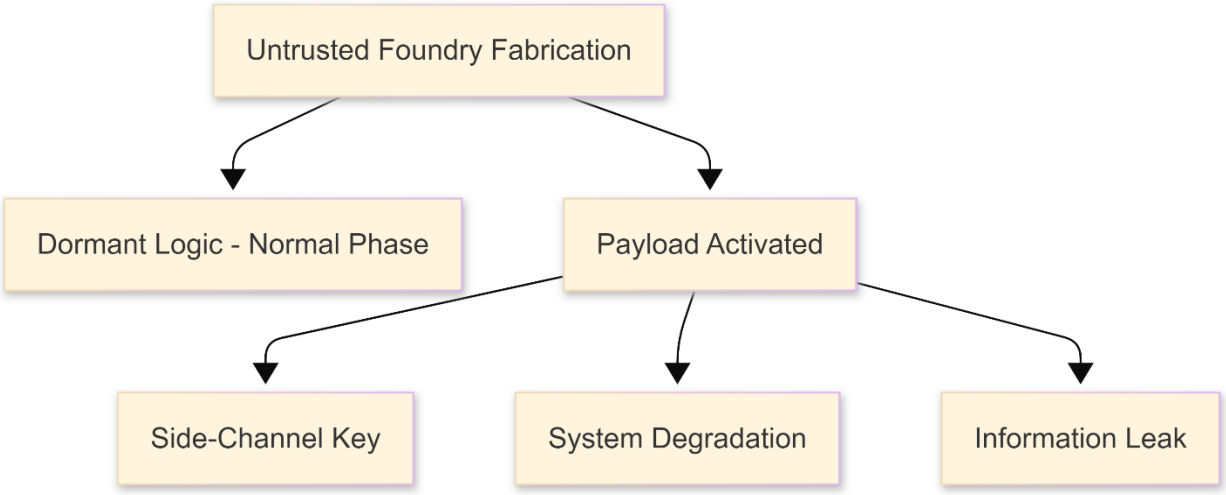
Hardware Trojans, Global Cyber-Physical Standards, Museum Protection Architecture, and Socio-Technological Implementation Dynamics

The Threat Landscape of Hardware Trojans in Video Surveillance Infrastructure

The globalized semiconductor supply chain has decentralized integrated circuit design, manufacturing, and testing, introducing severe systemic vulnerabilities to physical security devices. Outsource-based production models allow adversaries to insert malicious alterations, known as hardware Trojans, directly into the silicon layout. When integrated into video surveillance systems (VSS) utilized in smart city networks, critical infrastructure, or high-security facilities, these physical backdoors present a catastrophic threat of data compromise, functional sabotage, and covert lateral network movement.



High-profile cyber-espionage and counter-intelligence operations underscore the severity of the hardware security landscape. For example, reports have surfaced detailing the compromise of municipal traffic feeds and video networks, such as the targeting of the Iranian Leader's Office (Bait-e-Rahbari) traffic cameras by external intelligence agencies to track security personnel.

Conversely, reciprocal cyber campaigns have targeted Western and Middle Eastern surveillance networks. The "Cyber Islamic Axis" reportedly breached over 120 Israeli VSS cameras and internet servers on the southern military front, while the "Rachel Hunter" hacking group infiltrated VSS storage servers and facial recognition databases monitoring sensitive religious sites in Jerusalem.

These incidents demonstrate that physical video networks are key targets for geopolitical intelligence gathering. This vulnerability is further exacerbated by the "CCTV Mafia"—a term coined to describe networks of corrupt or underqualified security actors who undermine the domestic supply chain.

Actor Category	Exploitative Mechanism	Operational and Security Impact
Corrupt Consultants	Draft copy-pasted, obsolete	Secures multi-billion Toman

Actor Category	Exploitative Mechanism	Operational and Security Impact
	technical specifications for public tenders.	municipal contracts while deploying insecure, open-port legacy hardware.
Dishonest Vendors	Badge-engineer low-quality VSS cameras and recording equipment.	Inflates hardware prices up to 20 times their actual import value, primarily targeting state projects.
Commission Brokers	Pose as regulatory or law enforcement liaisons without technical skills.	Monopolizes VSS hardware sales and actively lobby against mandatory laboratory security standards.

Taxonomy and Behavioral Characteristics of Hardware Trojans

A hardware Trojan is characterized by its physical structure, activation mechanism (trigger), and executed action (payload). These malicious modifications are explicitly designed to remain dormant and undetectable during conventional post-fabrication tests, activating only under extremely rare conditions. In VSS architectures, these threats are categorized into distinct functional and operational groups, as detailed in the following matrix:

Trojan Class	Primary Objective	Architectural Impact	Detection Complexity
Functional Trojans	Alter circuit behavior or logic operations under specific triggers.	Modifies routing or control gates; bypasses cryptographic engines to output plaintext streams.	High; remains completely silent during standard functional validation sweeps.
Information Trojans	Exfiltrate highly sensitive data (e.g., encryption keys, firmware credentials).	Leaks cryptographic key bits via radio emissions or physical side-channels.	Extremely High; requires specialized side-channel measurements or physical layout comparison.
Destructive Trojans	Force logical bricking or permanent physical damage to components.	Overloads voltage lines, triggers critical clock loops, or permanently disables processing chips.	Moderate; payload triggers are catastrophic and immediately identifiable post-execution.
Reliability Reduction	Gradual, imperceptible degradation of the host chip's lifecycle.	Accelerates transistor aging; increases static power dissipation and micro-crack propagation.	Extremely High; disguised as normal silicon wear-and-tear and aging processes.

Trigger and Payload Mechanisms

The architecture of a hardware Trojan relies on two primary logical segments: the trigger and the payload.

Trigger Part

The trigger acts as the sensor that monitors internal circuit conditions, remaining dormant to bypass quality assurance and logic tests.

- **Rare Input Patterns**: Digital logic comparators that activate only when a specific, highly improbable combination of input bits occurs across multiple internal registers.
- **Internal State Counters**: Synchronous sequential logic that counts clock cycles or specific operations over long operational durations. The Trojan activates only when the counter reaches a high threshold, such as 2^{40} cycles, rendering short-term laboratory evaluations ineffective.
- **Physical Parametric Triggers**: Analog sensors monitoring temperature thresholds, voltage fluctuations, or electromagnetic patterns that toggle the trigger logic under specific environmental stress.

Payload Part

The payload contains the circuit logic that executes the malicious action once the trigger is pulled.

- **Information Leakage via Side Channels**: The payload modulates clock delays or power distribution networks slightly to transmit cryptographic key bits, enabling external observers to reconstruct secrets without leaving logical traces.
- **Bypassing Security Enclaves**: A single multiplexer added to the datapath can reroute video signals around cryptographic modules, transmitting raw plaintext video over the network while indicating successful encryption to the operating system.
- **Logical Denial-of-Service (DoS): The payload injects persistent wait states or timing violations into the system bus, causing the NVR interface to freeze or drop frames** during critical events.

Insertion Phase and Logical Abstraction Levels

Hardware modifications can be introduced at multiple stages of the integrated circuit lifecycle, spanning different abstraction levels of design and physical implementation.

