

# IP-Videoarchitektur



*Die Vorteile einer IP-gestützten, vernetzten Videoüberwachung sind im Vergleich zu herkömmlichen analogen Systemen signifikant. Oliver Vellacott, CEO von IndigoVision erklärt, dass der wirkliche Vorteil von IP-Video erst dann sichtbar ist, wenn die Lösung auf einer tatsächlich verteilten Architektur basiert.*

Dieser Artikel erörtert die gravierenden Probleme der Skalierbarkeit, die auftreten, wenn eine IP-Videoüberwachung auf eine zentralisierte Architektur gestützt ist und wie eine verteilte Architektur eine flexible und skalierbare Lösung liefert, wodurch man Systeme erhält, die verteilt über Einsatzorte, Städte und Länder eingesetzt werden.

## Speichern der IP Videodaten

Es gibt typischerweise zwei unterschiedliche Ansätze beim Speichern von Daten in einem IP-Videosystem. Bei einer zentralisierten Architektur wird eine Masterdatenbank verwendet, die sich normalerweise im zentralen Steuerraum oder im Hauptbüro befindet. Bei einer verteilten Architektur befinden sich die Daten rund um das Sicherheitsmanagementsystem und im Allgemeinen in der Nähe zu dem Ort, an dem sie erstellt oder gebraucht werden.

Die gespeicherten Daten können in zwei Arten unterteilt werden – Konfigurationsdaten und Live-Daten.

**Konfigurationsdaten** sind die Informationen des Einsatzortes, die das Design und den Aufbau des Sicherheitsmanagementsystems spezifizieren. Beispiele für Konfigurationsdaten umfassen Listen der Kameras, Nutzer, Nutzergenehmigungen, Struktur des Einsatzortes, Pläne, die das Layout des Systems und die Lizenzierungsinformation enthalten. Nach der anfänglichen Installation und der Inbetriebnahme des Sicherheitsmanagementsystems, werden die Konfigurationsdaten nicht routinemäßig geändert. Das Betriebspersonal hat routinemäßig Zugang. z. B., wenn es sich in das System einloggt.

Die **Live-Daten** sind typischerweise die Aufnahmen der Videoüberwachung und Alarminformation. Zu den Live-Daten besteht ständiger Zugang während des normalen Sicherheitsmanagementbetriebs, sei es durch Vorrichtungen, die die Daten speichern oder Betriebspersonal, das die Daten überprüft.

Die Konfigurationsdaten werden normalerweise in einer Datenbank aufbewahrt, die Datenbank des Einsatzortes genannt wird. So ist es für die Administratoren einfacher, Veränderungen vorzunehmen und zu verwalten, dass aber auch auch Probleme mit sich bringt. Führt ein Administrator Veränderungen der Datenbank des Einsatzortes durch, dann ist die Frage, wie diese Veränderungen zu den Nutzern gelangen, die über das gesamte Sicherheitsmanagementsystem verteilt sind.

Die naheliegende und einfache Lösung ist, die Datenbank des Einsatzortes zentral auf einem Masterdatenbankserver zu speichern und allen Nutzern Zugang zu diesem Server über das Netz zu ermöglichen. Dies wird als zentralisierte Architektur bezeichnet.

Viele Systeme nutzen eine zentralisierte Architektur, um neben der Konfigurationsdaten noch weitere Daten zu speichern. Dort können auch Live-Daten wie Videoaufnahmen- oder Alarmdaten gespeichert werden.

## Zentralisierte Architektur

Die Figur 1 zeigt ein Sicherheitsmanagementsystem, das aus einem oder mehreren Einsatzorten besteht, von denen jeder über ein eigenes lokales Netzwerk (LAN) verfügt, das an ein zentrales Büro angeschlossen ist. In dem zentralen Büro befindet sich auch der zentrale Dateiserver, der die Datenbank des Einsatzortes beherbergt. In dem zentralen Büro befinden sich zusätzlich Netzwerkvideorekorder (NVRs), die die Videoüberwachung und Alarmdaten aufnehmen.

Jede Kamera und jeder Arbeitsplatz in jedem Büro muss regelmäßig oder in manchen Fällen sogar ständig mit dem zentralen Büro in Verbindung stehen, um Veränderungen und Aktualisierungen der Datenbank des Einsatzortes zu prüfen. Dies umfasst das Prüfen der Lizenzgültigkeit oder das Speichern von Aufnahmen und Alarmdaten.

