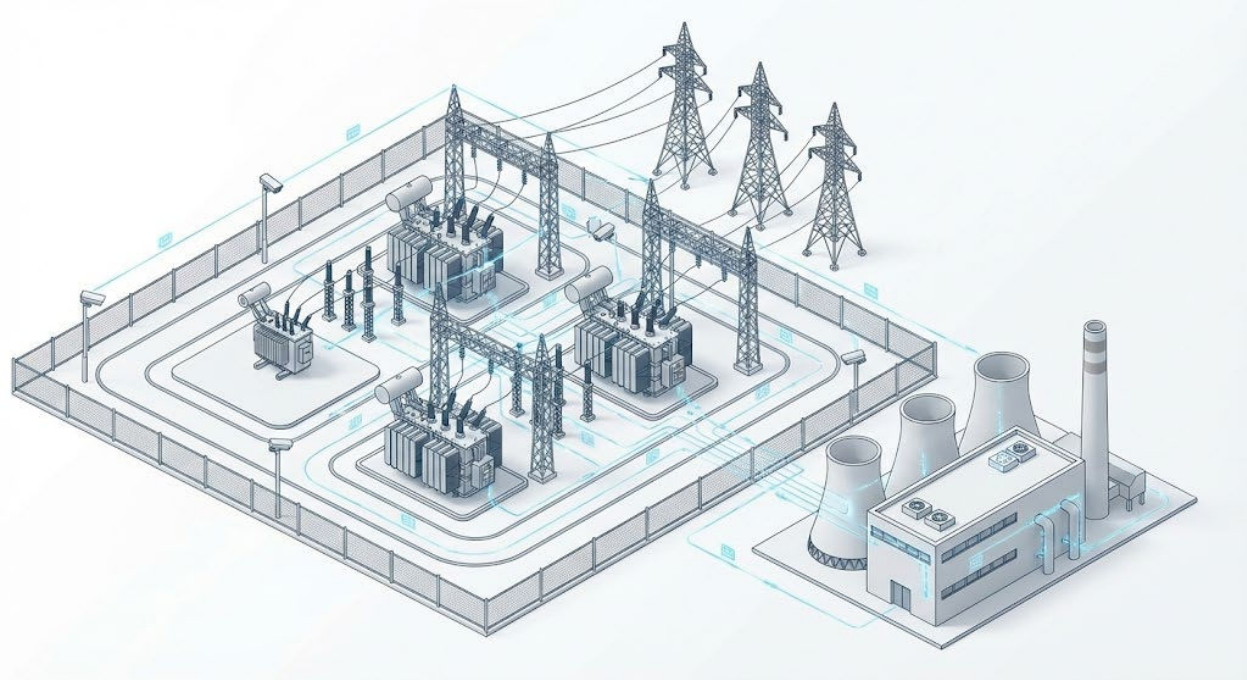
USE CASE DOCUMENTATION

Critical Infrastructure Protection

UTILITIES & ENERGY SECTOR

Video Security Solutions for Power Plants, Substations, and Energy Infrastructure



> *"Vega Systems has been an invaluable partner... helping us deliver world-class security solutions. Their team has been professional, knowledgeable, and responsive to our needs."*
>
> **— Krish Shetty, CEO, WizNucleus (Nuclear Cybersecurity)**

Executive Summary

Utilities operate in a high-stakes environment where security infrastructure must meet stringent regulatory requirements while maintaining uninterrupted operations. From remote substations miles from the nearest fiber line to nuclear facilities with zero tolerance for downtime, standard video security solutions are insufficient.

Vega Systems provides a resilience layer that maintains NERC CIP compliance and secures perimeters. Our comprehensive product suite addresses the unique challenges faced by power generation facilities, transmission networks, and distribution infrastructure.