- **Register Transfer Level (RTL)**: Malicious code is injected into the hardware description language (HDL) source files, such as Verilog or VHDL, during design. Although easier to identify through comprehensive static code analysis and formal verification, attackers can mask RTL additions by compromising CAD compilation scripts or logic synthesis tools.
- **Gate Level**: Trojans are inserted into the netlist post-synthesis by substituting standard logic cells or by using empty filler spaces in the gate array, allowing attackers to avoid detection during designer-level source code reviews.
- **Layout and Physical Level**: Subtle structural changes are applied directly to the photomask during fabrication. These include altering transistor dimensions, modifying dopant concentrations to change gate thresholds silently, or routing sub-micron wires to create parasitic connections.

Trojan Activation Methodologies

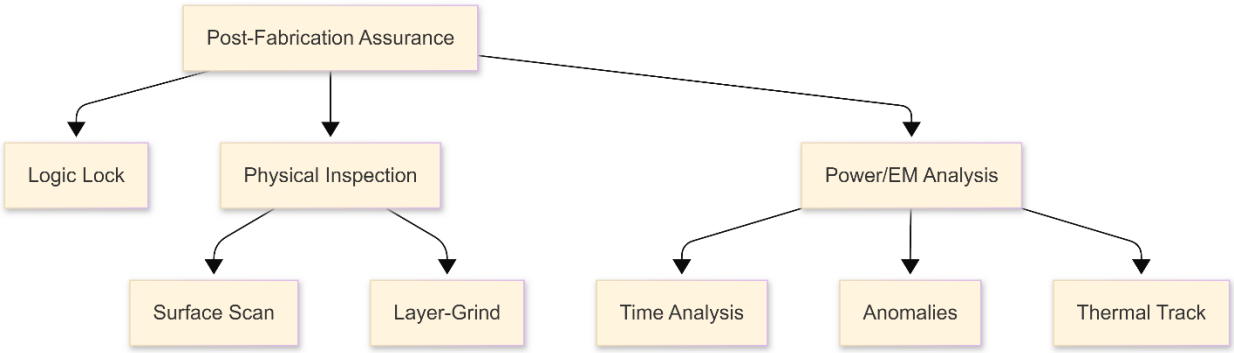
Once embedded, the host device's software and physical operating environment can be leveraged to activate the Trojan through three primary vectors :

- **Direct Execution of Malicious Files**: Attackers use social engineering or phishing to trick operators into executing untrusted files disguised as harmless documents or setup files (e.g., setup.exe or document.pdf.exe). Once executed, the code installs a boot-persistent Trojan in the system's memory or registry.
- **Exploitation of Software Vulnerabilities**: Attackers target unpatched firmware flaws (such as buffer overflows or remote code execution vulnerabilities) to run malicious payloads. A notable example is the exploitation of the SMB protocol vulnerability via EternalBlue, which enabled the automated spread of the WannaCry ransomware.

- **Automated Scripts and Scheduled Tasks**: Attackers configure system-level automation utilities (such as Windows Task Scheduler or Linux Cron jobs) to run background scripts periodically. These scripts maintain persistence, exfiltrate data, and check command-and-control (C2) servers for software updates.

Advanced Detection and Countermeasure Frameworks

Detecting hardware-level modifications is challenging because standard functional testing only monitors output patterns against known input vectors, which rarely activate the Trojan's trigger conditions. Modern hardware assurance demands sophisticated physical, logical, and run-time techniques.



Physical Inspection

High-resolution imaging is used to inspect suspect chips by systematically grinding away silicon layers and scanning the surface.

- **Scanning Electron Microscopy (SEM)**: Scans the silicon topography to map gate placement and wire routing.
- **Transmission Electron Microscopy (TEM)**: Provides sub-nanometer resolution profiling of transistor structures.
- **Differential Image Comparison**: The scanned layer floorplan is compared against the golden design layout. However, this destructive process is time-consuming, expensive, and cannot be performed on all production units.

Parametric Side-Channel Analysis

These non-destructive methods measure physical characteristics and compare them against a verified "golden model".

- **Signal Path Delay Analysis**: Because any added gate or trigger wire increases capacitive loading, measuring signal propagation times across specific paths can reveal modifications.
- **Power and Electromagnetic (EM) Fingerprinting**: Monitors power consumption and EM radiation during execution. Advanced statistical methods identify the micro-watt power anomalies introduced by a Trojan's dormant logic.

Design-for-Trust (DFT) and Run-time Monitoring

Integrated active protection systems verify hardware integrity during operation.

- **Barrier-Integrated Self-Authentication (BISA)**: Design houses fill unused layout spaces with active

functional cells and self-authentication logic. If an attacker attempts to place a Trojan in these spaces, the authentication logic fails to output the correct response to a randomized input challenge.

- **Kalman Filter Thermal Tracking**: Run-time thermal sensors feed temperature metrics into a state estimator. The Kalman filter equations estimate expected thermal states based on logical workloads, as modeled by: where x_k is the temperature state, u_k is the system workload power input, z_k is the measured sensor temperature, and w_k and v_k are the process and measurement noise matrices, respectively. Dynamic deviations of z_k from the estimated states indicate localized power dissipation caused by Trojan activation.

Technical Analysis of Cybersecurity Standards in Video Surveillance

Gaps in the IEC 62676 Legacy Architecture

The international standard family IEC 62676 (often harmonized as EN 62676) defines the standard performance requirements, video transmission protocols, interfaces, and application guidelines for VSS used in security installations.

- **Part 1-1 (System Requirements)**: Defines performance indicators, functional blocks, and system management parameters, excluding installation and maintenance.
- **Part 1-2 (Video Transmission - Performance)**: Focuses on transmission delay and bandwidth requirements.
- **Part 2 (Transmission Protocols)**: Specifies interoperability profiles for network-based video streaming, covering HTTP, REST, and web services.
- **Part 3 (Video Interfaces)**: Outlines physical connections and analog/digital interfaces.
- **Part 4 (Application Guidelines)**: Offers planning, selection, design, testing, commissioning, and maintenance guidance.
- **Part 5 (Data Specifications and Image Quality)**: Details metrics for camera testing, including resolution, dynamic range, OECF, and noise.

While technically comprehensive for image validation and system interoperability, IEC 62676 is fundamentally insufficient as a cybersecurity framework.

1. **Explicit Exclusion of Cybersecurity Controls**: The standard explicitly states that detailed information security, data privacy, and legislative compliance parameters are outside its scope, leaving critical network installations unprotected against modern cyber-physical threats.
2. **Focus on Image Quality Over System Hardening**: The standard defines physical parameters such as resolution targets and frame rates, but lacks technical specifications for device authentication, host integrity verification, and cryptographic strength.
3. **Lack of Secure Lifecycle and SDLC Requirements**: It does not mandate secure software development lifecycles (SDLC), cryptographic firmware signing, or automated vulnerability patch distribution, leaving devices exposed to common exploits.
4. **Absence of Chain-of-Custody and Cryptographic Integrity**: The framework lacks rigorous specifications for tamper-evident event logging, system log protection, and cryptographic export signing, making recorded video easily manipulable and vulnerable to legal challenges.