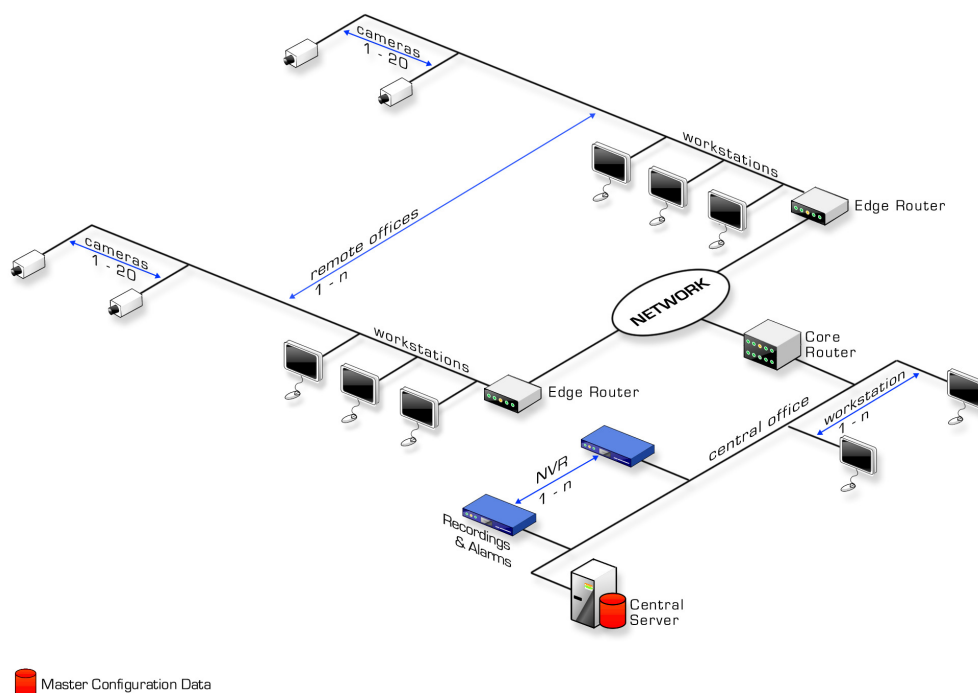


Figure 1: Typical Centralized Architecture

Eine zentralisierte Architektur ist die Ursache von vier großen Problemen:

1. **Kosten** – Alle Nutzer befinden sich in ständiger Kommunikation mit dem Hauptbüro. Bei einer LAN bedeutet das, dass teure qualitativ hochwertige Switch gekauft werden müssen und bei einem Fernnetz (WAN) bedeutet es, wertvolle Bandbreite zu nutzen.
2. **Verlässlichkeit und Ausfallsicherheit** – Was geschieht, wenn ein Switch des WAN oder LAN ausfällt? Entfernte Nutzer können dadurch keinen Zugang zu den Live-Videos und den Aufnahmen von den Kameras haben, die sich eigentlich bei ihnen in der Nähe und auf einer funktionierenden LAN befinden.
3. **Einziger Störungspunkt** – Was geschieht, wenn der Server ausfällt, auf dem sich die Datenbank des Einsatzortes befindet? Alle Systemnutzer hängen von dem Zugang zur Datenbank des Einsatzortes ab. Zum Beispiel zum Prüfen der Loginzugangsdaten oder der Lizenzgenehmigungen. Wenn die Datenbank des Einsatzortes ausfällt, bricht das gesamte Sicherheitsmanagementsystem zusammen.
4. **Skalierbarkeit** - Das System verstopft, wenn mehr Kameras und Nutzer jedem Büro zugeordnet werden und mehr Büros dem Netzwerk. Die lokalen LANs, WAN-Verbindungen und zentralen Server verstopfen in dem Versuch mit dem erhöhten Verkehr fertig zu werden, der für das Überprüfen der Datenbank des Einsatzortes, die Lizenzvalidierungen und das Speichern von Aufnahmen und Alarmen anfällt.



Weniger als 0,1% der Videos werden jemals angesehen, warum sollte man also unnötig wertvolle WAN-Bandbreite verschwenden? Verwenden Sie das WAN nur, um die relevanten aufgenommenen Videodaten umzuspeichern.