Key Requirements Addressed:

- Sub-second live video recovery during failure episodes
- Redundant video storage with automatic failover
- Low-latency threat event alert delivery
- NERC CIP compliance for physical security controls
- Remote site connectivity without fiber infrastructure
- Zero-downtime system modernization and migration

Industry Challenges

The utilities sector faces unique security challenges that traditional video management systems cannot adequately address:

1. Zero Tolerance for Downtime

Power generation and distribution facilities operate 24/7/365. Any loss of situational awareness poses a risk to public safety and critical infrastructure. Nuclear facilities have stringent requirements for the near-instant recovery of live video during failures.

2. Geographically Distributed Assets

Utilities manage hundreds of remote substations, pipelines, and transmission facilities spread across vast geographic areas. Many of these locations lack fiber connectivity, making traditional VMS architecture impractical. Security teams need real-time visibility on these unmanned sites without the capital expense of dedicated network infrastructure.

3. Regulatory Compliance (NERC CIP)

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards impose strict requirements for physical security, access control, and audit trails. Regulatory fines for data loss or security gaps are substantial. Facilities must maintain complete footage of restricted area entries and demonstrate compliance during audits.

4. Legacy Infrastructure Constraints

Many utilities operate on aging video security infrastructure because system upgrades are considered too risky. Fear of creating security blind spots during migration hinders modernization. Facilities need upgrade paths that minimize downtime and maintain continuous protection throughout the transition.

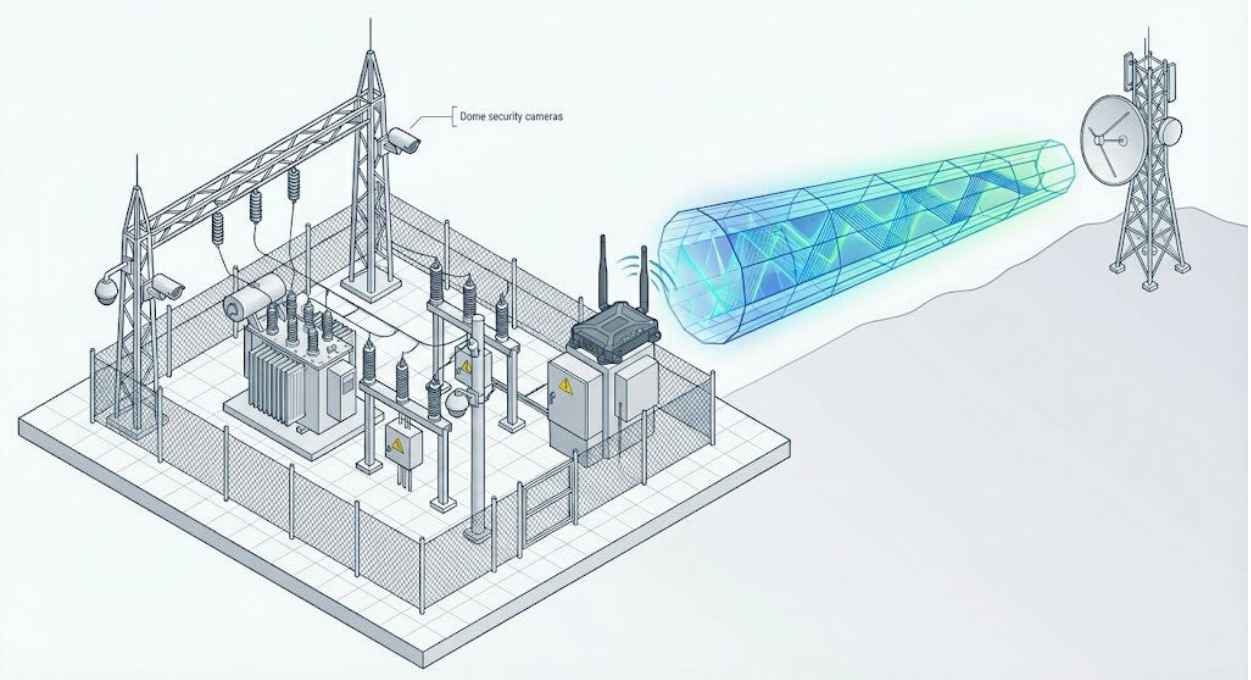
Vega Systems Solutions

Vega Systems offers a comprehensive suite of products designed to address the specific challenges of utilities and critical infrastructure protection. Our solutions integrate seamlessly with Milestone XProtect VMS to provide enterprise-grade resilience.

