

WECC POWER SYSTEMS SECURITY CONFERENCE • DAY 1: PHYSICAL SECURITY

A Practical Guide to Mobile Surveillance and Rapid Security Deployment

Rob Oldham

CPP • PSP • PCI • CPTED • MBA

Vice President & Co-Owner, Backstreet Surveillance

President, ASIS International — Utah Chapter

Salt Lake City, Utah • August 2026

Backstreet Surveillance • Rob Oldham, CPP, PSP, PCI, CPTED, MBA



Who is talking to you

CPP

Certified Protection Professional — ASIS board certification in security management. The profession's benchmark credential.

PSP

Physical Security Professional — ASIS board certification specific to physical security assessment, design, and integration.

PCI

Professional Certified Investigator — ASIS board certification in investigations and case management.

CPTED

Crime Prevention Through Environmental Design — Florida Atlantic University.

MBA

Master of Business Administration — the business case is half of every security decision.

ASIS Utah

Chapter President, ASIS International Salt Lake City Chapter — statewide.

All three ASIS certifications are active and board certified. Roughly a few hundred people worldwide hold all three.

Source: [ASIS International](#)

The road here — 26 years

Combat veteran

Operation Iraqi Freedom — Kuwait, Iraq, Iran. Where I learned defense in depth as a survival requirement, not a chapter heading.

SimplexGrinnell

One of the world's largest fire and security companies. Enterprise-scale life safety and security delivery.

Axis Communications — 10 years

The company that invented the IP video surveillance camera. Product development, system design, training, consulting, and leadership.

Metravib Défense (Lyon, France)

Gunshot detection and acoustic tracking — product commercialization, deployment, and development.

Backstreet Surveillance

Vice President and co-owner. Solar Guard towers, Guard Box, SentryPro, Scout, and the new Ranger.

Where the lessons came from

Critical infrastructure consulting and deployment:

Federal & Energy

WAPA · Bureau of Reclamation · Hoover Dam · USACE · Idaho National Laboratory · Solar farms

Government & Defense

U.S. Capitol Police (18-acre campus) · Border wall · West Point

Transportation & Campus

Regional and international airports · Universities · Hospitals

Commercial & Industrial

Data centers · Mag 7 technology companies · Large construction programs



THE GROUND TRUTH

Samarra, Iraq The retrans site

A re-transmission site is a small, isolated, high-value node. No town. No fence line worth the name. No help within an hour. If it goes down, everyone downstream goes deaf.

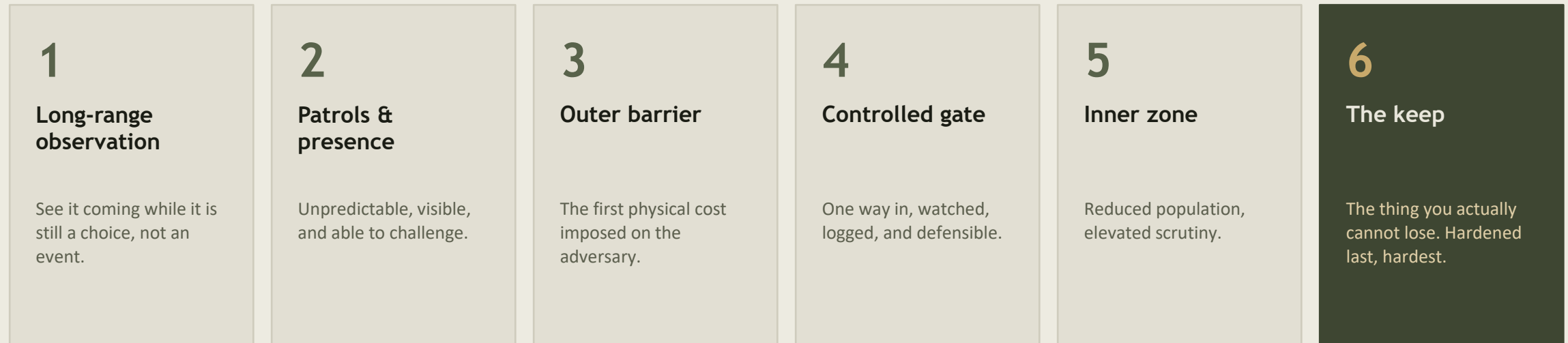
- We could not make it impenetrable. We could only make it expensive, slow, and loud.
- Everything we built bought one thing: time. Time to see, time to decide, time to respond.
- Detection had to happen at the far edge — not at the wire, where it is already too late.
- The layers had to work when a layer failed. Because layers fail.



Operation Iraqi Freedom — Kuwait, Iraq, Iran

The castle approach

Nobody ever built a castle with one wall. Every layer exists to make the next layer survivable.



The adversary does not face one problem. He faces a sequence of problems & each one costs him time and gives you information.

Source: [ASIS Protection of Assets](#) · [Sandia National Laboratories PPS methodology](#)

Every protection system does three things

If your design cannot name where each of these happens, you do not have a system — you have equipment.

DETECT

Sense that something is happening & get that information to someone who can act on it.

Detection without annunciation is a recording, not a detection.

DELAY

Slow the adversary's progress so that response has time to arrive and matter.

Delay is only worth what response can do with it.

RESPOND

Put capable people on the problem before the adversary completes the task.

Response time is the clock every other number is measured against.

Defense in depth means these three functions are present across the entire path from the outside world to the asset — not concentrated at one point.

Source: [Sandia National Laboratories, Security Technology Testing and Evaluation Manual \(2021\)](#)

The 5 D's — and the sixth one

DETER

Make the site a bad choice before anything happens. Visible mast, light, signage, and a voice.

DETECT

Deep learning analytics on every frame — people, vehicles, loitering, crowding, intrusion — in real time.

DELAY

A challenged intruder slows down, hesitates, or leaves. Hesitation is delay you did not have to build.

DENY

Verified alert drives action: close the gate, lock the door, cut the access, stage the responder.

DOCUMENT

High-quality video, LPR, radar tracks, and time-stamped event logs that survive a courtroom.

DEFEND

The sixth D. That same documentation defends you — with insurers, regulators, and plaintiffs' counsel.

A properly designed mobile platform delivers all six from a single trailer, on the day it lands.

Anatomy of a real incident

Alarm #89880 · Trailer 261 · Bay Point, California · 00:20:39 PDT

- 00:20:39** ■ Deep learning analytic fires: person detected, zone 01.
- 00:20:42** ■ Operator on the event. Response time: 2.12 seconds.
- 00:23:03** ■ Outbound call to site contact initiated.
- 00:23:18** ■ Camera action alert — audio warning clip played on scene.
- 00:24:21** ■ Contact made with site representative.
- 00:27:10** ■ Law enforcement dispatch accepted.
- 00:30:08** ■ Operator note: male on site running, appears to be hiding, backpack, dark hoodie.
- 00:30:43** ■ Full clear — authorities dispatched. Total handle time: 10 minutes 1 second.

Every line of this is time-stamped, exportable, and defensible. That is the sixth D doing its job.

Incident Report

Alarm #89880

Authorities Dispatched

Response - 2.12s

Customer

Site

Address

Date / time

Event code

Handle time

Talk Down Attempts

Call Out Attempts

Disposition

NextGen

Trailer 261

2840 Willow Pass RdBay Point, CA 94565 USA

06/24/2026 00:20:39 PDT

EV03 — Evolon Video Event Person Detected

10m 1s

1

2

Full Clear - Authorities Dispatched

Event capture & site location



Event capture - 06/24/2026 00:20:39 PDT

Click image to view live clip

Site location

2840 Willow Pass RdBay Point, CA 94565 USA

Contra Costa County

Call Out Summary

Police dispatch — Call-Dispatch Accepted — Accepted at 00:27:10 PDT · OP 100 WILL DISP REF #17

Outbound call — Call-Contact Made — Contact made at 00:24:21 PDT · TOM REQ DISP - REQ A CALL BCK IF ANY ISSUES

Operator action timeline

06/24/2026 00:20:39 PDT

EV03 - Evolon Video Event Person Detected

"Motion Detected (Zone: 01)"

06/24/2026 00:20:42 PDT

Access on Dispatch Window (MH)

Dial Phone (MH)

06/24/2026 00:23:03 PDT

EV16 - Camera Action Sent Alert

"Warning (Play Audio Clip)"

06/24/2026 00:24:21 PDT

Call-Contact Made (MH)

"TOM REQ DISP - REQ A CALL BCK IF ANY ISSUES"

06/24/2026 00:24:44 PDT

Dial Phone (MH)

Call-Dispatch Accepted (MH)

06/24/2026 00:27:10 PDT

Dispatch Accepted-Dispatch Accepted (MH)

Comment (MH)

06/24/2026 00:30:08 PDT

"MALE ON SITE SEEN RUNNING LOOKING LIKE HES TRYING TO HIDE - HAS A BACKPACK W/ A DARK HOODIE"

2.12 sec

operator response

10m 01s

detection to full clear

- 1 talk-down
- 2 call-outs
- 1 dispatch

This is your data, not mine

Physical security intrusions reported to DOE in the West Interconnection

107

Reported in 2023

220

Reported in 2024 — more than double

4

Cyber intrusions reported in 2024, up from 2 in 2023

-
- Incident types included assault, ballistic damage, intrusion, vandalism, theft, and suspicious activity.
 - WECC notes much of the increase came from one entity reporting minor incidents, which is itself the finding: most of this is invisible until somebody decides to count it.
 - Very few incidents affected load. That is not reassurance — that is the near-miss population you get to learn from for free.
 - Nationally, physical attacks and vandalism threatening grid reliability rose 77% to 163 incidents in 2022, across three dozen states and ~90,000 customers.

Source: [WECC State of the Interconnection 2025](#) · [DOE OE-417 Annual Summaries](#) · [Bloomberg \(2023\)](#)

Compliance is a floor, not a program

- CIP-014 was approved by FERC in November 2014 and applies to transmission stations at 500 kV and above, plus certain 200–499 kV stations meeting a weighted-value threshold.
- It covers roughly 200 or fewer of the approximately 55,000 transmission substations in the United States — owned by around 30 companies.
- It does not cover generation, and it does not cover distribution substations.

~200

substations covered by a mandatory federal physical security standard

55,000

transmission substations in the United States

Source: [NERC CIP-014-1](#) · [NERC Report on CIP-014-3 \(April 2023\)](#) · [ASIS, The Power of Physical Security](#)

The theft you actually see every week

18,400 incidents

Copper theft incidents reported by 618 utilities in the industry's worst recorded year, costing \$22 million in repairs — an average of \$1,200 per incident, with one utility absorbing \$2 million alone.

\$2.8 million

Damage from a single copper wire theft at a 9,000-panel solar farm in Fresno County, California. It knocked out ~80% of power to a nearby county justice campus for months. The wire — over \$100,000 of it — was never recovered.

21% recovered

Of 11,574 equipment theft reports recorded in NCIC in one year, only 2,442 resulted in a recovery. Average stolen equipment value: \$29,258.

Under 7%

Recovery rate for construction site thefts across 15,274 NIBRS-recorded incidents, at an average loss of \$5,865 each. Tools, heavy equipment, and building materials were the top three targets.

DOE's own analysis found no evidence that utility copper theft is motivated by sabotage or terrorism. It is purely economic — which is exactly why deterrence works on it.

Source: [DOE, Assessment of Copper Wire Thefts from Electric Utilities \(2010\)](#) · [Fresno County Sheriff \(2024\)](#) · [NER/NICB Equipment Theft Report](#)

The attack surface is growing faster than the perimeter budget

+49%

Growth in total U.S. solar operating capacity expected by the end of 2027 versus the end of 2025

~70 GW

New solar generating capacity coming online in 2026–2027 alone

424 bn

kWh

Projected 2027 utility-scale solar generation, up from 290 billion kWh in 2025

-
- Every one of those projects is a remote, unfenced, high-copper-content, low-population site during construction — and a remote, high-value, low-staff site for thirty years after.
 - Utility-scale solar is now the fastest-growing source of U.S. electricity generation. The security model has not scaled with it.
 - These sites are precisely where fixed infrastructure is hardest to justify: no power at the perimeter, no network, no permanent staff, and a footprint measured in square miles.

Source: [U.S. Energy Information Administration \(January 2026\)](#)

Why guards alone cannot close the gap

Guards are irreplaceable. Presence, judgment, and the ability to physically respond cannot be bought any other way. But a guard post is not a coverage strategy.

COST

The U.S. mean security guard wage is \$19.44/hour. Covering one post 24/7/365 takes roughly 4.5 FTE once relief, PTO, and sick coverage are counted — about \$182,000 per year in wages alone, before benefits, overhead, or supervision.

COVERAGE

A guard is in exactly one place at a time. The moment a patrol moves or a call pulls him away, the rest of the site is uncovered — and an adversary watching for two nights knows the pattern better than the guard does.

HUMAN FACTORS

Fatigue, distraction, turnover, and inconsistent performance are not character flaws; they are predictable properties of the job. A stretched program converts them directly into vulnerability.

The goal is not fewer people. It is people who are pointed at the right problem, because software watched every frame and only interrupted them when it mattered.

Source: [U.S. Bureau of Labor Statistics, OEWS \(May 2023\)](#)

The false alarm tax — and why nobody comes

94-98%

of police alarm responses are false

\$1.8 bn

estimated annual cost of responding to ~36 million alarm activations

0.3%

of Salt Lake City alarm calls resulted from an actual crime

-
- False alarms consume 10–25% of all police calls nationwide — roughly 20 minutes and two officers each. DOJ estimated the burden as equivalent to tying up 35,000 officers.
 - Salt Lake City adopted verified response in 2000 and freed the equivalent of five full-time officers. Cities adopting verified response saw alarm calls fall roughly 90%.
 - This is the single most important reason to design for verification: an unverified alarm is a request. A verified alarm with live video and a voice on scene is an emergency, and it gets treated like one.

Source: [DOJ COPS Office, False Burglar Alarms, 2nd Ed.](#)

PART TWO

What the evidence actually says

Forty years of research on whether cameras work — and the one variable that decides it.

40 years, 76 evaluations, one decisive variable

MONITORED

About 15% less crime

...than a matched area with no cameras. Odds of that being luck: under 1 in 1,000.

PASSIVE

No measurable difference

...from having no cameras at all. The result is indistinguishable from chance.

The largest and most rigorous Surveillance Camera meta-analysis ever conducted found that cameras which are actively monitored significantly reduce crime, and cameras which are not, do not. The hardware is not the intervention. The response is.

Cameras combined with other measures — lighting, patrols, signage — produced about 34% less crime, the largest effect of any configuration studied. Cameras alone, with nothing else, showed no measurable effect.

Source: [Piza, Welsh, Farrington & Thomas, Criminology & Public Policy 18\(1\), 2019](#)

Where cameras work best — and where they don't

Car parks / parking lots	37% less crime
Residential areas	12% less crime
Drug crime	20% less crime
Property crime	14% less crime
Vehicle crime	14% less crime
Violent crime	No measurable effect
City centres	No measurable effect

**The single best-evidenced use of a camera on the planet is watching an open area.
Which is exactly what a trailer does on day one.**

Source: [Piza et al., Criminology & Public Policy 18\(1\), 2019](#)

What that actually looks like



Car park, 21:15 on a Saturday

Roughly 200 vehicles, an active crowd, retail frontage. This is the exact setting the meta-analysis rates as the strongest use of a camera anywhere in the literature.



Illegal dumping, after hours

A box truck backs into an empty lot and offloads. No sabotage, no ideology — somebody solving their disposal problem with your asphalt. Purely economic, and therefore deterrable.

Neither of these is a rifle attack on a substation. Both drain real budget — and both are what monitored cameras reduce.

Those numbers are the floor, not the ceiling

THE LADDER —

Camera alone

36 studies

No measurable gain

+ someone actually watching

54 studies

15% less crime

+ light, voice, patrol/response

14 studies

34% less crime

THE STACK — what that means on a trailer

LIGHT

Deployable light towers cut outdoor nighttime index crime by at least 36% across 80 NYCHA developments — a randomized trial, not a vendor claim. Fixed street lighting: 14% across 17 studies.

VOICE

Across 1.6M monitoring events at 18,258 U.S. sites, 62.4% of high-priority events were resolved with no police dispatch. 96.1% ended at a voice-down.

VERIFIED DISPATCH

ANSI/TMA AVS-01 (rev. Dec 2024) scores every alarm 0–4 so agencies triage on evidence, not on a contact list. Adopted by NETCOM 911, San Diego County, Fresno PD, Nashville, Alameda County; IACP resolution in support.

Same cameras every time. The only thing that changed is what was around them.

Source: [Piza et al. 2019](#) · [Chalfin et al., lighting RCT](#) · [Welsh, Farrington & Douglas 2021](#) · [Interface Systems 2026 \(vendor\)](#) · [TMA AVS-01](#) · [LPRC ePVM trial](#)

Two stops in 60 days on a live transmission site



► [Copper theft in progress — deterred by remote guard](#)

Source: [Backstreet Surveillance field footage](#) · [Evolon \(vendor-published\)](#)

NOT A CASE STUDY — THIS IS OURS

Subjects on site to take cable. Analytics detected them, an operator verified in seconds, and a live voice ended it before anything left the yard. Twice in the first sixty days after deployment.

No arrest. No damage. No outage. No truck roll.

WHAT THAT LOOKS LIKE AT SCALE

9 / 10 deterrence success

< 3 sec verified response time

Evolon, vendor-published

Design changes behavior before technology does

Natural surveillance

People can see into and through the space. Offenders behave differently when they can be seen — even by strangers, even when nobody is looking back.

Natural access control

Paths, doors, and barriers steer people where they are supposed to go, so being somewhere else becomes a visible decision.

Territorial reinforcement

It is unmistakably obvious where public space ends and controlled space begins. Ambiguity is an invitation.

Maintenance and image

A cared-for property signals that somebody is in control. Neglect signals the opposite, and it compounds.

- Oscar Newman's defensible space research showed that when users can see and "own" shared space, crime and disorder drop — because offenders feel visible and challengeable.
- A visible mast, active lighting, clear signage, and a human voice do all four of these at once. That is CPTED delivered on a trailer hitch.

Source: [CPTED](#) · [Newman, Defensible Space](#)

PART THREE

Mobile surveillance, practically

Defense in depth for places you cannot trench, permit, or staff.

Mobile Surveillance as a Service

- Traditional fixed systems take months of design, permitting, trenching, and construction before a single camera goes live. The risk does not wait for the schedule.
- MSaaS deploys self-contained units, trailers, solar towers, building-mounted pods, that already integrate cameras, analytics, lighting, speakers, communications, and monitoring.
- Pre-engineered and remotely managed. Set up in minutes, left as long as needed, then moved as risk moves — or converted to a permanent installation.
- You should not have to wait on power, network, and permitting to get meaningful protection in place.

WHERE IT EARNS ITS KEEP

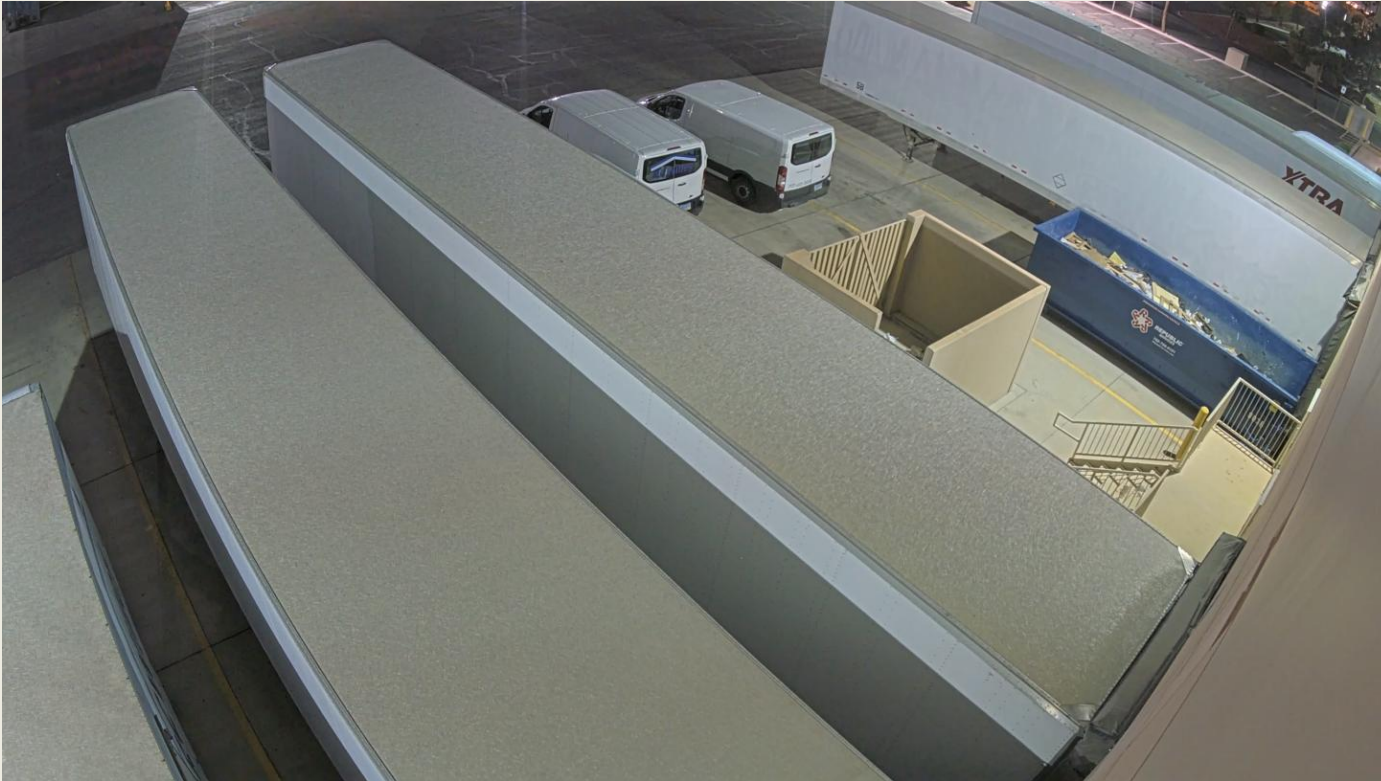
- Substations and switching yards outside CIP-014 scope
- Solar farms and wind sites under construction
- Laydown yards, staging areas, and material storage
- Storm restoration and mutual aid staging
- Transmission corridors and remote access roads
- Outage and turnaround work with temporary crews
- Fire watch in high-hazard areas
- Anywhere a threat assessment moved and the cameras did not

Rapid deployment: risk moves, so should you



- Dropped, mast extended, and recording in under ten minutes.
- Solar frame, audio, and advanced analytics configured remotely — from anywhere.
- No trenching. No permits. No conduit. No panel upgrade.
- When the threat assessment changes, the asset relocates the same afternoon. A trenched camera cannot do that at any price.
- Fleet model: a handful of units covering a rotating risk map beats a fixed camera at a site that stopped being the problem two years ago.

Deep learning analytics: software watches every frame



- Classification, not motion: person, vehicle, bicycle — plus loitering, crowding, intrusion, and direction of travel.
- Legacy motion detection triggers on rain, headlights, spiders, tumbleweed, and a flag. Deep learning asks a different question: is that a person?
- This is the answer to the false alarm tax. Fewer, better alerts is what makes a human operator possible at all.
- Advanced models extend to PPE and hard-hat compliance, animal discrimination, and operational thresholds — safety and productivity data from a security asset.

Instead of hoping somebody happens to be looking in the right direction at the right moment, software is looking at every frame of every camera, all night, without getting bored.

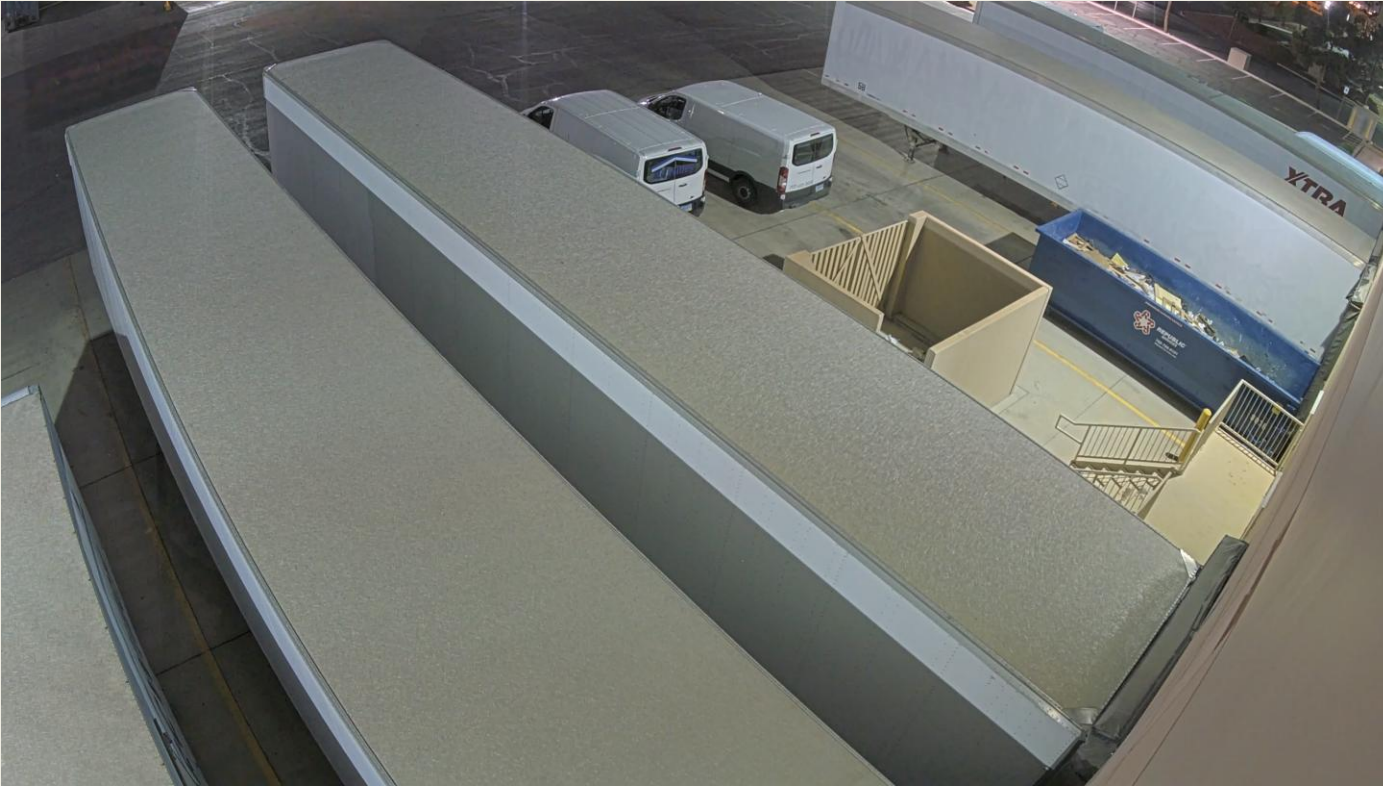
The live talk-down: the site stops being passive



- A recorded speaker says they are noticed. A human voice describing what you are wearing says a person is watching you right now.
- In one 2025 benchmark across 18,258 U.S. locations and 1.6 million monitoring events, 62.4% of high-priority security events were resolved without any police dispatch when interactive remote video monitoring was used.
- In an AI perimeter sub-analysis of 23,810 activations, 96.1% were resolved by a staged voice-down protocol and only one resulted in a police dispatch.
- This is where Deter and Delay stop being separate D's. The challenge is the delay.

Source: [Interface Systems 2026 Retail Loss Prevention Benchmark \(vendor-published, n = 1.6M events\)](#)

When talk-down is not enough: verified dispatch



- The ladder: analytic detection → operator verification → staged voice-down → outbound call to site contact → law enforcement dispatch with live description.
- The operator is not reporting an alarm. The operator is reporting a crime in progress, with clothing, direction of travel, and vehicle description — while watching it.
- That is the difference between joining the 97% false-alarm queue and getting a unit rolling.
- Dispatch is the last rung, not the first. Most events never reach it — which is precisely what preserves your relationship with the responding agency.

Specify the outcome, not the megapixels

DORI is being replaced. IEC/EN 62676-4:2025 expands four operational levels into seven — and raises the ceiling substantially.

LEVEL	THRESHOLD	WHAT IT ACTUALLY SUPPORTS	LEGACY DORI
Overview	20 px/m	Detect movement	Legacy: Detect ≈ 25 px/m
Outline	40 px/m	Outline and direction of travel	
Discern	80 px/m	Distinguish person, vehicle, animal	Legacy: Observe ≈ 63 px/m
Perceive	125 px/m	Perceive movement and activity	Legacy: Recognize ≈ 125 px/m
Characterize	250 px/m	Person type, gait, behavior; vehicle type	Legacy: Identify ≈ 250 px/m
Validate	500 px/m	Verify a known person; read a plate	No legacy equivalent
Scrutinize	1,500 px/m	Establish identity with high certainty	No legacy equivalent

Pixel density is measured at the target, not somewhere in the scene. More megapixels spread across a wider field of view does not buy you a single pixel where it matters.

Source: [Axis Communications, Pixel density based on IEC 62676-4:2025](#) · [JVSG](#)

Why 18 feet beats 33 feet

- Height expands the ground footprint in the image. Same resolution, more area — fewer pixels on the target where the incident actually happens.
- Height steepens the viewing angle. You get tops of heads and vehicle roofs instead of faces and plates. Facial analytics generally want tilt under 15° and horizontal deflection under 30°.
- A taller mast is a longer lever arm in wind. Small motion at the mast becomes large displacement in a telephoto scene — and stabilization crops the image to compensate.
- PTZ still needs a usable overview to detect and verify before it zooms. Zoom should enhance a good base image, not rescue a bad one.
- 18 feet clears most vehicles and clutter while keeping human-scale geometry in the working zone around the trailer.

THE TRAP

A 33-foot mast creates an impressive command view in a demo.

It also spreads finite resolution over more acreage, steepens every angle, and shakes more in wind.

The question is never how much you can see. The question is what visual task the image supports at the point where the incident occurs.

Source: [Axis Communications, Pixel Density and DORI](#) · [NtechLab camera requirements](#) · [SCW mounting height](#)

Power is where mobile systems actually fail

- Solar sizing is a winter problem, not a summer problem. Design for the worst consecutive sunless stretch at your latitude — not the annual average.
- Ten-plus days of autonomy is the practical target. A system that dies on day four of a storm is not a security system; it is a liability with a mast on it.
- Recovery matters as much as capacity: after a full drain, the system should resume operation within hours of returning sun, not days.
- Remote power management is non-negotiable — charge performance, load, state of charge, and operational status, visible before somebody drives four hours to find out.
- Shore power for 110V charging when it exists. Design as if it never will.



Ask every vendor one question: what happens on day nine of an inversion, and how would I know before I drove out there?

It has to work on the worst night of the year



- Sustained hurricane winds. 80,000 customers without power. The camera stayed up, stayed online, and kept a usable image.
- A wiper is not a luxury on a storm asset — a water-sheeted dome is a blind camera, and blind is the same as absent.
- Storm performance is exactly when situational awareness is worth the most and available the least: crews deployed, roads closed, and every fixed asset on the site is dark.

Communications: assume nothing is there

CELLULAR

Multi-carrier is the requirement, not a feature. A unit that scans AT&T, Verizon, and T-Mobile at startup and locks the strongest signal will deploy in places a single-carrier unit will not.

SATELLITE

Satellite closes the gap for genuinely remote sites — transmission corridors, backcountry substations, and anywhere the carrier map is optimistic fiction.

WI-FI / PRIVATE

Long-range Wi-Fi or a private network where you already own the infrastructure. Cheapest bandwidth you will ever get, and it stays on your network.

- Design the video architecture around the worst link you will actually have, not the best one you tested in the yard. Shallow-bandwidth, edge-recorded, cloud-managed beats a beautiful high-bitrate stream that dies at the site that needed it.
- Serverless and edge-recorded: full-resolution video stored on the unit, low-bandwidth review and alerting over the link, no on-site server to power, cool, patch, or replace.
- Health monitoring on the link itself. You need to learn a camera is down from an automated alert, not from an investigator asking for footage you do not have.

PART FOUR

Own it. Open it. Don't be a hostage.

How you buy determines what you can do with it for the next ten years.

Own rather than lease

LEASE / MONITORING-AS-A-SERVICE

- Payment never ends, and neither does the escalator
- Access to your own footage is a subscription line item
- Provider chooses the hardware, the VMS, and the roadmap
- Configuration and integration limited to what the plan allows
- Leaving means losing the asset, the archive, and the workflow

OWN

- Capital cost is finite and depreciable; it ends
- The footage is yours, on your terms, forever
- You choose the cameras, analytics, and the VMS
- Redeploy, reconfigure, and integrate without permission
- The asset holds residual value and can be converted to fixed

Run the arithmetic over 36 months on any lease you are considering, then compare it to purchase plus data plus optional monitoring.

Third-party market reporting puts mobile surveillance trailer rental at roughly \$800–\$3,500 per month, with purchase in the \$15,000–\$75,000 range depending on configuration. Rent-to-own structures exist that convert payments into ownership.