Vulnerabilities Exposed in VSS Lacking Dedicated Cybersecurity Standards

Deploying IP-based video surveillance networks without dedicated cybersecurity standards leaves systems highly vulnerable.

- **Unauthenticated Access and Credential Vulnerabilities**: Devices often use default factory credentials, and standard protocols lack brute-force protection, multi-factor authentication, or integration with centralized identity systems (such as RADIUS or TACACS+).
- **Cleartext Transmission and RTSP Spoofing**: Real-Time Streaming Protocol (RTSP) sessions are frequently transmitted unencrypted over TCP/UDP Port 554. Attackers can sniff video streams, intercept credentials, or execute packet-injection attacks to replay mock footage.
- **Firmware Flaws and Device-Level Pivoting**: IP cameras are edge-based Linux computers with active operating systems. Vulnerabilities in network services (like buffer overflows in RTSP or UPnP) allow remote code execution. Attackers can use the compromised camera as an internal jump-box, bypassing firewalls to access internal networks.
- **ONVIF and P2P Protocol Exploits**: The Open Network Video Interface Forum (ONVIF) standard requires open ports (HTTP-80, RTSP-554, WS-Discovery-3702), creating a highly visible attack surface. Additionally, Peer-to-Peer (P2P) automatic cloud discovery features establish persistent outbound connections that bypass firewalls. If the vendor's cloud is compromised, attackers gain direct, unauthenticated access to the private network.

Case Studies of VSS Exploitations

Historical security breaches demonstrate the operational consequences of VSS security gaps:

Year of Incident	Target System / Scope	Attack Origin and Vector	Core System Failure	Operational Consequences
2016	Global VSS Infrastructure.	Mirai Botnet malware propagation.	Weak factory-default telnet credentials and lack of patch management.	Recruited tens of thousands of IoT cameras to execute massive distributed denial of service (DDoS) attacks.
2021	Verkada Surveillance Network.	Compromise of highly privileged administrative credentials.	Lack of multi-factor authentication and decentralized access logs.	Allowed unauthorized access to over 150,000 live feeds in psychiatric hospitals, schools, and corporate offices.
2022	UK Healthcare Network.	Local network sniffing of video data.	Unencrypted RTSP transmission and lack of network segmentation.	Leaked private emergency room patient footage onto public domains.
2023	Middle Eastern City VSS.	Stream interception and packet injection.	Absence of frame-level cryptographic	Intercepted municipal camera

Year of Incident	Target System / Scope	Attack Origin and Vector	Core System Failure	Operational Consequences
			integrity watermarking.	streams and injected mock video loops, blinding traffic control centers.

Global Standards and Regional Technical Regulations

To address the cybersecurity gaps in generic VSS standards, several nations have implemented dedicated cybersecurity frameworks specifically for video surveillance networks.

- **Taiwan (TAICS TS-0014 and TS-0015)**: The Taiwan Association of Information and Communication Standards developed a four-part standard detailing security requirements for IP cameras, video recorders, and network-attached storage (NAS). It mandates physical security testing (such as tamper-proof casing), authentication controls, and encrypted communication protocols.
- **Vietnam (QCVN 11:2026/BCA)**: Vietnam's Ministry of Public Security issued Circular No. 48/2026/TT-BCA, enforcing QCVN 11:2026/BCA to replace the previous QCVN 135:2024/BTTTT standard. The updated QCVN requires all imported and domestic IP-based cameras to bear the CR conformity mark, certifying compliance with baseline requirements for data encryption, vulnerability management, and secure software updates.
- **European Union (ETSI EN 303 645 and NIS-2)**: The ETSI standard enforces baseline cybersecurity controls for consumer and industrial IoT devices, including VSS components. It prohibits the use of default passwords, mandates vulnerability disclosure programs, and requires secure software updates. The NIS-2 Directive expands these requirements to protect critical infrastructure supply chains against software tampering.
- **United States (NDAA Section 889 and California SB 327)**: NDAA Section 889 bans federal procurement of surveillance systems containing silicon from designated foreign manufacturers. At the state level, California SB 327 requires all internet-connected devices to feature unique default passwords to prevent botnet recruitment.

National Electronic Security Standard 14279 and Museum Security Architecture

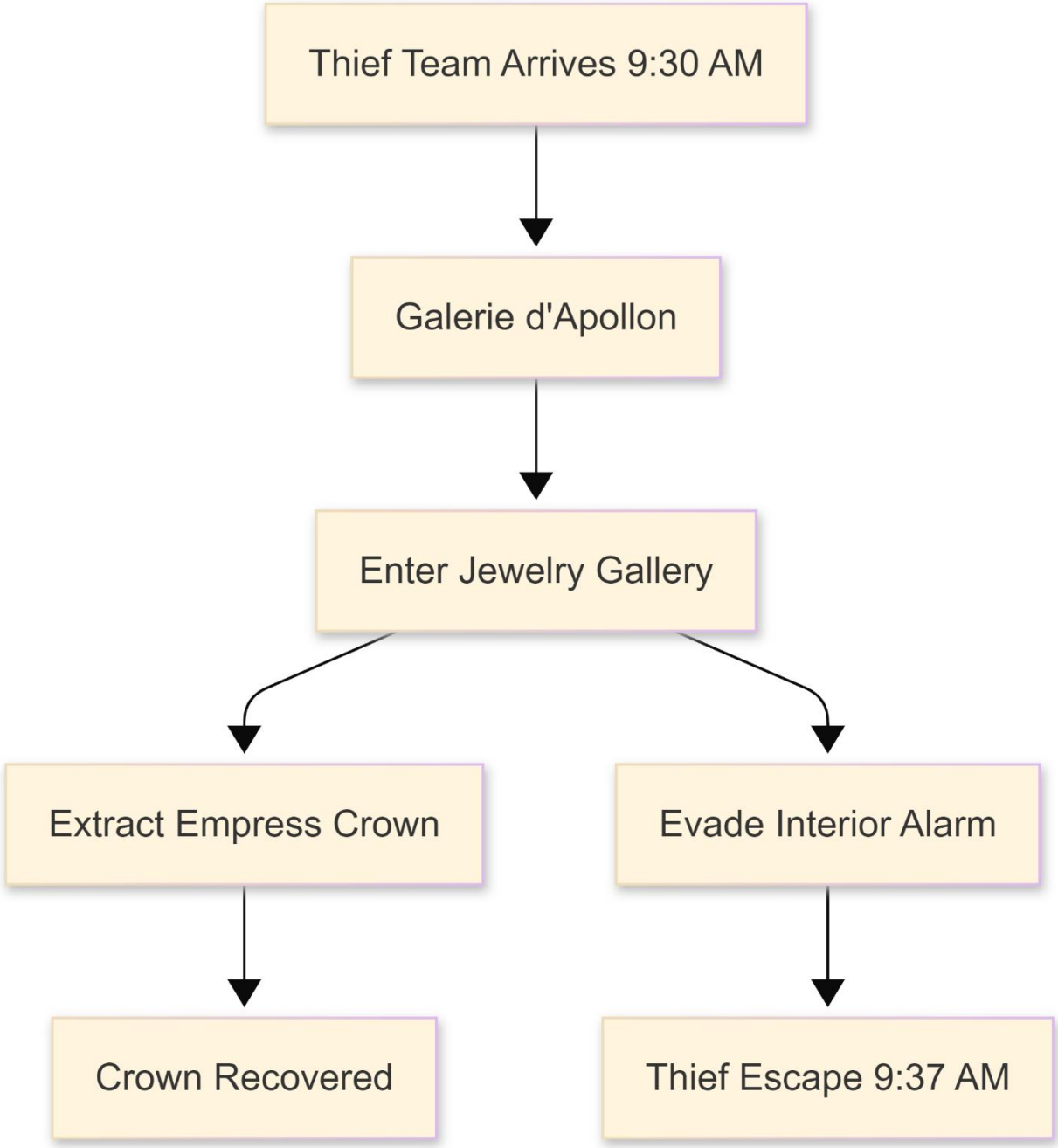
The Socio-Technological Impact of the 2025 Louvre Museum Heist

