Viakoo Labs | Open Letter to the Physical Security Community

Proposing a Coordinated Response To Threats at AI Speed

VIAKOO

Key Points/Takeaways

- Cyber Threats to Physical Security Systems are Growing at AI Speed
- Current Approaches Are Not Capable in Speed or Scope
- Collective Awareness and Action Is Needed By End Users, Solution Vendors, and Service Providers

- **Call To Action: Interested Parties Are Invited to Participate in Online (Date TBD) and In-Person (at GSX) Town Hall Meetings To Improve Awareness and Coordination**

ISC West 2025

To our colleagues in the Physical Security Community,

The increasing convergence of physical and cyber systems presents a critical juncture for our industry. The evolving landscape of threats, now heavily influenced by AI, demands a unified and collaborative response from the physical security community to protect our Cyber-Physical Systems (CPS). Gartner in a February 2025 report defines the term cyber-physical systems to encompass concepts such as IoT, smart city and systems created as a result of operational technology (OT) and IT convergence. CPS systems have one foot in the physical world and the other in the cyber world. Definitionally, physical security systems are cyber-physical systems and represent the largest number of CPS deployments. The rapid growth of the CPS attack surface and AI-driven threats has created unprecedented exposure management challenges, requiring remediation at a scale and speed never seen before. Beyond the sheer volume and diversity of CPS in physical security, we recognize that there are critical process and architecture issues that demand our collective attention to solve them.

Cyber-Physical Threats are Growing at AI Speed. New Solutions Are Urgently Needed.
The physical security community must proactively engage in understanding and mitigating AI-driven threats to its CPS infrastructure by working collaboratively. We believe as a community that just as scientific discoveries happen through partnership and collaboration, so should be the process for securing exposed CPS devices which have 1000x more processing, memory, and storage than enterprise servers had 20 years ago (when cybercrime began to explode). This advancement must be the product of a cross-community partnership, which includes not only asset discovery, threat assessment, and remediation solution vendors, but also the security integrator and managed service provider communities whose ability to deploy solutions quickly is needed to address the scale and the impact of physical security vulnerabilities. The accelerating pace of AI-driven threats demands immediate and concerted action from our community to prevent potentially devastating consequences.

Securing Physical Security: A Foundation for Broader CPS Resilience
Today (March 2025) we can see that the nature of threats to physical security systems is shifting and now includes AI-powered attacks on smart locks, video surveillance systems, intrusion detection systems, and building management systems. The challenges from AI-driven threats that we face today can overwhelm us if we do not step outside of the traditional approaches to securing physical security systems.

The current CPS security crisis includes use cases from various verticals including:

- Healthcare – AI-powered manipulation of access control to restricted areas containing sensitive patient data or critical equipment.
- Retail – AI-driven attacks on smart building systems leading to disruptions or security breaches.
- Oil & Gas – AI exploiting vulnerabilities in industrial control systems (ICS) that manage physical or chemical processes.
- Financial services – AI targeting smart surveillance systems to bypass security controls for financial transactions.
- Transportation – AI compromising the security of connected vehicles or mass transit infrastructure.

Today’s IoT security measures are weak as compared to IT security measures. Attempts to build on the legacy IT security infrastructure will become increasingly expensive and fragile. One example is how agent-based security was designed for use inside a datacenter but cannot be applied to CPS devices (which do not accept agents). Most concerning is that there are now several areas where cybersecurity architectures when applied to CPS are already running into issues of scalability and capability and must change direction.

Broader Industry Awareness and Dialogue: A Path to Rapid Improvement
Within our community we see many physical security professionals already aware that cybersecurity issues are accelerating and have started taking action through training and education (for example, SIA’s SICC certification). Their voices are clear: the time is now to implement better cybersecurity solutions that can address AI-driven threats. They are also looking for disruptive innovation in physical security management to reach this next level of capability.

As such, we believe the CPS and Physical Security communities must pursue a new set of best practices to act as their “North Star”:

- We urge physical security professionals to actively seek knowledge and training on AI-driven threats to CPS.
- We call for increased collaboration between physical security vendors, IT security teams, and cybersecurity experts to develop comprehensive solutions.
- We encourage the development of industry best practices and standards, particularly in areas like secure CPS device deployment, AI-driven threat detection and response, and lifecycle management of connected physical security systems.
- We propose the formation of working groups within the physical security community to address specific challenges related to AI and CPS security.
- We invite organizations to share and benchmark their best practices with other physical security operators.

Interested Parties Are Invited to Participate in Online (Date TBD) and In-Person (at GSX) Town Hall Meetings To Improve Awareness and Coordination. Viakoo is committed to fostering and engaging in this crucial dialogue. We invite you to join us in this collaborative effort by registering at [www.viakoo.com/ai-driven-threats] to share your specific issues and initiatives.and to become part of upcoming meetings. This platform will allow us to collectively identify challenges, benchmark best practices, and work towards unified solutions.

The time to act is now. By working together, the physical security community can effectively address the growing threat of AI-driven attacks on our critical security infrastructure. We believe that through open collaboration and a shared commitment to security, we can build a more resilient future for our CPS deployments. Let us unite as a community to tackle these challenges head-on and ensure the continued safety and security of our organizations.

Regards,
John Gallagher
Vice President, Viakoo Labs
Viakoo, Inc.

Register Here: www.viakoo.com/ai-driven-threats