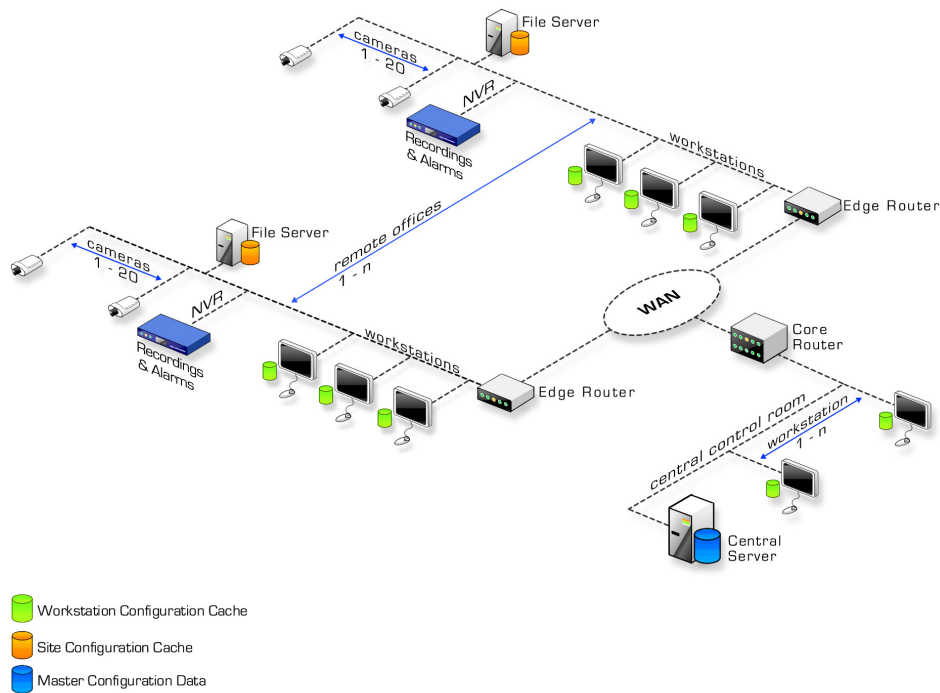
## Lösung der Probleme einer zentralisierten Architektur

Die vier großen Probleme, im Zusammenhang mit einer zentralisierten Architektur, werden mit einer verteilten Architektur überwunden:

1. **Kosten** – Es wird keine wertvolle WAN-Bandbreite für die ständige Kommunikation mit allen entfernten Geräten benutzt. Stattdessen werden die Konfigurationsdaten gezielt verteilt. Im Falle eines betrieblichen Zwischenfalls müsste nur das benötigte Live-Überwachungsvideo über das WAN oder das erweiterte LAN geleitet werden. Die Notwendigkeit einer Prüfung der Lizenzdaten über das Netzwerk entfällt vollständig. Kostengünstige Hauptnetzwerk-Switch können ausgelegt werden, um die reduzierten Netzwerklasten zu bewältigen.
2. **Verlässlichkeit und Ausfallsicherheit** – Eine potenzielle Fehlerquelle im Sicherheitsmanagementnetzwerk ist das WAN. Man kann Geld investieren, um die Verlässlichkeit der WAN-Anschlüsse zu verbessern. Es ist jedoch viel wirksamer die Daten so zu verteilen, dass die Nutzer trotz eines Ausfalls der WAN-Verbindungen weiterhin ein funktionierendes Sicherheitsmanagementsystem zur Verfügung haben.
3. **Einziger Störungspunkt** – Eine weitere Fehlerquelle innerhalb eines Sicherheitsmanagementsystems ist die Datenspeicherung – entweder der zentrale Datenbankserver des Einsatzortes oder die Aufnahmegeräte. Man kann auch hier Geld investieren, um die Leistung und Verlässlichkeit dieser Geräte zu verbessern. Es ist aber viel wirksamer die Daten so zu verteilen, dass die Nutzer trotz eines Ausfalls dieser Komponenten weiterhin ein funktionierendes Sicherheitsmanagementsystem zur Verfügung haben.
4. **Skalierbarkeit** – Bei einer verteilten Architektur können Kameras und Nutzer einem lokalen Büro hinzugefügt werden, wobei der WAN-Verkehr nur geringfügig zunimmt, das Video wird lokal geleitet und gespeichert. In ähnlicher Weise ist ein zusätzliches entferntes Büro nur das Duplikat bestehender Büros mit lokalem LAN und Speicher. Für noch größere Systeme können multipel zentrale Server verteilt und synchronisiert werden, indem noch eine Schicht für Verteilung und Ausfallsicherheit hinzugefügt wird.