Source: [TrueLook cost guide](#) · [Complete Security Rental](#)

Open platform, or hostage as a service

- Open standards — ONVIF and equivalents — let cameras, recorders, and video management from different manufacturers work together. The standards body itself frames this explicitly as avoiding vendor lock-in.
- Best of breed beats best of catalog. Thermal here, radar there, LPR at the gate, the analytics engine that actually performs on your scene — chosen on merit, not on who owns the platform.
- Augmentation over replacement: an open platform absorbs the access control, the SCADA alarm, the gunshot detector, and the drone feed you buy in three years. A closed one makes each of those a change order or a rip-out.
- The real cost of proprietary is not the license. It is that every future decision gets made by someone whose interests are not identical to yours.
- Ask one question of every platform: if I fire you, what do I keep? The camera, the recording, the archive, the configuration, the integrations. Get the answer in writing before you sign.

In July 2026 ONVIF released a draft Profile V specifically to enable cloud video architectures without vendor lock-in — the standards community is moving in this direction because the market demanded it.

Source: [ONVIF, Profile V draft release \(July 2026\)](#)

NDAA Section 889 — know what is in your yard

- Section 889 of the FY2019 NDAA prohibits federal agencies and federal grant recipients from procuring video surveillance and telecom equipment from Huawei, ZTE, Hytera, Hikvision, and Dahua — plus subsidiaries and affiliates.
- It reaches further than most buyers assume: contractors, grantees, and loan recipients using covered equipment as a substantial or essential component of a system tied to federal work can be in scope. Federal infrastructure loans and grants pull a lot of utilities into that net.
- All five manufacturers have been on the FCC Covered List since March 2021. New FCC equipment authorizations for Covered List gear were blocked effective February 2023, and in 2026 the FCC moved to close the remaining pathway for previously authorized legacy equipment.
- Installed equipment is not required to come out — there is no kill switch. The exposure is different: a shrinking supply of legal replacement parts for a system you still depend on.
- OEM relabeling is common. The name on the housing is frequently not the name on the board. Demand documented chain of manufacture, not a sales assurance.

This is a fast-moving regulatory area. Verify current status against the FCC Covered List before making a procurement decision on it.

Source: [U.S. EAC, What is Section 889](#) · [FCC Covered List](#) · [IPVM, Where Dahua and Hikvision Are Banned](#)

Ten questions to ask before you buy anything

- | | | | |
|----|--|----|--|
| 01 | What visual task must this image support, at what distance, in what light? | 06 | What is the autonomy on the worst consecutive sunless stretch here? |
| 02 | How many pixels land on the target — not the scene — at that point? | 07 | How will I know it is down before I need the footage? |
| 03 | Who or what is watching this alert, and what are they empowered to do? | 08 | If I fire this vendor, what do I keep? |
| 04 | How long from detection to a human being on the event? | 09 | Can I add a camera, an analytic, or a sensor they do not sell? |
| 05 | Can it talk? And is there a documented escalation ladder before dispatch? | 10 | Show me the incident report. Not the brochure — a real one, with timestamps. |

If a vendor cannot answer number ten, nothing above it is real.

Beyond the Demo: The Ground Truth

- A podcast about what actually works in commercial security and surveillance — deployments that succeeded, deployments that failed, and the lessons in between.
- Industry veterans, installers, consultants, manufacturers, and working practitioners. No spec sheets, no marketing, no pretending the demo is the deployment.
- Recent episodes: Why AI Fails in the Real World · The Future of PTZ Cameras · Flock Cameras and the Surveillance State Debate · Thermal and Radar Tech · Deploying the Ultimate Security Trailer.

New episodes weekly on YouTube and Spotify.

Watch and subscribe: backstreet-surveillance.com/podcast



ASIS International — Utah Chapter

Join the chapter

The Salt Lake City chapter covers the entire state. Monthly meetings, site tours, and the single best professional network in Utah security. Membership is the cheapest professional development available to anyone in this room.

Upcoming PSP course

Chapter-run Physical Security Professional certification prep. If you design, assess, or specify physical security, PSP is the credential that maps directly to the work — and passing it is dramatically easier with a cohort.

State Capitol tour

A chapter tour of the Utah State Capitol with State Security Chief Matt Pennington — a rare walk-through of how a live, public, high-profile government facility is actually protected.

Chapter site, events, and membership: ASISSLC.org

Come find me during the break — I will personally walk you through membership, the certification path, and which credential is actually worth your time for the job you have.

THANK YOU

You should not have to wait on
power, network, and permitting to
get meaningful protection.

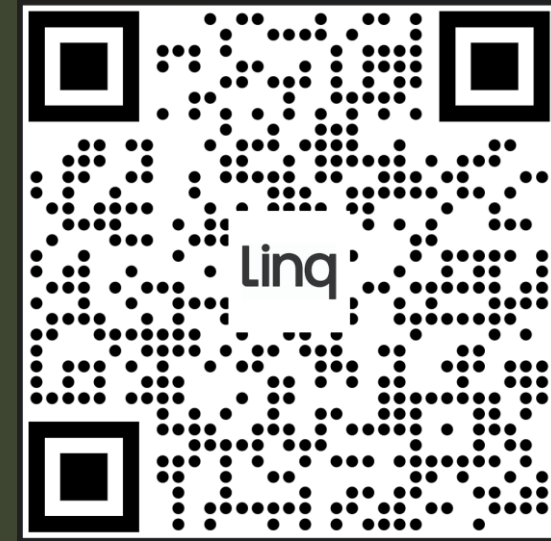
Rob Oldham, CPP, PSP, PCI, CPTED, MBA

Vice President & Co-Owner, Backstreet Surveillance

President, ASIS International — Utah Chapter

Host, Beyond the Demo: The Ground Truth

backstreet-surveillance.com · ASISSLC.org · [LinkedIn](#)



Questions

Ask me the hard ones.

Grid Security Solutions

Over 100 years of addressing critical operational threats to grid resiliency



CHALLENGES



SOLUTIONS TOUR



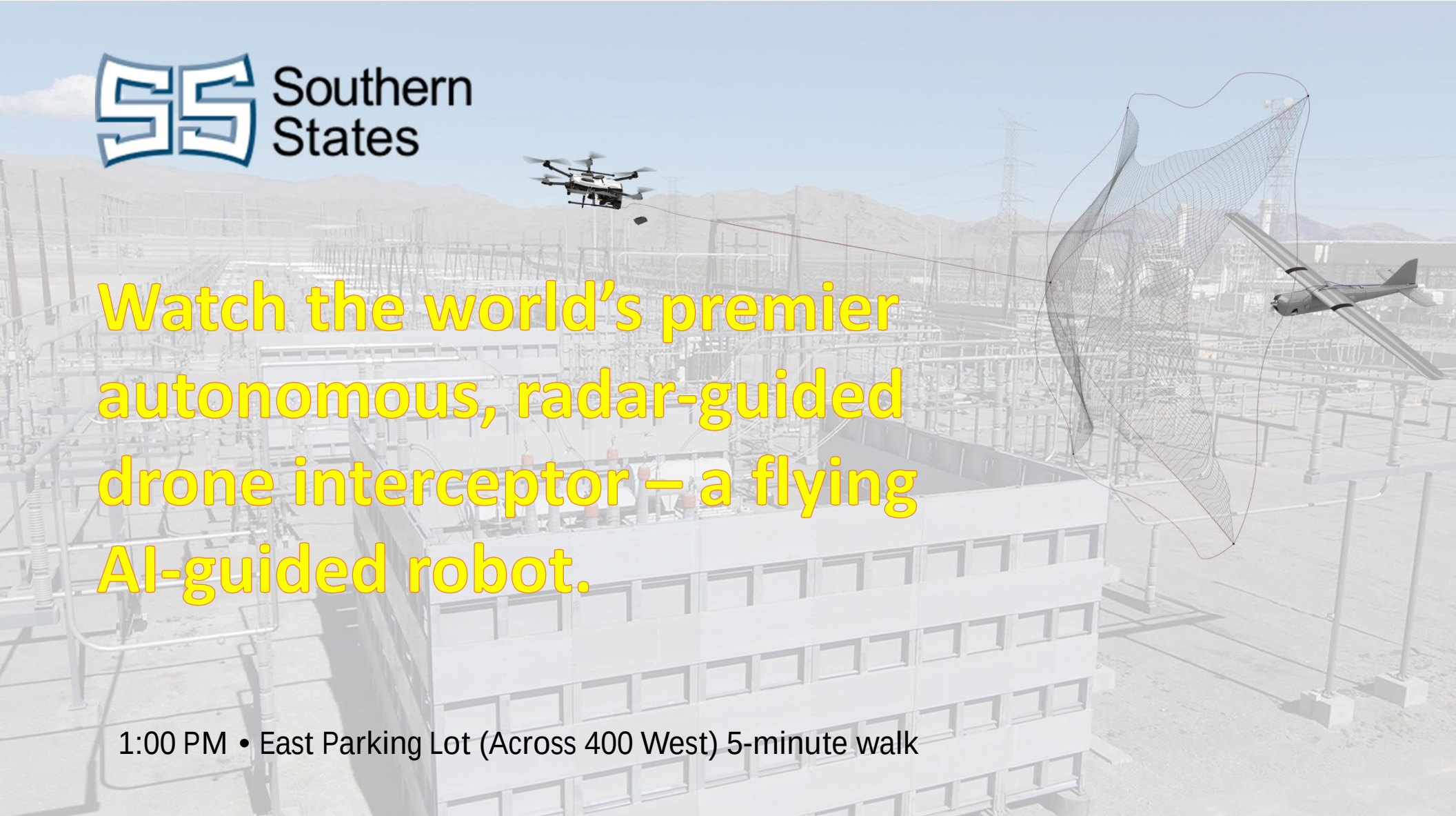
OUR ADVANTAGES

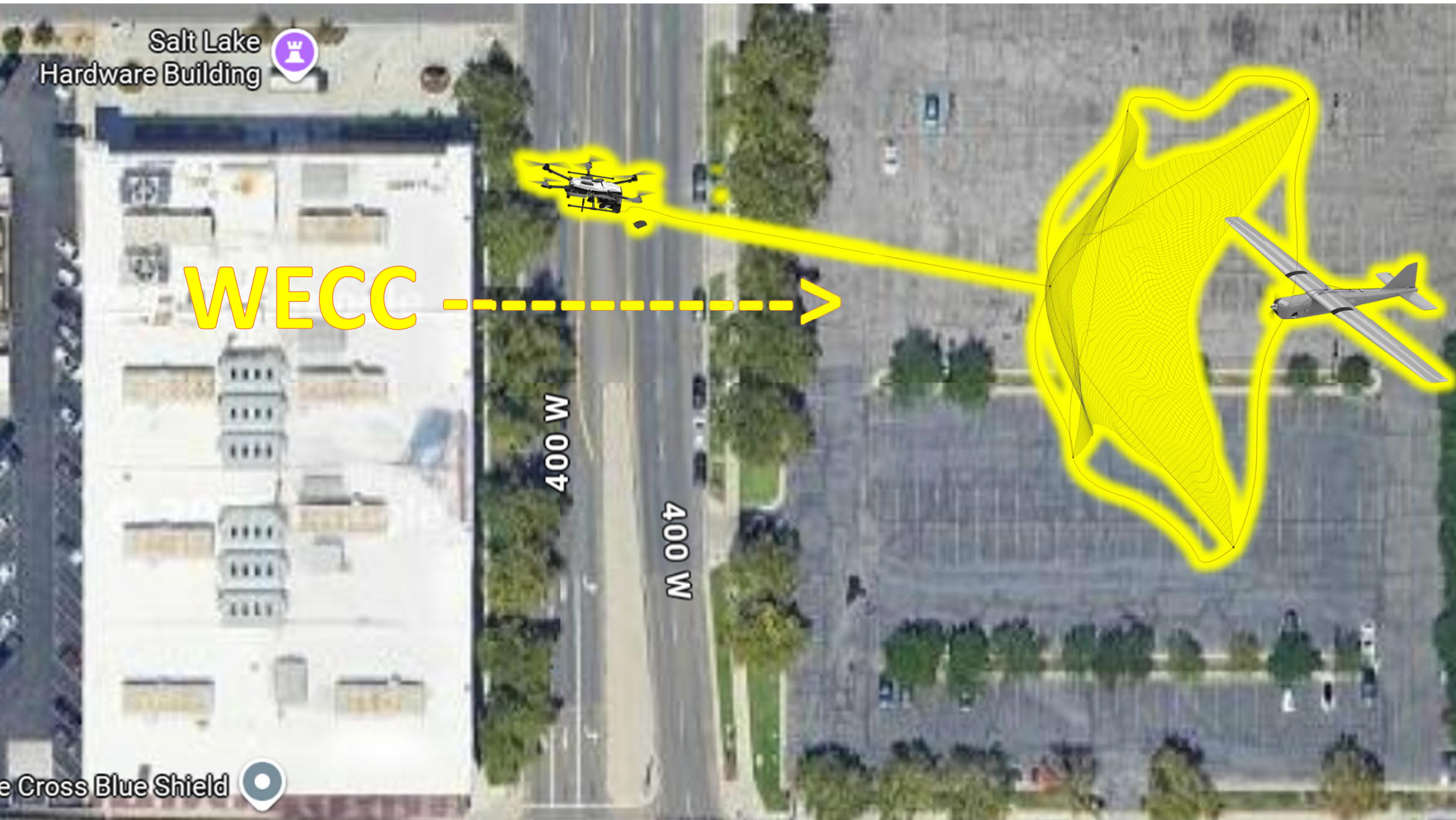
SELECT YOUR FOCUS AREA



Watch the world's premier autonomous, radar-guided drone interceptor – a flying AI-guided robot.

1:00 PM • East Parking Lot (Across 400 West) 5-minute walk





<Public>



<Public>



Questions?

Southern States LLC
In Partnership with Fortem Technologies

AIRSPACE SECURITY LIVE DEMONSTRATION & FACILITY TOUR

Securing Infrastructure Airspace: From Risk To Resilience

Thursday, Oct 15, 2026
8:00 AM – 2:00 PM (Mountain Time)
Fortem Technologies HQ | Lindon, Utah



Thank you for your interest in attending this exclusive Counter-UAS demonstration hosted by **Southern States LLC** in partnership with **Fortem Technologies**. We look forward to an informative and impactful day of live demonstrations, technical discussion, and collaboration focused on securing the airspace above our nation's critical infrastructure.

EVENT DETAILS

Date	Thursday, October 15, 2026
Time	8:00 AM – 2:00 PM (Mountain Time)
Location	Fortem Technologies Headquarters 1855 W 500 N, Lindon, Utah 84042
Host	Southern States LLC In partnership with Fortem Technologies

AGENDA OVERVIEW

8:00 AM	Guest arrival and check-in at Fortem HQ
8:45 AM	Transport to F4 facility with Fortem history briefing en route
9:30 AM	Live Demonstration and Q&A;
11:15 AM	Return to HQ
11:30 AM	Catered lunch and technical discussion panel
1:30 PM	Facility and office tour
2:00 PM	Adjourn

WHAT YOU WILL SEE

- TrueView® Radar — 360° persistent 3D drone detection at 6+ mile range
- SkyDome® Manager — Real-time airspace command & control software
- DroneHunter® — Live autonomous kinetic intercept demonstration
- DroneHangar™ — Autonomous 24/7 launch and recovery system
- VisionFlex™ — Radar-cued long range OE/IR camera

TRAVEL & ACCOMMODATIONS

Please fly into **Salt Lake City International Airport (SLC)**. Southern States is pleased to provide complimentary local transportation upon request.

Recommended Hotels:

- **Hilton Garden Inn Lehi**
3150 N Hotel Loop, Lehi, UT 84043
- **Hyatt House Pleasant Grove** (Ask for the Fortem Technologies Rate)
544 S Pleasant Grove Blvd, Pleasant Grove, UT 84062

QUESTIONS & CONTACT

Questions? Contact Patrick James
Director, Grid Security Solutions
Southern States LLC
Text or Call: 678-570-8937

WHY ATTEND THIS DEMONSTRATION

- Witness the only DHS-authorized non-lethal kinetic counter-drone solution
- See live autonomous intercept technology currently protecting U.S. Army installations worldwide
- Evaluate the system that protected all 11 U.S. 2026 FIFA World Cup venues
- Understand how Lockheed Martin's investment validates this technology and is doubling production capacity
- Engage directly with Fortem Technologies engineering and Southern States security specialists
- Learn why Fortem Technologies was selected as Prime Contractor on a 5-Yr DHS Counter-Drone IDIQ worth more than \$1B

RSVP HERE

Southern States LLC | Grid Security Solutions | southernstatesllc.com | 678-570-8937

In Partnership with Fortem Technologies • Securing Infrastructure Airspace: From Risk To Resilience
This event is by invitation only. All attendees are subject to Fortem Technologies facility access requirements.



Thank You

To Those Who Attended The Live Demo

Any Demo Q & A?

Airspace Security-Physical Security Above the Fence Line

Substation Operational Security

Ultimate Physical Security | Unmatched Innovative Technology



BALLISTIC PROTECTION



ASSET MONITORING

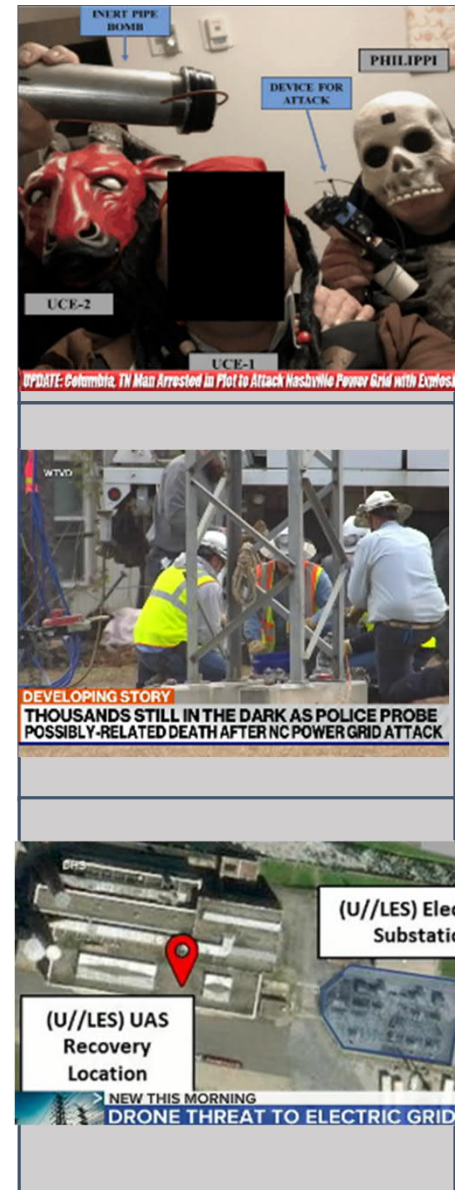


AIRSPACE MITIGATION



Problem: Lack of Airspace Security

- Grid #1 Terrorist Target in USA, according to Congress
- **“We know that terrorist organizations have an interest in using drones... the expectation is that it is coming here—imminently.”** FBI Director 2022
- Near peer competitors to USA
- Vulnerability– “9/11 times 100”
Our infrastructure in the continuous 48 states is unprotected.



Solution: Which Airspace Protection?

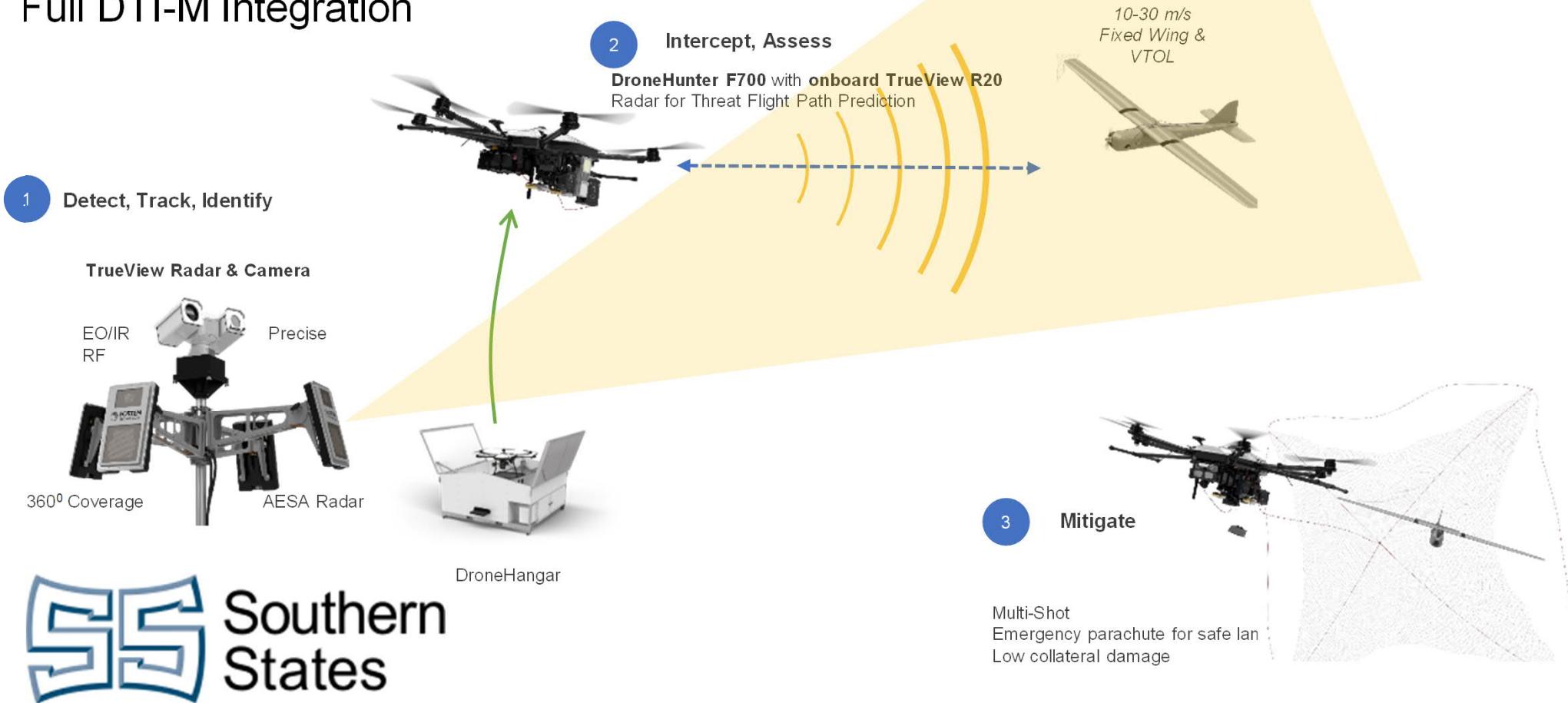
- Fortem Technologies
- Sentrycs
- D-Fend/Motorola
- Axon/Dedrone
- SkySafe

FBI & DHS recommends layered mitigation. Try jamming / takeover first, then DroneHunter second. That is flawed but the status.



Solution: Complete Airspace Protection

Full DTI-M Integration



Example: Airspace Security Deployment

FIFA World Cup

Qatar, November 21-December 18, 2022; USA 2026



Why Now?

Differentiation between those Utilities who prepare and those who do not

- Real Threat
- Currently Happening Across the USA
- Devastating Impact
- Large Opportunity Cost
- Changing Federal Regulations expanding mitigation authorities



Did You Read Our White Paper?

WHITE PAPER

Current Approaches and Regulations in the
United States to:

Protect Energy Production and Grid Infrastructure from today's Drone Threats

**Current Mitigation Options and Approaches,
Operational Model,
and a Call to Action**



PREPARED FOR: North American Transmission Forum (NATF)

AUTHOR: Southern States, LLC DATE: April 2026

<https://www.southernstatesllc.com/products/grid-security-products/airspace-security>



[Products](#) [Markets](#) [Services](#) [About](#) [Resources](#) [Contact](#)

GRID SECURITY

Airspace Security



Request a Quote



<https://www.southernstatesllc.com/products/grid-security-products/airspace-security>



[Products](#) [Markets](#) [Services](#) [About](#) [Resources](#) [Contact](#)

[Schedule Airspace Risk Assessment](#)

Product Literature

Additional Resources



Protect Energy Production and Grid Infrastructure from today's Drone Threats

[Download](#)

Sec 4.0 – 6.0 Executive Briefing

- What Can Utilities Do Today (FAA Sec 2209)
- Layered Detection, Tracking & Identification (DTI) Architecture
- Interceptor Drone Mitigation Systems & Regulatory Considerations



Sec 4.0 – What Can Utilities Do Today (FAA Sec 2209)

- Utilities cannot legally jam, spoof, capture, or destroy drones; mitigation is reserved for authorized federal agencies and trained SLTT law enforcement.
- FAA Section 2209 provides a path for utilities to request protected no-fly airspace around qualifying critical infrastructure.
- A three-phase strategy works today: secure protected airspace, deploy detection, and coordinate mitigation with law enforcement.
- Three options exist today: A) DTI + DroneHunter alerting SLTT/federal partners, B) federal pilot program, or C) interceptor in “pursuit and observation” mode only.

Sec 5.0 – Layered Detection, Tracking & Identification (DTI) Architecture

- Radar is the foundational sensor — the only reliable way to detect autonomous, RF-silent "dark" drones at range, in all weather, day or night
- EO/IR cameras add visual confirmation and threat classification, but need radar to cue their narrow field of view onto fast-moving targets
- RF detection and Remote ID identify cooperative/compliant drones, enabling whitelisting and reducing false alarms
- True protection comes from integrating all three sensor types into one fused, distributed command-and-control picture — no single sensor is sufficient alone

Sec 6.0 – Interceptor Drone Mitigation Systems & Regulatory Considerations

- Interceptor drones (like the Fortem DroneHunter) must be on the DHS/DOJ approved counter-UAS list — approval takes multiple years and involves FAA, FCC, NTIA, and FBI coordination
- Systems physically net-capture hostile drones and return them for forensic analysis, rather than jamming or destroying them
- Operations can run locally at a site or remotely from a security operations center, always coordinated with trained law enforcement
- Platforms are being engineered now for FAA Part 108 compliance — Remote ID, anti-collision lighting, geofencing, encrypted C2 links, and detect-and-avoid

Safer Skies Act – December 2025

- Expanded Mitigation Authority

State, Local, Tribal & Territorial (SLTT) agencies can disable, disrupt, or seize drones posing threats to utility assets — once trained and certified by DOJ on approved equipment

- Supports CUAS Investment Justification

Federal standards will help utilities validate technology choices and budget requests.

Implications for Utilities

- Utilities will need formal processes with local law enforcement for site protection

But more is coming.....





Politics

Sen. Tom Cotton pushes bill to allow drones to be stopped by critical infrastructure operators

By Nicole Sganga

April 23, 2026 / 10:01 AM EDT / CBS News

Add CBS News on Google

Washington — Sen. Tom Cotton is pushing new legislation to grant operators of the nation's most sensitive infrastructure the authority to defend against and stop potentially hostile drones in real time, arguing that current law leaves our power grid and wastewater plants, along with other high-risk sites exposed to emerging aerial threats.

Critical Infrastructure Airspace Defense Act 2027

- Mitigation authority to critical infrastructure owners and operators
 - Bulk power substations
 - Transformer stations
 - Nuclear generating facilities
 - Grid control centers
 - Water and wastewater facilities
 - Certain contracted security providers
- Major shift because today utilities have very limited direct mitigation authority.
- Broad bipartisan support. It is expected to pass in 2027, the delay giving room for learnings from the Safer Skies Act.



Aug 4, 2026 6:00 AM Eastern Daylight Time

Fortem Technologies Selected as Prime Contractor on 5-Year DHS Counter-Drone IDIQ Worth More Than \$1B

Share      ...

Every DHS component can now issue task orders directly to Fortem, the only small business among the seven companies selected for the contract's Track 1

LONDON, Utah--(BUSINESS WIRE)--Fortem Technologies, the global leader in airspace security and counter-drone solutions, today announced it has been selected as a prime contractor on the Department of Homeland Security's Counter-Unmanned Aircraft Systems (C-UAS) indefinite-delivery/indefinite-quantity (IDIQ) contract, a five-year, multiple-award vehicle for counter-drone technology and services.

Fortem Technologies

Leader in Airspace Security and Defense for detecting and defeating dangerous drones.



Security: Fortem has SECRET Facility Clearance under NISP, SECRET data retention, COMSEC eligible, multiple SECRET cleared staff through TS-SCI



Investors / Partners



Strategic Collaboration



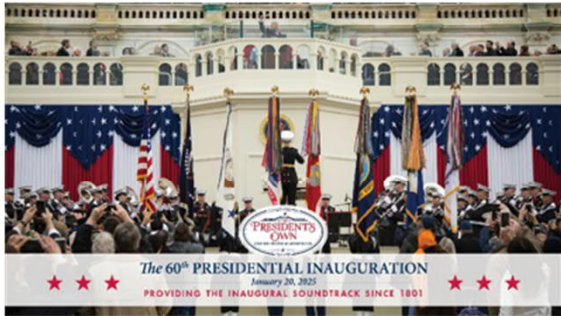
Customers Worldwide



US Border Patrol – Operational Captures on Mexico Border

DEPARTMENT HOMELAND SECURITY (DHS)

- Sept. 2022: DHS Funded CUAS Testing of SkyDome / DroneHunter via Sandia National Laboratory
- Oct. 2024: Working with DHS and Custom's Border Patrol Fortem achieves Operational Success in Rio Grand Valley capturing UAS entering U.S. via the US Mexico Border
- Jan. 2025: Approval gained for use in the National Capital Region (NCR) in support of Presidential Inauguration and Parade.