On Sunday, October 19, 2025, the Louver Museum in Paris was targeted in a daring, professional daylight heist that highlighted critical vulnerabilities in its physical security and operational protocols.
At approximately 9:30 AM—30 minutes after the museum opened—four masked thieves used a cargo basket lift on the Quai François Mitterrand exterior to reach a second-floor window in the Galerie d'Apollon. The window area was under active renovation, creating an architectural and security vulnerability. The thieves forced the window, entered the gallery, bypassed five on-duty security officers, smashed the display cases, and stole eight pieces of historical French Crown Jewels. The stolen items included:

- Queen Marie-Amélie and Queen Hortense's sapphire diadem, necklace, and earring.
- Empress Marie-Louise's emerald necklace and earrings.
- Empress Eugénie's pearl and diamond tiara.

- A historical reliquary brooch.

The total monetary value of the stolen items was estimated at €88 million ($102 million), with invaluable cultural and historical heritage. During their escape, the thieves attempted to steal Empress Eugénie's imperial crown (adorned with 1,354 diamonds, 56 emeralds, and 8 golden eagles). However, because the protective glass resisted their tools, they attempted to force the crown through a tight opening, deforming its lightweight structure and causing parts to detach. The crown was dropped on the sidewalk outside and recovered on the day of the theft. The entire operation lasted less than seven minutes, with under four minutes spent inside the gallery, and the thieves fled on motorcycles.



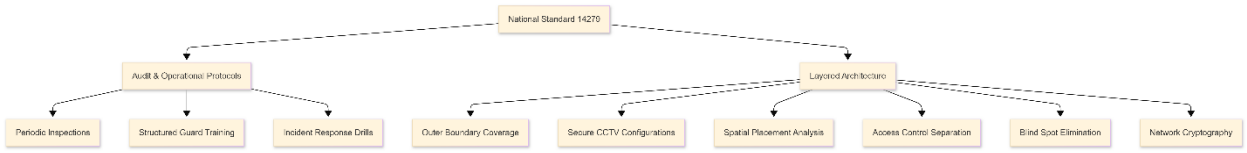
This incident was part of a broader wave of high-value cultural property thefts reported globally in late

2025. At the Egyptian Museum in Cairo, a 3,000-year-old gold bracelet from the Pharaoh Amenemope collection was stolen from a restoration laboratory. Similarly, the Royal Albert Memorial Museum (RAMM) in Exeter, UK, suffered a forced break-in where thieves stole 17 antique pocket watches and historical weapons. These incidents underscore a growing pattern of professional art thefts targeting precious stones and metals that can be dismantled or melted down for black-market sale.
These heists expose major vulnerabilities that occur when technical systems operate in isolation from physical security designs :

1. **Compromised Perimeter During Construction**: Physical site alterations during the renovation bypassed standard alarm sensors.
2. **Physical Limitations of Alarm Systems**: Although interior sensors triggered a response, police arrived within minutes only to find the highly organized, fast-moving thieves had already fled on motorcycles.
3. **Display Case Sourcing Flaws**: The glass display cases were not engineered to resist physical attacks, allowing thieves to quickly smash them and extract priceless artifacts, damaging the recovered crown in the process.
4. **Failure to Integrate Local and Central Operations**: On-site guards could not intervene without risking personal safety, and automated monitoring rooms could not lock down exit pathways or coordinate with physical barriers.

Analysis of the National Electronic Security Standard for Museums (Standard 14279)

Originally compiled in 1391 (2012) under the direction of Dr. Mohammad Ghalamchi and in collaboration with the National Standards Organization and the Cultural Heritage Organization of Iran, **Standard 14279 (الزامات حفاظت الکترونیکی موزه‌ها - Requirements for Electronic Protection of Museums)** provides a comprehensive security framework for high-value cultural assets.
Standard 14279 treats electronic security as an integrated system that combines technology, operations, and architectural design.



Operational Domain	Core Protective Mandate	Key Implementation Standards
System Design and Risk Analysis	Conduct venue-specific threat modeling and structural risk classification.	Evaluates asset valuations, visitor traffic, local climate conditions, and potential physical entry points.
Smart VSS Architecture	Deploy high-definition cameras for 24/7 coverage with no blind spots.	Mandates tampering alarms, motion tracking, and secure, write-once, read-many (WORM) storage.
Integrated Access Control	Enforce multi-tier authentication for sensitive areas.	Combines biometric or smart card readers with real-time intrusion detection and silent alarms.
Physical Infrastructure Safety	Protect critical server rooms, VSS storage, and network switches.	Integrates backup power supplies, early fire detection, and automated suppression systems.

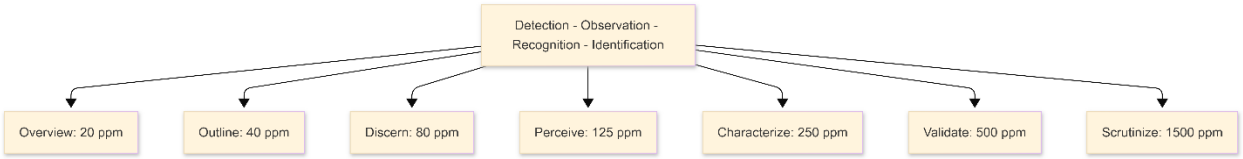
Operational Domain	Core Protective Mandate	Key Implementation Standards
Isolated Security Networks	Restrict access to security networks and VSS interfaces.	Requires dedicated VLAN segmentations, encrypted device communication, and firewall barriers.
Operational and Audit Protocols	Ensure ongoing system reliability and staff readiness.	Mandates quarterly third-party compliance audits, periodic maintenance, and staff crisis drills.