## IP-Videoüberwachungssysteme für Firmen

Eine verteilte Architektur ist eine grundlegende Anforderung für große Firmensysteme mit Tausenden von Kameras, die auf viele Örtlichkeiten verteilt sind. In einigen Fällen sind diese Örtlichkeiten geografisch über Einsatzorte, Städte oder sogar Länder verstreut, wie im Falle von großen Konzernen, Städteüberwachung, Eisenbahnnetze oder Straßensysteme. In anderen Fällen kann es an einem großen Einsatzort eine hohe Kameradichte geben, die in verschiedene Kameragruppen unterteilt sind, wie im Falle von Casinos oder Flughäfen. Für Firmensysteme ist dies eine grundlegende Anforderung, aber auch für kleinere Systeme ist das wichtig. Die Figur 3 zeigt das typische Layout eines großen verteilten Sicherheitsmanagementsystems.



Figur 3: Große Distributed Security Management System

Große Systeme haben gewöhnlich auch einen zentralen Steuerraum, von dem aus das gesamte System überwacht werden kann. Einige Systeme verfügen über verschiedene zentrale Steuerräume. Das gesamte Netzwerk ist durch ein WAN verbunden, das geleaste Linien, kabellose Verbindungen, DSL-Anschlüsse, Satellitenverbindungen und sogar das öffentliche Internet nutzen kann.

Bei einer verteilten Architektur hat jede Örtlichkeit oder Kameragruppe einen lokalen Dateiserver und alle Arbeitsplätze sowie diese Örtlichkeit haben Caches. Die Masterkonfigurationsdatenbank befindet sich in einem zentralen Steuerraum auf einem zentralen Server. Jede Örtlichkeit verfügt auch über einen lokalen Dateiserver. Die lokalen Dateiserver werden alle mit der zentralen Masterdatenbank synchronisiert.

Bei jeder Örtlichkeit kommunizieren die individuellen Arbeitsplätze nur mit dem lokalen Dateiserver, niemals mit dem zentralen Server im Hauptsteuerraum. Zusätzlich verfügt jeder Arbeitsplatz über ein lokales Cache der Konfigurationsdaten. Jede Örtlichkeit verfügt über ausreichend lokalen Speicherplatz in Form von NVRs, um alle lokal erstellten Video- und Alarmdaten aufzunehmen, womit der Verkehr auf dem WAN verringert wird.

Fällt der zentrale Server aus oder bricht die WAN-Verbindung zusammen, hat das Betriebspersonal die lokalen Caches der Datenbank des Einsatzortes, sodass immer noch Zugang zu jedem Gerät auf der LAN besteht. Zusätzlich führt das Verteilen der Aufnahmeleistungsfähigkeit dazu, dass das Betriebspersonal, das sich lokal zu dem Zwischenfall befindet, Zugang zu Live-Videos, aufgenommenen Videos und Alarmdaten für ihre lokalen Kameras hat, selbst wenn die Kommunikation mit dem zentralen Büro ausgefallen ist.

## Zusammenfassung

Die Systemdesigner und Endverbraucher sollten sich vergewissern, wenn sie eine IP-Videoplattform für ihr Sicherheitssystem auswählen, dieses auf einer verteilten Lösung basiert, da sonst die fehlende Skalierbarkeit das zukünftige Wachstum behindern kann und aufgrund eines einzigen Störungspunktes der Betrieb unzuverlässig sein kann.



### Der Verfasser

Oliver Vellacott gründete 1994 IndigoVision. Er arbeitete zuvor als Produktmanager mit dem Schwerpunkt intelligenter Kameraprodukte. Oliver Vellacott studierte zunächst Klavier an der Guildhall School of Music, machte am Londoner Imperial College einen Abschluss im Bereich Softwareentwicklung und schloss sein Studium an der Universität Edinburgh mit dem Dokortitel im Bereich Elektrotechnik ab.

*Dr. Oliver Vellacott, CEO,  
 IndigoVision Group plc,  
 Charles Darwin House  
 The Edinburgh Technopole  
 Edinburgh, Großbritannien, EH26 0PY  
 Tel.: +44 131 475 7200  
 Fax: +44 131 475 7201  
 www.indigovision.com*