Product	Capability
RMF	Cybersecure redundancy with active-active architecture, sub-second failover, and high-availability alarms
SureStream	Direct camera-to-client streaming when servers fail, maintaining perimeter visibility
Atlas	Secure video transport over cellular/satellite for remote substations and pipelines
Nidhi	Automated backup and restore, for regulatory compliance and audit trail protection
XPort	Zero-downtime migration for legacy system modernization

Use Case 1: Remote Substations & Pipelines

THE CHALLENGE: *"We have 50 remote substations. Trenching fiber is impossible, but we need eyes on the transformers."*



Solution: Atlas Secure Edge Transport

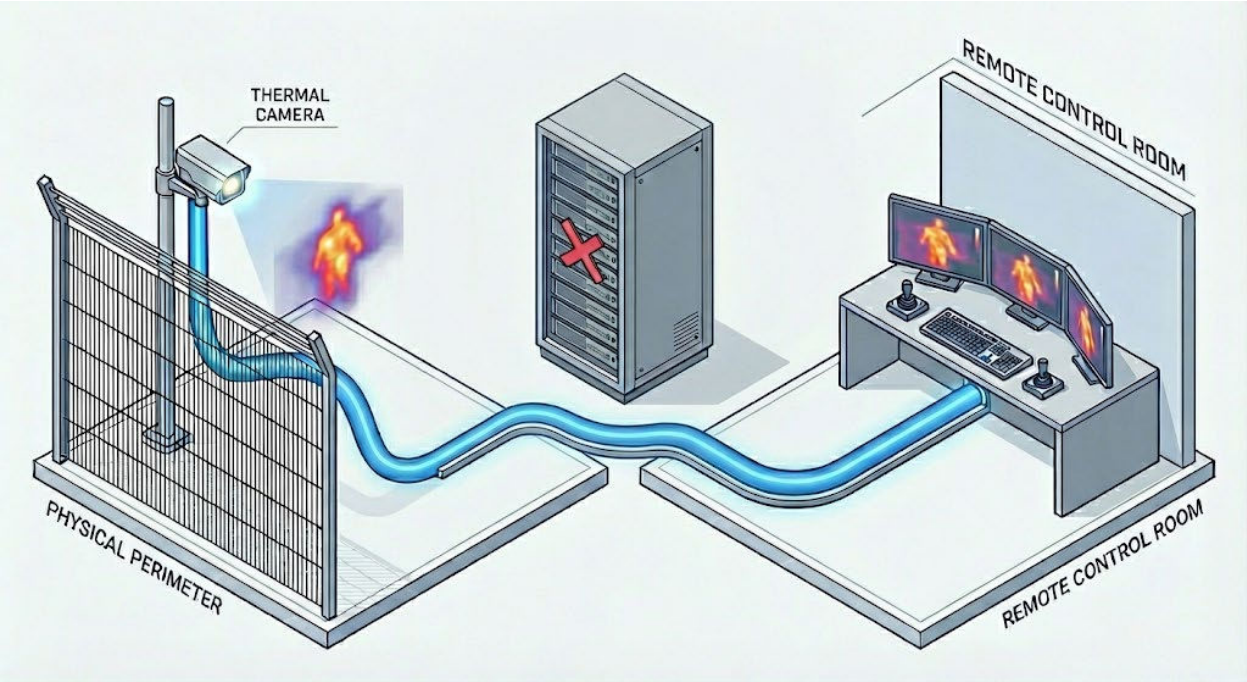
Atlas is purpose-built for edge deployments where fiber infrastructure is impractical or cost-prohibitive. By utilizing 4G/5G/Satellite connections, Atlas creates a stable, encrypted pipeline for thermal and optical video feeds.