Standard 14279 establishes a structured risk assessment model, categorizing potential threats to help prioritize security resources :

Threat Category	Probability	Potential Severity	Consequent Vulnerability Analysis
Physical Theft of High-Value Assets	High.	Very High.	Professional thieves exploit blind spots during construction or renovations, resulting in permanent cultural and financial losses.
Cyber Penetration of VSS Networks	Medium.	High.	Attackers compromise unencrypted networks to disable camera feeds, access layouts, or manipulate alarm systems.
Detection and Alarm Failure	Medium.	High.	Poor maintenance, lack of battery backups, or configuration errors prevent real-time alerts from reaching responders.
Physical Sabotage of Infrastructure	Low.	Medium.	Attackers cut main power lines or sabotage network cabling to turn off local and remote security systems.
Loss of Public Trust and Prestige	Low.	Medium.	Major security breaches undermine public confidence, leading to fewer visitors and reduced international collaborations.
Irreparable Cultural Loss	Low.	Very High.	Stolen artifacts are often destroyed, damaged, or melted down for black-market sale, permanently erasing cultural heritage.

Spatial Intelligence and Spatiotemporal Visual Analytics

The integration of spatial intelligence into video surveillance represents a major technological transition. Traditional VSS systems relied on manual human monitoring or isolated pixel-level change detection, but modern architectures leverage location-aware AI to contextualize physical movements, trajectories, and interactions across both space and time.



The Transition from DORI to OODPCVS in IEC 62676-4:2025

The release of **IEC 62676-4:2025 (OODPCVS)** on October 9, 2025, replaced the traditional 2014 DORI model (Detection, Observation, Recognition, Identification) with a more precise seven-tier framework. The updated standard defines realistic pixel-density requirements for modern high-resolution IP cameras, accounting for digital compression, sensor performance in low-light conditions, and AI video analytics.
To calculate the required pixel density (D) at a specific target distance (d), the standard utilizes focal length (f), sensor dimensions, and target resolution parameters. The relationship is modeled as:
where R_h is the horizontal sensor resolution in pixels, f is the lens focal length in millimeters, W_s is the physical sensor width in millimeters, and d is the target distance in meters.
The OODPCVS model categorizes target specifications into two primary groups based on operational requirements :

Low Pixel Density Object (LPDO)

1. **Overview (20\text{ pix/m})**: Designed for basic scene monitoring and perimeter protection, allowing operators to detect moving objects at far distances.
2. **Outline (40\text{ pix/m})**: Captures basic shape details and direction of movement, which is useful for tracking simple object trajectories.
3. **Discern (80\text{ pix/m})**: Provides sufficient detail to distinguish between individual targets, vehicles, or animals in a crowd.

High Pixel Density Object (HPDO)

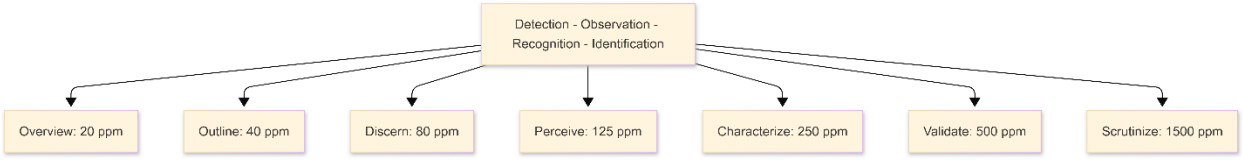
1. **Perceive (125\text{ pix/m})**: Provides high-contrast tracking of crowd activities.
2. **Characterize (250\text{ pix/m})**: Allows operators to identify specific attributes, including clothing details, gait, behavioral patterns, and vehicle classifications.
3. **Validate (500\text{ pix/m})**: Provides the resolution necessary to validate identity against a database or read license plates, satisfying the baseline requirement for automated facial recognition software.
4. **Scrutinize (1500\text{ pix/m})**: Delivers forensic-level detail equivalent to international passport photo standards, enabling high-certainty identification and inspection of small object details.

This framework replaces the traditional 2014 DORI model, which struggled with variable lighting and motion blur, with standard resolution values optimized for automated facial recognition and advanced machine perception.

Category	Zone Name	Old DORI Density (2014)	New OODPCVS Density (2025)	Algorithmic and Analytical Focus
LPDO	**Overview**	12\text{ pix/m} (Monitor).	20\text{ pix/m}.	Basic scene monitoring and tracking moving objects.
LPDO	**Outline**	2[span_182](start_span)[span_182](end_span)[span_186](start_span)[span_186](end_span)5\text{ pix/m} (Detect).	40\text{ pix/m}.	Detects physical boundaries and tracks movement direction.
LPDO	**Discern**	62\text{ pix/m} (Observe).	80\text{ pix/m}.	Distinguishes between individuals and isolates crowd behaviors.
HPDO	**Perceive**	125\text{ pix/m} (Recognize).	125\text{ pix/m}.	Identifies distinctive features, such as clothing and backpacks.
HPDO	**Characterize**	250\text{ pix/m} (Identify).	250\text{ pix/m}.	Profiles gait, specific physical traits, and behavior.
HPDO	**Validate**	[span_188](start_span)[span_188](end_span)[span_190](start_span)[span_190](end_span)500\text{ p[span_165](start_span)[span_165](end_span)ix/m} (Strong Ident).	500\text{ pix/m}.	Feeds high-resolution facial views into biometric engines.
HPDO	**Scrutinize**	1000\text{ pi[span_167](start_span)[span_167](end_span)x/m} (Inspect).	1500\text{ pix/m}.	Extracts fine details, micro-expressions, and physical markers.

Computational Spatiotemporal AI Modeling

Spatial intelligence systems deploy deep neural network topologies to interpret object behaviors within the physical environment.



- **Convolutional Neural Networks (CNN)**: Extract frame-by-frame visual features, including bounding box dimensions, object types, and facial details.
- **Graph Neural Networks (GNN)**: Model spatial relationships by treating detected objects as nodes (V) and their physical distances and interactions as edges (E), creating a dynamic spatial graph G = (V, E).
- **Spatiotemporal Trajectory Analysis**: Tracks changes in node states over time to model movement paths. The system evaluates these trajectories against defined behavioral classes.
    - *Tailgating*: Detects when the distance vector between two moving nodes is less than a minimum threshold near a restricted access gate.
    - *Suspicious Loitering*: Triggers an alert if a target's trajectory vector remains within a defined spatial coordinate range for longer than a specified time window (t > t_{\text{limit}}).
    - *Erratic Crowd Dynamics*: Measures velocity changes across nodes; a sudden, outward acceleration of multiple nodes indicates panic or a security incident, triggering automatic alarms.

Multi-Sensor Fusion and GIS Integration

Integrating video analytics with Geographic Information Systems (GIS) and IoT data enhances situational awareness across large networks.

- **GIS Mapping and Coordinate Alignment**: The system translates pixel coordinates from camera views into global geographic coordinates (GPS) on a 3D digital twin map.
- **IoT Sensor Integration**: Aligns video data with inputs from radar sensors, LiDAR (laser scanners), physical access control systems, and environmental monitors.
- **Unified Analytical Display**: Security teams monitor a single, cohesive spatial map that shows tracked subjects and triggered events across different camera fields of view, reducing context switching.
- **Operational Effectiveness**: Combining spatial intelligence with multi-sensor inputs improves event detection accuracy by up to 35% and cuts emergency response times by 30%.

