System (OS) and application on a dedicated flash chip

Figure 1: Detail on the back of the X-Series recorder. The three network ports available on the X-Series are designed to offer different communication paths for local cameras (0/1), primary (0/0) and redundant (0/2) connectivity with a corporate network.



Cameras

We supervise the manufacturing of our cameras and customize the firmware to have full control of all the available features in order to minimize the occurrence of hardware issues or software bugs. When combined with our mass management capability, we can ensure all IP cameras are always running the latest firmware containing bug fixes and security patches, which results in smooth device operations.

Application layer redundancy

As previously noted, selecting a reliable solution consisting of recorder, switch and cameras is the prerequisite to reduce onsite system downtime. The next step is to work on the system architecture to further strengthen the solution.

Mitigate camera to recorder disconnection

In the event of a network disconnection between cameras and recorder, it's possible to configure on-camera recording using an SD card when using March Networks cameras and Command software. This is called March Networks Shadow Archiving feature. The recording on the camera's SD card can then be passed to the NVR once the disconnection has been resolved. The video can be placed in the exact sequence/timeframe required for seamless recording coverage.

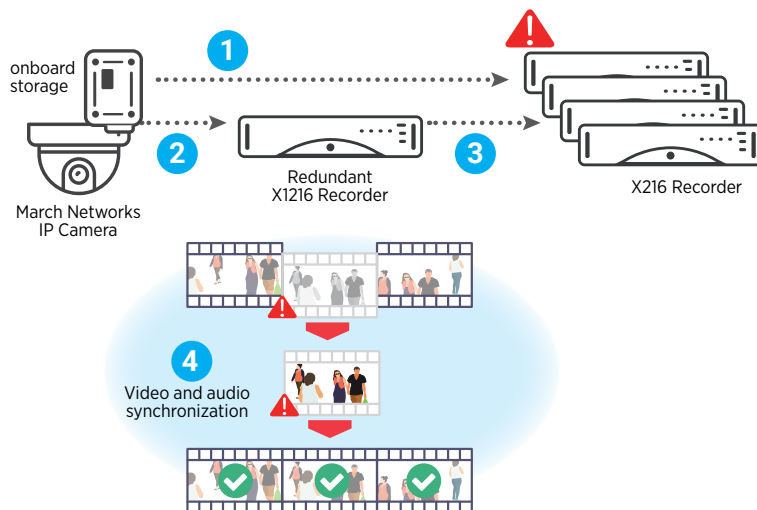


For select camera models, it's also possible to have redundant power supply (Power over Ethernet (PoE) and an external power supply), which keeps the camera operational in case the switch fails.

Mitigate the recorder failure

Our X-Series Hybrid Recorders and VMS software (Command Recording Software or CRS) both support an M:N redundancy. Meaning, it's possible to configure M standby units to actively monitor N production recorders. In the case that one of N fails, one of the M standby recorders will take its place. The most common scenario is to have a spare recorder monitoring one or more production recorders, offering redundancy in case of a single failure and giving margin to the maintainer to replace the faulty unit. March Networks Command software can be configured to automatically transfer the temporary archive created on the redundant recorder to the production recorder once it's back in service.

Figure 2: Normally IP cameras will stream to respective production NVRs (path 1). In the case of NVR failure, a redundant NVR will resume from stand-by and replace the faulty NVR (path 2). Then it will send recorded video once the production NVR has resumed (path 3 including activity 4 for recorded video synchronization). In addition, camera onboard storage will back up any video during the process to avoid any gap in the recordings.



Central services redundancy

Our central management software (Command Enterprise Software or CES) is used to monitor the health status and user activities from each site, perform mass management on firmware and configure recorders and cameras. It also offers customizable user access rights, so system administrators can grant different levels of access to various users. This multi-server software solution also hosts additional applications such as our Searchlight business intelligence software. It's clearly crucial to keep this service operational at all times to allow complete system usability.

Let's discuss available options to strengthen the reliability of CES services. These options are dependent upon the size of the installation and on the available IT resources. This will lead to one of the following configurations:



CES connected to an SQL Express database running on the same physical server

For small to medium installations (consisting of up to 250 recorders/sites), it's still possible to install CES software relying on an SQL Express instance created on the same server.

During the installation process, it's possible to select "Internal Database" so that the installation package also installs SQL Express edition on the same server and configures the environment to create connectivity between the CES service and SQL instance. This is the easiest way to install CES and usually requires minimum engagement from the customer's IT department.