Key Capabilities:

- **Outbound-Only Cloak:** Zero open ports or public IP addresses, preventing exposure to Shodan scanners and botnets
- **Adaptive Stream Switching:** Dynamic adjustment to network conditions for smooth video, even in low-bandwidth zones
- **Universal VMS Translation:** Standard ONVIF output to any VMS, including Milestone XProtect
- **Centralized Fleet Management:** Monitor all remote sites from a single dashboard

Use Case 2: Perimeter & Thermal Analytics

THE CHALLENGE: *"If the recording servers go down, the perimeter fence is blind. We cannot afford that risk."*



Solution: SureStream Client-Side Failover

SureStream acts as your security underwriter. When every server in your data center fails, SureStream maintains a direct, autonomous video path from thermal cameras to the Control Room. The physical perimeter is never unmonitored, even when the IT infrastructure collapses.

How It Works:

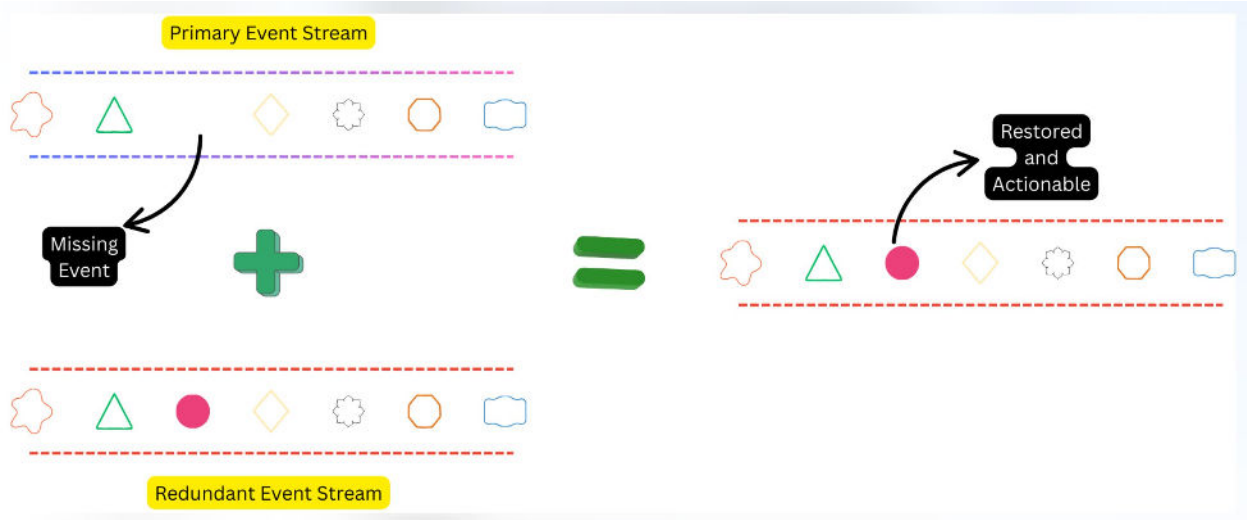
1. **Standard Operation:** Video flows through Recording Server to Smart Client
2. **Server Failure Detected:** User activates the SureStream direct camera-to-client path
3. **Continuous Visibility:** Operators maintain live situational awareness without interruption

Key Benefits:

- Native integration within Milestone XProtect Smart Client
- No external appliances or new applications to learn
- Enterprise-grade resilience without doubling hardware footprint

Use Case 3: Control Room Alarm Aggregation

THE CHALLENGE: *"We missed a perimeter breach because the primary recorder was patching during the event."*