Architectural Challenges in Spatiotemporal Implementations

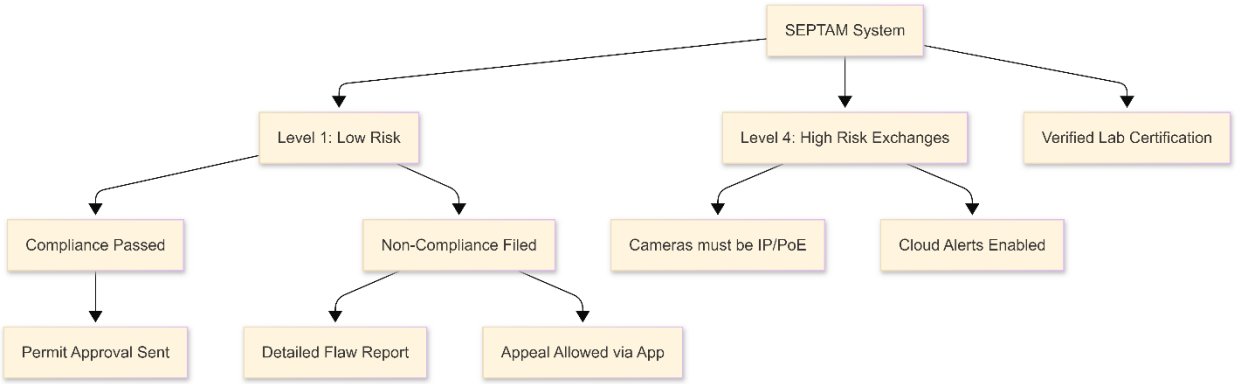
While highly capable, spatial intelligence architectures introduce significant technical and operational hurdles:

- **Massive Data Volumes and Computational Overhead**: High-resolution IP VSS networks generate terabytes of complex visual data daily. Transporting and processing these streams centrally demands immense bandwidth and high infrastructure costs. To address this, developers use edge computing devices to process spatial analytics locally before sending metadata to central servers.
- **Heterogeneous Data Formats and Interoperability**: Combining raw video streams with GPS data, GIS files, and IoT telemetry requires unified formatting. The Open Geospatial Consortium (OGC) is actively developing open standards to ensure compatibility across different manufacturers and platforms.
- **Data Privacy and Spatial Anonymization**: Tracking spatial behaviors risks exposing personally identifiable information (PII). To mitigate this, advanced architectures deploy homomorphic encryption and spatial anonymization (e.g., dynamic face masking at the edge) to protect privacy while maintaining analytical utility.

Technical Architecture and Socio-Political Dynamics of the Iranian SEPTAM System

Functional Architecture and Regulatory Integration of SEPTAM

The **Specialized Video Surveillance Compliance Monitoring System (سامانه پایش تطابق‌سنجی امنیت الکترونیک - SEPTAM / سـپتام)** is a national compliance monitoring portal in Iran. It manages, registers, and audits electronic security systems installed in commercial, public, and high-risk businesses.



Operated in coordination with the Public Places Police (پلیس اماکن فراجا) and the National Licensing Portal (درگـاه ملی مجوزهـا), SEPTAM acts as a mandatory checkpoint for businesses seeking to obtain or renew commercial operating permits.

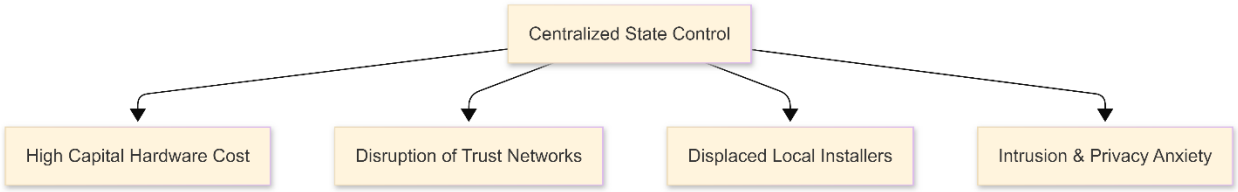
1. **Mandatory Portal Registration**: Business owners submit identity, location, and business permit information on the saptam.ir platform.
2. **Standardized Hardware Verification**: Applicants register installed VSS hardware, including cameras, NVRs, and storage devices. SEPTAM maintains a verified database of approved devices; only IP-based, Power-over-Ethernet (PoE) compliant hardware that has passed designated laboratory security audits is accepted. Analog or uncertified equipment is automatically flagged for replacement.
3. **Guild Risk Stratification**: Businesses are categorized into four security tiers based on asset values, vulnerability, and public density :
    - *Security Level 1*: Low-risk, small-scale commercial operations.
    - *Security Level 4*: High-security operations, including currency exchanges, gold dealers, and banks. These require high-definition cameras, continuous six-month local and cloud-based video backups, standardized cabling with visible labeling, and automated system alerts.
4. **On-Site Field Inspections**: Certified inspectors perform detailed physical audits to verify camera coverage, cabling standards, and network security.
5. **Permit Approval and Regulatory Issuance**: If the system passes inspection, SEPTAM issues a digital compliance certificate, which automatically notifies the Public Places Police to approve the business permit.
6. **Integrated Cloud Alarm Services**: Compliant installations can connect to a secure cloud monitoring architecture. This system uses automated video diagnostics to detect device tampering, video loss, or unauthorized intrusions, sending real-time alerts directly to police, fire, or medical dispatch centers.

The pricing structure for SEPTAM's inspection and cloud backup services is tiered by security level, as shown in the following table:

Guild Security Level	Standard Scope and Infrastructure Requirements	Inspection and Service Fees
Security Level 2	Standard retail and public spaces require moderate-resolution cameras and local storage.	24,000,000 Tomans annually.
Security Level 3	Medium-risk commercial environments; requires high-definition coverage of entrance paths and registers.	18,000,000 Tomans for 6 months.
Security Level 4	High-security institutions (such as banks and currency exchanges). Requires six-month redundant video storage, PoE networking, and cloud monitoring.	21,000,000 Tomans for 6 months.

Sociological Analysis of Guild and Business Resistance

Despite its objective of improving public safety, SEPTAM faced widespread pushback from the business community, prompting the Public Places Police to suspend the system in mid-October 2025. This resistance can be analyzed through several sociological and political-economy frameworks.



Collective Action and Social Capital (Putnam, Olson)

Mancur Olson's collective action theory posits that individuals act rationally, weighing the direct costs of compliance against perceived collective benefits. For small business owners, SEPTAM's mandatory fees and hardware upgrade costs were seen as an immediate financial burden with unclear security benefits. Robert Putnam's social capital framework highlights how horizontal networks of trust and peer relationships sustain community cooperation. SEPTAM disrupted these organic structures by imposing a top-down, state-monitored surveillance system that converted community-based safety expectations into a rigid, mandatory compliance program.

Social Constructivism and Discursive Legitimacy (Wendt)

Social constructivism emphasizes that technological legitimacy is co-created through public communication and shared understanding. A discursive conflict marked the implementation of SEPTAM.

- *The State Discourse*: Focused on public safety, systematic order, and legal compliance.
- *The Guild Discourse*: Viewed the system as an intrusive administrative burden, a threat to operational independence, and an unnecessary cost.

