

Critical Infrastructure Organization Modernizes Classified Control Room Operations with Secure Unified KVM Architecture

BACKGROUND

A critical infrastructure organization initiated the development of new mission-critical control centers as part of a broader modernization initiative. The project focused on building next-generation operational environments capable of managing both classified and non-classified systems within highly secure infrastructures.

After visiting a Black Box Experience Center and reviewing live demonstrations, the organization identified a unified IP KVM ecosystem as the foundation for its new control room strategy.

The deployment includes:

- A main control center featuring a large video wall environment
- Secondary backup control centers located kilometers away
- Fully isolated network environments supporting classified and non-classified workflows



CHALLENGE

The organization faced several critical technical and operational requirements:

Secure Access to Classified and Non-Classified Systems

Operators required seamless access to multiple systems while maintaining strict security boundaries. Classified servers were located in secure environments, while other operational data sources existed on separate networks.

Key constraints included the use of certified secure KVM technologies to separate classified and non-classified environments, in combination with a closed IP-KVM ecosystem to connect operators and sources in multiple locations with encrypted data transmission and strict user access management.

Secure and non-secure video feeds needed to be visible on centralized video walls without compromising security policies.

Legacy Infrastructure Limitations

Previous video wall infrastructure relied on outdated processing hardware and aging displays that frequently failed, limiting operational reliability. For the new facilities, the organization decided to replace their video walls based on LCD-technology in favor of high-resolution, bright LED video panels for enhanced situational awareness; flexible visualization capable of combining multiple data sources; and simplified operator workflows across secure environments.

Strict Network Separation Requirements

The architecture required fully air-gapped networks, a dedicated KVM network carrying only video signals, and additional physical isolation layers to prevent unauthorized data transfer.

SOLUTION

Black Box designed a unified control room architecture combining Emerald® Control Ecosystem technology and NIAP PP4.0-certified Secure KVM devices.

Secure Multi-Network Architecture

Key elements included separate networks for classified and non-classified systems. The use of Secure KVM Defender™ devices at the sources provides air-gapped physical channel isolation, while ensuring only unidirectional data flows to the operator console as an additional security layer.

Operators can access and manage sources at any location – classified and unclassified – while controlling video wall content. Emerald 4K receiver units are combined with NIAP PP 4.0-certified 4K KVM Switches ensuring complete data isolation while simultaneously managing high- and lower-classification systems. ControlBridge® touch panels provided and programmed by Black Box automate source routing and workspace layouts allowing simplifying workflows with instant, error-free one-touch preset buttons.

Unified Visualization and Operator Control

The solution integrates long-lifetime LED video walls driven by Emerald DESKVUE receivers to visualize any source connected through a dedicated KVM network designed exclusively for visualization traffic.

Distributed Control Centers

Multiple control centers operate within the architecture:

- Main facility with extensive source capacity and large LED visualization environment
- Secondary redundant control rooms, located kilometers away, connected via fiber links

RESULTS

The deployment delivers secure simultaneous access to classified and non-classified systems; improved operational visibility through high-resolution LED video wall panels; simplified operator workflows within strict security environments; and fully redundant architecture supporting mission-critical continuity.

Why This Matters

This project demonstrates how critical infrastructure organizations can modernize control rooms and centrally manage multiple control locations while maintaining strict security compliance by combining:

- IP KVM-based flexibility
- NIAP PP 4.0-certified Secure KVM channel isolation
- Unified operator visualization and simplified workflows
- Distributed resilient architectures

Emerald IP KVM Ecosystem

NIAP PP 4.0-certified Secure KVM