Solution: RMF High-Availability Alarms

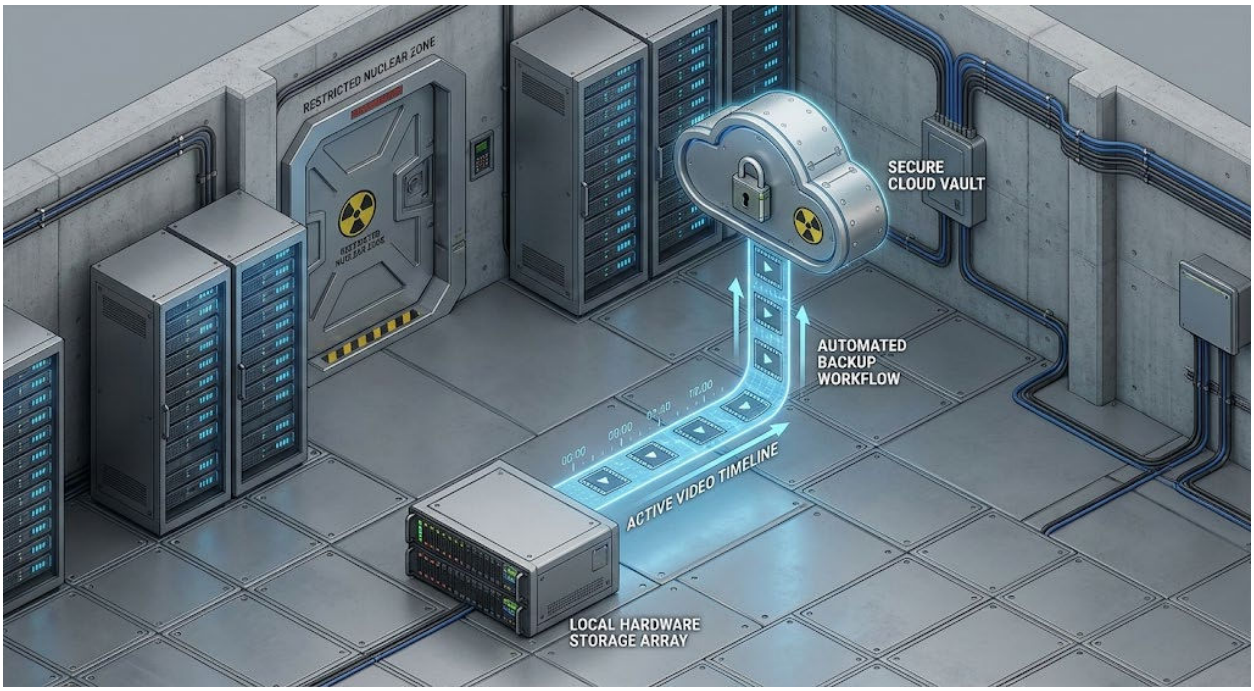
In critical infrastructure, missing an alarm is not an option. The **Redundancy Management Framework (RMF)** orchestrates redundant alarm pipelines as a fail-safe. If the primary recorder misses an event due to maintenance or failure, the secondary recorder delivers it. RMF manages this flow to ensure the operator ***always*** receives the alert, filtering duplicates only when both systems succeed.

RMF Core Capabilities:

- **Active-Active Architecture:** Both data centers are fully operational, delivering services 24/7
- **Sub-Second Recovery:** Client-side intelligence enables near-instantaneous live video recovery
- **Cybersecure Object Synchronization:** Prevents malicious changes from propagating between sites
- **Datacenter Isolation:** Eliminates shared attack surfaces and blocks lateral threats
- **Automatic Playback Switching:** Retrieves archived footage from a redundant site when the primary is missing content

Use Case 4: NERC Audit & Compliance

THE CHALLENGE: *"We lost a hard drive containing footage of a restricted area entry. We failed the audit."*