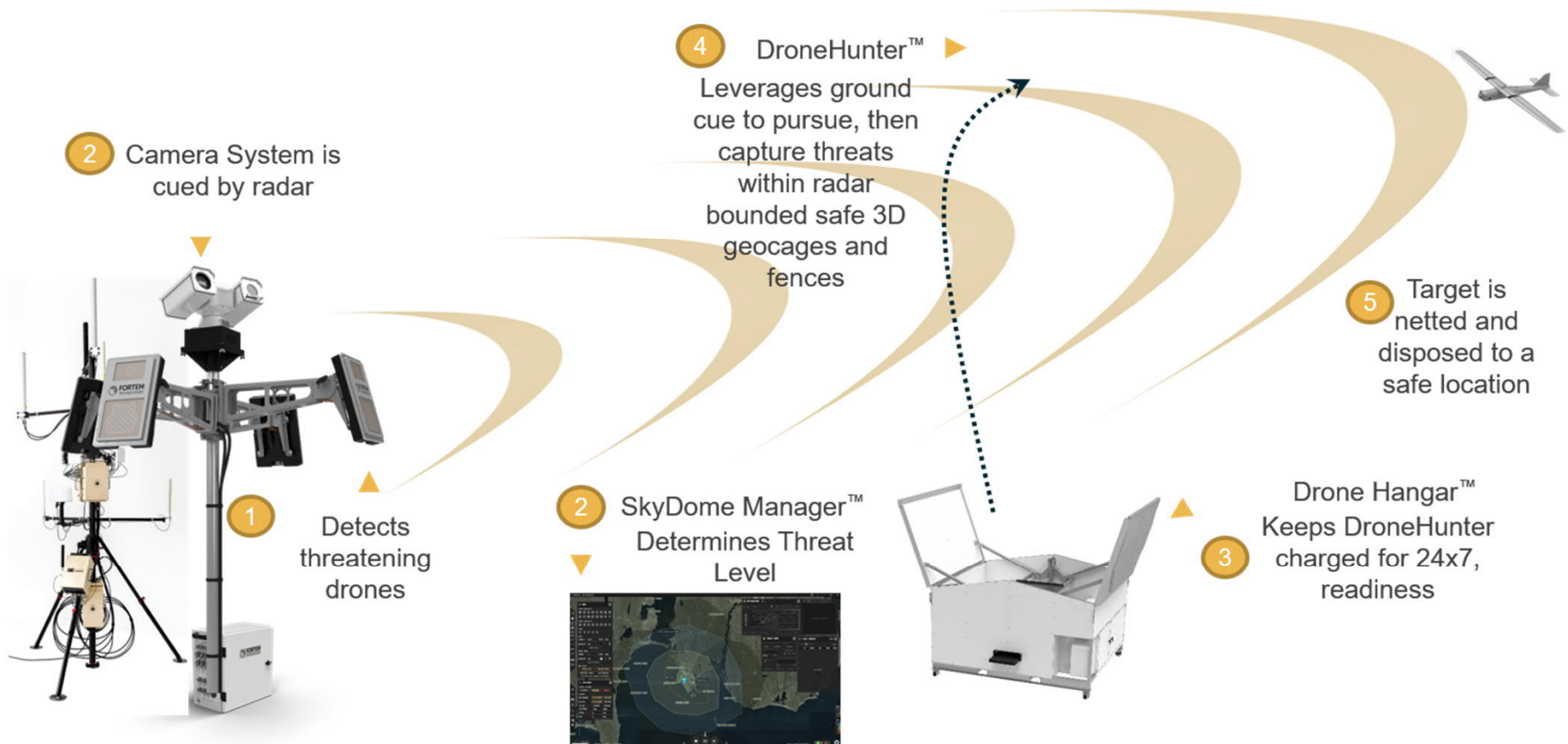


US Border Patrol Agents
Rio Grande Valley
Captured UAS entering the
U.S. via the US/Mexico Border

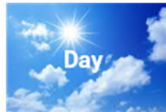
DroneHunter: Only CUAS Kinetic Effector
Approved for use in CONUS



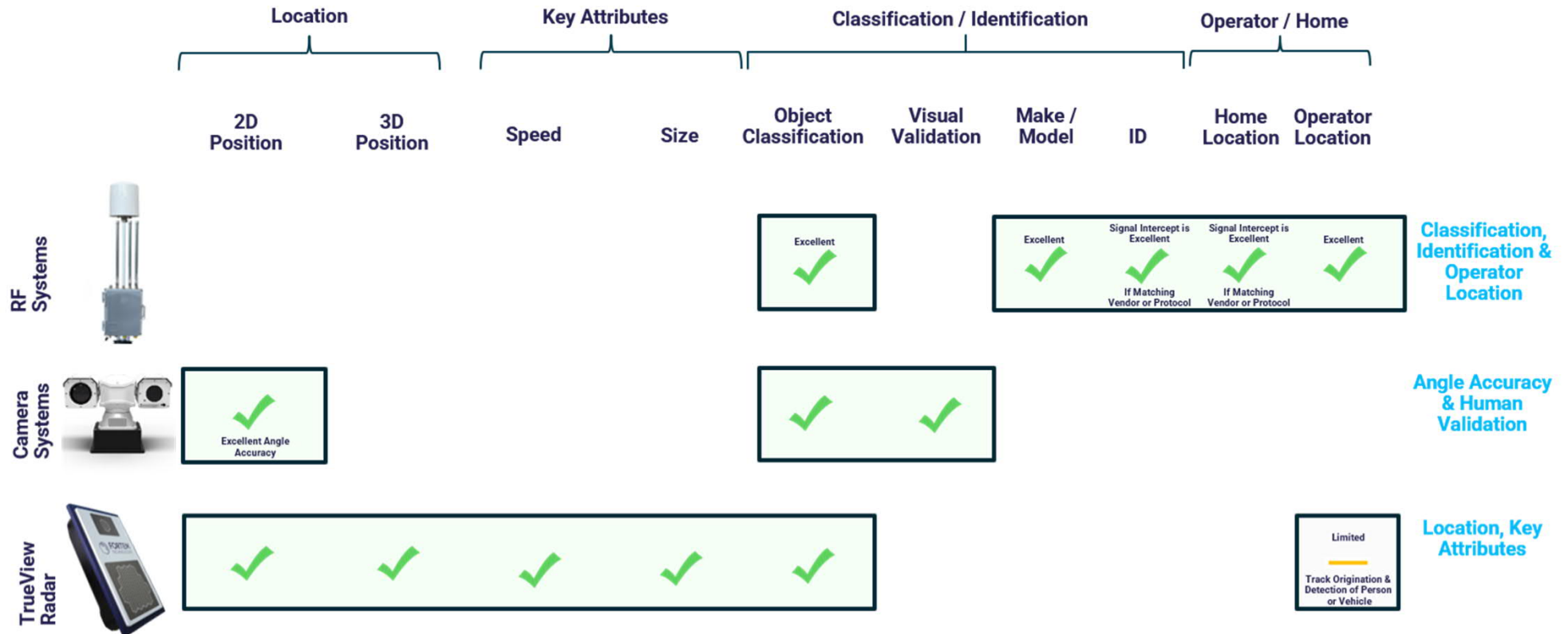
Fortem Low-Collateral Counter UAS System



Radar – Foundation for Complete Detection

Environmental Conditions				RF Use						
										
Camera Systems 	✓	✓ \$\$\$	✗	✗	✓	✓	✓	✓	✓	Poor 360 Detector, Limited Env. Conditions
RF Systems 	✓	✓	✓	✓	✗ Antenna & Library Don't Match	✓ Antenna & Library Match	✗ Antenna & Library Don't Match	✗	✗	Gaps in Universal RF Coverage, RF Dark Risk
TrueView Radar 	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Camera & RF System as Supplemental to Radar



<Public>

Layered Detection (Radar + RF + Camera)



RF Detection-Only is NOT Security

Entry Level Solutions

- Only ISM Bands 2.4 and 5.8 GHz

Professional Solutions

- Primary ISM Bands 433 MHz to 5.8 GHz
- Requires multiple antennas – Ask which you get for the price, still limited by library.

Dual Purpose Spectrum Analyzers

- Varies, but can cover from <300 MHz to 40GHz
- Challenge lies in discerning drones from other devices as they are less specialized

5G – All Drone Vendors are “Working on it”

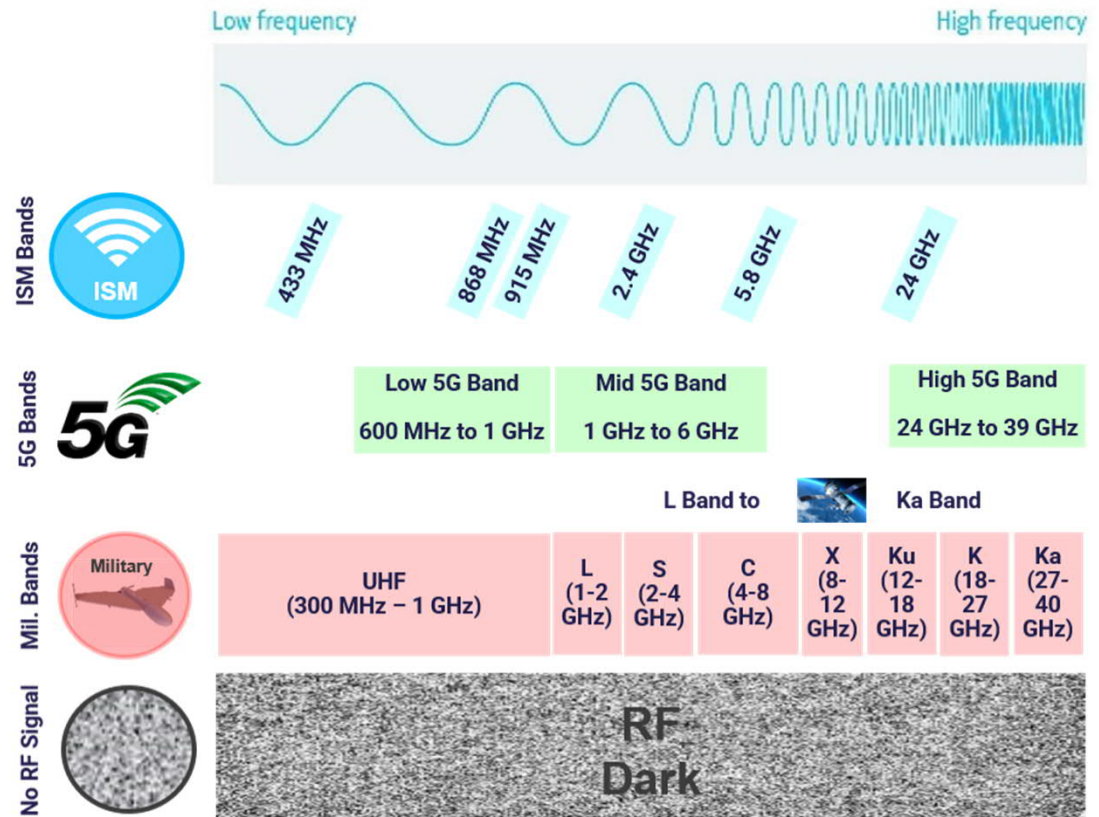
- Drone vs phone?
- Lose all operator location details

Near Peer Threats Communicate w/ Drones from UHF to Ka

- Use both ISM bands & Reserved Military Bands
- Deploy detection mitigation technologies
- Often directly communicating with satellites

RF-Dark Drones

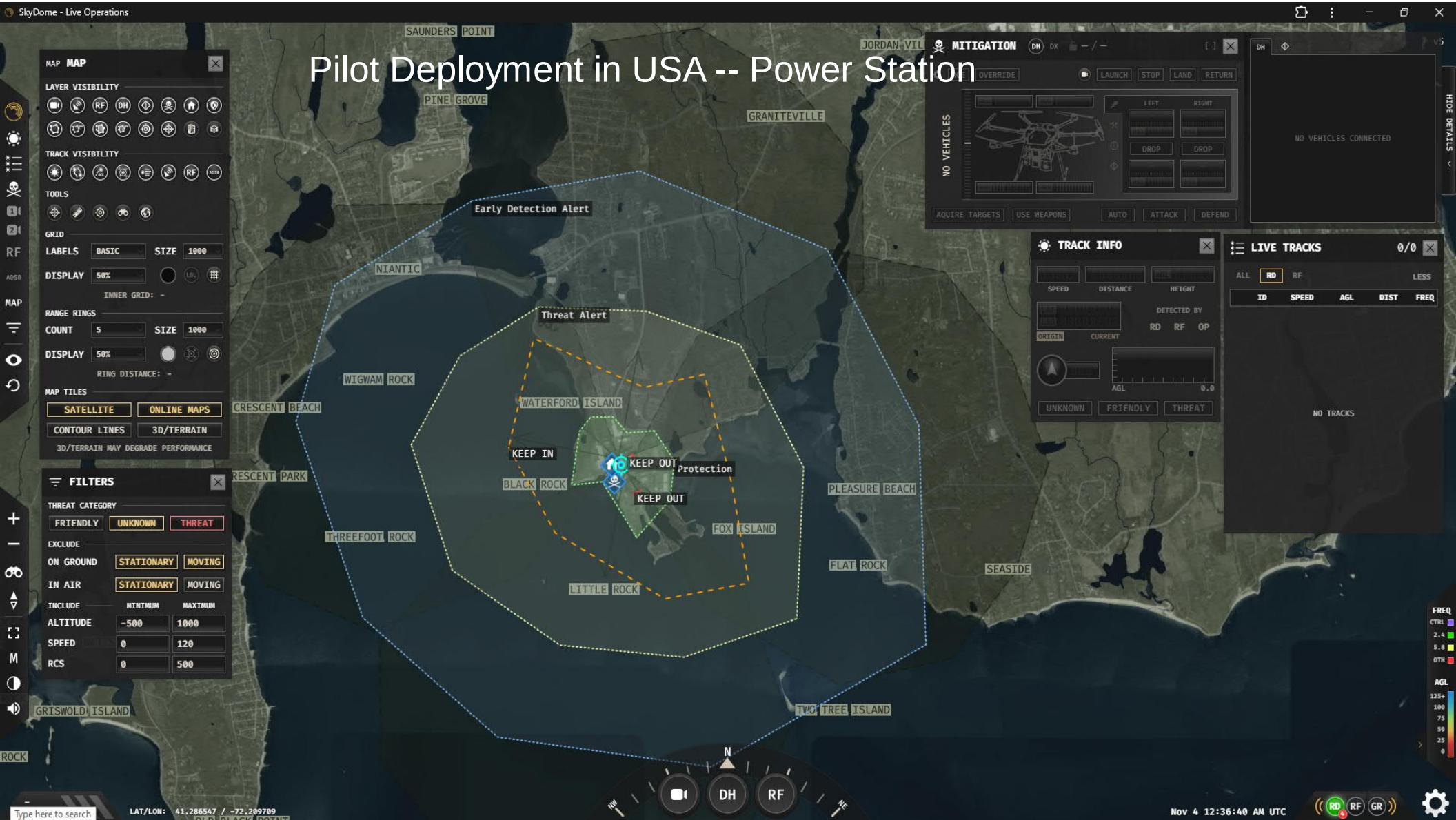
- Use Waypoint or Fly-by-wire Methods
- May or may not use GPS/GNSS
- Used by military, terrorists, criminals and hobbyists



<Public>



<Public>





DroneHunter® F700 Video



DroneHangar™ ▼



Weather-proof hangar allowing for 24/7 readiness.

Summary

- **Why Layered Detection:** Radar, Camera, and RF systems together ensure full drone detection while reducing false alarms and providing evidence needed to prosecute the operator.
- **Why Low-collateral DroneHunter Mitigation:** A low-collateral **Drone Interceptor** provides the safest, most effective defeat of both RF-emitting and RF-dark drones in any environment near civilians.
- **Why Fortem is Trusted:** Fortem is a trusted and proven CUAS provider with deep partnerships and investments with global Defense contractors (Boeing, Lockheed Martin, Toshiba, Hanwha, etc.). We have captured thousands of drones. We have been selected and deployed to protect VIPs at International Events (Presidential Inauguration, World Economic Forum, multiple G7 summits, Olympics, and FIFA World Cup). We have been deployed to protect critical infrastructure (Nuclear plants, power plants, etc.) as well as US, NATO and NATO friendly bases around the world.



<Public>



Questions?

Southern States LLC
In Partnership with Fortem Technologies

AIRSPACE SECURITY LIVE DEMONSTRATION & FACILITY TOUR

Securing Infrastructure Airspace: From Risk To Resilience

Thursday, Oct 15, 2026
8:00 AM – 2:00 PM (Mountain Time)
Fortem Technologies HQ | Lindon, Utah



Thank you for your interest in attending this exclusive Counter-UAS demonstration hosted by **Southern States LLC** in partnership with **Fortem Technologies**. We look forward to an informative and impactful day of live demonstrations, technical discussion, and collaboration focused on securing the airspace above our nation's critical infrastructure.

EVENT DETAILS

Date	Thursday, October 15, 2026
Time	8:00 AM – 2:00 PM (Mountain Time)
Location	Fortem Technologies Headquarters 1855 W 500 N, Lindon, Utah 84042
Host	Southern States LLC In partnership with Fortem Technologies

AGENDA OVERVIEW

8:00 AM	Guest arrival and check-in at Fortem HQ
8:45 AM	Transport to F4 facility with Fortem history briefing en route
9:30 AM	Live Demonstration and Q&A;
11:15 AM	Return to HQ
11:30 AM	Catered lunch and technical discussion panel
1:30 PM	Facility and office tour
2:00 PM	Adjourn

WHAT YOU WILL SEE

- TrueView® Radar — 360° persistent 3D drone detection at 6+ mile range
- SkyDome® Manager — Real-time airspace command & control software
- DroneHunter® — Live autonomous kinetic intercept demonstration
- DroneHangar™ — Autonomous 24/7 launch and recovery system
- VisionFlex™ — Radar-cued long range OE/IR camera

TRAVEL & ACCOMMODATIONS

Please fly into **Salt Lake City International Airport (SLC)**. Southern States is pleased to provide complimentary local transportation upon request.

Recommended Hotels:

- **Hilton Garden Inn Lehi**
3150 N Hotel Loop, Lehi, UT 84043
- **Hyatt House Pleasant Grove** (Ask for the Fortem Technologies Rate)
544 S Pleasant Grove Blvd, Pleasant Grove, UT 84062

QUESTIONS & CONTACT

Questions? Contact Patrick James
Director, Grid Security Solutions
Southern States LLC
Text or Call: 678-570-8937

WHY ATTEND THIS DEMONSTRATION

- Witness the only DHS-authorized non-lethal kinetic counter-drone solution
- See live autonomous intercept technology currently protecting U.S. Army installations worldwide
- Evaluate the system that protected all 11 U.S. 2026 FIFA World Cup venues
- Understand how Lockheed Martin's investment validates this technology and is doubling production capacity
- Engage directly with Fortem Technologies engineering and Southern States security specialists
- Learn why Fortem Technologies was selected as Prime Contractor on a 5-Yr DHS Counter-Drone IDIQ worth more than \$1B

RSVP HERE

Southern States LLC | Grid Security Solutions | southernstatesllc.com | 678-570-8937

In Partnership with Fortem Technologies • Securing Infrastructure Airspace: From Risk To Resilience
This event is by invitation only. All attendees are subject to Fortem Technologies facility access requirements.



Thank You!



WHITE PAPER

Current Approaches and Regulations in the United States to:

Protect Energy Production and Grid Infrastructure from today's Drone Threats



Current Mitigation Options and Approaches, Operational Model, and a Call to Action

PREPARED FOR: North American Transmission Forum (NATF)

AUTHOR: Southern States, LLC DATE: April 2026

CONTENTS

Executive Summary	2
Objective	3
1.0 The Emerging Drone Threat to Energy Infrastructure	3
2.0 Regulatory Framework Governing Counter-UAS Detection, Tracking, and Identification (DTI) in the United States	3
2.1 Radar Detection	4
2.2 RF Detection, Remote ID, and Applicable Federal Statutes	4
2.2.1 Regulatory Context	4
2.2.2 Applicable Federal Statutes	4
2.3 Relationship to Federal Counter-UAS Authorities (6 U.S.C. §124n)	4
2.4 Compliance Position of Layered DTI Architectures	5
3.0 Regulatory Framework Governing Counter-UAS in the United States	5
3.1 Current Federal Authorities for Drone Mitigation	5
3.2 New State, Local, and Tribal Law Enforcement (SLTT) Authorities for Drone Mitigation: Safer Skies Act of December 2025	6
3.3 Proposed New Private Security Team Authorities for Drone Mitigation at Utilities and other Critical Infrastructure	6
3.4 FAA Regulatory Environment	7
3.4.1 Part 107	7
3.4.2 Remote ID (Part 89)	7
3.4.3 Federal Aviation Administration (FAA) Part 108 Rules for Drone Operation	7
4.0 What can Energy Producers and Utilities do Today to Stop Dangerous Drones	8
4.1 Option A	8
4.2 Option B	9
4.3 Option C	9
5.0 Approach – Layered Detection, Tracking, and Identification (DTI) Architecture	9
5.1 Radar Sensors	9
5.2 EO/IR Camera Sensors	9
5.3 RF Detection, Remote ID, and Whitelisting	9
6.0 Approach – Interceptor Drone Mitigation Systems and Regulatory Considerations	10
6.1 Legal Reality	10
6.2 Interceptor Drone Operations	10
6.2.1 Local or Remote Control	10
6.2.2 Technical Readiness for FAA Part 108	10
7.0 Summary – Overall Operational Model	11
8.0 Call to Action	11
Conclusion	12

<Public>
EXECUTIVE SUMMARY

Unmanned aerial systems (UAS), commonly referred to as drones, have rapidly evolved from hobbyist devices into tools capable of surveillance, sabotage, and kinetic attack with easily obtained energetics from local retail stores throughout the United States. Energy producing sites and the supporting pipeline and transmission infrastructure – including substations, generation facilities, pipelines, and control systems – represent one of the most strategically attractive targets for near peer adversaries and terrorist organizations seeking to attack the United States.

Recent geopolitical developments, including ongoing tensions with China and military actions involving Iran and its proxy networks, have heightened concerns regarding asymmetric threats to U.S. infrastructure. At the same time, domestic incidents and news reporting in the United States have documented increasing drone activity near critical infrastructure facilities, including power generation and grid assets.

In Iran, Ukraine, and other places, the first places targeted are energy sites. Terrorists know this also.

Many commercially available RF-based detection systems rely on signal libraries and are limited to identifying drones that emit command-and-control or telemetry signals. However, a significant portion of modern threat drones operate autonomously using pre-programmed waypoint navigation. No terrorist is using a joystick or is anywhere near the site being attacked. These terrorist drones often emit no detectable RF signal, relying instead on passive GPS reception or, in more advanced cases, visual odometry that eliminates dependence on GPS entirely. As a result, these “RF-silent” or “dark” drones are not detectable using RF listening technologies and cannot be disrupted using electronic jamming or protocol exploitation.

Accordingly, radar remains the only reliable method for early detection and tracking of non-cooperative or autonomous drones. Radar systems operate within regulated spectrum environments governed by the Federal Communications Commission (FCC) and are widely deployed across aviation and defense applications. When properly authorized and configured, these systems present no risk to the National Airspace System.

Given the limitations of electronic countermeasures, effective mitigation of non-cooperative drones must ultimately rely on physical (kinetic) means, such as interception or capture. These drone interceptors are being deployed across the United States and have been widely used at major events such as the Olympics and the World Cup.

Unlike military installations, most energy infrastructure was not originally designed with aerial surveillance or drone intrusion in mind. Fortunately, regulatory and technological conditions allow deployment today, with additional regulations rapidly evolving in favor of increased simplification of the operations for infrastructure protection:

- The SAFER Skies Act, in December 2025, now allows trained state and local law enforcement (SLTT) agencies to conduct drone mitigation in partnership with utilities and owners of private infrastructure.
- The FAA is advancing Part 108, which will enable expanded Beyond Visual Line of Sight (BVLOS) drone operations with performance-based safety requirements.
- Modern sensor architecture now allows utilities to monitor airspace around substations and generation sites with high confidence at reasonable price points.
- Kinetic mitigation techniques such as interceptor drones have been developed in partnership with Federal agencies and are now approved for the United States airspace. For example, these are being used in this year’s World Cup sites because they are proven safe and effective to use in commercial settings to defeat terrorist drones.
- Regulatory movement is under consideration via a pending Executive Order, which would allow certain infrastructure providers to mitigate drones over their property unilaterally without the coordination required today with local and state law enforcement.

While detection, tracking, and Identification (DTI) capabilities are legal for NATF members to deploy within the current regulatory framework, the mitigation authorities are still controlled, now by state and local law enforcement in addition to federal components.

There are options for NATF members to deploy the mitigation assets now in 2026 to be ready by 2027.

While mitigation authorities continue to be extended in this heightened threat environment, interceptor drones – highly recommended over missiles and electronic warfare/jamming approaches – can be used today most easily from remote security operations centers with law enforcement cooperation. The owner of the infrastructure is encouraged to deploy the mitigation assets immediately, develop procedures, processes, ownership, and operational methods allowing their use today in various modes with current regulations, while in parallel establishing coordination with law enforcement.

THIS WHITE PAPER OUTLINES:

1. The evolving regulatory framework governing drone detection, tracking, identification, and mitigation
2. A proven layered approach for protecting energy infrastructure
3. Options and operational pathways utilities can deploy today and be within the regulations today to detect, track, identify, and mitigate terrorist drones

The objective is to provide confidence to NATF members that regulatory conditions exist and are continuing to shift in favor of responsible infrastructure protection, allowing utilities to begin implementing layered drone defense strategies in coordination with law enforcement and federal partners today.

1.0 The Emerging Drone Threat to Energy Infrastructure

Electric utilities have historically focused security investments on physical and cyber threats. However, drones introduce a **third operational domain: low-altitude airspace security**.

Threat vectors include:

- Surveillance of substations and switching yards
- Delivery of explosives or payloads to energy producing sites, such as dams, nuclear plants, etc., and key substations serving millions of energy users
- Kinetic disruption of transformers or control centers

Small commercial drones now possess:

- Ranges exceeding 10 km
- Autonomous navigation
- High-resolution cameras
- Payload capacity for explosive devices

These systems are inexpensive, widely available globally, and are not detected by traditional drone RF antennas because they are flown without emitting any radio signals.

Several recent domestic incidents reported in U.S. media outlets have documented suspicious drone activity over critical infrastructure locations, including energy facilities in California and other states. While many incidents remain under investigation, the trend has drawn increasing attention from federal law enforcement and homeland security agencies.

The concern is not hypothetical.

Nation-state actors have already demonstrated drone-based attacks on energy infrastructure in Ukraine and the Middle East, including coordinated strikes on oil facilities.

The energy grid presents a similarly attractive asymmetric target.

2.0 Regulatory Framework Governing Counter-UAS Detection, Tracking, and Identification (DTI) in the United States

Effective counter-UAS operations require the ability to detect, track, identify, and mitigate (DTI-M) unauthorized or malicious drones. While mitigation authorities remain tightly controlled under federal law (as discussed in Section 3.0), detection, tracking, and identification capabilities are broadly permissible when implemented in compliance with applicable communications, privacy, and aviation regulations.

This section outlines the regulatory considerations applicable to DTI systems deployed by critical infrastructure owners.

A key regulatory distinction must be emphasized:

- Detection, tracking, and identification (DTI): Generally

permissible under U.S. law when conducted using passive or non-interfering technologies

- Mitigation (e.g., jamming, spoofing, takeover, capture, or destruction): Restricted to authorized federal entities and trained state and local law enforcement under statutory authorities such as 6 U.S.C. §124n and 10 U.S.C. §130i

DTI systems must therefore be designed to observe and characterize airspace activity without interfering with aircraft operations or communications.

The Southern States' solution for countering drones is compliant with all these regulations as they exist today.

2.1 Radar Detection

Radar systems form the foundation of non-cooperative drone detection and are governed by U.S. spectrum regulations.

Radiofrequency emissions in the United States are regulated by the **Federal Communications Commission (FCC)** for non-federal users and the **National Telecommunications and Information Administration (NTIA)** for federal spectrum coordination.

Key regulatory considerations include:

- Operation within authorized frequency bands (licensed or compliant with applicable FCC rules, such as Part 15 or Part 90 where applicable)
- Coordination near sensitive environments, including airports and federal installations
- Compliance with RF exposure safety standards for personnel and the public

Modern counter-UAS radar systems are engineered to operate within established regulatory limits for spectrum use and electromagnetic exposure.

These systems typically utilize low-power emissions relative to traditional aviation radar and are designed to support safe deployment in proximity to populated or operationally sensitive environments, subject to proper coordination.

When required, deployment may involve a standard FCC licensing or coordination process, which is well-established and routinely used for commercial and infrastructure applications. For example, AM/FM radio is widely broadcast at airports in the United States and is seen as safe given FCC licensing. To deploy a radar for counter-UAS, Southern States can help customers obtain an FCC license at their site. The process has a usual lead time of about 30 days and requires a small application fee.

2.2 RF Detection, Remote ID, and Applicable Federal Statutes

2.2.1 Regulatory Context

RF-based detection systems operate by passively monitoring radiofrequency activity associated with unmanned aircraft. These systems may identify:

- Signal characteristics (frequency, modulation, power)
- Drone and controller location (via signal triangulation)
- FAA-required Remote ID broadcast information

Importantly, compliant systems do not access or decode the content of communications (e.g., video payloads or

command data) but instead analyze signal metadata and publicly broadcast identification information.

The FAA Remote ID rule (14 CFR Part 89) requires drones to broadcast identification and location data over publicly accessible frequencies, explicitly intended to be receivable by third parties for safety and accountability purposes.

As affirmed in *Brennan v. Dickson*, 45 F.4th 48 (D.C. Cir. 2022), such broadcasts are not considered private communications.

2.2.2 Applicable Federal Statutes

Several federal statutes govern electronic surveillance and communications monitoring. Properly designed DTI systems operate within these legal boundaries:

- Wiretap Act (18 U.S.C. § 2511): Prohibits interception of the *contents* of communications. Passive monitoring of signal characteristics or publicly broadcast Remote ID data does not constitute interception of content.
- Pen Register and Trap and Trace Statutes (18 U.S.C. §§ 3121–3127): Apply primarily to routing and addressing information in telecommunications networks (e.g., phone numbers), and do not restrict analysis of RF signal characteristics or publicly broadcast drone identification data.
- Communications Act (47 U.S.C. § 605): Prohibits unauthorized interception and disclosure of non-public communications. It does not apply to publicly broadcast signals or signal-level analysis.

Consistent with these statutes, compliant RF detection systems:

- Do not intercept or store communication content
- Operate on signals that are either publicly broadcast or inherently observable in the RF environment
- Support aviation safety objectives by enhancing situational awareness

This approach aligns with federal guidance and existing case law, including distinctions drawn in *Joffe v. Google*, where liability was tied to the collection of payload data rather than signal characterization.

2.3 Relationship to Federal Counter-UAS Authorities (6 U.S.C. §124n)

Section 124n provides authority for the Department of Homeland Security and the Department of Justice to conduct counter-UAS activities that would otherwise violate certain federal laws.

However, this authority is only required when an activity involves:

- Interference with communications
- Capture, destruction, disruption, or control of aircraft
- Access to protected communication content

DTI systems that are passive, non-interfering (such as a radar with an FCC license), and/or are limited to signal detection and publicly available information do not trigger these statutory restrictions. Accordingly, such systems can be lawfully deployed by infrastructure owners without requiring federal counter-UAS authorization.

2.4 Compliance Position of Layered DTI Architectures

A properly designed layered DTI architecture – combining radar, RF detection, and EO/IR sensors – can be deployed

<Public>

in full compliance with U.S. law when it adheres to the following principles:

- Non-interference: No jamming, spoofing, or protocol manipulation
- No content collection: No interception of payload data or communications content
- Use of public or observable signals only: Including Remote ID and RF emissions
- Spectrum compliance: Operation within FCC and, where applicable, NTIA guidelines
- Privacy-by-design: Minimization of data collection and alignment with civil liberties expectations

Such architecture provides critical airspace awareness capabilities while remaining clearly distinct from regulated mitigation activities.

3.0 Regulatory Framework Governing Counter-UAS Mitigation in the United States

Drone detection and mitigation in the United States are governed by a layered framework of federal statutes, aviation regulations, and communications laws.

The key regulatory reality today is that **detection is broadly permissible. Mitigation authority is tightly controlled.**

3.1 Current Federal Authorities for Drone Mitigation

The core legal authority enabling counter-drone operations is the Preventing Emerging Threats Act of 2018, codified at 6 U.S.C. 124n. Federal law enforcement domestic counter-UAS operations are governed by 6 U.S. Code § 124n - *Protection of certain facilities and assets from unmanned aircraft*. 6 U.S. Code § 124n, part of the 2018 FAA Re-authorization, has been extended each year without update or change since its first expiration in 2022.

Department of Defense domestic authorities come from for 10 U.S. Code § 130i which is similar in terms of the coordination process required to mitigate a drone in the United States.

In summary, DHS, DOJ, DoW, and in limited cases DOE, have authority to disrupt, mitigate, and stop a drone in the United States. Only a few components in DHS have the authority to stop drones (USSS/ CBP / USGG / FPS, not TSA). Within DOJ, the FBI, USMS, DEA, and BOP can be authorized by the Attorney General. The USSS and FBI deploy most frequently within the DOJ construct in support of SEAR events and NSSE's with significant caveats and

following an in-depth coordination process.

Process for authorized Federal components to act on a 124n or 130i mission:

- Component appeals to the Department-level Program Office to include a new covered facility or asset with a requisite risk-based assessment.
 - Some covered facilities or assets are considered inherently high-risk, negating the risk-based assessment requirement.
- Submit the Concept of Operation document detailing all aspects for the proposed deployment to the FAA for coordination.
- Concept of Operations covers:
 - NOTAMS
 - TFRs
 - Public outreach
 - Privacy notifications
 - Authorized enforcement area
 - Anticipated enforcement area
 - Inter and intra-agency notification process
 - Identification of authorized agent
 - Component and FAA leadership (SES) sign a joint coordination official memorandum (OM) on behalf of their respective Director/Administrator stating all coordination is complete and both sides concur.
 - Final approval to deploy is made by the Department Cabinet Head (Sec DHS, AG, or Sec Def) for the respective requesting component.

This process is well known by the authorized components. Approval happens quickly, provided all criteria are met.

This process is completed multiple 100's of times a year, with the USSS the most frequent user.

Authorized components must go through the coordination process to deploy counter UAS equipment for each location and mission with final approval to deploy assigned to the Cabinet level executive (Secretary Homeland for DHS / Attorney General for DOJ / Secretary of Defense for DoW – or designee). Authorities only cover counter-UAS missions as they relate to components' authorized duties. For example:

- For U.S. Secret Service protection operations:
 - Security or protection functions of the U.S. Customs and Border Protection
 - Protection of facilities pursuant to Title 40 (Government Buildings) Federal Protective Service
 - Missions authorized to be performed by the United States Coast Guard
- For DOJ protection operations, it must relate to missions pertaining to personal protection operations conducted by:
 - Federal Bureau of Investigation
 - United States Marshals Service (courts and witnesses)
 - Federal Bureau of Prisons
 - Or support of missions performed by DHS or DOJ for NSSEs, SEAR events, and in support of SLTT - upon request through the governor of the state to DHS.

3.2 New State, Local, and Tribal Law Enforcement (SLTT) Authorities for Drone Mitigation: Safer Skies Act of December 2025

The Safer Skies Act, in December 2025, is a tidal shift in the counter-drone industry. The act expands the role of state and local law enforcement (SLTT) by granting authority to allow state and local law enforcement to mitigate drones. SLTT must be certified via federal training before protecting critical infrastructure and large events, such as the World Cup in 2026.

The act also reauthorizes and expands federal counter-drone authorities through 2029 and establishes FAA counter-UAS performance standards, expands covered sites, and strengthens privacy protections.

Federal training programs – including those conducted at the FBI facility in Huntsville, Alabama – are preparing operators for:

- Detection, tracking, and identification with advanced systems supporting classification

- Legal compliance
- Mitigation execution, including interceptor drones

3.3 Proposed New Private Security Team Authorities for Drone Mitigation at Utilities and other Critical Infrastructure

As of today, August 2026, the Critical Infrastructure Airspace Defense Act (S.4380) remains in the introduced stage. Even though it has broad bipartisan support, it has not yet advanced out of committee.

The bill was introduced April 22, 2026, by Senator Tom Cotton (R-AR) and was referred to the Senate Homeland Security and Governmental Affairs Committee. There is no reported markup, committee vote, Senate floor vote, or House companion bill movement yet. However, it is expected to pass in late 2027, the delay giving room for learnings from the Safer Skies Act (Section 3.2). Congress is being briefed on the latest safe mitigation techniques that will protect spectrum across the country. To this end, Southern States is preparing a series of videos to educate Congress on the latest approaches and best practices for safe drone mitigation.