Because the regulatory authorities introduced the system through top-down mandates without public engagement, education, or financial support, the business community rejected the program's legitimacy, leading to organized resistance and petitions.

The Political Economy of Surveillance Technology (Zuboff)

Shoshana Zuboff's critique of surveillance capitalism explains how technological systems can shift economic control and concentrate power. SEPTAM's requirement for certified, laboratory-tested hardware disrupted the local security market. It marginalized independent technicians and local distributors, redirecting profits toward a small network of government-authorized hardware suppliers, testing labs, and service providers. This concentration of economic benefit triggered strong pushback from local merchant guilds, leading to coordinated political pressure that ultimately resulted in the program's suspension.

Autonomy, Privacy, and State Intrusion Concerns

The requirement for cloud-based backups connected to police infrastructure sparked significant privacy concerns among business owners. Guild members expressed anxiety that constant, remote video streaming would expose private business operations and confidential customer transactions to government agencies. This perception of government intrusion into commercial spaces became a rallying point for collective resistance, highlighting the sociological challenges that arise when implementing large-scale surveillance technology without clear boundaries, public consent, and robust data privacy protections.

Works cited

1. Hardware Trojan Detection & Prevention - Dr. Domenic Forte, https://faculty.eng.ufl.edu/dforte/research/hardware-trojan-detection-and-prevention/ 2. Detecting and Protecting from Hardware Trojans - Secure-IC, https://www.secure-ic.com/applications/challenges/hardware-trojans/ 3. What is a Hardware Trojan. In a nutshell | by Surabhi Misra | MeetCyber - Medium, https://medium.com/meetcyber/what-is-a-hardware-trojan-66c8fe66331e 4. Hardware trojan - Wikipedia, https://en.wikipedia.org/wiki/Hardware_trojan 5. The CCTV Backdoor: Securing Surveillance Networks from Hijacking - TerraZone, https://terrazone.io/securing-ip-surveillance-networks/ 6. TRUSTWORTHY HARDWARE: IDENTIFYING AND CLASSIFYING HARDWARE TROJANS - Google Research, https://research.google.com/pubs/archive/37398.pdf 7. Cybersecurity Threats and strategies in physical security and video surveillance - AxxonSoft, https://www.axxonsoft.com/blog/cybersecurity-threats-and-strategies-in-physical-security-and-video-surveillance 8. دانلود تحقیق شناسایی تروجان های سخت افزاری با استفاده از تحلیل تاخیر - سیگمالند, https://sigmaland.ir/%D8%AA%D8%AD%D9%82%DB%8C%D9%82-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%D8%AA%D8%B1%D9%88%D8%AC%D8%A7%D9%86-%D8%B3%D8%AE%D8%AA-%D8%A7%D9%81%D8%B2%D8%A7%D8%B1%DB%8C/ 9. IEC 62676-4:2025, https://webstore.iec.ch/en/publication/83425 10. IEC 62676 — Video Surveillance - Imatest, https://www.imatest.com/imaging/iec-62676/ 11. From DORI to Visual Performance in IEC 62676-4:2025 | Axis Communications, https://newsroom.axis.com/blog/iec-62676-4-video-surveillance 12. Specification/Standard - TAICS, https://www.taics.org.tw/eng/Publishing.aspx?PubCat_id=2 13. Publishing - TAICS, https://www.taics.org.tw/eng/Publishing.aspx?p=2 14. Cybersecurity Standard for Video Surveillance System- Part 2: IP Camera, https://www.taics.org.tw/files/FileDownload/TAICS_TS-0014-2Ev2.0-Video_Surveillance_System_Cybersecurity_Standard-Part2.pdf 15. Global Market Access News Update - Bureau Veritas, https://cpstp.bureauveritas.com/BVInternet/News/7413;mainIDX=7413 16. 【VN】New Vietnamese Standard Sets Cybersecurity Requirements for Cameras, https://www.theonelab.co/%E3%80%90vn%E3%80%91new-vietnamese-standard-sets-cybersecurity-

requirements-for-cameras/ 17. Vietnam Issues New IP Camera Security Standards-MRT, https://www.mrt-cert.com/en/gjxw/4817.html 18. Vietnam: Approving Technical Regulation on Network Information Security Requirements for Surveillance Cameras by Circular No. 21/2024/TT-BTTTT, https://www.tuvsud.com/en-us/e-ssentials-newsletter/consumer-products-and-retail-essentials/e-ssentials-1-2025/vietnam-circular-212024ttbtttt-on-surveillance-camera-network-security 19. Webinar series: Eye on Security - 20-Minutes Expert Insights - Dallmeier electronic, https://www.dallmeier.com/service/webinar 20. TROJAN Redeployable CCTV Camera - revader, https://www.revader.com/redeployable-camera 21. سرقت جواهرات موزه لوور ظرف 4 دقیقه - آوای بورالان, https://booralan.com/post/louvre-museum-robbery 22. جواهرات ناپلئون از موزه لوور فرانسه دزدیده شد؛ ماجرا چیست؟ • دیجی‌کالا مگ, https://www.digikala.com/mag/jewels-stolen-from-the-louvre-museum/ 23. Louvre Museum Closed After Dramatic Daylight Heist - Hyperallergic, https://hyperallergic.com/louvre-museum-closed-after-dramatic-daylight-heist/ 24. دستبرد به لوور - ویکی‌پدیا، دانشنامهٔ آزاد, https://fa.wikipedia.org/wiki/%D8%AF%D8%B3%D8%AA%D8%A8%D8%B1%D8%AF_%D8%A8%D9%87_%D9%84%D9%88%D9%88%D8%B1 25. کدام جواهرات از «لوور» دزدیده شد؟ - ایسنا, https://www.isna.ir/news/1404072818362/%DA%A9%D8%AF%D8%A7%D9%85-%D8%AC%D9%88%D8%A7%D9%87%D8%B1%D8%A7%D8%AA-%D8%A7%D8%B2-%D9%84%D9%88%D9%88%D8%B1-%D8%AF%D8%B2%D8%AF%DB%8C%D8%AF%D9%87-%D8%B4%D8%AF 26. Jewels stolen from Louvre worth an estimated $102 million, Paris prosecutor says - PBS, https://www.pbs.org/newshour/world/jewels-stolen-from-louvre-worth-an-estimated-102-million-paris-prosecutor-says 27. Louvre Museum Jewels Heist - Expert Opinon | BU Today | Boston University, https://www.bu.edu/articles/2025/louvre-museum-jewels-heist-expert/ 28. Jewel Thieves Dropped This Crushed Crown as They Fled the Louvre. Now, the Historic Headdress Will Be Restored to Its Former Glory - Smithsonian Magazine, https://www.smithsonianmag.com/smart-news/jewel-thieves-dropped-this-crushed-crown-as-they-fled-the-louvre-now-the-historic-headdress-will-be-restored-to-its-former-glory-180988151/ 29. استاندارد ایرانی؛چارهٔ مواجهه با رسوایی سرقت از موزه لوور پاریس, https://eghtesadegardeshgari.com/22360/%D8%A7%D8%B3%D8%AA%D8%A7%D9%86%D8%AF%D8%A7%D8%B1%D8%AF-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86%DB%8C%D8%9B%DA%86%D8%A7%D8%B1%DB%80-%D9%85%D9%88%D8%A7%D8%AC%D9%87%D9%87-%D8%A8%D8%A7-%D8%B1%D8%B3%D9%88%D8%A7/ 30. با نگاه ویژه به پدافند غیرعامل کنگره تخصصی امنیت الکترونیک, https://www.ictpress.ir/news/12451/%D8%A8%D8%A7_%D9%86%DA%AF%D8%A7%D9%87_%D9%88%DB%8C%DA%98%D9%87_%D8%A8%D9%87_%D9%BE%D8%AF%D8%A7%D9%81%D9%86%D8%AF_%D8%BA%DB%8C%D8%B1%D8%B9%D8%A7%D9%85%D9%84_%DA%A9%D9%86%DA%AF%D8%B1%D9%87_%D8%AA%D8%AE%D8%B5%D8%B5%DB%8C_%D8%A7%D9%85%D9%86%DB%8C%D8%AA_%D8%A7%D9%84%DA%A9%D8%AA%D8%B1%D9%88%D9%86%DB%8C%DA%A9_%D8%A8%D8%A7%D9%86%DA%A9_%D8%A8%D8%B1%DA%AF%D8%B2%D8%A7%D8%B1_%D9%85%DB%8C_%D8%B4%D9%88%D8%AF 31. نخستین دوره تخصصی امنیت الکترونیکی موزه ها پایان یافت, https://www.ictpress.ir/news/11808/%D9%86%D8%AE%D8%B3%D8%AA%DB%8C%D9%86_%D8%AF%D9%88%D8%B1%D9%87_%D8%AA%D8%AE%D8%B5%D8%B5%DB%8C_%D8%A7%D9%85%D9%86%DB%8C%D8%AA_%D8%A7%D9%84%DA%A9%D8%AA%D8%B1%D9%88%D9%86%DB%8C%DA%A9%DB%8C_%D9%85%D9%88%D8%B2%D9%87_%D9%87%D8%A7_%D9%BE%D8%A7%DB%8C%D8%A7%D9%86_%DB%8C%D8%A7%D9%81%D8%AA 32. IEC/EN 62676-4: 2025 OODPCVS support - JVSG, https://www.jvsg.com/iec-62676-4-oodpcvs/ 33. IEC 62676-4:2025 Sets a New Benchmark for Video Surveillance Systems, https://euro-security.de/en/iec-62676-42025-sets-a-new-benchmark-for-video-surveillance-systems/ 34. Deghaidy: OODPCVS: The New Model For DORI Performance Classification in CCTV Systems | PDF | Closed Circuit Television - Scribd, https://www.scribd.com/document/998689380/1760785778021 35. Online IP Video Guide - JVSG, https://www.jvsg.com/software/online-ip-video-guide/ 36. New release of IEC 62676-4 (Application