Solution: Nidhi Automated Backup & Restore

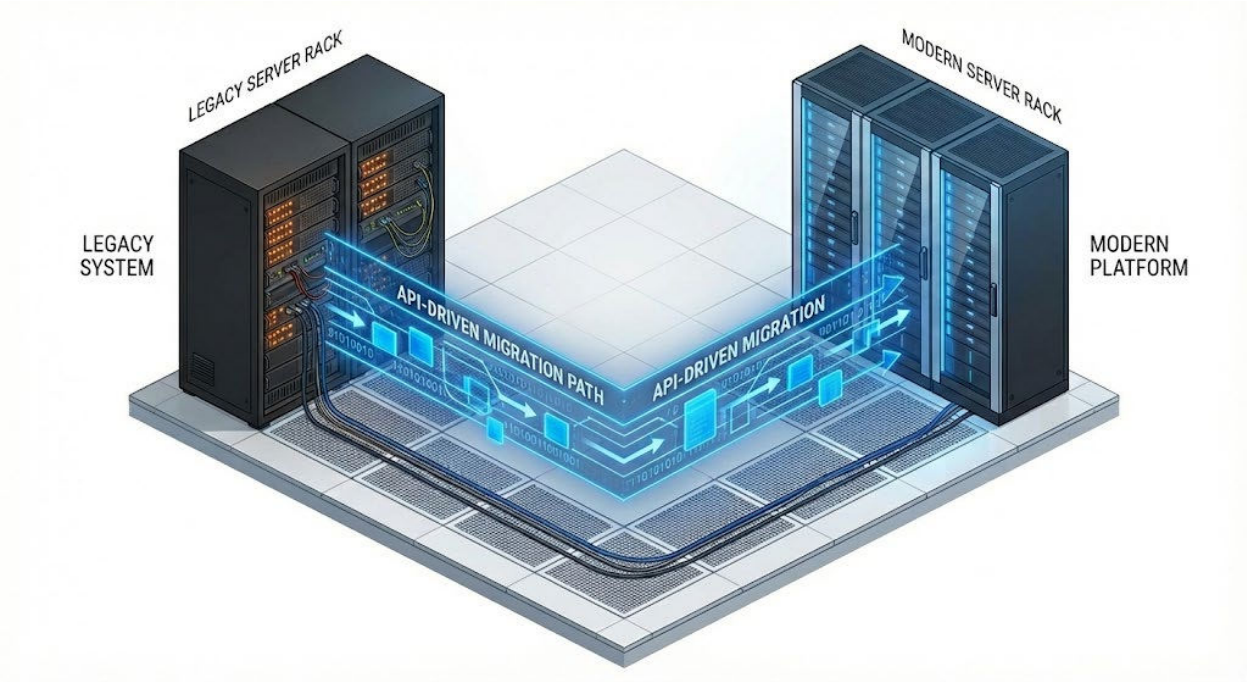
Regulatory fines for data loss are substantial. **Nidhi** automates evidence protection by mirroring footage from restricted zones (such as reactor entries or server rooms) to a secure vault. If a local drive fails, Nidhi rebuilds the timeline, ensuring you always have the required audit trail.

Key Features:

- **Real-Time Mirroring:** Continuous backup to Cloud or SMB vault
- **Bandwidth Scheduler:** Throttle during business hours, full speed overnight
- **Volume Restoration Wizard:** Quickly recover from single drive failures
- **Total Hardware Resurrection:** Restore entire recorder configuration after catastrophic failure
- **Native XProtect Integration:** Embedded MIP plugin for single pane of glass management

Use Case 5: Legacy Plant Modernization

THE CHALLENGE: *"We operate 24/7. We can't shut down the security system to upgrade our old Milestone XProtect servers."*