This bill is one of the most significant Counter-UAS bills ever proposed because it would allow designated critical infrastructure owners and operators – including:

- Bulk power substations
- Transformer stations
- Nuclear generating facilities
- Grid control centers
- Water and wastewater facilities
- Certain contracted security providers

to obtain authority to detect, track, identify, and mitigate threatening drones, after federal training and certification requirements are met. This would represent a major shift because today utilities largely must rely on federal, state, or local partners and have very limited direct mitigation authority.

Although the standalone bill has stalled in committee (August 2026), there is growing Congressional momentum around drone security due to increasing drone incursions over critical infrastructure, particularly the growing concern regarding Chinese-made drones and sabotage risks. Because of this, many observers believe portions of S.4380 could ultimately be attached to larger legislation such as the FY2027 National Defense Authorization Act (NDAA), FAA Reauthorization follow-on legislation, or Homeland Security authorization packages rather than passing as a standalone bill.

When enacted substantially as written, it could create a clear pathway for utilities to deploy persistent Counter-UAS systems and conduct mitigation operations themselves.

3.4 FAA Regulatory Environment

The FAA governs the National Airspace System.

Key elements of the FAA regulatory framework for drones include:

3.4.1 Part 107

Part 107 currently governs commercial drone operations, where today drones must be flown by an operator with line of sight (LOS), and not over people, and not at night. Beyond Visual Line of Sight (BVLOS) operations today require waivers under 14 CFR Part 107.

3.4.2 Remote ID (Part 89)

Requires drones to broadcast identity and location.

Remote ID provides a mechanism to distinguish compliant drones from unidentified or potentially hostile aircraft.

Under the FAA Remote ID Rule, the aircraft must broadcast:

- serial number / session ID
- aircraft position
- altitude
- velocity
- control station location

This information has a similar cooperative effect as does ADS-B information broadcast by commercial airlines and general aviation aircraft. The FAA does not want drones broadcasting ADS-B Out because it can overload the surveillance system. Relevant rule: 14 CFR §91.225. Instead, the FAA encourages ADS-B IN for traffic awareness. Interceptor systems use ADS-B data and Remote ID data to improve safety.

3.4.3 Federal Aviation Administration (FAA) Part 108 Rules for Drone Operation

The new FAA Part 108 rules enable Beyond Visual Line of Sight (BVLOS) operations under performance-based standards.

This rule is expected to become law in 2026 or early 2027, significantly expanding the number of drones in United States airspace and subsequent innovations in technology. The notice for proposed rulemaking (NPRM) was closed in October 2025, with the notice most often becoming

law 6-12 months after the NPRM is closed. However, with hundreds of thousands of comments, the FAA reopened the comment period in January 2026 and closed it again in February 2026 to work through some final regulations related mostly to right-of-way decisions.

The FAA Part 108 rules require operators to meet certain performance standards and do not prescribe technology. One of the key performance requirements is adequate Detect and Avoid (DAA) capability to deal with scenarios of conflicting traffic as well as maintain conformity with operational intent. In practice, this means that most utilities will likely need to consider radar corridor infrastructure, ADS-B receivers, weather sensors, Remote ID Sensors and/or related LTE or 5G communications to automate a DAA service. FAA Part 108 does not require this, but such infrastructure may simply become the easiest way to satisfy DAA and scale operations economically and with increased certitude than manual efforts. Utilities and infrastructure owners using drones BVLOS, or security drones such as the Fortem DroneHunter, will benefit from an airspace awareness system already in place for counter-drone defense.

The rule also requires the drones flying BVLOS to be equipped for safety:

- Redundant power and control
- Redundant command and control (C2) links to BVLOS drones and lost link procedures, such as linger in place, land, etc.
- Ground risk mitigation, such as parachutes
- Deconfliction capabilities such as geo cages, altitude limits, and other safety features.
- Demonstration of wind tolerance, precipitation tolerance, and icing limitations
- Cybersecurity standards such as:
 - AES-256 encryption
 - Certified to the US Government that we are NIST SP 800-171 compliant, meeting U.S. Defense Federal Acquisition Regulation Supplement (DFARS) 252.204.7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting."
 - End-to-end encryption through SSL.
 - TLS certificates.
 - Passwords are encrypted, and access controls are used to differentiate authority on the system.
 - JSON Web Tokens (JWTs) are used for all API and direct access to the system, and these tokens expire frequently every hour.
 - Upgrade processes are protected using PGP encryption.

- Software builds are run against NESSUS Scans to validate OS and Application-level protection against viruses and third-party vulnerabilities.
- Detect and avoid (DAA) radar data feeds are hardwired into customer network(s)
- Emitted radar signals have an extremely specific center frequency, pulse rate (PRF), and bandwidth. It would be nearly impossible to “inject” false tracks.

- Jamming the radar on its specific frequency and over the entire bandwidth exceedingly difficult.

With the new FAA Part 108 imminent, the volume and sophistication of drones will exponentially increase, especially in the United States. This creates strategic opportunities for automation and cost savings, as well as the need for utilities to invest in the infrastructure to manage and secure the airspace around critical sites.

4.0 What can Energy Producers and Utilities do Today to Stop Dangerous Drones and FAA Section 2209

Federal laws restrict private mitigation actions. As a result, utilities cannot independently Jam, Spoof, Capture, or Destroy drones. Mitigation must be conducted by authorized federal or trained state and local law enforcement (SLTT) entities. It is currently illegal (August 2026) for any private security team that is not a trained SLTT or any Federal agency to mitigate a drone. This is because of the freedom granted to Americans to fly. Vast areas of the country are unrestricted airspace. This means that despite the observable potential national security threat from drones, the offenders flying the drones may not technically be breaking any U.S. law. There is just not any common air picture for drones that exists today, like there is for commercial or general aviation aircraft. However, this is changing quickly as airspace management shifts a bit from freedom to security. The FAA Section 2209 is establishing a process to declare no-fly zones over critical infrastructure.

FAA Section 2209 is very important to energy production, transmission, and distribution facilities (as well as stadiums, oil and gas sites, etc.) because it creates a legal mechanism to ask the FAA to prohibit or restrict unmanned aircraft flights in close proximity to qualifying critical-infrastructure sites.

Under the FAA's May 2026 proposal, an eligible utility could apply for an Unmanned Aircraft Flight Restriction (UAFR) around a particular qualifying facility to have the legal context to stop drones, but no authority yet. The FAA anticipates hundreds of thousands of sites applying for UAFR. Sites showing a real risk will get priority. Having DTI equipment in place will only help with the application process approval process.

For utilities, Section 2209 is Phase 1 of a broader counter-UAS strategy:

Phase 1: Obtain FAA-recognized protected airspace around critical facilities.

Phase 2: Deploy detection technologies (radar, RF, cameras)

Phase 3: Coordinate with authorized law enforcement for mitigation

Future Phase: When Congress expands mitigation authorities, then critical infrastructure operators will be ready.

For utilities, Section 2209 is therefore not simply an aviation rule – it is becoming a foundational element of how you justify, design, and integrate drone detection systems with future mitigation authorities

IMPORTANT: With FAA Section 2209 establishing a process to make it illegal to fly drones over designated sites, that law now gives the context to enforce the law. However, as of August 2026, mitigation is only allowed by Federal authorities and trained State and Local authorities (Section 3 above)

Therefore, the most viable regulatory pathway to stop drones today under current regulations (August 2026) would be a combination of three options.

4.1 Option A

1. Utility deploys Detection, Tracking, and Identification system (DTI) and the Fortem DroneHunter on site with all Part 107 and Part 108 safety measures.
2. Detection, Tracking, and Identification alerts Federal or SLTT partner in real-time
3. Authorized Federal or SLTT use of Fortem DroneHunter
4. The solution used at the World Cup is the same proposed by Southern States LLC, but includes integrations and operational capabilities suited to long-term fixed-site security deployments and security system integrations.

AND / OR

4.2 Option B

Deploy DroneHunter under a federal pilot program with SLTT, DHS, or DOJ oversight.

AND / OR

4.3 Option C

Interceptor drone systems, such as the Fortem DroneHunter, enable a graduated response model that aligns with current regulatory constraints. In a “pursuit and observation” mode, an interceptor may:

- Track a non-cooperative drone at a safe stand-off distance
- Provide real-time video and telemetry to a Security Operations Center
- Enable threat assessment and escalation decisions
- Operate within current FAA Part 107 rules or applicable waivers (and future Part 108 frameworks)

In this configuration, the interceptor is not performing mitigation but rather enhancing situational awareness and supporting lawful response decisions, including coordination with authorized law enforcement partners. This approach provides immediate operational value while remaining compliant with existing federal law.

In limited circumstances, questions arise regarding whether a property owner or security provider may act to protect

persons or property from an imminent drone-related threat. While federal law generally preempts unauthorized interference with aircraft, courts and legal scholarship have begun to explore the intersection of drone activity with:

- Reasonable expectation of privacy
- Trespass and nuisance doctrines
- Self-defense and protection of property principles

Several notable cases and legal developments illustrate this evolving landscape, for example: in *Boggs v. Merideth* (Kentucky, 2017), a property owner shot down a drone he claimed was surveilling individuals on his property. While criminal charges were dismissed, the civil case highlighted unresolved tensions between airspace rights and privacy expectations. Legal commentary and state-level statutes increasingly recognize that low-altitude drone operations over private property, particularly when invasive, may implicate privacy and nuisance concerns, though clear federal precedent remains limited.

It is important to emphasize that there is no broad legal authorization today for private entities to unilaterally disable or destroy drones. However, the legal environment continues to evolve, particularly where credible threats to safety, privacy, or critical infrastructure exist. In all cases, actions taken outside established federal authorities carry legal risk and should be carefully evaluated in coordination with legal counsel and law enforcement partners.

5.0 Approach – Layered Detection, Tracking, and Identification (DTI) Architecture

Effective protection requires a layered, multi-sensor approach.

5.1 Radar Sensors

Radar provides the foundational counter-drone sensor:

- Radar remains the most reliable technology for detecting small drones at long range. Examples include FMCW counter-UAS radar systems capable of:
 - detecting drones several kilometers away
 - tracking multiple objects simultaneously
 - operating in all weather conditions
- Radar provides the earliest possible detection of airborne threats.
- Tracking of RF-silent drones
- High accuracy for camera and mitigation cueing.

- Radar systems are inherently resistant to spoofing due to waveform characteristics, while layered architecture provides resilience against disruption.
- Creation of 3D volumetric airspace zones, when entered by a classified drone, triggers escalations, with some zones forbidding even whitelisted drones.
- Remote ID antenna to feed C2 and align with radar tracks.

5.2 EO/IR Camera Sensors

Cameras vary in price due to range, zoom, slew-and-cue speed, etc. They provide:

- Visual confirmation of drone, threat level
- Classification, distinguishing birds from drones, etc.
- Payload assessment

- Key is the integration between the EO/IR and Radar in a distributed and modular command and control systems, easily integrated with existing other security systems.
- Slew and cue speed and zoom capability. Radar sees a broad airspace simultaneously with a 360-degree field of view, where cameras see a very narrow 1–2-degree field of view. Radar systems can slew and cue a camera and control the zoom to keep a fast-moving drone on frame for inspection, classification, and escalation decision-making.

5.3 RF Detection, Remote ID, and Whitelisting

RF systems – such as those provided by partners like SkySafe – enable:

- Identification of compliant drones via Remote ID
- Detection of known signal signatures to give the make and model of drones that are cooperative.
- Approximate operator location

Remote ID enhances identification and reduces false positives. Authorized drones can be identified and whitelisted through Remote ID and Integration with utility drone lists.

6.0 Approach – Interceptor Drone Mitigation Systems and Regulatory Considerations

6.1 Legal Reality

Mitigation technologies, including interceptor drones, are restricted to authorized operators.

Counter-UAS Equipment and Technology Controls

Under federal law, mitigation systems must be on the DHS and DOJ approved list of counter-UAS systems that can be deployed. Approval takes multiple years and requires coordination with:

- Federal Aviation Administration (airspace safety)
- Federal Communications Commission (spectrum)
- National Telecommunications and Information Administration (federal spectrum)
- Federal Bureau of Investigation (training)

Systems are evaluated for:

- spectrum interference
- aviation safety
- cybersecurity risks
- counterintelligence risks

Any mitigation system must meet these requirements in the United States.

6.2 Interceptor Drone Operations

A typical model includes:

- Deployment at critical infrastructure sites
- Remote operation from centralized control by authorized operators
- Physical capture of hostile drones
- Recovery for forensic analysis

The time is now to ready mitigation systems with FAA Part 108 in 2026. While detection is critical, the ability to safely

remove hostile drones from protected airspace is also essential. Net-capture interceptor drones, which physically capture hostile drones and safely remove them from the airspace, are now being deployed at military bases and the World Cup in the United States.

6.2.1 Local or Remote Control

Interceptor systems can be positioned at critical infrastructure sites and deployed when a drone threat is confirmed. Operations may be conducted either locally at the site or remotely through a security operations center.

In either approach, both can be coordinated with trained law enforcement operators. The interceptor systems are valuable because they also return captured drones for forensic investigation.

6.2.2 Technical Readiness for FAA Part 108

The FAA is expected to introduce Part 108, enabling expanded BVLOS operations. Interceptor platforms developed for counter-UAS missions are being engineered to comply with anticipated Part 108 requirements, including:

- Remote ID broadcasting
- Anti-collision lights
- Geofencing and flight envelope protections
- Encrypted command-and-control links
- Detect-and-avoid operation

Additional capabilities – such as redundant communications links, strategic airspace deconfliction, and integration with Unmanned Traffic Management (UTM) networks – are expected to further strengthen compliance with future FAA performance standards.

7.0 Summary – Overall Operational Model

The security professionals for each utility will need to create roles, responsibilities, processes, and procedures to mitigate this new threat. These resources will also be key points of contact with federal, state, and local law enforcement to operate a practical security model, which includes:

- 1. Deployment of Detection, Tracking, and Identification Systems** Radar, EO/IR, and RF sensors deployed at critical sites
- 2. Centralized Monitoring** Integration of multiple sites into a unified airspace picture
- 3. Threat Identification** Sensor fusion combining radar,

EO/IR, and RF (including SkySafe inputs when a rogue drone is emitting)

- 4. Escalation and Coordination** Automated alerts to authorized law enforcement partners
- 5. Mitigation Execution** Get the mitigation assets in place now. Operate legally with Pursue-only functions or in coordination with authorized local, state, or federal partners at centralized locations

This architecture enables utilities to establish a persistent airspace security posture while remaining fully compliant with current regulations.

8.0 Call to Action

It is hard to remember a world without metal detectors at airports. The truth is, it was exceedingly difficult for a metal detector company to sell their product before the events of 9/11 in 2001.

Similar events with drones have already happened in the world.

In 2026, the United States needs these counter-drone assets put in place throughout the country, as our Golden Dome does not cover lower-altitude airspace and threats from within the country. The world has changed, and security is now required above the fence line for key sites. It is imperative that energy companies work in partnership with government regulatory teams (like utilities with NERC and FERC) to work in a virtuous cycle of deployment, learning, and adapting to these threats in a future proof evolution of technology and safe kinetic defeat capability.

The trends and threats are such that NATF needs to expand its relationship and coordination activities with federal, state, and local law enforcement as it relates to the protection of the energy producing sites and the national electric grid. Utilities can act today by deploying detection,

tracking, and identification systems, with mitigation systems also in place for use under current regulations. The key is to put these mitigation assets in place now as the threat profile increases. It is important to continue to expand coordination pathways with SLTT and Federal authorities as your situation demands.

There are many trends that support this call to action, including:

- Increasing drone threats to infrastructure
- Expansion of federal and SLTT authorities for mitigation with technologies available today that are future proof and usable under current regulations.
- Expanding mitigation authorities
- Advancements in detection, tracking, and identification technologies
- Emerging BVLOS regulatory frameworks require investment that can serve a dual use for safety and security above the fence line.
- The need to designate your key sites under FAA Section 2209

<Public>
CONCLUSION

Energy infrastructure and the electric grid are foundational to national security.

Drone threats represent a rapidly evolving risk that requires a coordinated, technology-enabled response. Regulatory frameworks – while complex – are increasingly supportive of infrastructure protection.

Utilities can take meaningful action today by deploying detection systems, integrating layered sensor architectures, and establishing coordination with authorized mitigation partners.

NATF and its members are well positioned to lead the adoption of airspace security as a core component of infrastructure protection to get these assets in place around our country.

The time to act is now.



24/7 emergency support line: (770) 946-4565

SouthernStatesLLC.com

30 Georgia Avenue | Hampton, GA 30228

phone (770) 946-4562

fax (770) 946-8106

Sales@SouthernStatesLLC.com

UAS SECURITY CONSIDERATIONS FOR CRITICAL INFRASTRUCTURE

AUGUST 11, 2026



Cybersecurity and Infrastructure Security Agency Introduction

The **Cybersecurity and Infrastructure Security Agency (CISA)** leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.



To address growing UAS threats, CISA advises and assists public and private sector partners with **managing UAS cyber and physical risk to critical infrastructure and public gatherings.**



**UAS Cyber and Physical
Security Guidance**



**UAS Flight Restriction
Guidance and
Coordination**



**UAS Information
Sharing and Expertise**



UAS Threat Types

<Public>



Disruption

Crash

Contraband

Weaponization

Surveillance

Cyber Intrusion



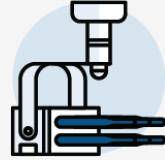
UAS Capabilities

<Public>

Cargo Delivery



Portable Jammers



High-Definition Cameras



Cyber-Based Platforms



Infrared Sensors



LiDAR



Sprayers



Drop Mechanisms



Thermal Imaging Sensors



How are UAS Incidents ^{<Public>} Affecting Critical Infrastructure?



Commercial Facilities Sector incidents include disrupting sporting events and crashing into amusement park rides.



Energy Sector incidents include UAS crashing into electricity substations, damaging powerlines, and conducting surveillance on oil and natural gas facilities.



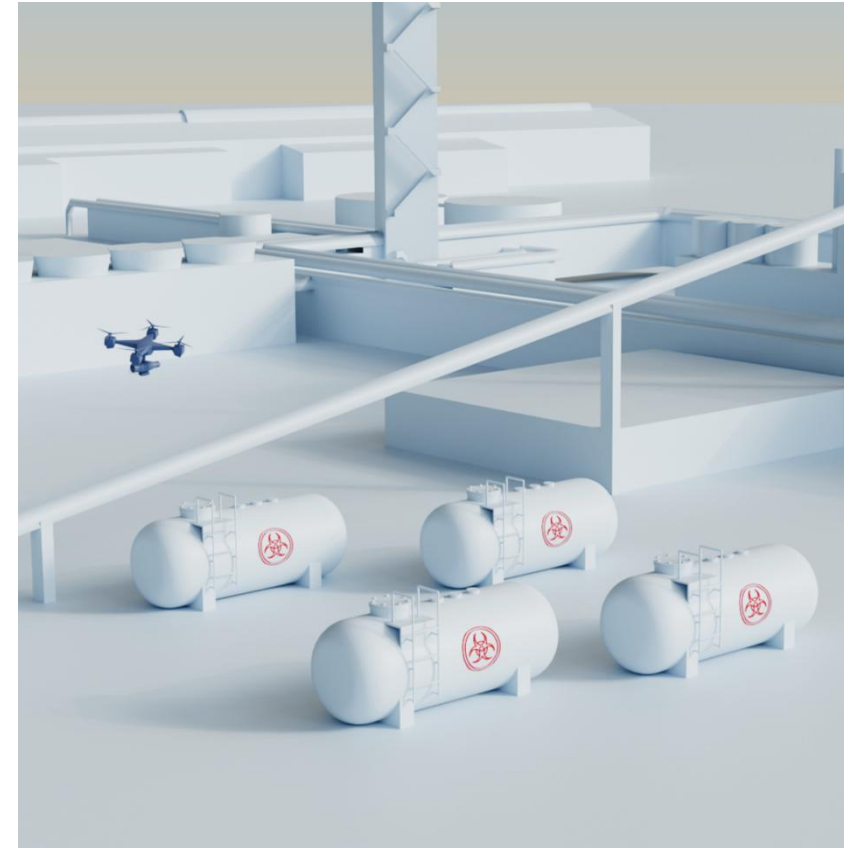
Transportation Systems Sector incidents include disrupting air operations and suspicious activity around rail facilities and pipelines.



Chemical Sector incidents include conducting surveillance around chemical facilities and UAS landing/crashing in secure areas.



Nuclear Reactors, Materials, and Waste Sector incidents include attacks on cooling systems and suspected surveillance.



Incidents and Potential Sector-Specific Vulnerabilities

Incident Examples



Nashville, TN

September 2025

Man with white nationalist ties pleaded guilty after trying to bomb a Nashville electricity substation using a drone.



Waco, TX

December 2025

Amazon drone damaged an overhead utilities cable after getting stuck.

Potential Vulnerabilities

Exposed Above-Ground Assets

Transmission lines, transformers, and other critical equipment are openly accessible from the air, leaving them vulnerable to crashes, interference, or payload drops.

Easily Identified Critical Components

Key assets can be simple to locate visually, enabling malicious actors to use UAS for reconnaissance.

Remote Infrastructure

Many facilities are located in rural or lightly monitored areas, making them easier for adversaries to access or observe without detection.

Operational Sensitivity During Weather or Restoration

UAS activity during outages or repair operations can disrupt line crews and delay restoration when the grid is already stressed.



UAS Security Assessments^{<Public>}

✓ Understand UAS Capabilities and Threat Types

- Understand how UAS capabilities could be leveraged to facilitate attacks or disruptions.
- Understand common UAS threat types.

✓ Identify Assets and Operations Vulnerable to UAS

- Consider how a UAS could access and exploit sensitive assets, areas, and information.
- Assess potential consequences of a UAS incident.
 - Consider harm to people or property, security, economic impacts, and environmental consequences.
 - Include impacts to both the facility and the surrounding area.

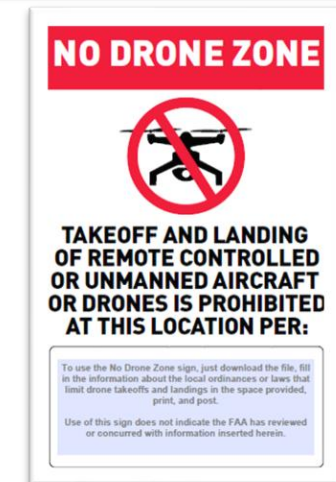
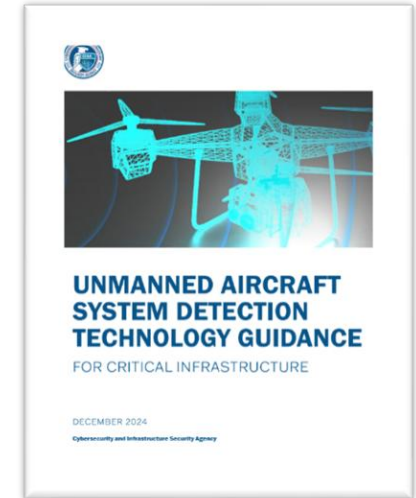
✓ Apply Risk Reduction Measures

- Incorporate security measures that protect against aerial threats.
- Consider a range of options based on facility characteristics, risk appetite, resources, etc.



UAS Security Options to Consider

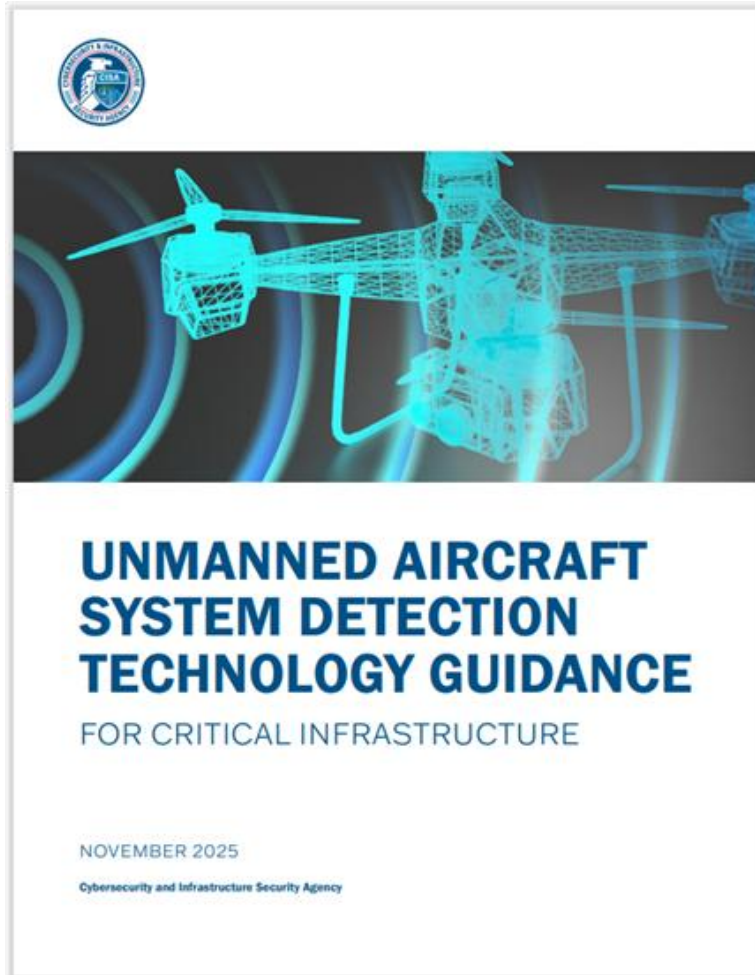
- Integrate UAS into **assessments; identify** and **monitor** possible UAS **launch** and **landing zones**.
- **Engage local communities** and post signage where UAS takeoff or landing may be restricted by state or local laws or ordinances.
- **Restrict access, obscure, or harden critical assets** vulnerable to aerial threats.
- Consider UAS **detection-only** technology,* Remote ID receivers, and/or configure video surveillance system cameras to monitor for aerial threats.
- Update **incident response** plans and partner with local law enforcement to address **suspicious activity**.
- Conduct **exercises and train** staff in UAS response.
- Understand current and applicable federal, state, and local **laws and regulations**.



* If considering using UAS detection technology, entities are encouraged to seek legal counsel informed by the [*Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems*](#).

UAS Detection Technology Guidance for Critical Infrastructure

<Public>



AUDIENCE

Critical infrastructure owners and operators who are considering investing in UAS detection technology to enhance air domain awareness and respond effectively to UAS threats.

GOALS

- 1 Establish UAS detection technology capability requirements.
- 2 Determine the most site-appropriate UAS detection technology.
- 3 Integrate UAS detection technology into existing security plans.



Permanent Flight Restrictions

FAA Extension, Safety, and Security Act of 2016 (FESSA 2209)

Requires FAA to establish a process for critical infrastructure to apply for a **permanent flight restriction** over a fixed site critical infrastructure facility.

FESSA 2209 is significant because most flight restrictions are temporary in nature and are **not issued over fixed sites** without an established national security justification.

The notice of proposed rulemaking (NPRM) was posted for a 90-day public review and comment period which **closed on August 5, 2026**.



Critical Infrastructure Flight Restrictions – Cross-Sector Eligibility Criteria* <Public>

Facility Information

Meets the definition of:

- Fixed-Site Facility
- Critical Infrastructure

Applicant and Facility Information (§ 74.52)

- Owners/Proprietors
- Facility Name, Address, Phone Number, Email, Website (if applicable)
- Facility Description

Unmanned Aircraft Flight Restriction (UAFR) Information

- Altitude Ceiling (§ 74.60)
- Lateral Boundaries (§ 74.58)



Restricting Drones Near Critical Infrastructure Sites

The FAA's proposed rule establishes a process for operators of certain critical infrastructure to petition the FAA to restrict drone operations over their sites for safety and security reasons. We're seeking to balance security needs with economic growth and public interest.

The rule is necessary to address the rapid increase in drone operations and the risks they could pose to sensitive facilities. It aligns with President Trump's Executive Order 14305 on *Restoring Airspace Sovereignty*, and it addresses a provision of the *FAA Extension, Safety and Security Act of 2016*.

Eligible Sites

- Chemical
- Commercial
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government services and facilities
- Healthcare and public health
- Information technology
- Nuclear reactors, materials, and waste
- Transportation systems
- Water and wastewater

To Get a Restriction

Applicants would have to show that the restriction is necessary for aviation safety, protecting people and property on the ground, national security, or homeland security. The FAA would create a website portal where applicants could submit information demonstrating the facility meets the eligibility criteria and that there is a safety or security need for the restriction.

Unmanned Aircraft Flight Restriction (UAFR)

Would have specific vertical and lateral boundaries that limit drone operations within its boundaries. The restriction would not be a physical or electronic barrier.

Facility Security

Protective Security (§ 74.56)

- Restricted Access
- Designated Security Personnel
- Security Monitoring
- Remote ID Receiver

Demonstration of Need (§ 74.66)

- Existing Unmanned Aircraft Traffic Patterns
- Vulnerability to UAS
- Consequences of UAS Incident

Security and Incident Response Plans (§ 74.64)



* As proposed in the [Designation-Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility](#) NPRM.

Critical Infrastructure Flight Restrictions – Sector-Specific Criteria*

Energy Sector (§ 74.88)

Electricity

- Power-generation facility with ≥ 500 MW capacity;
- Electrical substations with ≥ 500 kV of power; or
- Electrical substations with ≥ 345 kV of power in the Electric Reliability Council of Texas.

Oil

- Facility that converts crude oil into petroleum product, and
- Produces $\geq 100,000$ barrels/day of a petroleum product.

Natural Gas

- Facility that processes natural gas into dry natural (i.e., pipeline quality or consumer grade), and
- Has processing capacity of ≥ 500 MMcf/day of natural gas.



* As proposed in the Designation-Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility NPRM.

SAFER SKIES Act

<Public>

The Department of Homeland Security and Department of Justice published the SAFER SKIES Act Interim Final Rule (IFR) on July 6, 2026.

Established a national framework for eligible SLTT law enforcement and correctional agencies to **conduct authorized counter-UAS operations**.

Outlines required training, technology approvals, spectrum coordination, airspace notifications, reporting, and privacy protections for detection, warning, and mitigation activities.

The IFR became effective July 1, 2026.

DHS and DOJ are seeking public input on all aspects of the rule.

Comments may be submitted through [Regulations.gov](https://www.regulations.gov) until September 4, 2026.



Selected CISA Resources

► UAS Security Guidance and Coordination

- Cybersecurity and physical security guidance available at [Be Air Aware](#)[™]
- Flight restriction guidance and coordination support
- Information sharing and technical assistance

► Security Advisors

- Security experts located throughout the U.S.

► Security Assessments

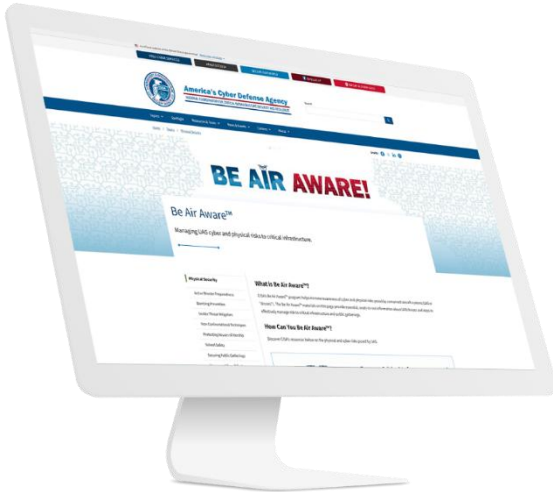
- Security Assessment at First Entry (SAFE)
- Infrastructure Survey Tool (IST)

► Training and Workshops

- Cybersecurity, bombing prevention, insider threat

► Exercises

- Exercise planning and conduct services
- CISA Tabletop Exercise Packages (CTEP)





Q&A





For more information:



<https://www.cisa.gov/topics/physical-security/be-air-aware>

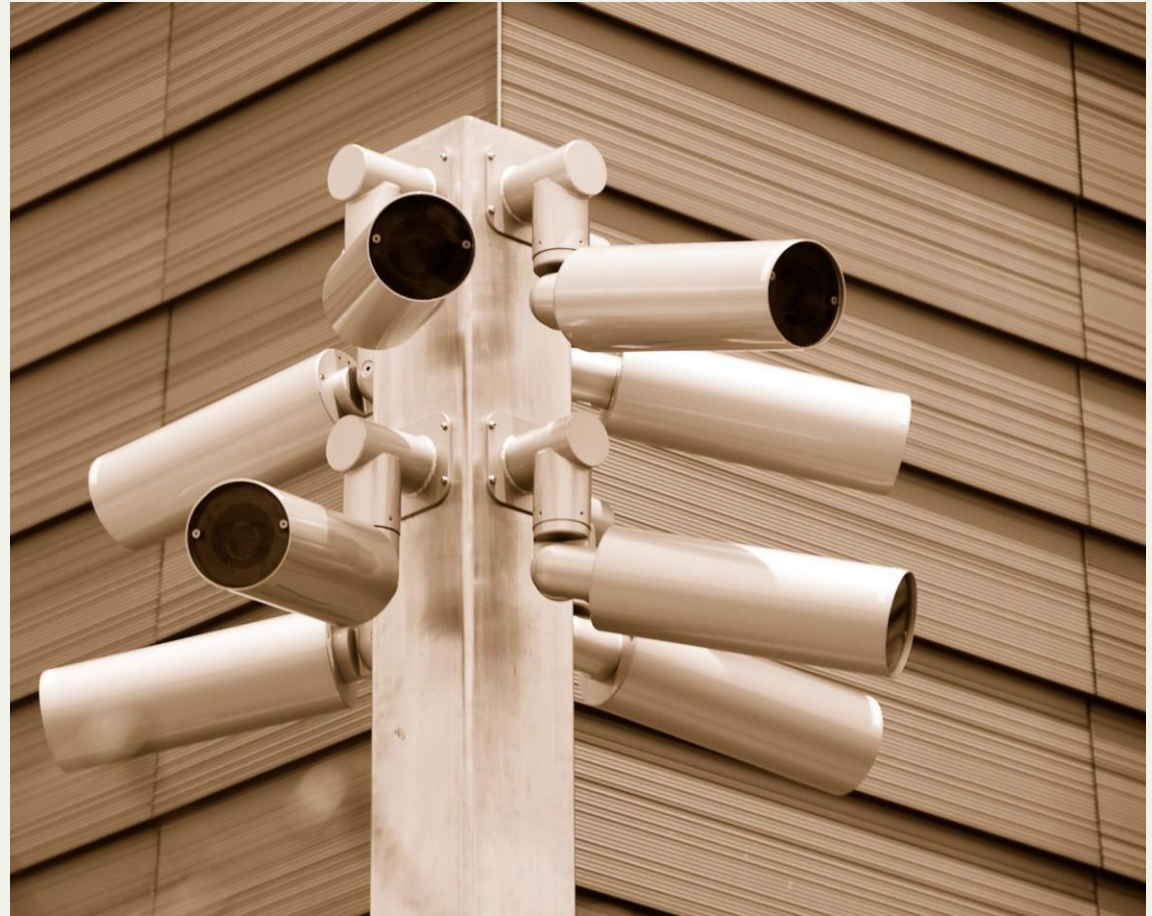


Questions?



sUASsecurity@cisa.dhs.gov

Active Deterrence



Who We Are



Proudly Public Power & Water

Created by voter initiative in 1936



97% carbon-free power supply



2nd largest public utility in Washington state



850,000 people and **20,000** businesses served



Where Everyone Feels Welcome

1,100 employees



The current way

- Intrusion prevention
 - Fences, gates, no cut etc
- Cameras
 - Monitored 24/7 (maybe)
 - Might have motion alerts, or other smart wall functions that alert staff
- Investigative
 - Scrub video and investigate after an incident occurs

It is all reactive!!



