



PHYSICAL SECURITY FOR OT ENVIRONMENTS ·
BUILT FOR WHAT AUDITORS ASK NEXT

Velocity Central Platform Overview

For OT And ICS Security
Managers At Utilities And Critical
Infrastructure Operators | 2026

HIRSCH
PHYSICAL SECURITY FOR CRITICAL
INFRASTRUCTURE

Unified Security.
Limitless Possibilities.

The Gap Between Your SIEM And Your Substation Gate

Most utility security and OT teams have invested heavily in network visibility. Your SIEM sees every network event. Dragos or Claroty see the ICS protocol traffic. Your SOC has a clear picture of what is happening on the OT network.

The question the auditor asks — and the question you should be asking first — is different: can your security platform see who opened the substation gate, who badged into the control building, and what the perimeter sensor showed in the 15 minutes before that access event? And does that physical event feed into the same monitoring environment your OT security team is already watching?

The audit question

CIP-006 requires physical access monitoring for electronic security perimeters. CIP-007 requires system security management for BES cyber systems. The evidence for both often sits in separate systems across separate teams — and when an auditor asks for a correlated view, the utility assembles a manual narrative. Hirsch Velocity Central is built to close that gap.

What Velocity Central is (and what it is not)

Velocity Central is the Hirsch unified physical security management platform. It consolidates physical access control, perimeter intrusion detection and video surveillance into a single command and monitoring environment — from edge to core.

Velocity Central is not a SIEM. It is not a cyber tool. It is a physical security platform, and it has been built for critical infrastructure environments for more than 45 years. The integration paths to your OT security and network monitoring tools are intentional and documented.

More Information About Velocity Central

Physical Access Control

OSDP-based access control for substation control buildings, electronic security perimeters and battery rooms. Named, encrypted, non-repudiable access events. Non-shared credentials. CIP-006 R3 compliant.

Perimeter Detection

Hirsch Protech fibre-optic fence sensing integrated natively into the Velocity Central event stream. Zone-level alarm classification with automatic camera call-up. False-positive rate typically under 5% in calibrated deployment.

Video Surveillance

Integrated VMS with support for Milestone, Genetec, Bosch, Axis and Avigilon camera estates. Video call-up is automatic on perimeter alarm or access event. Camera events appear in the same timeline as physical access events.

Unified Event Timeline

A single, correlated record of physical events per site: perimeter state, access events, camera call-ups. One export covers what CIP-006 and CIP-014 auditors are asking for.

Federated Multi-Site Management

Manage 1 to 1,000+ sites from a single Velocity Central instance. Site-level configuration, alarm routing and evidence packaging are independent per site.

OT Monitoring Integration

Structured physical event export to Splunk, Microsoft Sentinel, Dragos and Claroty. OSDP access events, Protech perimeter events and VMS alerts forwarded as syslog or API-driven telemetry into the existing OT security stack.

The SIEM integration:

Physical events into your existing OT monitoring stack

Most utility OT security teams are running a SIEM — Splunk and Microsoft Sentinel are the most common in the TX/AR/LA footprint. Most OT-specific platforms (Dragos, Claroty) have network-level visibility but not physical access visibility.

Velocity Central sends physical events — who opened a gate, who badged into a control building, when the perimeter sensed a disturbance, when camera motion was detected in a restricted zone — into the same monitoring tool your network team is already using. The people watching the network and the people watching the fence are looking at the same timeline.

Platform	Integration Method	Data Flow
Splunk	Syslog or HTTP Event Collector (HEC). Velocity Central forwards structured OSDP access events, Protech alarm events and VMS alerts. Compatible with Splunk for Industrial IoT and Splunk ES.	Physical access events correlated with network events in a single Splunk timeline. CIP-006 and CIP-014 evidence exportable from Splunk dashboards.
Microsoft Sentinel	CEF syslog connector or custom Sentinel Data Connector. Physical events ingest into the same Sentinel workspace as OT network telemetry.	Physical event correlation with Microsoft Defender for IoT alerts. Unified incident view across physical and OT network domains.
Dragos Platform	Dragos integration receives Velocity Central physical access events via syslog. Events are tagged with site and asset context that aligns with Dragos asset inventory.	Physical intrusion context alongside Dragos network behavior detections. Supports correlation of physical access with ICS protocol anomalies at the same site.
Claroty XDome	REST API integration. Velocity Central physical events forwarded to Claroty for correlation with OT asset visibility and network segmentation data.	Physical access to control building cross-referenced with network activity by BES cyber asset. Supports insider threat and anomalous access detection workflows.

CIP-006 And CIP-007: What Velocity Central Produces For Your Audit Team

CIP-006 and CIP-007 evidence requirements are frequently managed across separate teams using separate systems. The result is that an auditor asking for a correlated view of who had physical access to an electronic security perimeter and what OT system activity was associated with that access period receives a manually assembled response.

