Executive Summary

LED video walls are becoming increasingly common for control rooms and other mission-critical and secure environments and applications. Many LED displays rely on lower-cost Chinese controllers, like NovaStar or Colorlight, which can offer powerful visual performance but are not built with enterprise-grade cybersecurity in mind. Their networked design, firmware updates, remote access, and closed software raise concerns about cybersecurity, supply chain integrity, firmware security, physical access, and operational resilience. When integrated into control-room environments displaying sensitive data, these systems should be treated as **high-risk, untrusted devices** requiring layered defenses.

This document outlines the potential areas risk and possible attack vectors that should be considered when specifying an LED display controller.

Why This Matters

- Control room video walls display sensitive operational data.
- Many lower-cost, non-TAA compliant controllers are network-enabled, firmware-driven devices.
- These devices are often outside traditional IT organizational oversight with unpatched, unmonitored, default credentials.
- These devices and details of their software are closed, private, and controlled by a known adversarial nation.
- Potential vector for:
    - Data manipulation or blackouts
    - Network intrusion
    - Reputational or operational disruption

Architectural Overview

A typical LED video wall system using a popular Chinese controller Includes:

- A controller/processor box (input from HDMI/SDI/DP, output to receiving cards)
- Receiving (and/or sending) cards/modules which take the controller output and drive the LED modules/panels.
- The LED panels/modules (tiles) are arranged into a large array.
- Network/communication links (Ethernet/UART/USB) are used to manage the controller, perform configuration, firmware updates, calibration software (e.g., NovaLCT).

In this architecture there are many layers (hardware, firmware, network, management software, physical access) where insecurity can manifest

Attack Surface

The processing system is the only portion of an LED display that interfaces with the network, is user accessible has a direct ability for software injection. This point of attack could have the following threat vectors:

Layer	Insecure Aspect	Example Risk in Secure Environment
Firmware	Unsigned or outdated firmware	Attacker installs backdoored firmware, compromising wall integrity or data confidentiality.
Network	Open web management ports, weak authentication	Unauthorized remote access allows malicious image injection or lateral movement.
Supply Chain	Closed-source hardware, Chinese origin (No SBOM or audit trail.	Embedded malware or data-exfiltration backdoors before arrival on site.
Physical	Exposed ports, unsecured racks	Insider or visitor connects malicious USB, alters configuration.
Operational	Lack of monitoring/logs	Malicious reconfiguration unnoticed, content modified or suppressed.

Risk Matrix

By exploiting one or more of these vectors, an attacker could launch several types of attacks with varying levels of risk. In the table below we outline a few potential risks that are associated with known vectors.

Risk Category	NovaStar Likelihood	Aurora Likelihood	Impact	Risk Rating	Example Scenario
Unauthorized Access to Controller	Medium	None	High	**High**	Attacker alters video feeds, uploads malicious software, or shuts down wall during incident.
Firmware Tampering	Medium	Low	Very High	**Critical**	Malicious firmware installed via USB or update server.
Network Pivot Attack	Medium	Low	High	**High**	Compromised controller used to move laterally to other assets
Display Manipulation / Disinformation	Low	None	High	**High**	Rogue image or data injected into SOC visualization.
Physical Tampering	Medium	None/Low	Medium	**Medium**	Contractor installs rogue card or taps Ethernet.
Code injection/Data Exfil	low	Low	High	**High**	Attacker injects code on the controller they might exploit side-channels or optical leakage
Supply-Chain Compromise	Low	None	High	**Medium**	Pre-loaded malicious code exfiltrates data via covert channel.
Uncontrolled Disclosure of System Communication Protocol	High	Low	High	**Critical**	Attackers can change system configuration by having access to these protocols without any authentication/security validation.

Summary & Recommendations

In summary:

- The use of Chinese-controller units in LED video-wall systems introduces technology that is visually capable and cost-effective but also carries distinct security risks due to firmware/updates, remote access, physical access, and network connectivity.
- These systems are often overlooked in the facility security architecture as "just AV gear," while in fact they can be both a target and a pivot point for attackers.
- A structured, multi-layered approach (governance, network isolation, firmware hygiene, physical security, monitoring) is required to mitigate the risk effectively.
- For high-impact or high-security installations (control rooms, public signage, broadcast), treat the LED wall controller as an enterprise-grade asset: assume it is reachable, treat management interfaces as attack surfaces, and plan for failure or compromise.
- If commissioning or upgrading such systems, include cybersecurity requirements in procurement:
    - Security assurances
    - Digitally signed software
    - Chain of custody/supply chain origin
    - US made or controlled LED processors
    - Access Management
    - Firmware control and change logs