Overview of Active Deterrence Concepts

Real-time Threat Intervention

Active deterrence detects and intervenes immediately to stop unauthorized activities in real time.

Integrated Detection and Response

Combines cameras, sensors, audio warnings, and alarms to influence intruder behavior proactively.

Centralized Monitoring Benefits

Centralized teams protect many remote sites efficiently, reducing need for on-site guards.

Proactive and Preventive Security

Active deterrence shifts security from reactive to proactive, preventing incidents before damage occurs.

Why Traditional Security Measures Are No Longer Enough



Limitations of Traditional Security

Physical barriers like fences and locks only delay intruders without providing real-time monitoring or insights.

Challenges of Passive Controls

Intruders exploit blind spots and tools to bypass passive security, causing breaches discovered post-incident.

Need for Active Deterrence

Active security integrates sensors, automation, and instant response to detect abnormal activities as they occur.

Importance for Modern Utilities

Utilities must adapt security to evolving threats and regulations by deploying intelligent, real-time protection systems

Business and Security Benefits of Active Deterrence

Incident Prevention and Cost Savings

Active deterrence prevents intrusions, avoiding outages and costly equipment damage for power companies.

Regulatory Compliance and Documentation

Enhanced visibility and documentation support compliance and demonstrate proactive risk management to stakeholders.

Operational Efficiency and Safety

Faster detection and response protect grid reliability and ensure safer working conditions for personnel.

Cost Reduction and Deterrence

Active deterrence reduces reliance on guards and discourages repeat offenders at high-risk sites.

Core Technologies of Active Deterrence

Sensors, Audible/Visual Deterrence and Video Analytics

AI-Powered Video Analytics

Artificial intelligence distinguishes normal activities from threats, reducing false alarms and improving detection accuracy.

Automated Security Responses

Video analytics enable automated triggers like audio warnings and lighting without constant human supervision.

Scalable Situational Awareness

These technologies provide scalable security monitoring across multiple sites with consistent threat detection

Audio Warning Systems

Two-way speakers and live or pre-recorded voice warnings inform intruders they are monitored and command them to leave.

Visual Deterrence Lighting

High-intensity and motion-activated lighting eliminate concealment and increase intruder identification risk.

Psychological Deterrent Effect

Combined sound and light disrupt intruder behavior and reduce unauthorized activity effectively.

Benefits for Remote Sites

Deterrence mechanisms protect unmanned locations by preventing damage and minimizing need for law enforcement.

<Public>

Snohomish PUD Active Deterrence Solutions

Mobile Trailers

Deployable

Can be deployed and operational within hours of an incident.

Mobile

Can be moved from site to site as needs arise

Automated Security Response

Video analytics enable automated triggers like audio warnings and lighting

Effective

Everywhere we have deployed a trailer the issue we were dealing with stopped



Permanent Speaker/Camera Combo

Automated Security Response

Video analytics enable automated triggers like audio warnings and lighting

Customizable

Can change light pattern, voice message, response time/aggression

Lower one-time cost

Allows for a one-time cost and permanent installation

Effective

Everywhere we have deployed these the issue we were dealing with stopped



Best Practices and Implementation Considerations

Layered Defense Strategy

Combine passive and active controls to create a robust, multi-layered defense system for enhanced security.

Risk Assessment

Conduct regular risk assessments to determine best sites to install active deterrence measures.

Operator Training and Response

Train operators to interpret alerts, communicate effectively, and follow protocols

Environmental and Budget Considerations

Account for weather, sun exposure and budget when deciding on solutions



Challenges and Future Trends

Operational Challenges

Remote locations and harsh environments increase difficulties in connectivity, maintenance, and equipment reliability.

Budget

Getting money allocated to update or procure new security devices and or technologies can be challenging.

Emerging Technologies

AI, machine learning, predictive analytics, drones, and smart sensors will enhance threat detection and coverage and can be paired with active deterrence devices to create robust solutions.

The Security Program You Wish You Had

From Disconnected Data to Operational Intelligence

EVERY SECURITY LEADER
WANTS THE SAME THING

CLARITY

Know what matters. | Act with confidence. | Demonstrate your value.

EVERY SECURITY LEADER
WANTS THE SAME THING

CLARITY CONFIDENCE

Know what matters. | Act with confidence. | Demonstrate your value.

<Public>

EVERY SECURITY LEADER
WANTS THE SAME THING

CLARITY
CONFIDENCE
SPEED

Know what matters. | Act with confidence. | Demonstrate your value.

<Public>
EVERY SECURITY LEADER
WANTS THE SAME THING

CLARITY
CONFIDENCE
SPEED
VISIBILITY

Know what matters. | Act with confidence. | Demonstrate your value.

WE'VE NEVER HAD MORE INFORMATION

PHYSICAL SECURITY ASSESSMENT REPORT

Riverview 230kV Substation
Prepared for: Security Services
Date: 05/06/2024



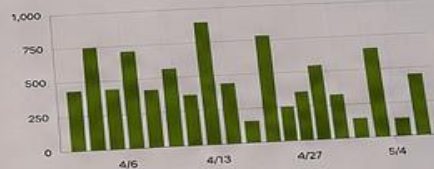
Guidehouse
Outwit Complexity

ALARM ACTIVITY SUMMARY

Substation West - Last 30 Days

2,842
Total Alarms

612
Unique Alarms



Guidehouse
Outwit Complexity

WORK ORDER SUMMARY

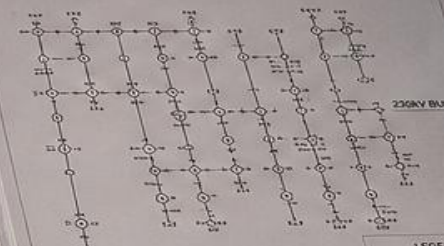
127

Open Work Orders

WO #	Priority	Type	Status
WO-240987	High	Perimeter Fence Repair	Open
WO-240912	Medium	Camera Adjustment	In Progress
WO-240655	Medium	Gate Maintenance	Open
WO-240742	Low	Lighting Outage	Open
WO-240689	High	Access Control Repair	In Progress
WO-240615	Low	Signage / Hardware	Open
WO-240509	Medium	Patrol Findings	Open

Guidehouse
Outwit Complexity

SUBSTATION ONE-LINE DIAGRAM



LEGEND	
CB	Circuit Breaker
DS	Disconnect Switch
VT	Voltage Transformer
LA	Lightning Arrester

RIVERVIEW 230KV SUBSTATION

NERC CIP-014-3¹ PHYSICAL SECURITY

Requirement R5
Physical Security Plan

Version 3.0
May 2, 2024

Guidehouse
Outwit Complexity

GIS ASSET VIEW

- Layers
- Substations
- Transmission Lines
- Access Points
- Fences
- Cameras
- Lighting
- Buildings



SECURITY PRIORITIES

- ☒ Perimeter Integrity
- ☒ Access Control Review
- ☒ Camera Coverage Gaps
- ☒ Lighting Outages
- ☒ Alarm Thresholds
- ☒ Visitor Management
- ☒ Maintenance Backlog
- ☒ Threat Intelligence

INCIDENT LOG

Recent Activity

Date / Time	Type	Location	Description	Status
5/12 06:21	Intrusion	Perimeter - Gate 7	Fence Cut Detected	Investigating
5/12 07:11	Alarm	Bldg 2	Door Forced Open	Closed
5/12 04:53	Video	Perimeter - Gate 8	Suspicious Activity	Investigating
5/11 22:18	Access	Bldg 1	Card Denied	Closed
5/11 18:44	Alarm	Bldg 1	Motion Detected	Investigating
5/11 16:05	Access	Bldg 3	Card Denied	Closed
5/11 12:52	Maintenance	Yard 2	Light Outage	Open
5/10 23:17	Alarm	Perimeter - Gate 2	Door Ajar	Closed

EVERY SYSTEM ANSWERS A QUESTION,
BUT WE STILL NEED CLARITY:
WHAT DESERVES MY ATTENTION TODAY?

CONFIDENCE COMES FROM PRIORITIZATION.

Operational intelligence evaluates every facility across criticality, threat activity, incidents, vulnerabilities, and controls to **recommend where to invest**.



ENTERPRISE RISK PRIORITIES



200
FACILITIES EVALUATED



20
RECOMMENDED FOR INVESTMENT

HIGHEST PRIORITY



RIVERVIEW SUBSTATION



RECOMMENDED IMPROVEMENTS

- ✓ PTZ Cameras
- ✓ Fence Detection
- ✓ Lighting Upgrade
- ✓ Access Control Enhancement

ESTIMATED
RISK REDUCTION



BUDGET RECOMMENDATION

FUND TOP 20 FIRST
MAXIMIZE RISK REDUCTION IMPACT

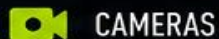
SPEED

FROM INFORMATION TO ACTION.

Operational Intelligence compresses the time between a question and an answer.



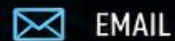
ALARMS



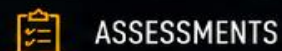
CAMERAS



GIS / MAPS



EMAIL



ASSESSMENTS



WORK ORDERS



REPORTS & DOCUMENTS

OPERATIONAL
INTELLIGENCE

DAYS. WEEKS. MONTHS.



MINUTES.

EXECUTIVE BRIEFING

TOP 5 PRIORITIES



OPEN CRITICAL ACTIONS

12

REQUIRING ATTENTION

EMERGING TREND



INCREASE IN TAILGATING
EVENTS ACROSS FACILITIES



EXECUTIVE SUMMARY

Operational risk is elevated at 3 facilities. Address top priorities to reduce exposure and strengthen posture.

VISIBILITY

GOOD SECURITY
SHOULD BE
INVISIBLE.

ITS **VALUE**
SHOULDN'T BE.

Operational Intelligence gives leaders visibility into the **health** of their security program—and **measurable** proof of the **value** it delivers to the business.



ENTERPRISE SECURITY SCORECARD

Visibility into your security program. Proof of its business value.



ENTERPRISE SECURITY HEALTH



OVERALL PROGRAM HEALTH

Enterprise Physical Security
Health Score

92%
Strong



ENTERPRISE RISK

Risk exposure reduction
vs. prior year

↓ 34%
Reduction



CRITICAL ASSETS PROTECTED

High / Critical asset coverage
with required controls

98%
Coverage



CORRECTIVE ACTIONS CLOSED

Completed within SLA

↑ 71%
Increase



CIP READINESS

Compliance posture across
applicable standards

96%
Ready



BUSINESS VALUE



SECURITY INVESTMENT EFFECTIVENESS

Risk reduction achieved
per dollar invested

3.8x
Risk Reduction



AVOIDED OPERATIONAL LOSSES

Estimated losses avoided
through risk mitigation

\$18.4M
Avoided



MANUAL HOURS ELIMINATED

Hours saved through
automation & efficiency

4,700
Hours



AUDIT PREPARATION TIME

Time to prepare for
internal / external audits

↓ 81%
Reduction



EXECUTIVE DECISION TIME

Time to turn information
into decisions

**Weeks →
Minutes**



OVERALL ASSESSMENT

The enterprise security program is reducing risk, improving resilience, increasing operational efficiency, and demonstrating measurable **business value**.



Guidehouse
Outwit Complexity

INFORMATION IS NOT INTELLIGENCE.

INFORMATION IS NOT INTELLIGENCE.

OPERATIONAL INTELLIGENCE

Intelligence begins with **context.**

ALARM
2:13 AM
Riverview
Substation

**CAMERA
OFFLINE**
Perimeter
North Gate

ASSESSMENT
Open Finding
Fire Lane
Obstruction

GIS ASSET
Substation
Riverview

EMAIL
Maintenance Team
Subject: Fence
Repair Update

INCIDENT
Report
#INC-7712
Under Review

WORK ORDER
#WO-34891
Open
24 Days

ACCESS CONTROL
Door Held Open
2 Events
This Month

TREND
Intrusion Alarms
+28%
Last 30 Days

COMPLIANCE
CIP-014 R2
Due in 45 Days

THREAT INTEL
Copper Theft
Increase
Regionally

WEATHER
Severe Storm
Expected
Tonight

KPI
MTTR
↑ 18%
This Quarter

INSPECTION
Fence Line
Overdue
17 Days

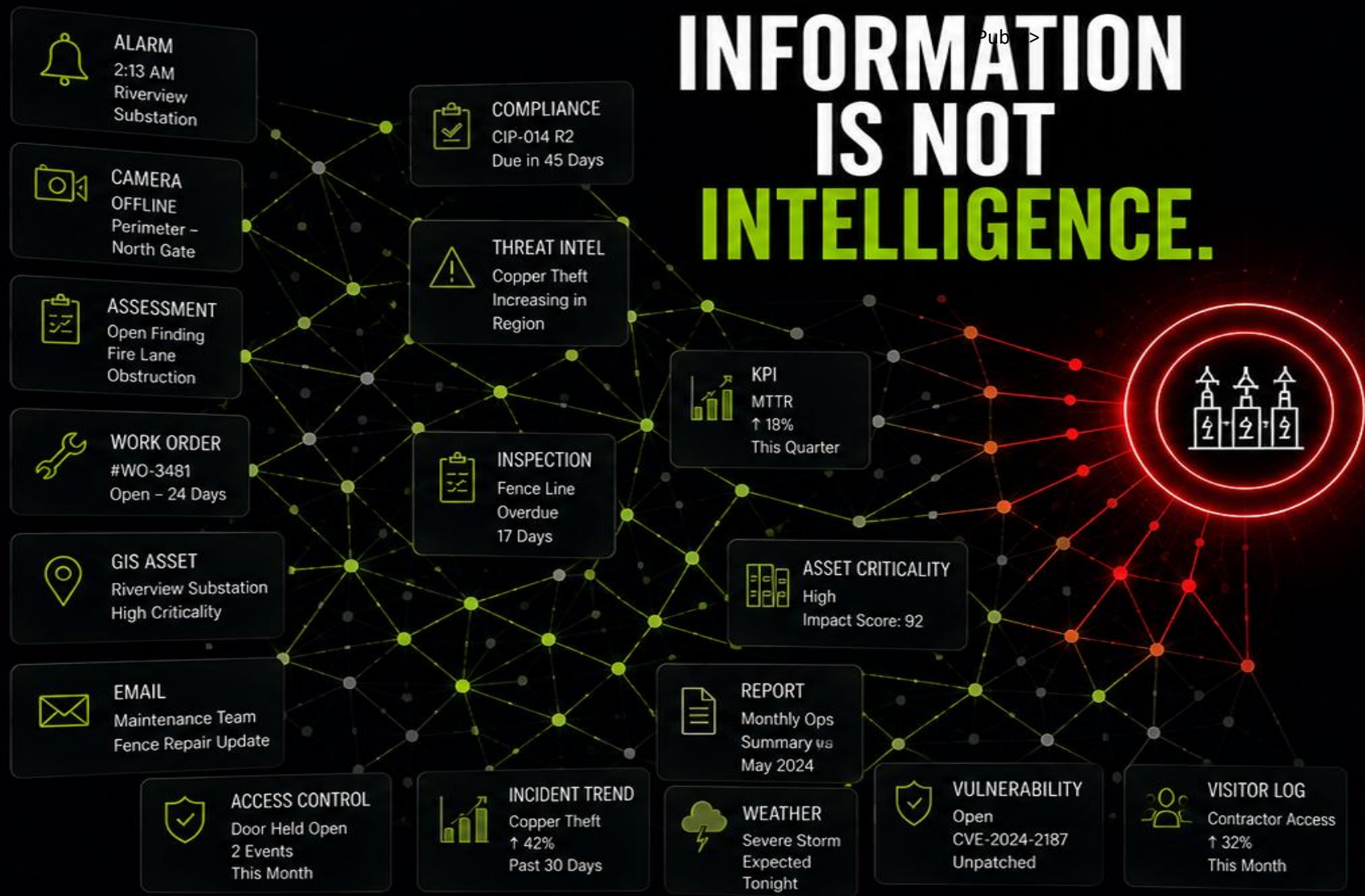
REPORT
Monthly Ops
Summary
May 2024

ASSET CRITICALITY
High
Impact Score: 92

VULNERABILITY
Open
CVE-2024-2187
Unpatched

VISITOR LOG
Contractor Access
↑ 32%
This Month

INFORMATION IS NOT INTELLIGENCE.



HIGHEST PRIORITY

RIVERVIEW SUBSTATION



ASSET PROFILE

Type: Transmission Substation
Voltage: 230 kV
Criticality: Bulk Electric
System Critical Asset
Region: Northwest

WHY THIS FACILITY

Multiple independent indicators are converging at this location, creating elevated physical security risk.

	Perimeter Security	Detection offline	●
	Corrective Actions	1 open, 24 days old	●
	Inspection Status	Fence inspection overdue	●
	Threat Environment	Copper theft increasing	●
	Asset Criticality	High consequence asset	●



INTELLIGENCE ASSESSMENT

This facility represents the greatest current physical security risk to the enterprise.

Intelligence identifies **what deserves your attention.**

THE NEXT EVOLUTION OF SECURITY ISN'T MORE SOFTWARE. IT'S **OPERATIONAL INTELLIGENCE.**



CONNECTED

Unify data from across systems,
tools, and processes.

See the whole picture.



ADAPTIVE

Tailored to your environment.
Evolves with your program
and priorities.

Always relevant.



PRACTITIONER-LED

Guided by practitioners who
understand your world.

Experience that drives results.



Technology alone can't transform a security program.
Operational Intelligence can.

IF THE TECHNOLOGY EXISTS... WHY ISN'T EVERYONE DOING THIS?

Because building Operational Intelligence
is **far more** than implementing AI.

OPERATIONAL INTELLIGENCE REQUIRES:



1. UNDERSTANDING YOUR ENVIRONMENT.

Every utility is unique.
One-size-fits-all platforms
struggle to reflect how your
organization actually operates.



2. UNDERSTANDING CONTEXT.

Every event, alarm,
or indicator means something
different depending on where,
when, and why it occurs.



3. UNDERSTANDING CONSEQUENCES.

Technology can process
information. Practitioners
understand operational
consequences.



AI can process information. But Operational Intelligence
requires technology that understands your world.

THE SECURITY PROGRAM YOU WISH YOU HAD?



CONFIDENCE

Trust your program.
Reduce risk.



VISIBILITY

See what matters.
Eliminate blind spots.



PRIORITIZATION

Focus on what drives
the most risk.



FASTER DECISIONS

Act quickly with the
right information.



EXECUTIVE INSIGHT

Communicate impact.
Drive better outcomes.



CONTINUOUS MONITORING

Always on.
Always up to date.

THIS IS WHAT WE BUILT TO MAKE IT POSSIBLE.



CONFIDENCE

Trust your program.
Reduce risk.



VISIBILITY

See what matters.
Eliminate blind spots.



PRIORITIZATION

Focus on what drives
the most risk.



FASTER DECISIONS

Act quickly with the
right information.



EXECUTIVE INSIGHT

Communicate impact.
Drive better outcomes.



CONTINUOUS MONITORING

Always on.
Always up to date.



GUSS

Guidehouse Unified Security Solution

OPERATIONAL INTELLIGENCE ENGINE



OCR & DOCUMENT UNDERSTANDING

Extracts and structures
unstructured data
with high accuracy.



RAG & CONTEXTUAL INTELLIGENCE

Understands context
and relationships to
surface what matters.



AI & ANALYTICS

Turns data into
actionable insights
and clear
recommendations.



RULES ENGINE

Applies your policies
and business rules
consistently at scale.



AUTOMATION & WORKFLOWS

Automates manual
processes and
drives efficiency.



CONTINUOUS MONITORING

Monitors changes
in real time.
Stays ahead
of risk.



INTEGRATIONS & APIS

Connects with your
existing systems
seamlessly.



SECURE BY DESIGN

Built with security,
privacy, and
compliance at
the core.



ONE UNIFIED PLATFORM. ALL YOUR DATA. END-TO-END VISIBILITY.
POWERING A SMARTER, STRONGER SECURITY PROGRAM.

WHEN SECURITY STOPS CHASING INFORMATION...

People get back to their mission.

ALARM LOGS

EMAILS

ACCESS EVENTS

REPORTS

THREAT INTEL

WORK ORDERS

COMPLIANCE DOCS

AUDIT REQUESTS

POLICIES

DATA EXPORTS

SITE REPORTS

WEATHER ALERTS

VENDOR DOCS

RISK ASSESSMENTS

CHANGE REQUESTS

TRAINING RECORDS

DAILY SUMMARIES

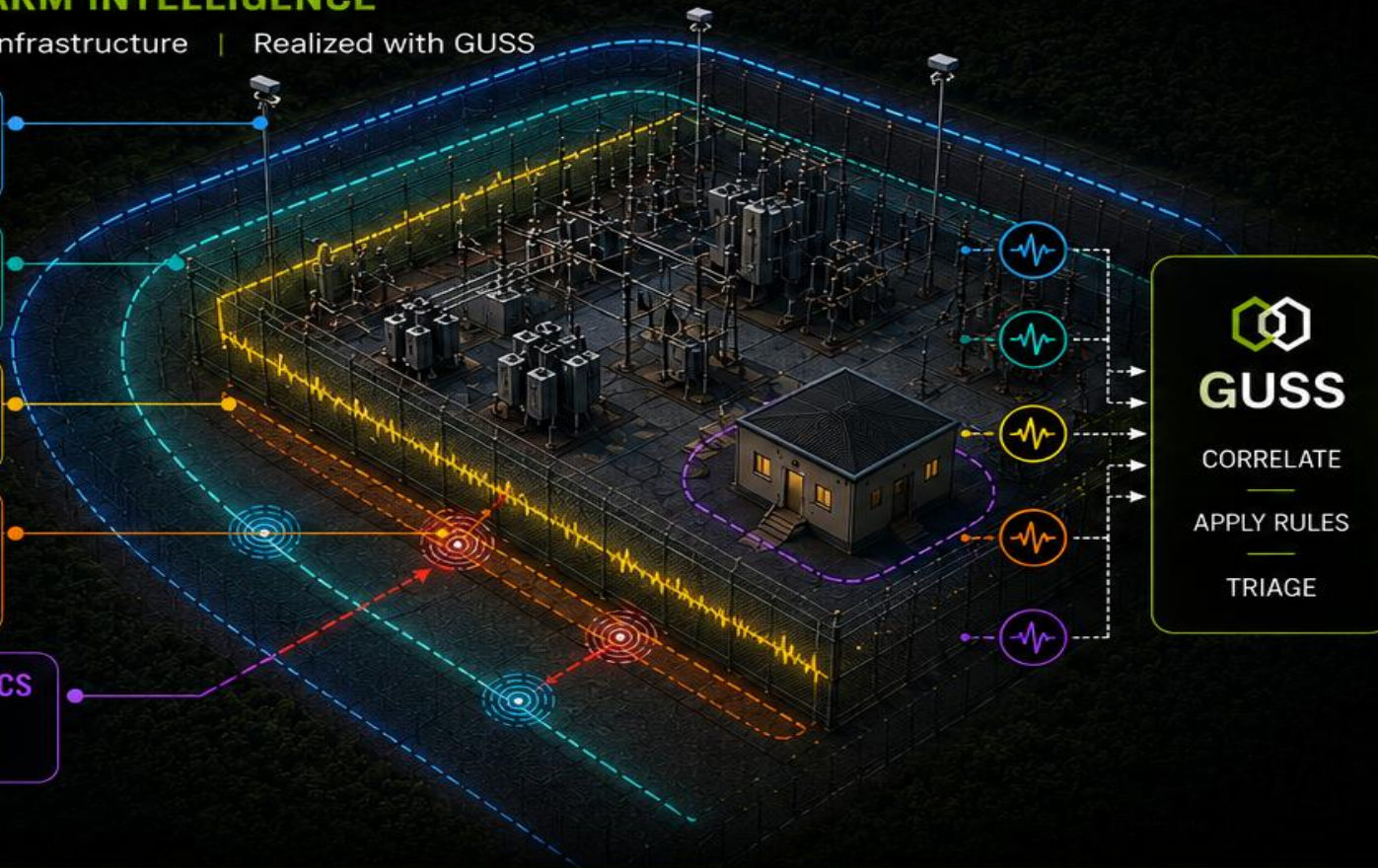
INCIDENT REPORTS

THE SYSTEMS WERE ALREADY THERE. THE INTELLIGENCE WASN'T.

PHYSICAL SECURITY ALARM INTELLIGENCE

Large Electric Utility | Existing Infrastructure | Realized with GUSS

-  **30 FT OUTSIDE FENCE**
Camera analytics detect activity ~30 ft from fence
-  **15 FT OUTSIDE FENCE**
Camera analytics detect activity ~15 ft from fence
-  **FENCE SHAKER**
Sensor in fence detects vibration / disturbance
-  **5 FT INSIDE FENCE**
Camera analytics detect activity within ~5 ft inside the fence line
-  **CRITICAL BUILDING / PACS**
Access control system & PACS alarms



 **TRACKED / SUPPRESSED**
Isolated or low-confidence activity.
Logged and available for visibility & trends.

 **No alert to SOC.**
Reduces noise.

 **ESCALATE**
Multiple indicators converge in sequence.
High-confidence meaningful activity.

 **Alert sent to Security Operations Center.**

EXAMPLE THREAT PATH →

- ① 30 FT detection
- ② 15 FT detection
- ③ Fence disturbance
- ④ 5 FT interior detection



**THE SENSORS DIDN'T CHANGE.
THE INTELLIGENCE BETWEEN THEM DID.**



REDUCES FALSE POSITIVES
& NUISANCE ALARMS



FOCUSES ATTENTION
ON REAL THREATS



IMPROVES RESPONSE
& OPERATIONAL READINESS

REAL-WORLD RESULTS

OPERATIONAL PROCESS AUTOMATION



Large Global Security Services Organization

PRODUCTION DATA | ONE REGION | ONE WEEK



HOURS AUDITED

10,008

Hours audited
automatically



BILLING ANOMALIES FOUND

\$15,377

Identified billing
discrepancies



PAYROLL ANOMALIES FOUND

\$10,985

Identified payroll
discrepancies



TOTAL VALUE SURFACED

\$26,362

Total financial impact
surfaced in one week



3-5 HOURS

Manager review eliminated
per report



REAL PRODUCTION DATA

Not a simulation.
Measured from live operations.



ONE PROBLEM **SOLVED.**

A MEASURABLE **OUTCOME.**

A FOUNDATION FOR **TRANSFORMATION.**

START WITH THE PROBLEM. BUILD AROUND YOUR ENVIRONMENT.

GUSS is the **agile** problem-solving capability in Guidehouse's security toolkit—**purpose-built**, **fast to value**, and designed to **work with what you already have**.



GUSS ISN'T HERE TO REPLACE.
IT'S HERE TO SOLVE.



FAST TO
DEPLOY



BUILT FOR
YOUR ENVIRONMENT



FOCUSED ON
OUTCOMES

1 BRING US THE PROBLEM

You know it. You live it. We've likely seen it before.



- Manual workloads
- Alarm noise & false positives
- Compliance & reporting burden
- Disconnected data & tools
- Unique operational challenges
- Something nobody has solved cleanly



Our team works with you to understand the root cause and desired outcome.

2 PURPOSE-BUILD THE RESPONSE

We configure GUSS around your environment, not the other way around.



- Use what you already have
- Integrate only what's needed
- Configure rules & logic around your operations
- Tailored dashboards & workflows
- Designed for your people
- Deployed with minimal disruption



Purpose-built. Environment-aware.
Operational from day one.

3 PROVE IT WORKS

Measure the result. Refine. Decide where it makes sense to go next.



- Measurable results quickly
- Refine based on real-world data
- Decide what to expand—and what not to
- Scale on your terms
- Continuous improvement



Prove value. Earn confidence.
Expand what makes sense.



GUSS DOESN'T REQUIRE YOUR ORGANIZATION
TO FIT THE TECHNOLOGY.
WE FIT THE TECHNOLOGY TO YOUR ORGANIZATION.



ADAPTS TO YOU
Your systems.
Your processes.
Your priorities.



WORKS WITH YOU
Your tools.
Your data.
Your teams.



DELIVERS FOR YOU
Better decisions.
Less noise.
Stronger security.



ENTERPRISE-CAPABLE.

PROBLEM-SIZED.

OUTCOME-DRIVEN.

BUILT TO DELIVER.



THE SECURITY PROGRAM YOU WISH YOU HAD IS BUILT AROUND YOU.

ALARM NOISE

MANUAL REVIEW

COMPLIANCE
BURDEN

DISCONNECTED
SYSTEMS

REPORTING
BACKLOG

RISK
PRIORITIZATION

FALSE POSITIVES

DATA SILOS

RESOURCE
CONSTRAINTS

WHATEVER
COMES NEXT



CLARITY.

See what matters.
Cut through the noise.



CONFIDENCE.

Make better decisions.
Defend your program.



SPEED.

Respond faster.
Stay ahead of risk.



VISIBILITY.

One view of what's happening.
Across your environment.

PURPOSE-BUILT TECHNOLOGY. | PRACTITIONER-LED EXPERTISE. | BUILT AROUND YOUR ENVIRONMENT.



Guidehouse
Outwit Complexity



BRADY PHELPS

Associate Director



bphelps@guidehouse.com



480.349.8262



NICK WEBER

Director



nweber@guidehouse.com



208.310.3398

WECC POWER SYSTEM
SECURITY CONFERENCE

15

<Public>



WECC CONFERENCE • PHYSICAL SECURITY

From Assessment to Evidence

How PG&E measures physical security effectiveness under CIP-014

Gary L. King, CPP • PSP • CISA
Gary.King2@pge.com

Why sites need a Security Program

These are the stations the grid cannot absorb losing. The assets are custom-built, so the consequence is measured in months of degraded transmission, not hours.

NERC CIP-014 — PURPOSE

To identify and protect Transmission stations and substations, and their associated primary control centers, that if rendered inoperable or damaged by a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

<Public>

Critical Asset Exposure

Transformers, bushings, and switchgear are custom-built and slow to replace — a single loss can be crippling.

Copper & Material Theft

Copper grounding, tooling, and stored materials are frequent, recurring targets.

Deliberate Attack

Ballistic and forced-entry attacks on grid assets are a documented threat (e.g., the 2013 Metcalf substation shooting).

Intrusion & Trespassing

Unauthorized access risks safety incidents, sabotage, and vandalism.

THE FRAMEWORK

A Risk-Based Framework

We measure risk, then invest where it makes sense — not everywhere equally.



Where controls matter: security measures lower **vulnerability** by strengthening the **Detect → Delay** → **Respond** chain, and lower **consequence** through hardening and enhancing resilience.

THE WORKFLOW

The End-to-End Workflow

From site capture to justified investment — each step builds on the shared digital model.