Solution: XPort Migration Tool

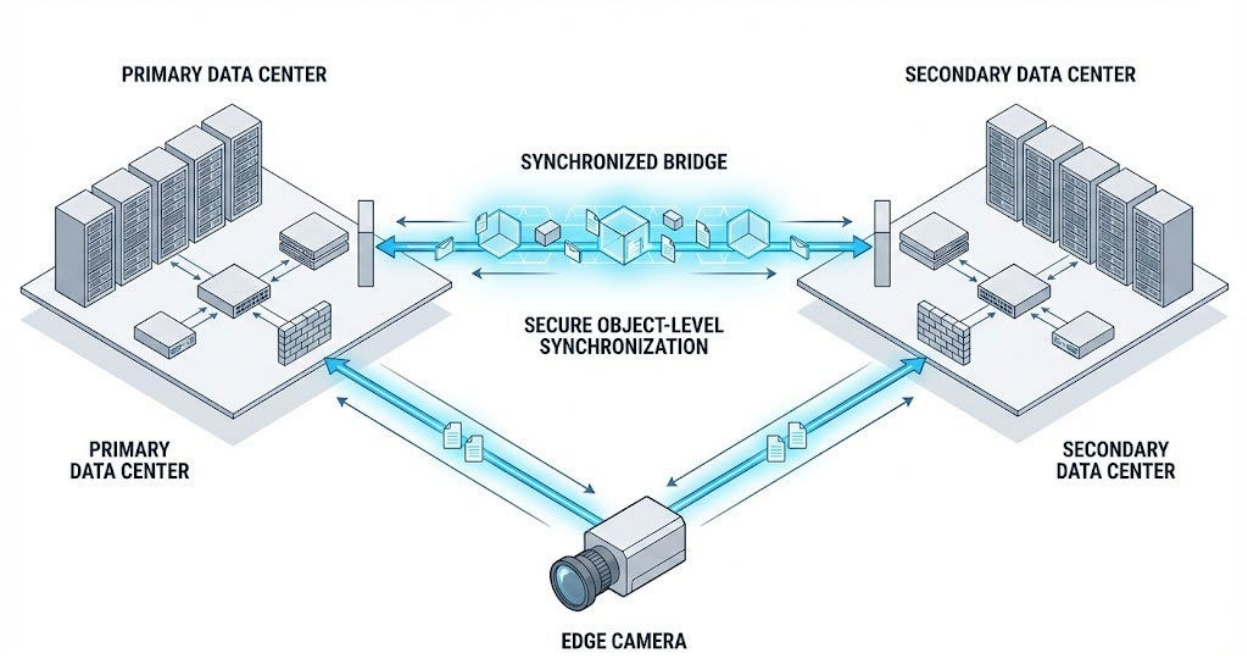
Utilities often run on aging infrastructure because upgrades are perceived as too risky. **XPort** de-risks the modernization process by automating the migration of configurations and cameras from legacy hardware to modern servers, reducing costs by up to 60% and minimizing blind spots during transition.

Migration Capabilities:

- **Same/Different Product Versions:** Migrate between XProtect versions and editions
- **One-to-One Migrations:** Move from old server to new server
- **Many-to-One Consolidation:** Merge multiple siloed deployments into a unified system
- **Fine-Grained Control:** Select specific devices, roles, views, and settings to migrate
- **Cloud Migration:** On premises to cloud deployments supported
- **Device Redistribution:** Rebalance of cameras across recorders during migration

Recommended Architecture

For utilities requiring maximum resilience, Vega Systems recommends deploying RMF in a Federated or Independent architecture. This approach provides:



Primary Data Center	Secondary Data Center
• Management Server • SQL Server • Recording Servers • Event Server • Mobile Server	• Management Server • SQL Server • Recording Servers • Event Server • Mobile Server

Architecture Benefits:

- **Complete Isolation:** No shared authentication, storage, or real-time database replication
- **Limited Blast Radius:** Cyber-attack on one site cannot propagate to the other
- **Selective Synchronization:** Object-level sync prevents malicious changes from spreading
- **Zero Lost Footage:** Every camera streams independently to each data center

Customer Testimonials

> *"Vega Systems has been an invaluable partner... helping us deliver world-class security solutions. Their team has been professional, knowledgeable, and responsive to our needs."*
>
> **— Krish Shetty, CEO, WizNucleus (Nuclear Cybersecurity)**

Next Steps

Ready to secure your critical infrastructure? Contact Vega Systems to schedule a consultation and learn how our solutions can address your specific requirements.

Request a Demo	Contact Sales
vega25.com	info@vega25.com +1-669-256-2357

Vega Systems Inc.

The Immune System for Video Infrastructure