Guidelines) - CCTV Buyers Guide and News, https://cctvbuyersguide.com/2025/10/new-release-of-iec-62676-4-application-guidelines/ 37. IEC Introduces New Standard for Video Surveillance: IEC 62676-4:2025 - Reddit, https://www.reddit.com/r/videosurveillance/comments/1o7cc9a/iec_introduces_new_standard_for_video/ 38. سامانه پایش تصویری اماکن - saptam.ir - مشاوره حقوق دینا - ورود به سایت سپتام, https://www.heyvalaw.com/web/articles/view/6098/%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87-%D9%BE%D8%A7%DB%8C%D8%B4-%D8%AA%D8%B5%D9%88%DB%8C%D8%B1%DB%8C-%D8%A7%D9%85%D8%A7%DA%A9%D9%86.html 39. Understanding OODPCVS, the new image detail classification framework in IEC 62676-4:2025 - Hikvision, https://www.hikvision.com/europe/newsroom/blog/understanding-oodpcvs--the-new-image-detail-classification-frame1/ 40. سپتام - درباره سامانه پایش تصویری اماکن, https://saptam.ir/about 41. سپتام چیست؟ سامانه سپتام چیست ؟ - 42. https://sarafyar.com/saptam/, همه چیز درباره سامانه پایش تصویری اماکن ایران - صراف یار پایگاه خبری اختبار, https://www.ekhtebar.ir/%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87-%D8%B3%D9%BE%D8%AA%D8%A7%D9%85-%DA%86%DB%8C%D8%B3%D8%AA-%D8%9F/ 43. سامانه سپتام چیست؟/ همه چیز درباره سامانه پایش تصویری اماکن عمومی - خبرگزاری میزان, https://www.mizanonline.ir/fa/news/4796998/%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87-%D8%B3%D9%BE%D8%AA%D8%A7%D9%85-%DA%86%DB%8C%D8%B3%D8%AA-%D9%87%D9%85%D9%87-%DA%86%DB%8C%D8%B2-%D8%AF%D8%B1%D8%A8%D8%A7%D8%B1%D9%87-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87-%D9%BE%D8%A7%DB%8C%D8%B4-%D8%AA%D8%B5%D9%88%DB%8C%D8%B1%DB%8C-%D8%A7%D9%85%D8%A7%DA%A9%D9%86-%D8%B9%D9%85%D9%88%D9%85%DB%8C 44. سامانه پایش تصویری اماکن - موسسه حقوق ثبت فردا, https://sabtefarda.org/%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87-%D9%BE%D8%A7%DB%8C%D8%B4-%D8%AA%D8%B5%D9%88%DB%8C%D8%B1%DB%8C-%D8%A7%D9%85%D8%A7%DA%A9%D9%86/ 45. سامانه سپتام (دوربین مداربسته مورد تایید اماکن), https://cruzcctv.ir/%D8%AF%D9%88%D8%B1%D8%A8%DB%8C%D9%86-%D9%85%D8%AF%D8%A7%D8%B1%D8%A8%D8%B3%D8%AA%D9%87-%D9%85%D9%88%D8%B1%D8%AF-%D8%AA%D8%A7%DB%8C%DB%8C%D8%AF-%D8%A7%D9%85%D8%A7%DA%A9%D9%86-%D8%B3%D8%A7%D9%85%D8%A7/ 46. سپتام - رسته صنف, https://saptam.ir/guild 47. سامانه «سپتام» متوقف شد - طبق اعلام پلیس نظارت بر اماکن عمومی فراجا ،سامانه «سپتام» متوقف شد, https://saricu.ir/1404/07/19/%D8%B7%D8%A8%D9%82-%D8%A7%D8%B9%D9%84%D8%A7%D9%85-%D9%BE%D9%84%DB%8C%D8%B3-%D9%86%D8%B8%D8%A7%D8%B1%D8%AA-%D8%A8%D8%B1-%D8%A7%D9%85%D8%A7%DA%A9%D9%86-%D8%B9%D9%85%D9%88%D9%85%DB%8C-%D9%81%D8%B1%D8%A7/ 48. اتاق اصناف ایران - سامانه «سپتام» متوقف شد, https://otaghasnafeiran.ir/ft13071404-asnaf-4/