1

Digital Twin Capture

Survey-grade 3D model

2

Baseline Assessment

Current controls – set
baseline score

3

Ballistic Line-of-Sight

Sightlines to assets

4

Blast & Standoff

Overpressure vs. distance

5

Camera Coverage

View-shed & task-based
CCTV

6

Sensors & Barriers

Selection & placement

7

Post Controls ASD

Re-run – measure effect

8

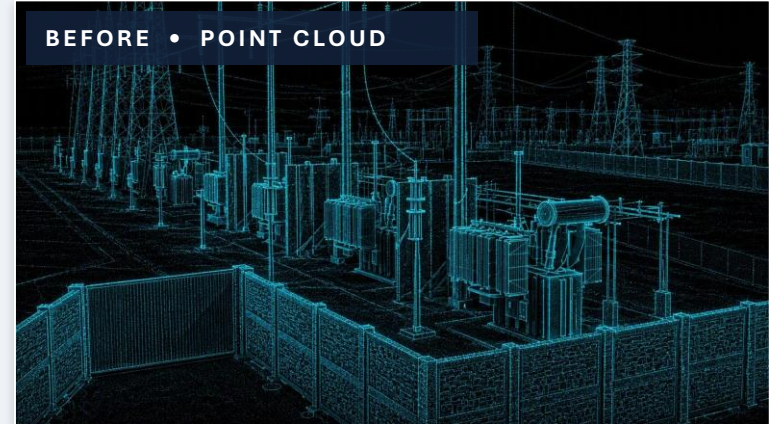
Risk & Cost

Quantify and justify

STEP 1

Capturing a Digital Twin of the Site

- A survey-grade 3D model of the whole Substation — terrain, structures, equipment, fence lines, and surroundings.
- Captured with drone photogrammetry and LiDAR laser scanning, fused into one measurable point cloud and mesh (illustrative accuracy $\pm 2\text{--}3\text{ cm}$).
- Becomes the single source of truth every later assessment runs on — no repeated site visits or guesswork.
- Safe to analyze off-site: sensitive testing happens in the model, not in the energized yard.



THE METHOD

Every Analysis Runs Twice

Measure the site as it stands, then measure the design — so improvement is evidence, not assertion.

THE FIVE INSTRUMENTS MEASURED IN BOTH PASSES

Ballistic Line-of-Sight

Site Exposure Index 0–100

Blast & Standoff

Assets in the severe zone

View-Shed & Cameras

Blind spots, pixel density

Barriers & Delay

Delay minutes per layer

Deterrence & Response

Lighting, signage, patrols

Every instrument feeds the 5 D Site Score — the site's single 0.0 – 5.0 number of record, measured the same way twice.

BASELINE RUN

Measure the site exactly as it stands today.

- No credit for controls that are proposed but not installed.
- Produces the score of record — the number every later claim is measured against.
- Exposes where the site actually is, not where we believe it is.



DESIGN RUN

Re-run the identical analysis with the proposed controls in the twin.

- Same model, same metric, same method — the only variable is the control.
- The difference is therefore attributable to the control, not to a changed assumption.
- Lets us rank options by risk reduced per dollar before anything is bought.

STEP 2 • MEASUREMENT

The 5 D's: One Score for Site Capability

Every critical site is scored against five defensive layers — each worth 0.0–1.0, summing to a 0.0–5.0 Site Score.

DETER

Discourage the attempt before it starts

Lighting, signage, visible cameras, guard presence, warning systems

DETECT

Recognize an intrusion as it happens

Intrusion detection, motion sensors, CCTV monitoring, access-control logs

DENY

Physically prevent entry to secure areas

Reinforced doors, barriers, turnstiles, card readers, secure perimeters

DELAY

Slow the intruder so response can arrive

Layered fencing, ballistic walls, controlled access points

DEFEND

Neutralize the threat once layers are breached

Rapid response teams, law-enforcement coordination, advanced technology

Site Score = Deter + Detect + Deny + Delay + Defend — a 0.0–5.0 capability value. The mean of all critical sites becomes the KPI.

Framework applied at the most critical Electric, Gas, and Power Generation locations.

STEP 2 • BASELINE TVA

The Threat & Vulnerability Assessment

A structured field and model review of every critical site — the assessment that sets the baseline score before any control is designed.

WHAT THE ASSESSMENT EXAMINES

Threat Assessment

Who would target this site, with what capability and intent — sabotage, ballistic attack, copper theft, trespass.

Vulnerability Assessment

Where the site is open: facility design, access control and badge gaps, camera and detection coverage.

Risk Analysis

Likelihood the threat is attempted against the consequence if it succeeds, weighted by site tier.

THE OUTPUT

Every finding is scored against the five defensive layers:

-  **Deter**
-  **Detect**
-  **Deny**
-  **Delay**
-  **Defend**

Baseline Site Score 0.0 – 5.0

Assess first, then score: the TVA gathers the evidence — the 5 D model on the next slides turns it into a number we can track and re-measure.

STEP 3 • IN DEPTH

Mapping Every Line of Fire

Ray-trace every off-site vantage point against the transformer bank — quantify exactly what a shooter can see, and hit.



Ground view — the full bank in one clear sightline.



Ray-traced — magenta marks surfaces with a clear off-site shot.

51.3

SITE EXPOSURE INDEX
SEVERE RISK

Several transformers sit in the highest-exposure band
Targeted ballistic barriers cut modeled exposure 74% on this site

STEP 3 • THE BETTER OPTION

Barriers Cut the Line of Fire

~180 linear ft of ballistic barrier shields the transformer bank's sightlines — modeled exposure falls 74%, from Severe to At Risk.



Before — the full bank exposed in one clear line of fire.



After — a ballistic steel barrier screens the bank's line of fire.

51.3

BEFORE
SEVERE



13.3

AFTER
AT RISK

STEP 4 • BLAST & STANDOFF

Blast Footprint: Hand-Thrown Charge

A handheld charge thrown over the perimeter wall — far tighter than a vehicle-bomb footprint.



Illustrative hand-thrown charge on the current site twin (●); damaging overpressure falls off within tens of feet, so equipment nearest the wall is most exposed. Fragmentation may reach beyond the Severe zone.

Damage zones — hand-thrown charge

- Severe • < 20 ft**
- Serious • 20–40 ft**
- Moderate • 40–75 ft**

MITIGATION PRIORITIES

- Raise or extend the perimeter wall to defeat lob-over throws.
- Set critical equipment back from the wall, beyond the Severe zone.
- Add wall-line intrusion detection and camera coverage.

STEP 4 • BLAST & STANDOFF

Blast: Standoff After Hardening

The same hand-thrown charge, re-run against the hardened perimeter — the design pushes every critical asset out of the severe zone.

MEASURE	BASELINE	AFTER DESIGN
Perimeter wall height	8 ft	12 ft + anti-lob crown
Critical assets in severe zone	4	0
Nearest asset standoff	14 ft	55 ft
Wall-line intrusion detection	none	full perimeter
Assessment coverage at wall	partial	every alarm assessed

4 → 0**ASSETS IN THE SEVERE ZONE**

WHAT CHANGED THE RESULT

Raising the wall

defeats the lob-over throw that set the baseline footprint.

Setting equipment back

moves critical assets beyond the severe overpressure band.

Detection at the wall line

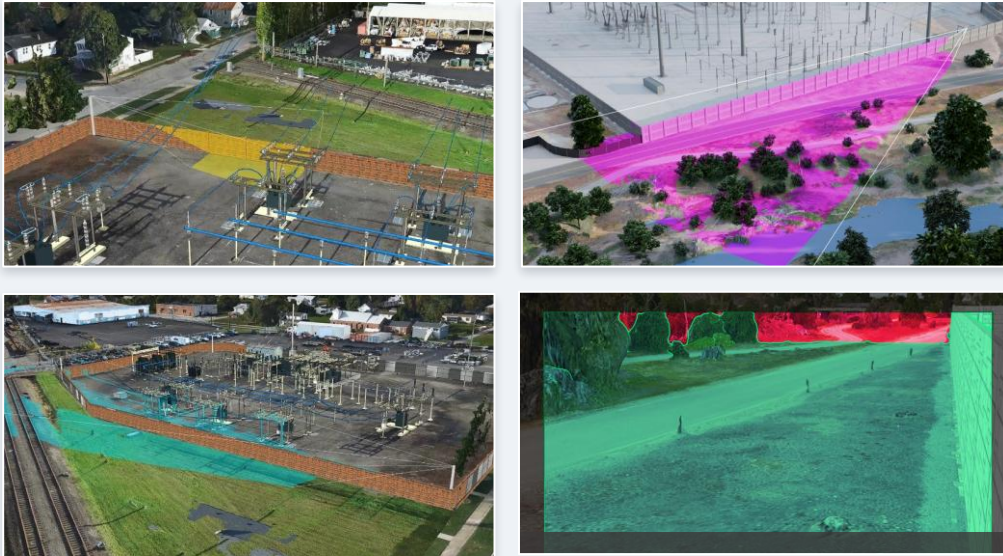
means the approach is seen before the charge is thrown.

Illustrative design-run figures on the same site twin; fragmentation may still reach beyond the severe band and is handled by setback and shielding.

STEP 5 • CAMERA COVERAGE

View-Shed Analysis

Model each camera's real-world coverage in the twin — close blind spots and hold pixel density where it matters.



Illustrative camera-coverage view-sheds. Each colored footprint is one camera's field of view; warm-to-cool bands show pixel density (DORI, EN 62676-4) falling with distance — revealing gaps and where identify-grade density runs out.

What the view-shed reveals

- Simulate every camera's field of view in the digital twin.
- Expose blind spots and overlap gaps across the perimeter and yard.
- Flag where range outruns DORI — detection-only where identify-grade is required.
- Pair fixed cameras (assess) with PTZ (follow); hold defender sightlines, deny outsiders theirs.

Barrier Selection & Placement

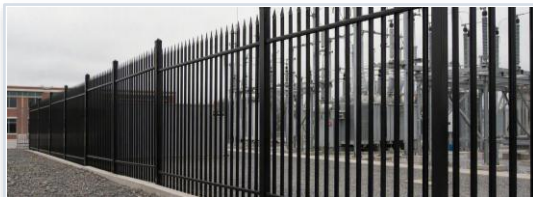
Standard barrier types, ordered by relative delay contribution



Tight-weave chain link

7 ft fabric + top guard

Est. delay: ~1-2 min



Ornamental palisade

8-12 ft welded pales

Est. delay: ~2-4 min



Expanded metal mesh

8-10 ft anti-climb / anti-cut

Est. delay: ~3-5 min



Reinforced concrete wall

12 ft precast, Tier 1 primary

Est. delay: ~5-8 min



Anti-dig barrier

24-30 in slurry or buried

Est. delay: +3-5 min to dig under



M30 / K4 ram-resistant gate

Stops 15,000 lb at 30 mph

Est. delay: ~5-8 min forced entry

Delay values are illustrative industry estimates, not published ratings — the standard does not publish delay values. Delay only counts after detection and under assessment.

STEP 6 • SENSORS & BARRIERS

Selecting Sensors and Barriers

Every layer gets the sensor that sees the breach and the barrier that holds it — selected and timed in the twin.

LAYER	SENSOR SELECTED	BARRIER SELECTED	DELAY
Approach	Ground radar, video analytics	Lighting and signage only	—
Perimeter fence	Fence-line fiber, thermal	12 ft wall, anti-lob crown	+4 min
Outer yard	Volumetric microwave	Interior fence, bollards	+3 min
Hardened door	Door contacts, duress switch	Ballistic door and louvers	+9 min
Critical asset	Asset vibration sensors	180 ft ballistic barrier	+5 min

21 MIN

TOTAL STACKED DELAY

SELECTION CRITERIA

Detect at the first layer

Delay before the alarm buys nothing, so sensing starts at the fence.

Rate barriers by breach time

Each layer is timed against hand and tool attack, not rated by material.

Place both in the twin

Coverage and barrier runs are modeled and timed before procurement.

Illustrative sensor and barrier selections on the same site twin; the delay ratings feed the adversary sequence later in the deck.

STEP 7 • POST-CONTROL ASD

Adversary Sequence Diagrams

The design run — time every layer, and one comparison decides it: who gets there first.

THE TIME RACE — DETECTION STARTS THE CLOCK, STACKED DELAY HAS TO OUTLAST IT



Detection

T+4 MIN • CLOCK STARTS

Sensors and camera assessment confirm the intruder at the fence. Delay before this point buys nothing.

Delay

17 MIN • BEYOND DETECTION

Detection at the fence starts the clock, so only the 3 – 9 – 5 stack beyond it counts against response.

Response

ON SITE T+19 • 2 MIN MARGIN

Dispatch begins at detection. The adversary needs T+21, so interruption happens first.

THE DECISION

Baseline vs. Post-Control Scorecard

Every instrument, re-measured on the same model — one page to approve the package on.

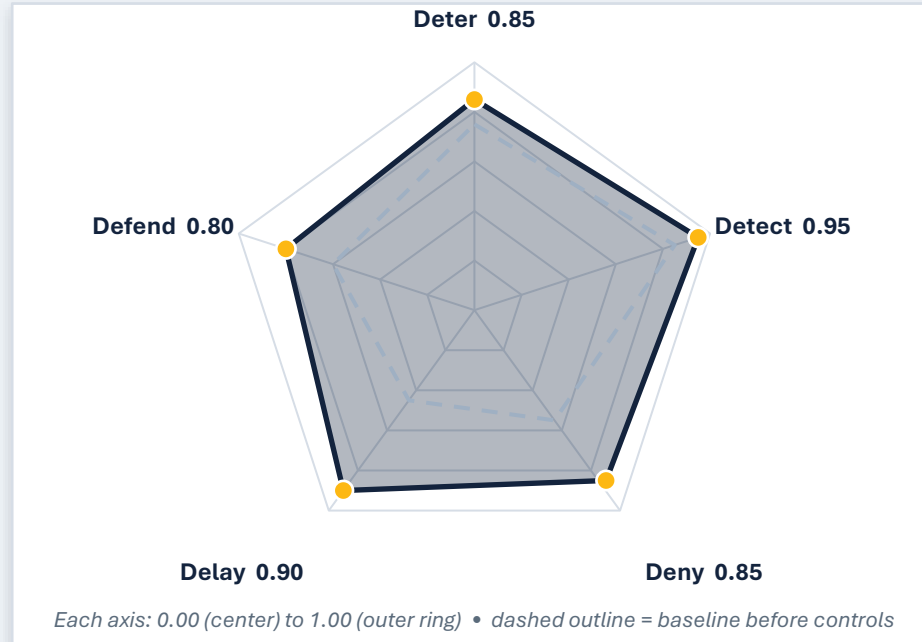
MEASURE	BASELINE	AFTER CONTROLS	CHANGE
Site Exposure Index	51.3	13.3	-74%
5 D Site Score (of 5.00)	3.20	4.35	+1.15
Probability of interruption P(I)	0.35	0.85	+0.50
Assets inside severe blast zone	4	0	-4
Perimeter blind spots	6	0	-6
Annualized Loss Expectancy	\$0.96M	\$0.30M	-\$0.66M / yr

Same model, same metric, same method. The only variable between these two columns is the control package — which is what makes the improvement defensible.

THE OUTCOME • 5 D SITE SCORE

Site Score After Controls: Tier 1 Substation

The same representative substation, re-profiled across all five layers with the modeled controls in place.



4.35

SITE SCORE • UP FROM 3.20 BASELINE

READING THE OUTCOME

Delay is no longer the weak axis.

The barrier stack lifts Delay from 0.45 to 0.90 — the single largest gain on the profile.

Detection now has time to matter.

With 21 minutes of stacked delay, response arrives first; P(I) moves from 0.35 to 0.85.

The profile is balanced, not spiked.

Every axis now scores 0.80 or better, and modeled exposure falls from 51.3 to 13.3.

Illustrative post-control profile for a representative Tier 1 site; scores are examples pending assessment data.

Quantifying and Justifying the Investment

The same before-and-after figures that prove the risk came down also put a price on it.

$$\text{Risk} = P(\text{attack}) \times P(\text{success} \mid \text{attack}) \times \text{Consequence}$$

- Risk falls when controls raise the probability of interruption — P(I) moves 0.35 to 0.85 and modeled exposure falls 74%.
- Consequence is estimated in dollars and downtime; likelihood comes from threat intelligence.
- Annualized Loss Expectancy = annual likelihood × consequence, so the benefit is the reduction in ALE.
- Rank projects by Cost-Benefit Ratio — avoided loss per dollar — and sequence them into a roadmap.

	Baseline	After controls
Annual likelihood	8%	2.5%
Consequence	\$12M	\$12M
ALE	\$0.96M	\$0.30M

*Illustrative — ~\$0.66M/yr in avoided loss against ~\$0.14M/yr amortized control cost: a **Cost-Benefit Ratio near 4.7×**.*

VALIDATE • AFTER DEPLOYMENT

Proving It in the Real World

Everything up to this point is modeled. Penetration testing is the only pass that produces measured evidence.

Sensor defeat

Attempt to cross the perimeter without raising an alarm — crawl, bridge, mask, and tailgate against live detection.

Response-force drill

Time a real dispatch against the modeled response window the adversary sequence assumed.

Barrier breach

Attack each barrier layer by hand and by tool; record actual delay against the rated delay.

Access & social engineering

Probe credentials, gate procedure, and control-house access — the paths that need no tools at all.

WHAT THE RESULTS CHANGE

Modeled scores become measured results.

Detect, Delay and Defend are re-scored on observed performance, not design intent.

Findings open the next assessment.

Every gap found becomes a line item in the following TVA — the loop closes and starts again.

Assess → design → re-run → deploy → test → re-assess. Penetration testing is what turns the 5 D score from a design estimate into an operating KPI.

IN CLOSING

Key Takeaways

1

Start with one accurate model The digital twin is the foundation every assessment and design decision relies on.

2

Test threats virtually Ballistic, blast, and view-shed analysis expose exposure before spending on hardware.

3

Let path analysis drive design Adversary sequence diagrams place sensors and barriers where they change the outcome.

4

Design coverage to the task Camera and sensor layouts are validated in the model — no blind spots, real overlap.

5

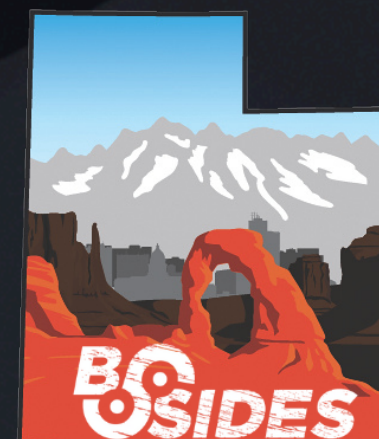
Quantify to justify Measured risk reduction and avoided loss turn security into a defensible investment.

Smart Buildings, Dumb Protocols

How to hack (and defend) your ICS/OT networks

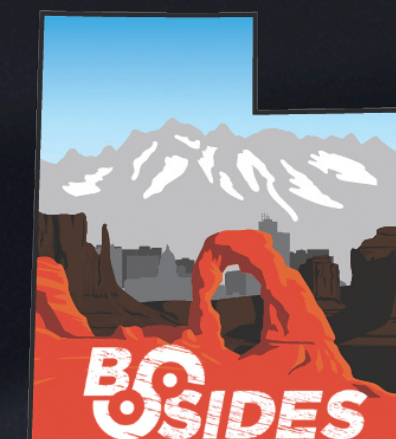
Who Are We?

- Technical Marketing Engineer
@Corelight
- Threat Hunter
@Black Hat NOC
- Board Member
@Utah Cybersecurity Society
- Organizer/Volunteer
@DC435, @SAINTCON



Who Are We?

- Sr. Director of Security Product Research & TME
@Corelight
- NOC Lead
@Black Hat
- Volunteer
@SAINTCON, @BSidesSLC, @BSidesCache
- Organizer
@DC435



Smart Buildings

- Current state of smart facilities
- Common attack vectors

Dumb Protocols

- Walkthrough of a simulated attack
- Debrief and evidence exploration

ICS/OT Landscape

- IT and OT Overlap
- Legacy Infrastructure
- Increased Demand for Remote Access
- APTs and AI
- Regulation
- Regulation?

Vulnerabilities and Causes

- Insecure protocols that are unencrypted
- Flat networks, guest Wi-Fi
- Exposed services and weak authentication
- Little to no network visibility
- Old or unpatched software and firmware
- Old and assumed air-gapped environments
- Lack of time and money
- Convenience and lack of experience
- Siloed environments and lack of money
- EOL hardware, EOL apps, and default configurations

Network Visibility

- Identify weak protocols
- Know what devices are on your network
- Verify that all your remote access is authorized and secure
- Identify recon before it becomes an incident
- Have better assessments “when” you have an incident

Lab Environment

- Lab Guide
- Navigation
- Screen

The screenshot displays the Corelight SmartBuild lab environment interface. The top navigation bar includes the Corelight logo, the text "Smart Buildings, Dumb Protocols", and a "Lab Guide" button. Below the navigation bar, the interface is split into two main panels. The left panel, titled "Lab Guide", contains a list of ten parts: "Part 1 - Getting Oriented", "Part 2 - Default Credentials and Credential Spray", "Part 3 - SQL Injection", "Part 4 - Privilege Escalation", "Part 5 - Command Injection", "Part 6 - Directory Traversal", "Part 7 - Building OT Baseline: BACnet Discovery and Modbus Override", "Part 8 - Power OT: Utility Gateway and Switchgear Protocols", "Part 9 - Power OT: Microgrid PLC, MQTT, S7, and OPC UA", and "Part 10 - Summary". The right panel displays the SmartBuild login screen, which includes the "SmartBuild" logo, the text "BUILDING MANAGEMENT SYSTEM", a "Username" field, a "Password" field, and a "Sign In" button. At the bottom of the right panel, the text "SmartBuild BMS v3.2.1 // Unauthorized access prohibited" is visible.

corelight  Smart Buildings, Dumb Protocols [Lab Guide](#)

 BMS Portal •  Terminal •  Splunk •  Corelight Fleet Manager (sign in with Cyberlab SSO) •

 Lab Guide — drag edge to resize

Work through each part in order. Click a header to expand it. Mark done as you go.

- 1 Part 1 - Getting Oriented
- 2 Part 2 - Default Credentials and Credential Spray
- 3 Part 3 - SQL Injection
- 4 Part 4 - Privilege Escalation
- 5 Part 5 - Command Injection
- 6 Part 6 - Directory Traversal
- 7 Part 7 - Building OT Baseline: BACnet Discovery and Modbus Override
- 8 Part 8 - Power OT: Utility Gateway and Switchgear Protocols
- 9 Part 9 - Power OT: Microgrid PLC, MQTT, S7, and OPC UA
- 10 Part 10 - Summary

SmartBuild
BUILDING MANAGEMENT SYSTEM

Username

Password

[Sign In](#)

SmartBuild BMS v3.2.1 // Unauthorized access prohibited

BMS Portal

- See the current status of your buildings
- Look at each tab
- Fix/break things
- Don't cause a nuclear meltdown
- Use the lab guide for help as needed

BMS Portal • **>_ Terminal** • **Splunk** • **Corelight Fleet Manager (sign in with Cyberlab SSO)**

SmartBuild SCADA
BUILDING MANAGEMENT SYSTEM

Dashboard

Process Ctrl

Sensor Search

Diagnostics

User Mgmt

FACILITY

SmartBuild Tower

Municipal Water Authority

Clearwater Power Station

Natanz Enrichment Facility

Building Overview Live 8:44:10 PM

HVAC System Fan 45%

Chiller Compressor 1000 RPM

Fire Pump 0 PSI

Generator Standby

Access Control 7 doors monitored

Lighting 6 zones active

FLOOR PLAN

SMARTBUILD TOWER — CROSS SECTION

Roof — Mechanical	85.3°F
Floor 4-5 — Executive / Data Center	71.0°F
Floor 3 — Labs	73.0°F LOCKED
Floor 2 — North Wing	71.5°F OPEN
Floor 1 — Lobby / Offices	72.0°F OPEN

CHILLER COMPRESSOR

1000 RPM

Compressor RPM

Discharge PSI **185** Suction Temp **42 °F**

FIRE PUMP **OFF**

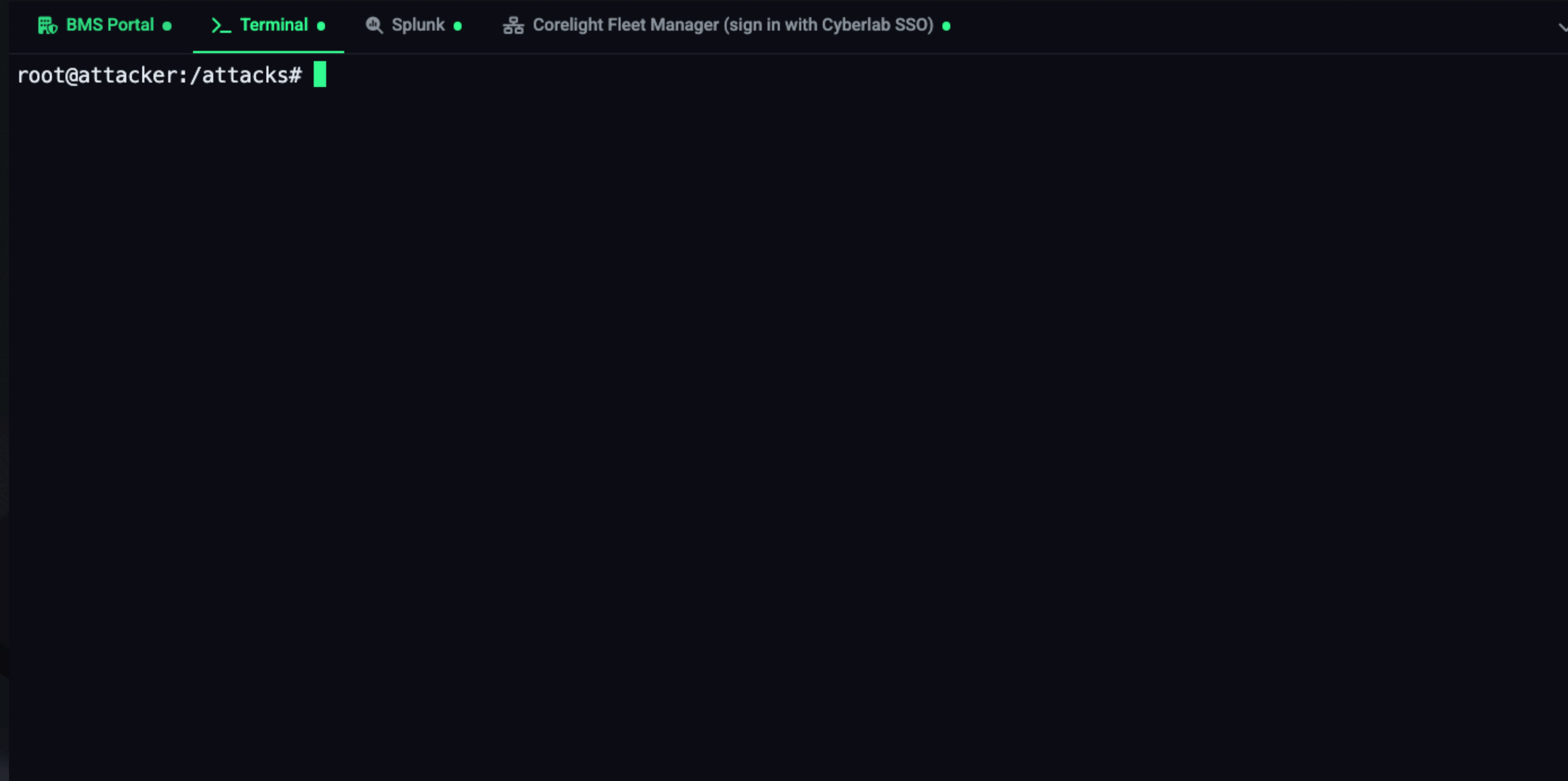
PUMP PRESSURE **0** PSI

GENERATOR **STANDBY**

Sign Out

Terminal

- Full Linux box
- Connected to BMS network
- Has attacker's scripts, code, and other goodies
- Used to run attacks
- 1s to get started
- Tab will reset
- Use the lab guide for help as needed



Splunk

- Search for network logs
- Find evidence of attacks
- Use the lab guide for help as needed

The screenshot displays the Splunk web interface. At the top, the navigation bar includes links for BMS Portal, Terminal, Splunk, and Corelight Fleet Manager. The main navigation menu features Search, Analytics, Datasets, Reports, Alerts, Dashboards, and Modules. The Search & Reporting section is active, showing a 'New Search' interface. A search query '*' is entered in the search bar, and the time range is set to 'Last 60 minutes'. The search results show 36,945 events from 8/12/26 1:56:00.000 AM to 8/12/26 2:56:49.000 AM. The results are displayed in a table format, showing the Time and Event details. The table has columns for Time and Event. The first row shows the time 8/12/26 2:56:46.903 AM and the event details: { [-] _path: modbus_detailed, _system_name: sensor.turquoisestarling-1.cyberlab.trycorelight.com, _write_ts: 2026-08-12T02:56:46.903018Z, func: READ_COILS, id.orig_h: 172.20.0.6, id.orig_p: 41146, id.resp_h: 172.20.0.2, id.resp_p: 502, is_orig: false, quantity: 8. The interface also includes a sidebar with 'SELECTED FIELDS' (host 1, source 4, sourcetype 41) and 'INTERESTING FIELDS' (address 4, dest 12, dest_ip 12, dest_port 12).

BMS Portal • >_ Terminal • Splunk • Corelight Fleet Manager (sign in with Cyberlab SSO) •

splunk>enterprise Apps ✓ corelight 1 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Modules Search & Reporting

New Search SPL Convert to SPL2 Save As Create Table View Close

* Time range: Last 60 minutes Q

✓ 36,945 events (8/12/26 1:56:00.000 AM to 8/12/26 2:56:49.000 AM) No Event Sampling Job

Events (36,945) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect 1 minute per column

Format Show: 20 Per Page View: List 1 2 3 4 5 6 7 8 ... Next

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 4
- a sourcetype 41

INTERESTING FIELDS

- # address 4
- a dest 12
- a dest_ip 12
- # dest_port 12

i	Time	Event
>	8/12/26 2:56:46.903 AM	{ [-] _path: modbus_detailed _system_name: sensor.turquoisestarling-1.cyberlab.trycorelight.com _write_ts: 2026-08-12T02:56:46.903018Z func: READ_COILS id.orig_h: 172.20.0.6 id.orig_p: 41146 id.resp_h: 172.20.0.2 id.resp_p: 502 is_orig: false quantity: 8

Splunk

- Each log contains key information
- Log type (path)
- Source and destination IPs/ports
- Post bodies
- Status codes

BMS Portal • Terminal • Splunk • Corelight Fleet Manager (sign in with Cyberlab SSO) •

< Hide Fields All Fields Format Show: 20 Per Page View: List < Prev 1 2 Next >

	i	Time	Event
<code>a vendor_action 2</code> <code>a vendor_product 1</code> <code># version 1</code> <code>a write_ts 28</code> 5 more fields + Extract New Fields	>	8/12/26 3:15:23.678 AM	<pre>{ [-] _path: http _system_name: sensor.turquoisestartling-2.cyberlab.cycorelight.com _write_ts: 2026-08-12T03:15:23.678248Z dest_host: nginx id.orig_h: 172.20.0.2 id.orig_p: 36844 id.resp_h: 172.20.0.7 id.resp_p: 80 method: POST orig_fuids: [[+]] orig_mime_types: [[+]] post_body: {"username": "root", "password": "root"} request_body_len: 40 resp_fuids: [[+]] resp_mime_types: [[+]] response_body_len: 47 status_code: 401 status_msg: Unauthorized tags: [[+]] trans_depth: 1 ts: 2026-08-12T03:15:23.676499Z uid: CbEOfK38NL07ozWsc6</pre>

Splunk

- Search for specific variables
- Search by source IP
- Create dashboards...

The screenshot displays the Splunk search results interface. On the left, a list of fields is shown, with 'a status_msg 2' highlighted. The main panel shows search results in a table format. The first result is a JSON object with fields like 'version', 'host', and 'sourcetype'. The second result is a simple event with 'Time' as '8/12/26' and 'Event' as '{ [-]'.

A modal window titled 'status_msg' is open, showing a summary of the field's values. It indicates '2 Values, 100% of events' and provides options to 'Yes' or 'No' for selected values. The modal also includes a 'Reports' section with links for 'Top values', 'Top values by time', and 'Rare values'. Below this, a table lists the values and their counts and percentages.

Values	Count	%
Unauthorized	19	65.517%
OK	10	34.483%

The modal window also features a close button (X) in the top right corner.

Let's Get Started

- Visit ics.trycorelight.com
- Look at the lab guide on the left to get started.

So What Now?