Velocity Central produces structured evidence that reduces the manual assembly burden and reduces the risk of inconsistency between the evidence narrative and the underlying system records:

CIP-006 R3

OSDP Access Event Logs

Named individual, credential, timestamp, site, door. Non-repudiable. Exportable per site, per date range, in a format aligned to TRE and SERC evidence requests.

CIP-006 R4

Perimeter Alarm Disposition Log

Event time, zone, classification, notified party, response action, closure. Every alarm has a disposition record. No manual narrative required.

CIP-006 R5

Two-Person Integrity And Escort Records Where Applicable

Velocity Central supports dual-credential access control and escort logging for high-assurance environments.

CIP-007

Supporting Evidence

Velocity Central physical event logs forwarded to the SIEM provide the physical access context for BES cyber asset access events. The auditor can see, in one place, that a specific individual accessed the physical space and then accessed the SCADA system in the same session.

Mercury Controller Compatibility: No Rip-And-Replace Required

Mercury hardware is widely deployed across the utility sector — LP1501, LP1502, LP4502 and SCP series controllers are common in both greenfield and legacy substations. Velocity Central integrates with Mercury controllers natively.

OSDP reader migration — moving from legacy Wiegand readers to OSDP at the door — does not require Mercury controller replacement. The Mercury controller passes OSDP events to Velocity Central in the same way it passes Wiegand events, with the addition of the encryption and non-repudiation that OSDP provides. A site migration from Wiegand to OSDP can be completed in a standard maintenance window, one door at a time, without taking the site offline.

Migration reference

A utility with 26 CIP-006 applicable access points across 8 substations completed OSDP migration in 11 months. No Mercury controllers were replaced. CIP-006 R3 compliance status moved from partial to full. The compliance team's evidence assembly cycle for those 8 sites dropped from four weeks to two days.

The Audit Conversation: What The OT Security Manager Needs To Be Able To Say

When A TRE Or SERC Auditor Asks The Correlated-Access Question During A CIP-006 Or CIP-014 Review, The OT Security Manager Needs To Be Able To Demonstrate Four Things:

- ✓ Physical access to every CIP-006 applicable electronic security perimeter is monitored, logged and non-repudiable. Named individuals. Encrypted credential events. Time-stamped.
- ✓ Perimeter detection at CIP-014 applicable substations is operational, calibrated, and generating alarm dispositions that are documented in real time. Not assembled retrospectively.
- ✓ Physical access events and OT network events can be correlated in a common timeline. The same individual who badged into the control building at 14:23 can be located in the SIEM record alongside the OT system activity from 14:23 onwards.
- ✓ The evidence can be exported in a structured, site-by-site format without a multi-week manual assembly process.

Velocity Central is the platform that makes all four of those answers possible in the same unified environment.

What A Velocity Central Deployment Looks Like For A Mid-Size Utility OT Team

A Mid-Size IOU Or G&T Cooperative In The TX/AR/LA Footprint Typically Has:

- ✓ 20–50 CIP-014 applicable substations with a mix of staffed and unmanned configurations
- ✓ A Mercury-based access control estate across control buildings and battery rooms at applicable sites
- ✓ A VMS estate with cameras at most applicable substations, often on a Milestone or Genetec platform
- ✓ An OT security SIEM (Splunk or Sentinel) and one or more OT network monitoring tools (Dragos or Claroty)

A Velocity Central Deployment For That Environment Includes:

- ✓ Velocity Central federated management instance, connected to existing Mercury controllers at all applicable sites
- ✓ OSDP reader upgrade at CIP-006 applicable access points, completed site-by-site in maintenance windows
- ✓ Hirsch Protech perimeter detection at all CIP-014 applicable unmanned substations, integrated into Velocity Central
- ✓ VMS integration with existing Milestone or Genetec system. No camera replacement required.
- ✓ SIEM integration configured to forward structured physical events to existing Splunk or Sentinel instance
- ✓ Velocity Central evidence export templates configured for TRE or SERC audit format

Request A Technical Walkthrough

This overview covers the platform at summary level. For a technical walkthrough of the Velocity Central integration architecture for a utility OT environment, contact the Hirsch utilities team and request the OT integration technical brief.

The technical brief covers the OSDP data flow architecture, the SIEM integration API specifications, the Mercury compatibility matrix, and the CIP evidence export format documentation.

Contact

To arrange a technical walkthrough or to request the OT integration brief, contact the Hirsch utilities team at hirschsecure.com. Reference the Velocity Central Platform Overview and your organization name. A Hirsch solutions engineer with OT environment experience will be in touch within one business day.



Thank You!

HIRSCHSECURE.COM

Velocity Central Platform Overview

HIRSCH

**PHYSICAL SECURITY FOR CRITICAL
INFRASTRUCTURE**

All Rights Reserved. This Guide Is Prepared For Field Deployment Teams And Does Not Supersede Site-Specific Safety Procedures, Outage Authorization Requirements, Or CIP Access Control Obligations. Always Follow Your Organization's LOTO And Site Access Procedures.

Unified Security.
Limitless Possibilities.