In terms of redundancy, a backup server is required to replace the faulty primary one. Before starting the CES service on the backup server, it's necessary to upload the last database and configuration backups taken from the primary CES server. More details on this procedure can be found in the [Command Enterprise Installation Guide](#) in chapter 4 "Backup and Restore — Failover to a Redundant Server".

To avoid stopping the CES service to backup database files, an attractive option is to install an independent instance of Microsoft SQL Express database on the primary server and choose "External Database" while installing the CES software. In this way, the customer's IT department will be able to access the database instance and schedule periodic database backups. More details on this procedure can be found in the [Command Enterprise Installation Guide](#) in chapter 4 "Migrating from the Internal Database to an External Database".

CES connected to an SQL Express database running on the same virtual server

This scenario will offer the same installation options described in the previous section (Internal or External Database using SQL Express on the same server — suitable for up to 250 servers/sites), but will greatly simplify the procedure to backup CES data. It is typically easy to take periodic snapshots of the whole virtual machine, making a disaster recovery quite straightforward to implement. Simply start the last working snapshot once the primary server has been detected as the faulty (usually the full procedure can be automatically managed by the virtualization management application). In the case of a software failure, it's not even necessary to use additional resources — just destroy the faulty virtual machine and execute the last working snapshot.

CES on a physical server and connected to an SQL Professional/Enterprise database running on a different server

This is the configuration we recommend for medium to large installations (more than 250 recorders/sites). In terms of redundancy, it's possible to schedule the CES configuration and external database backups as required without any limitation. Considering many enterprise organizations have SQL server instance as an available IT resource, it's possible to rely on such an existing structure to connect the CES service and benefit from their backup programs for the database.

In case of a primary CES server failure, it will be necessary to start a redundant server using the last primary CES configuration backup and, once online, this will connect to the existing SQL instance.



Customer Support and Assistance

North America, South America, & Australia

Direct: 1.613.591.1441

Toll Free (US & Canada):
1.800.472. 0116

E-mail:
techsupport@marchnetworks.com

EMEA

Direct: +39 0362 17935 ext. 3 (CET)

E-mail:
emeatechsupport@marchnetworks.com

Middle East & Africa

Direct: +00 971(0)52 818 8483

Email: supportmea@marchnetworks.com

CES on a virtual server and connected to an SQL Professional/Enterprise database running on a different server

This is possibly the most flexible approach. Since the server is virtual, it's a basic task to program periodic snapshots of the CES server and restore the last working snapshot in case of a software failure.

A hardware failure for the server hosting the CES service is typically not a problem. In large IT departments there are several procedures to effectively handle hardware redundancy.

Conclusion

March Networks considers overall reliability and cybersecurity to be two fundamental aspects when designing a video surveillance solution. We've described the main action items we incorporate in our solution to ensure our customers do not experience catastrophic system failures. We've also provided some guidelines on the best practices to ensure video will be available when it's required. Adopting a reliable system is a long-term investment that reduces system maintenance and unplanned onsite activities, which lowers the total cost of ownership of the solution.

Please contact March Networks' sales engineering team for further details. They will work together with you to identify the best option for your specific business requirements.

Company Overview

March Networks® helps organizations transform video into business intelligence through the integration of surveillance video, analytics, and data from business systems and IoT devices. Companies worldwide use our software solutions to improve efficiency and compliance, reduce losses and risk, enhance customer service and compete more successfully. With deep roots in video security and networking, March Networks is also recognized as the leader in scalable, enterprise-class video management and hosted services. We are proud to work with many of the world's largest financial institutions, retail brands, cannabis operators and transit authorities, and deliver our software and systems through an extensive distribution and partner network in more than 70 countries. Founded in 2000, March Networks is headquartered in Ottawa, Ontario, Canada. For more information, please visit: www.marchnetworks.com.



North America 1 800 563 5564
Latin America +5255 5259 9511
Europe +39 0362 17935
Asia +65 6818 0963
Australia and New Zealand +61 1300 089 419
Middle East and Africa +971 4 399 5525

© 2022 March Networks. All rights reserved. Information in this document is subject to change without notice. MARCH NETWORKS, March Networks Command, March Networks Searchlight, March Networks RideSafe, and the MARCH NETWORKS logo are trademarks of March Networks Corporation. All other trademarks are the property of their respective owners. 060-3469-00-A marchnetworks.com