- Zeek
 - Suricata
 - WireShark
 - TCPDump
-
- Identify every device on your network.
 - Look at all your network logs.
 - See what goes over the wire in plain text.
-
- Volt and Salt CTF



Using AI to Address Security Risks in Integrated IT/OT Systems

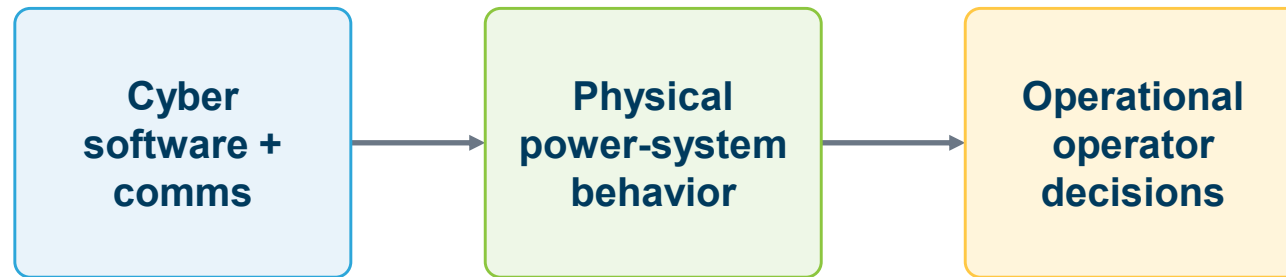
Cyberphysical security for substation SCADA and digital substations

Dr. Jonathan M. Tacke, EIT
Idaho National Laboratory
Power Systems Security Conference | August 2026



The core security problem

The grid is no longer just connected. It is tightly coupled.



A disturbance in software, communications, or automated control can propagate into physical impacts on the grid.

System operators must reason across all three domains to respond to anomalous events

Roadmap



Goal
shift from alarms to defensible context

Constraint
AI must be modular, testable, and initially advisory

Result
operators get a single narrative that merges cyber and electrical evidence

Digital Substations Shift the Boundary

Digital Substation

Time-synchronized measurements + device status + logs

Process bus
IEDs, relays, merging units,
PMUs

Substation bus
RTACs, virtualized apps, cyber
tools

Boundary
firewalls, routers, gateways

Operations
center
SCADA / EMS /
SOC

Ethernet-based OT network

Security implication:

The same integration that improves visibility also creates new paths for cyber compromise and misinterpretation.

Integration expands the defender's job

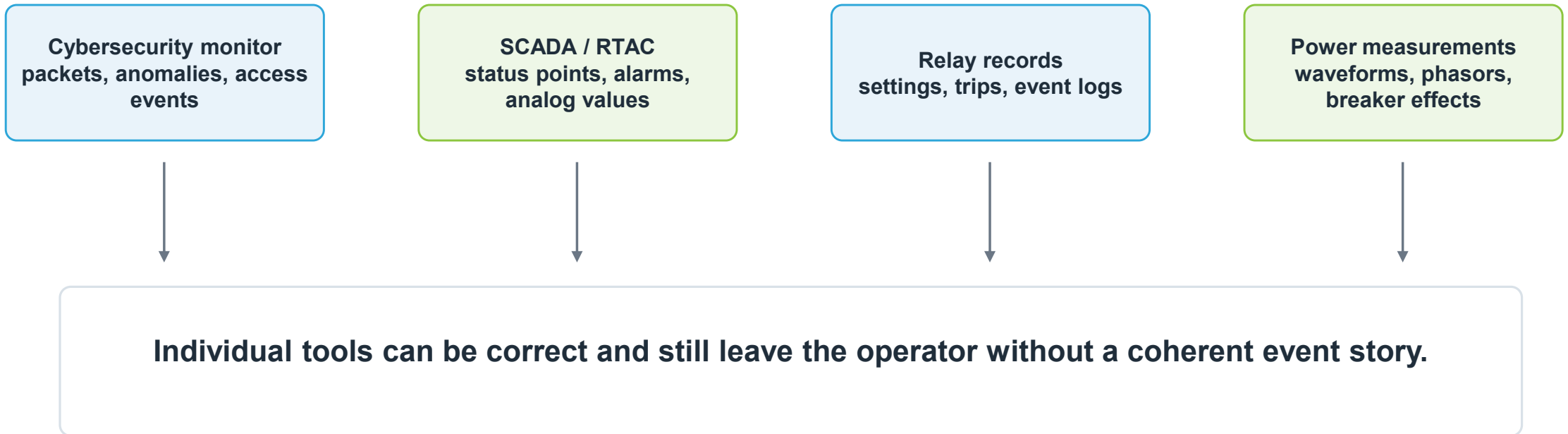
Two disciplines now share one operational consequence space.



- Digital control enables smarter operations but raises the cost of being wrong.
- A cyber alert without physical context is often ambiguous.
- A physical alarm without cyber context can miss intent and cause.

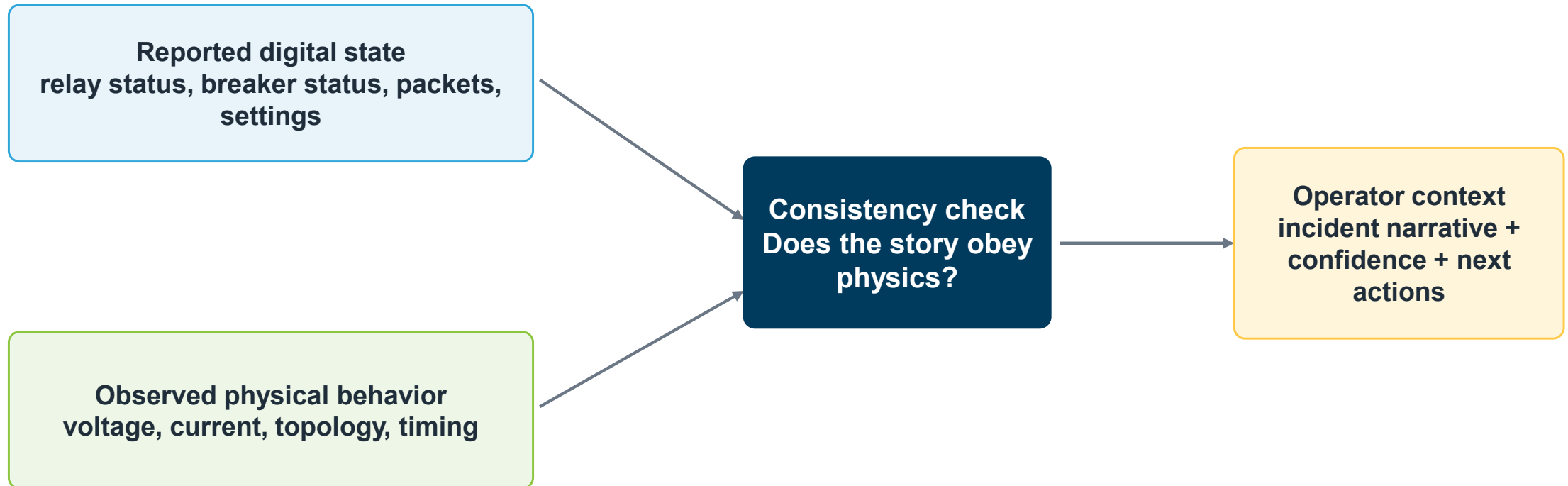
The security task becomes correlation, not just detection.

Why siloed monitoring is not enough



Typical result: valuable data is stitched together during post-event analysis, after the response window has passed.

Physics is a security signal



This is especially useful for subtle attacks: sensor spoofing, false data injection, malicious settings changes, latent supply chain compromise, and Living Off the Land behavior.

MSO: a digital substation overseer

A practical goal: the next best thing to a skilled operator in every substation.

Monitor. Validate. Explain. Escalate.

Oversight, not replacement

MSO oversight layer

observes existing systems, validates behavior, creates event records, and communicates context to operators

Existing substation systems

Relays

RTAC

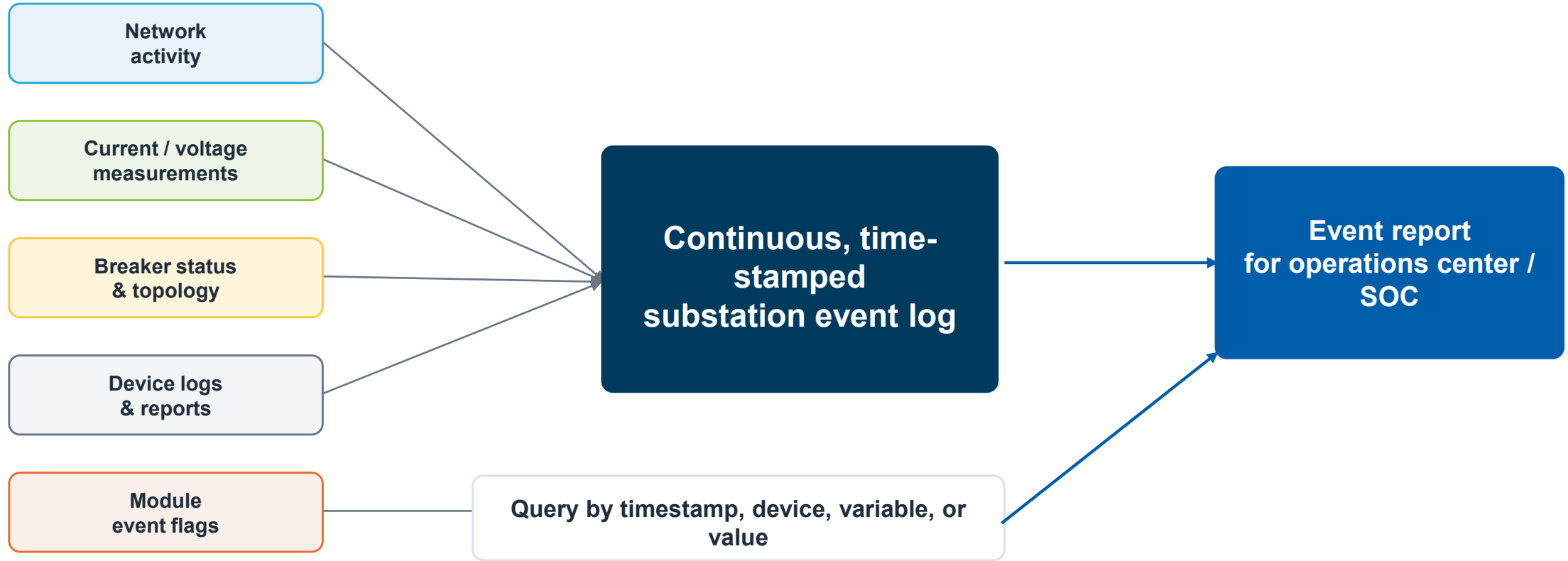
SCADA

Cyber tools

Sensors

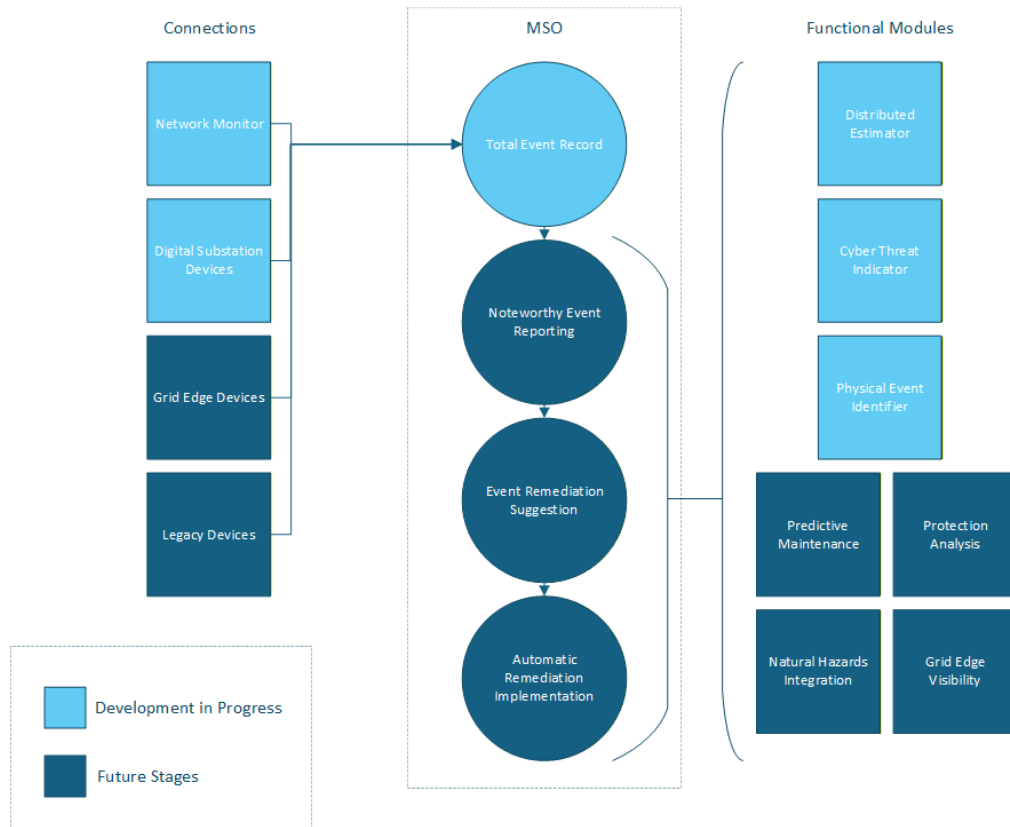
Initial deployment is informative only: alarms, suggestions, records, and reports.

A total event record



The event record turns distributed evidence into a single recoverable, reviewable timeline.

Core plus independent modules

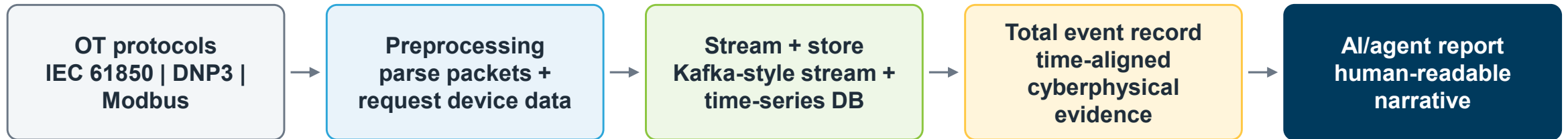


Modularity is the deployment strategy.

- MSO core performs data aggregation and logging.
- Modules generate event flags or specialized data handling.
- Users can choose the capabilities that fit their systems.
- Third-party modules can be added without rebuilding the core.

No single module is required for the core to perform its basic logging function.

From packets to operator context



1. Decode

Translate protocol traffic into text and numeric values useful for analytics.

2. Pull context

When modules raise flags, request settings, event reports, or local records not normally sent upstream.

3. Aggregate

Maintain a single queryable timeline by timestamp, device, variable, or value.

Current capability modules

MaSDE

Distributed Estimator

Estimates binary topology states such as breaker/switch status; flags mismatches between estimated and reported state.

MaSTI

Threat Indicator

Uses anomaly detection on network traffic to identify patterns that deviate from known normal substation communications.

MaSEI

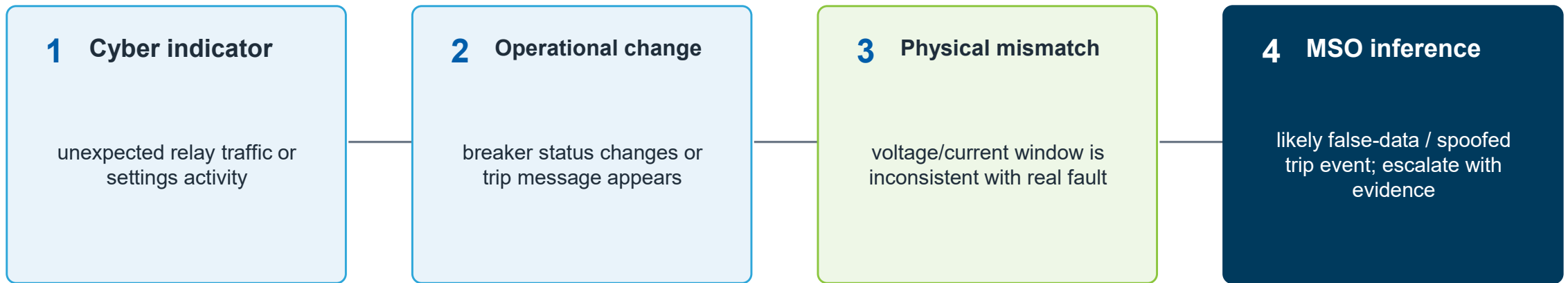
Event Identifier

Classifies electrical scenarios and validates whether protection behavior is consistent with measured current and voltage.

Together, the modules shift the system from monitoring isolated indicators to validating a substation event story.

A blended event the MSO can explain

Hypothetical: a relay appears to trip, but the electrical evidence does not support a real fault.



The point is not that any one indicator proves an attack. The point is that the combined story is more discriminating than any single alarm.

Operator-facing event narrative

ILLUSTRATIVE MSO EVENT REPORT

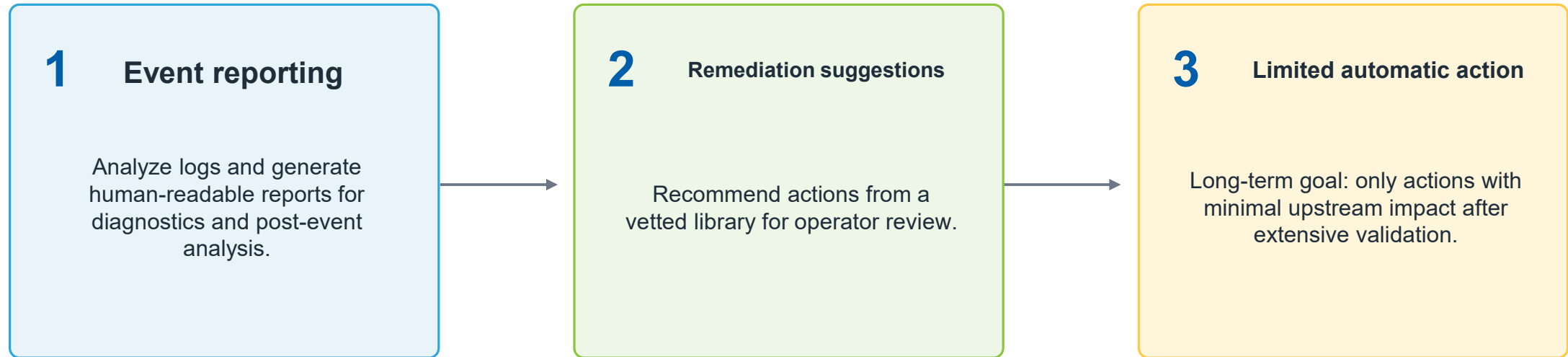
Event window	14:03:08-14:03:13 local, Feeder 2
Observed	Relay trip message; no matching fault signature in V/I window; abnormal traffic score elevated
Interpretation	Protection behavior is inconsistent with measured system state
Suggested action	Validate relay settings and event file; preserve packet capture; dispatch field check if status persists
Confidence	Advisory: requires operator review

Report mockup for presentation purposes only.

A useful AI output is not a magic answer. It is a concise, evidence-backed report that preserves context.

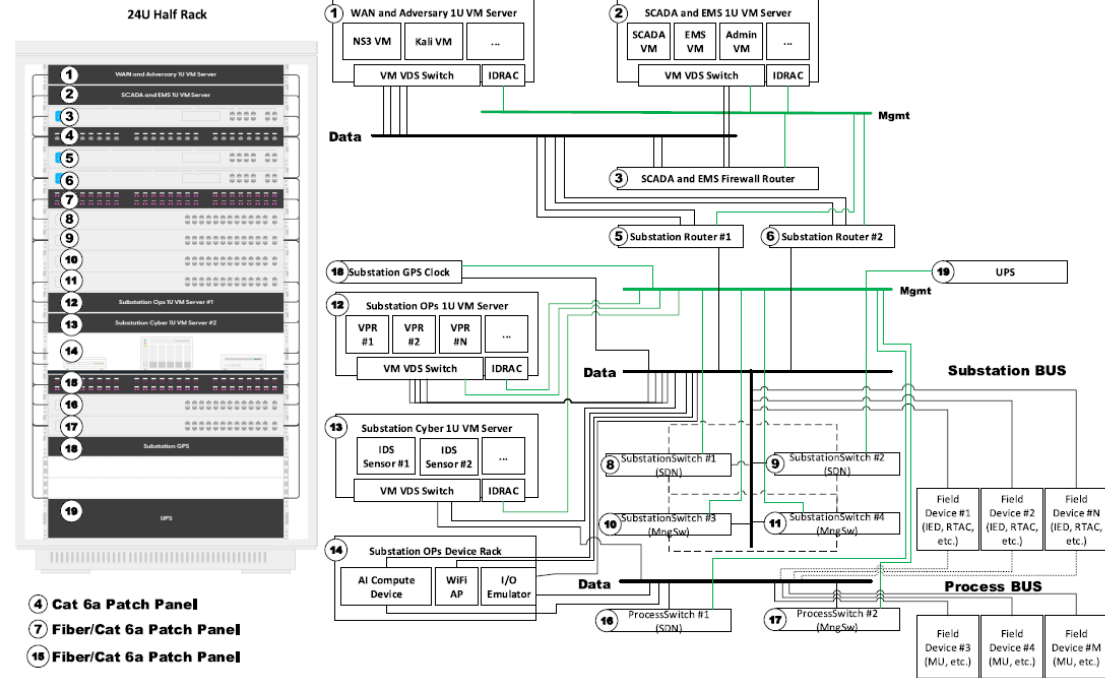
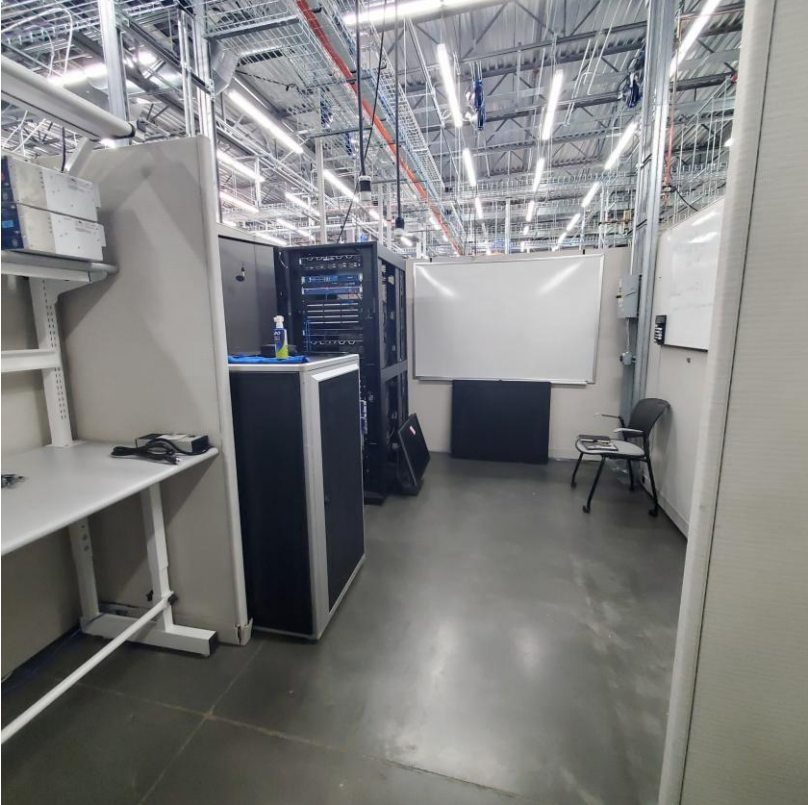
- Correlates cyber and electrical evidence
- Preserves raw data for review
- Labels uncertainty and confidence
- Keeps the operator in control during early deployments

Phased autonomy



The transition from reporting to action requires a proven period of performance, SME playbooks, validation, and explicit operational limits.

The digital substation testbed



- IEC-61850 digital substation with SDN options
- Process and substation bus traffic capture
- RTAC, network-to-physical meters, and multiple relaying options
- OPAL-RT hardware-in-the-loop and bridge to larger microgrid testing

DSTTL connects cyber traffic, digital substation devices, and physical emulation in one environment.

Security outcomes

Earlier triage

blended cyber/physical events can be escalated with context instead of isolated alarms

Better forensics

a single time-aligned record reduces time spent stitching together device reports

Settings assurance

protection behavior can be checked against measured electrical signatures

Operational resilience

operators receive response options that account for equipment state and cyber indicators

The security goal is not more dashboards. It is defensible operator context when cyber and physical evidence disagree.

Design constraints

Trust & interpretability

operators need evidence, not opaque automation

Model generalization

models must survive edge cases, new equipment, and changing data distributions

System integration

legacy systems, data quality, and compute limits must be handled deliberately

Cybersecurity exposure

the overseer and its inputs become part of the attack surface

MSO is intentionally incremental: deploy logging and reporting first, prove performance, then expand capabilities.

Path forward

Harden the core

robust logging, canonical event envelopes, retention, query, and provenance

Validate modules

broader data, realistic event scenarios, utility review, cyber/physical correlation

Build the agent

human-readable reports, SME playbooks, recommendation libraries, confidence labels

Expand ecosystem

utility pilots, vendor modules, university/lab research, standards and regulator engagement

The long-term vision is not a closed product. It is a framework for adding testable, domain-specific intelligence to substations.

Q&A

Three takeaways

-  **Integrated IT/OT substations require cyberphysical reasoning.**
A cyber alarm or physical alarm alone is not enough to deal with modern risks.
-  **AI is useful when it is constrained, modular, and evidence-driven.**
Reporting and validation come before autonomous action.
-  **MSO turns distributed substation data into defensible operator context.**
The immediate value is situational awareness, event validation, and faster triage.

Contact

Dr. Jonathan M. Tacke
Critical Infrastructure Researcher
Idaho National Laboratory

Slides may be shared with attendees.

2026 Power Systems Security Conference – WECC Risk Ranking for Cybersecurity and Physical Security

Scott Brooksby
Sr. Cybersecurity Risk Advisor

**Electric Reliability
& Security for the West**

August 13, 2026



OUR MISSION

<Public>

To effectively and efficiently mitigate risks to the reliability and security of the Western Interconnection's Bulk Power System



OUR VISION

A reliable and secure Bulk Power System in the Western Interconnection

ISO 31000 Risk Management Process



Risk Analysis Impact

Consequences/Impact — How could a *typical event due to this risk affect BPS reliability in the WI?

Severe (C5)	Impacts may have widespread effects on the WI.
Major (C4)	Impacts may have widespread effects on multi-subregions within the WI.
Moderate (C3)	Impacts may have widespread effects on a subregion within the WI.
Minor (C2)	Impacts may have effects on an entity within the WI.
Negligible (C1)	Impacts may have small or no effects within the WI.



Reliability Risk Matrix Likelihood

Likelihood—What is the reasonable probability that consequences will occur?

Almost Certain (L5)	Mandatory Controls—No NERC Reliability Standards in place for mitigation.
	Emerging Trends—Increasing trends have been identified.
	Event History—Documented events or widely publicized exploits have been recorded.
	Probability – Frequent (or) Multiple times per year (or) >90% chance.
Likely (L4)	Mandatory Controls—No NERC Reliability Standards in place for mitigation.
	Emerging Trends—Some trends have been identified.
	Event History—Documented events, or generally publicized exploits have been recorded.
	Probability – Probable (or) 1 to 2 times per year (or) 50% - 90% chance.
Possible (L3)	Mandatory Controls—NERC Reliability Standards in place for limited mitigation.
	Emerging Trends—Some trends have been identified.
	Event History—No documented events, or moderately publicized exploits have been recorded.
	Probability – Occasional (or) Once in 1 to 5 years (or) 15% - 50% chance.
Unlikely (L2)	Mandatory Controls—NERC Reliability Standards are in place for mitigation.
	Emerging Trends—Some trends have been identified.
	Event History—No documented events, or minimally publicized exploits have been recorded.
	Probability – Remote (or) Once in >5 years (or) 5% - 15% chance.
Very Unlikely (L1)	Mandatory Controls—NERC Reliability Standards in place for mitigation.
	Emerging Trends—No known trends identified.
	Event History—No documented events or publicized exploits have been recorded.
	Probability – Improbable (or) Once in >20 years to almost never (or) <5% chance.

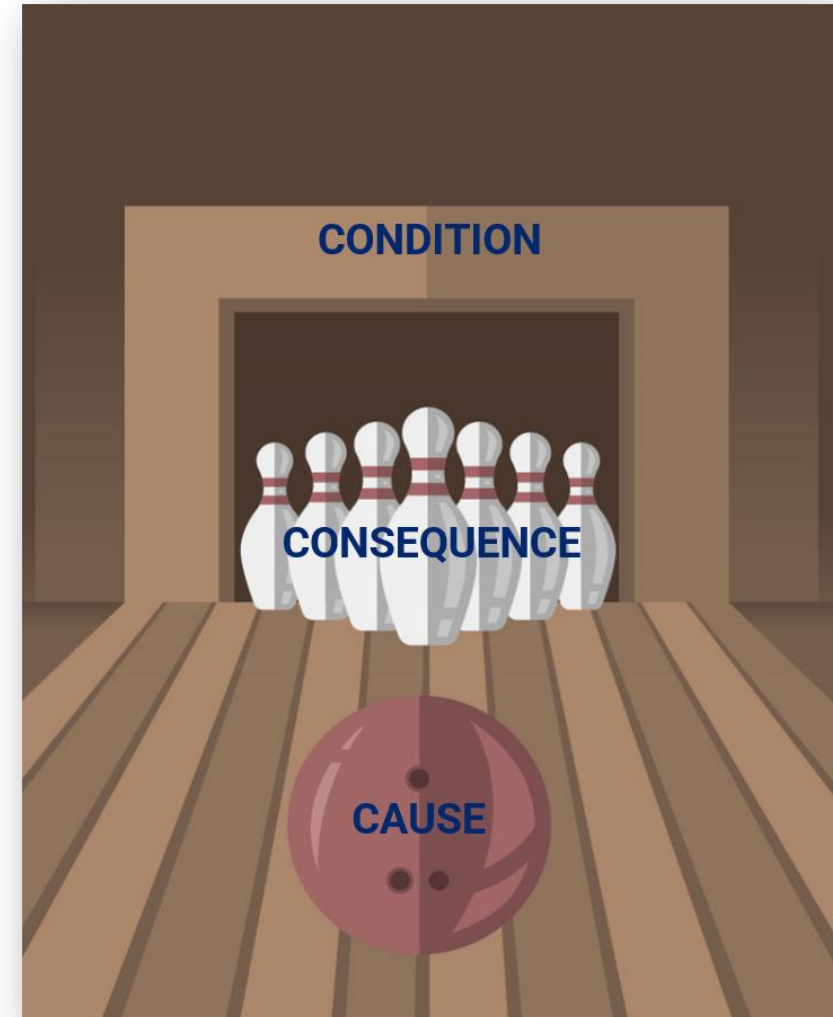
Risk Matrix

Reliability Risk Matrix											
Consequence /Impact (C)		Likelihood (L)									
		L1		L2		L3		L4		L5	
		Very Unlikely		Unlikely		Possible		Likely		Almost Certain	
C5	Severe	High	16	Extreme	21	Extreme	23	Extreme	24	Extreme	25
C4	Major	Medium	13	Medium	15	High	17	High	20	Extreme	22
C3	Moderate	Medium-Low	8	Medium-Low	10	Medium	11	High	18	High	19
C2	Minor	Low	5	Medium-Low	6	Medium-Low	7	Medium	12	Medium	14
C1	Negligible	Low	1	Low	2	Low	3	Low	4	Medium-Low	9

Elements of a Good Risk Statement

A good risk statement will include two or, potentially, three elements:

- The potential event or condition
- The consequences
- The cause of the event, if known



*Typical Event

- **Natural:** The most impactful event likely to occur in the next 50 years (1-in-50-year event)
- **Human-Made:** The most impactful event likely to occur within 10 years
- **Inherent:** The most impactful event likely to occur based on the current BPS design or the planned design (if the risk is based on a potential future state, i.e., 10- to 20-year planning)

*Typical Event Continued

- **Plausible event:** System assets or threats need to be related. Common mode failure (Unrealistic-related events are not plausible)
- **Assumptions:** Required to meet existing O&P/CIP Standards. Tariffs, contracts, state regulations, and interconnection agreements will be met with best effort.
- **Exceptions:** Risks that identify a more extended/different timeframe should be noted/defined within the "condition" statement. (i.e., the typical event (above) will be presumed in the condition of any WECC Risk Register item unless clearly stated otherwise)





<Public>

<Public>

Cybersecurity Risks

Cybersecurity Risks

Risk Name:

Artificial Intelligence

About The Risk:

Condition: Successful use of AI for reconnaissance, weaponization, and delivery of an exploit on the WECC top ~20 registered generation entities, or WECC top ~35 registered transmission entities.

Consequence: The first significant use of AI against the WI BPS will likely result in a generation loss of <500 MW, or loss of a single transmission facility, or inoperability at a single operator.

Cause: Public development of AI is rapidly growing and is out of entity control.

Risk Scale

Medium-L...



Likelihood

Possible

Impact

Minor

Cybersecurity Risks

Risk Name:

Insider Threat

About The Risk:

Condition: A trusted insider uses their authorized access to deliberately compromise assets or exfiltrate BPS-confidential information for use by a sufficiently resourced external threat (e.g., Nation State).

Consequence: Operational loss, control, visibility at a single site, control center, data center impacting an entity until restoration is completed.- or -Loss of BPS-confidential information or credentials that is used to successfully breach an entity.

Cause: 1. Disgruntled employee2. Bribe, threat, or coercion of an employee by an external threat actor.

Risk Scale

Medium-L...



Likelihood

Possible

Impact

Minor

Cybersecurity Risks

Risk Name:

Operational Network Breach

About The Risk:

Condition: Operational network at a larger entity (CIP Medium/High-impact) successfully compromised by a remote threat actor.

Consequence: Leading to inoperability up to 8 hours of >1% of load or > 230 kV transmission.

Cause:1. Geopolitical motivation to create instability in the BPS or create fear.2. Ransom

Risk Scale

Medium-L...



Likelihood

Possible

Impact

Minor

Cybersecurity Risks

Risk Name:

Compromised Hardware/Software Supply Chain

About The Risk:

Condition: Critical/key BPS operations software or microprocessor-based hardware (defined: software/hardware installed on BPS-controlled assets or utilized across 20% of WI operations) within the asset/owner/operator Operational Technology (i.e., SCADA) networks that are actively compromised or have been publicly disclosed as compromisable.

Consequence: A critical BA/TOP/GOP asset is compromised or damaged for >30 minutes, impacting >230 kV and >500 MW.

Cause: Intentional compromise of the supplier's assets by a threat actor or unintentional failures due to supplier negligence.

Risk Scale

Medium-L...



Likelihood

Unlikely

Impact

Minor

Cybersecurity Risks

Risk Name:

Malware

About The Risk:

Condition: Malware infection, from any source, of at least one critical asset within an entity's Operating Technology network.

Consequence: Loss of visibility/control at a single entity or single-site operations through ransomware, IOControl Malware, data corruption of control systems, or Denial-of-Service (DoS).

Cause: Threat actors motivation to control, damage, or extortion.

Risk Scale

Medium-L...



Likelihood

Unlikely

Impact

Minor

Cybersecurity Risks

Risk Name:

Third Party Operations

About The Risk:

Condition: Third-party (non-NERC-registered) access or operation of cyber assets.

Consequence: Unverified third-party security controls can lead to unintended misoperation of critical cyber assets.

Cause: 3rd-party operation of cyber assets may be necessary for cost-benefit reasons and may provide security controls beyond what a Registered Entity could afford to implement.

Risk Scale

Medium-L...



Likelihood

Unlikely

Impact

Minor

Low-Risk Cybersecurity

Name	Score	Likelihood	Impact
Phishing & Social Engineering	3	Possible	Negligible
Perimeterless Operational Technology	2	Unlikely	Negligible
Zero-Day Exploit	2	Unlikely	Negligible
Physical Attacks on Cyber Assets	1	Very Unlikely	Negligible
Industrial Internet of Things (IIoT)	1	Very Unlikely	Negligible
Public Cloud / Cloud Computing	1	Very Unlikely	Negligible



<Public>

<Public>

Physical Security Risks

Physical Security Risks

Risk Name:

Infrastructure Sabotage

About The Risk:

Condition: Generation and transmission infrastructure are physically attacked. (Single motivated threat on one critical asset)

Consequence: Generation and transmission infrastructure are damaged, rendering the asset (e.g., generation, transmission, telecommunications) completely inoperable.

Cause: Primarily theft, vandalism, and potentially intended asset harm.

Risk Scale

Medium



Likelihood

Unlikely

Impact

Major

Physical Security Risks

Risk Name:

Drones and Unmanned Aircraft

About The Risk:

Condition: Drones (Unmanned Aerial Vehicle) are used at a low cost/effort to surveil or carry a payload across the utility perimeter, likely in isolated events.

Consequence: Physical attacks on infrastructure, resulting in inoperability at a critical asset.

Cause: The low cost and ease-of-use of drone technology have made it readily available to both threat actors and hobbyists.

Risk Scale

Medium-L...



Likelihood

Unlikely

Impact

Moderate



ENGAGE WITH WECC





engage@wecc.org



www.wecc.org | 801-582-0353



155 N 400 W, Salt Lake City, Utah 84103, USA



AUG 13, 2026

Automation and AI as Security Enablers

Chris Luras

Partner

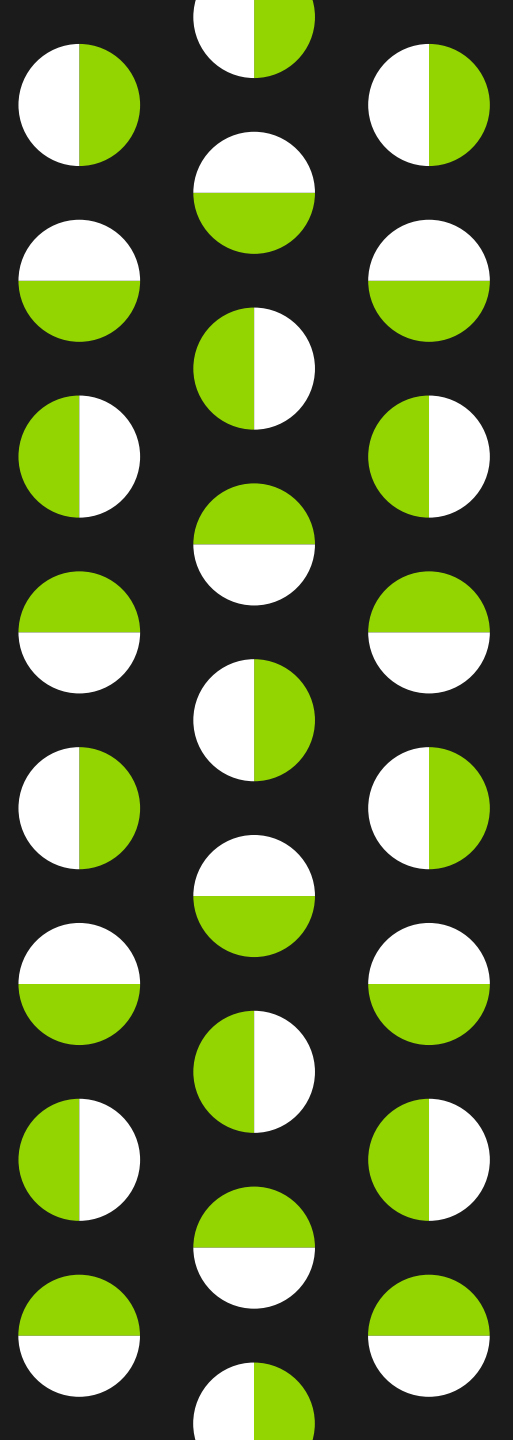
Keshav Sarin

Director

outwit complexity™



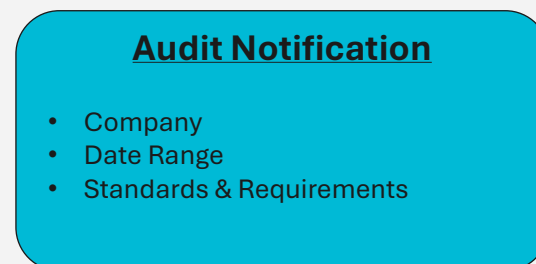
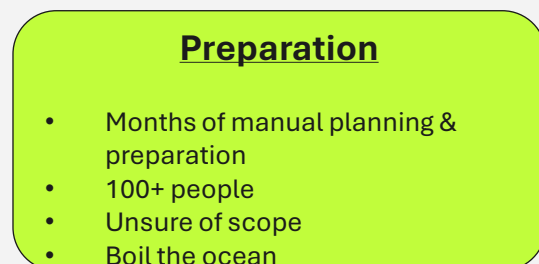
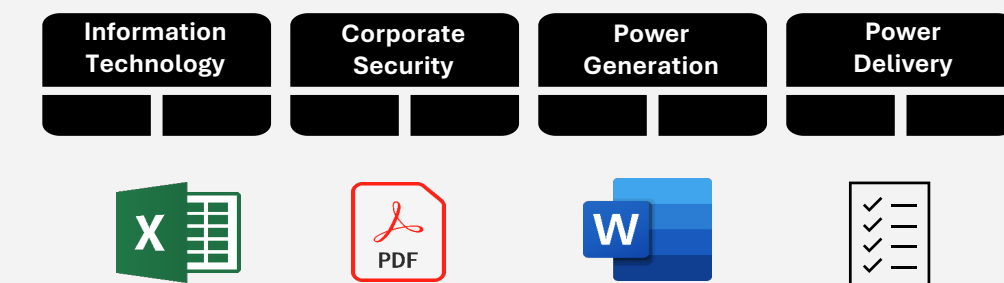
Energy industry challenges for security compliance



In 2020, FPL saw an opportunity and a need to reimagine its approach specific to its NERC compliance program.

Before

Spin up the audit machine / Reactive

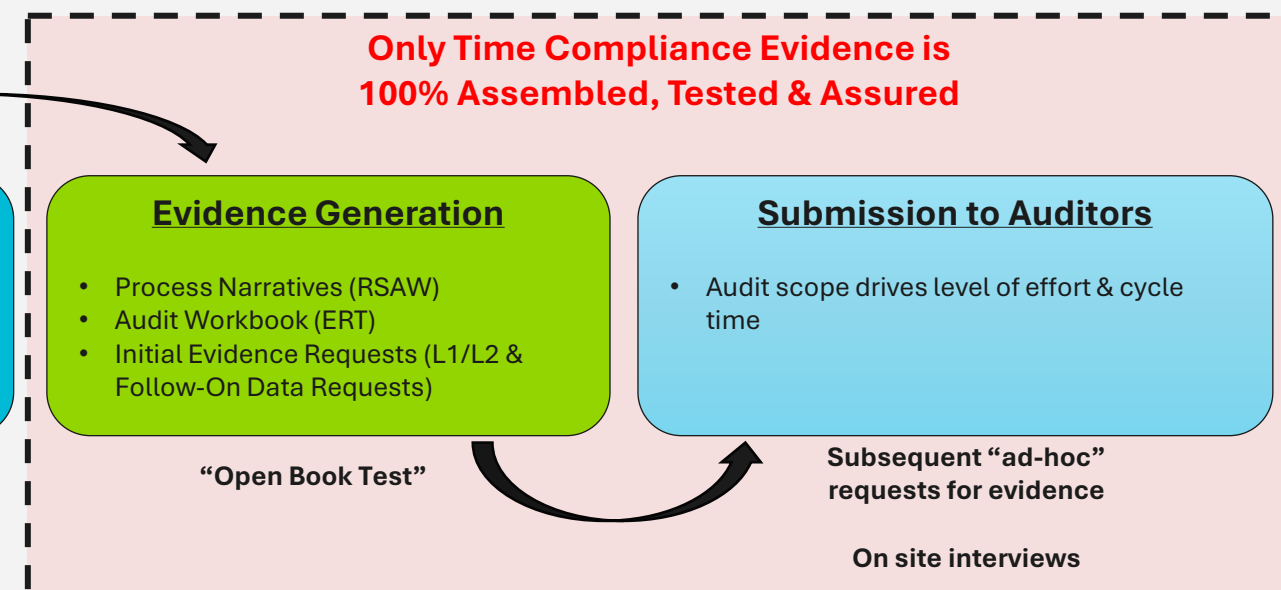


Hours devoted to manual prep work not relevant to audit scope could have been used elsewhere

After

Always Audit Ready / Proactive

- Manual evidence production / minimal information validation
- Different processes and interpretations of what was needed to substantiate compliance
- Presentation by business unit (vs. Registered Entity) resulted in fragmented view / representation of the registered entity
- O&M costs associated with audit support and execution continued to increase
- Focus was on compliance not on managing security risk



Transforming Compliance with Guidehouse's NERC Information Compliance Command Center

AN INNOVATIVE APPROACH TO RELIABILITY & COMPLIANCE

Industry Recognition



President's Award



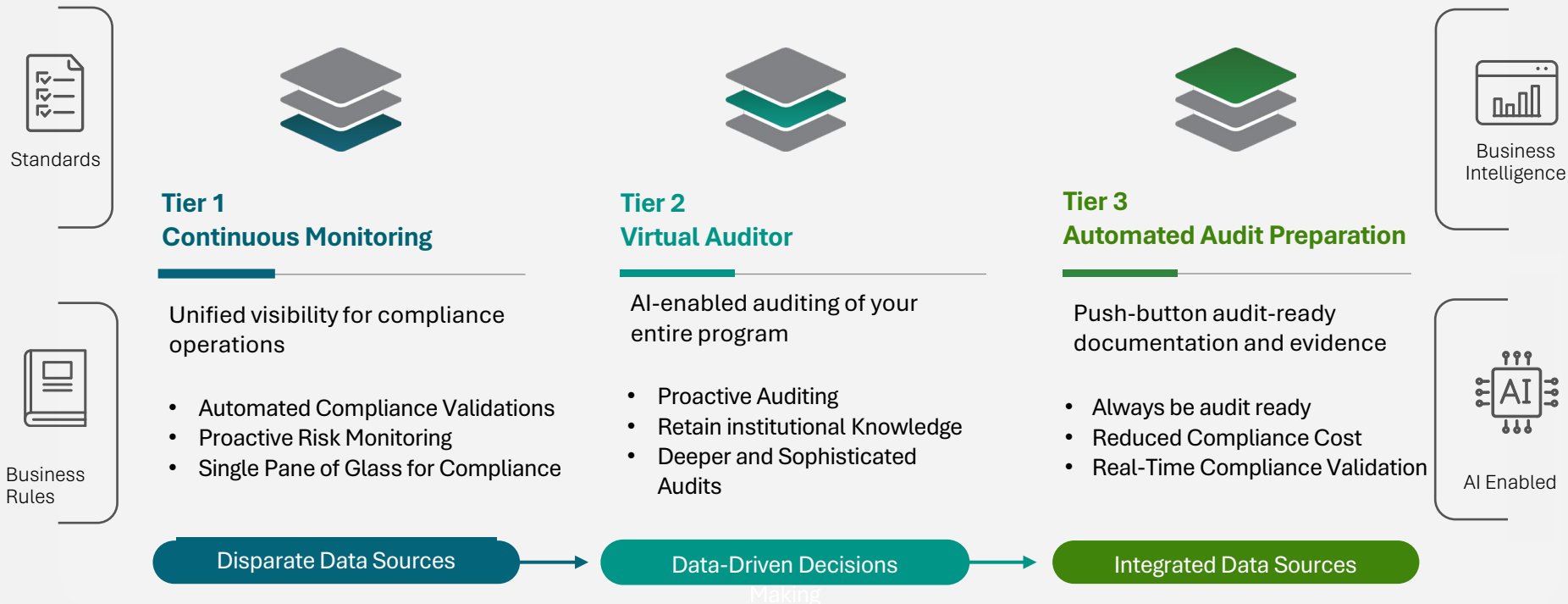
National Electrical Infrastructure Security Award



Innovation in Reliability

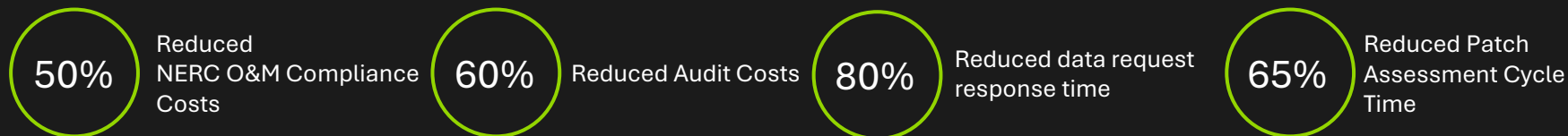
NERC Information Compliance Command Center

Digitize and Automate Compliance. Manage Risk. Free up Resources.



Proactive measures to reduce risk and safeguard security and reliability

Demonstrated Results and ROI from Capital Investment



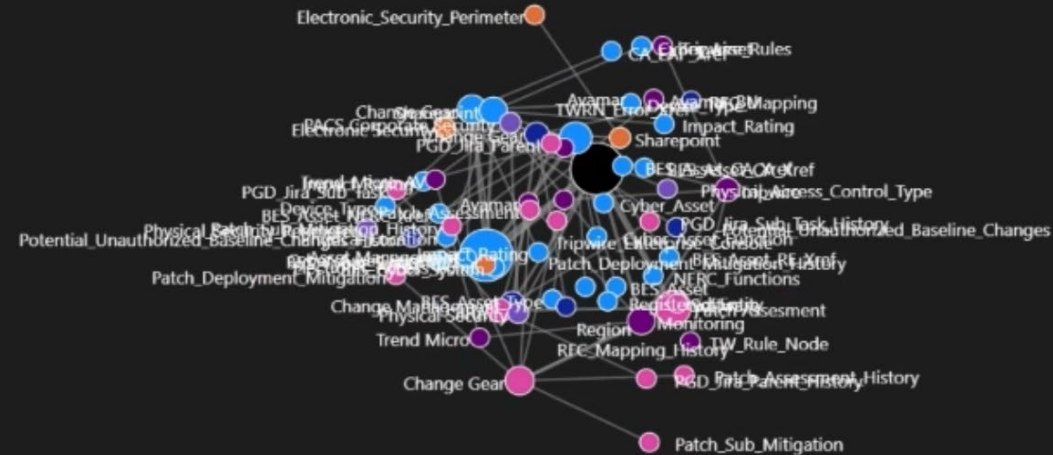
Integrated and aggregated data across the enterprise

30+ data sources
in one data
warehouse

Data across CIP
& O&P domains

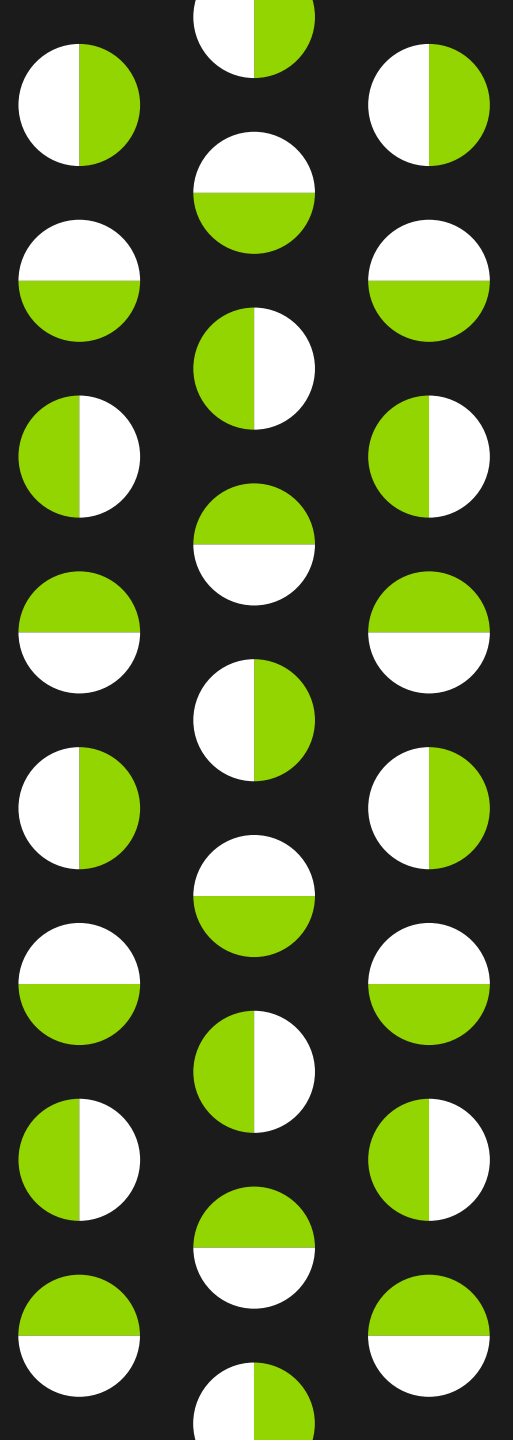
Thousands of
interconnected
data fields

Endless integrated
reporting solutions





Security **Patch** Management



Mitigating Failure Modes of Patching Lifecycle

Inventory Cyber Assets, software and patch sources

- ✓ Continuous monitoring—meet
- ✓ Audit preparation (L1, L2)
- ✓ AI (LLM)

1. Inventory

Identify and assess patches within timeframe

- ✓ Continuous monitoring
- ✓ Audit preparation (L1, L2)
- ✓ AI (LLM)

2. Identify & Assess

Security Patch Lifecycle

Test/Install patch

- ✓ Continuous monitoring
- ✓ Audit preparation (L1, L2)

4. Test/Install

3. Mitigation Plan

Develop and manage patch mitigation plan

- ✓ Continuous monitoring
- ✓ Audit preparation (L1, L2)
- ✓ AI (LLM)

From January 2021 to August 2022, a total of 21 out of 65 samples selected specific to CIP007 R2 – Security Patch Assessments exceeded the 35-day max allowed cycle time by an average of 1-7 days – a 32% Defect Rate!

Inputs

SMEs



Patch Sources



Applicability Logic Applied

Available



Applicable



Outputs

IT Patch Assessments

Stored in SharePoint



PGD Patch Assessments

Stored in PGD Documentum



Corp Sec Patch Assessments

Stored in CS Documentum

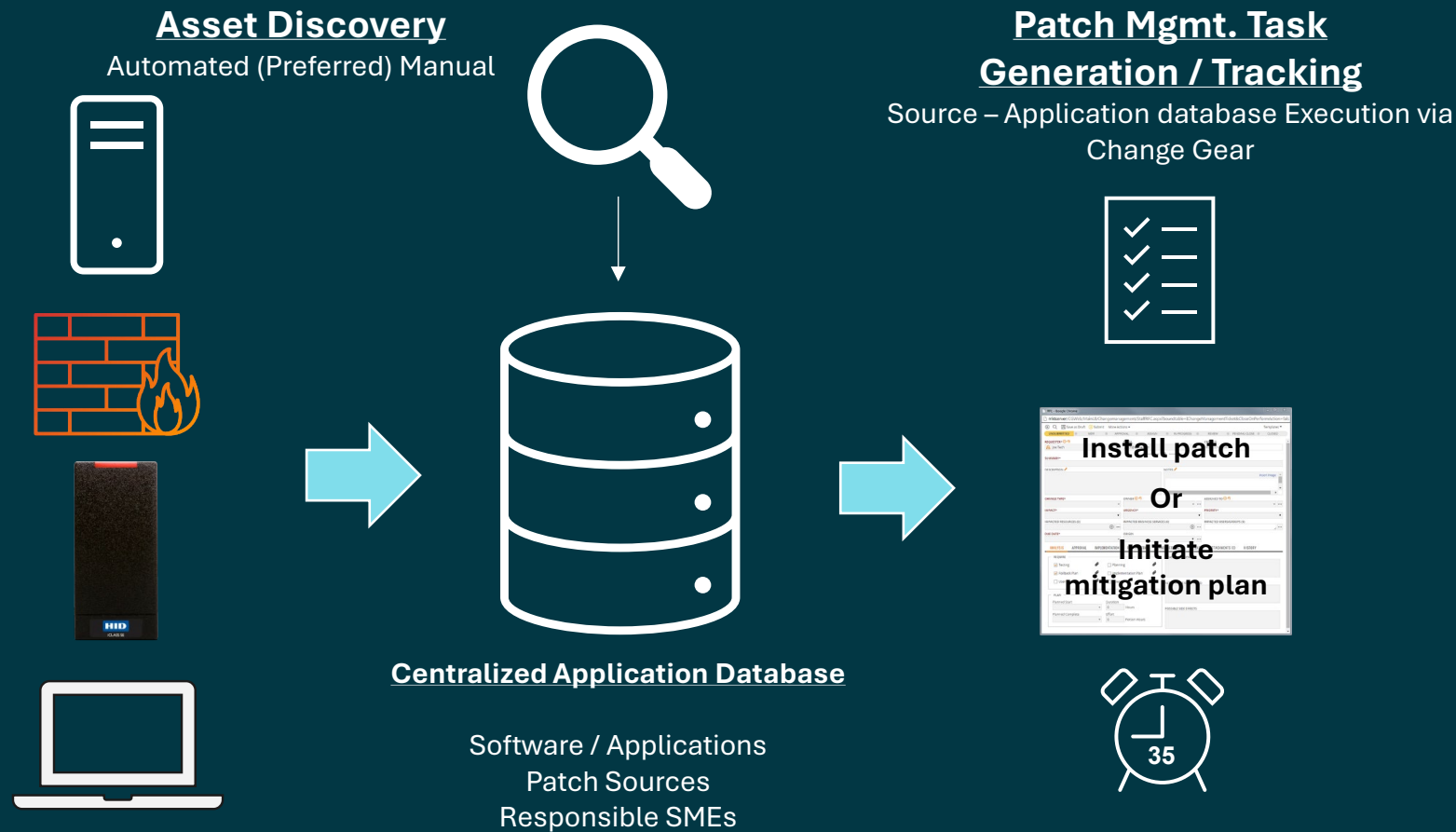


PD Patch Assessments

Stored in PD Documentum



From January 2021 to August 2022, a total of 21 out of 65 samples selected specific to CIP007 R2 – Security Patch Assessments exceeded the 35-day max allowed cycle time by an average of 1-7 days – a 32% Defect Rate!



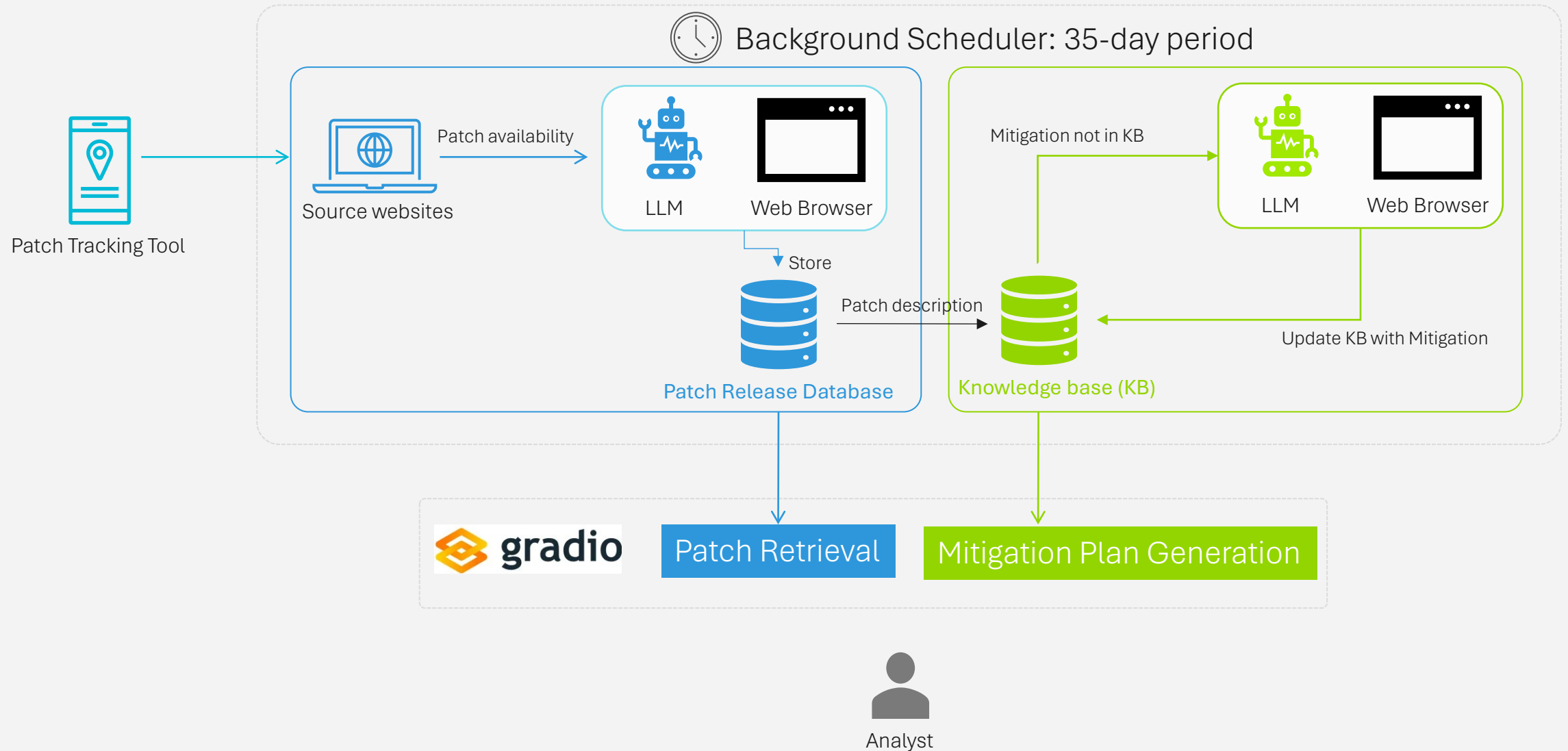
NERC Information Command Center (NICC)

- Real Time Monitoring
- Condition Response
- Trend Analysis
- Process Execution Evaluation

FPL CIP Program is now realizing a **41% decrease in average time to complete** patch assessments.

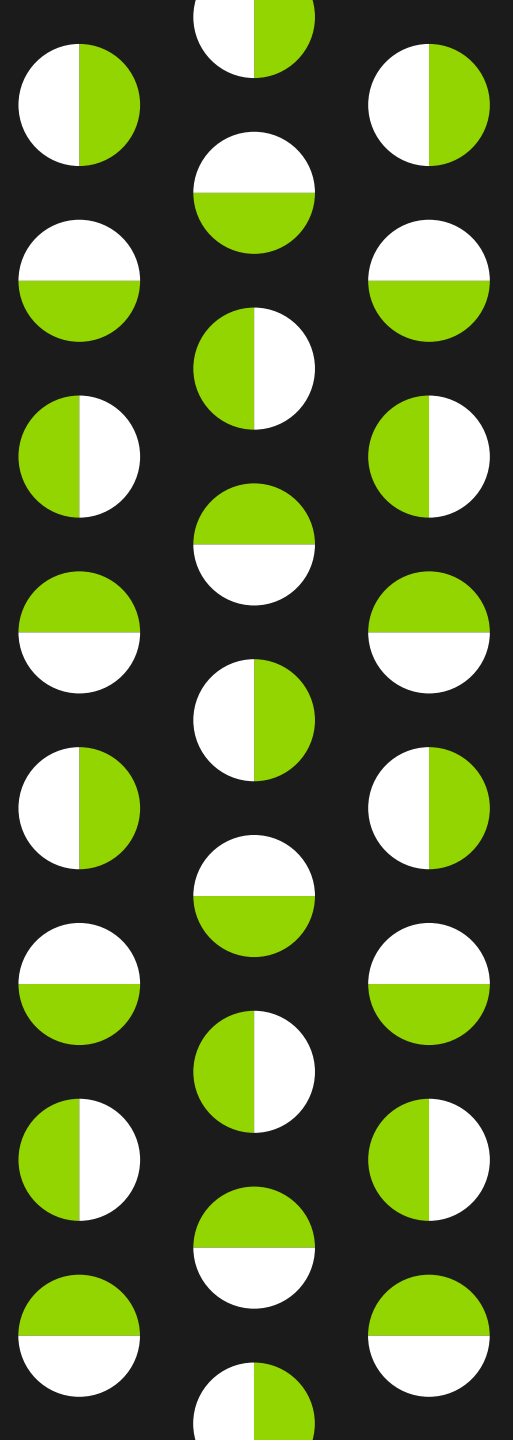
	June 2026	June 2026	June 2026	July 2026	July 2026	July 2026
	Total Patch Assessments Required to Perform (Opportunities)	Total Patch Assessments Completed (Actuals)	Average Completion Window	Total Patch Assessments Required to Perform (Opportunities)	Total Patch Assessments to Complete (Opportunities)	Average Completion Window
Information Technology	271	271	23 Days	255	255	24 Days
Corporate Security	8	8	25 Days	11	11	17 Days
Power Delivery (TSO)	70	70	23 Days	66	66	24 Days
Power Delivery (GCS)	134	134	22 Days	231	231	21 Days
Power Delivery (PDC)	13	13	24 Days	13	13	25 Days
Power Generation	16	16	25 Days	15	15	23 Days
Totals	512	512	24 Days	591	591	22 Days

Patch Automation Architecture





Today's Approach vs Tomorrow



Today's Approach versus Tomorrow

Leveraging Automation and LLMs



Labor-intensive, periodic, driven by manual evidence collection and human review

-
- **Staff** gather logs, configuration data, scan results, and policy artifacts from disparate systems, **analyze them offline**, update **spreadsheets and control narratives**, and brief risk posture on a scheduled (often **quarterly or annual**) basis rather than in near real time.
 - The approach is often **more costly and less secure**



Processes become near-real-time, intelligence-driven, and proactive

-
- Controls are **continuously assessed through integrated telemetry** (logs, vulnerabilities, configurations, identity, and cloud signals), **automated control testing and scoring replace periodic evidence gathering**, and **LLMs synthesize data** across tools to **interpret risk**, generate narratives and dashboards, and provide **proactive, context-aware insights** to leadership

An Information Command Center Approach to Security and Compliance

ICC is a governance, risk, and security compliance platform that sits above an organization's existing technical landscape to continuously monitor change, turn technical signals into security controls and framework context, and automate the workflows that keep security posture current.

It aggregates documents and data, security controls, compliance requirements, and processes into one operating model so leaders get clearer risk visibility, while technical teams get earlier, evidence-based insight into what changed, why it matters, and what action needs to happen next.

Collect. Intelligence. Automate.

ICC sits on top of your existing stack. It turns technical change into a current environment, usable auditor judgment, and action before approval.

COLLECT

ICC continuously monitors the technical landscape for change, drift, and exposure.

INTELLIGENCE

ICC turns raw signal into evidence-grounded answers, governance context, and decision-ready judgment.

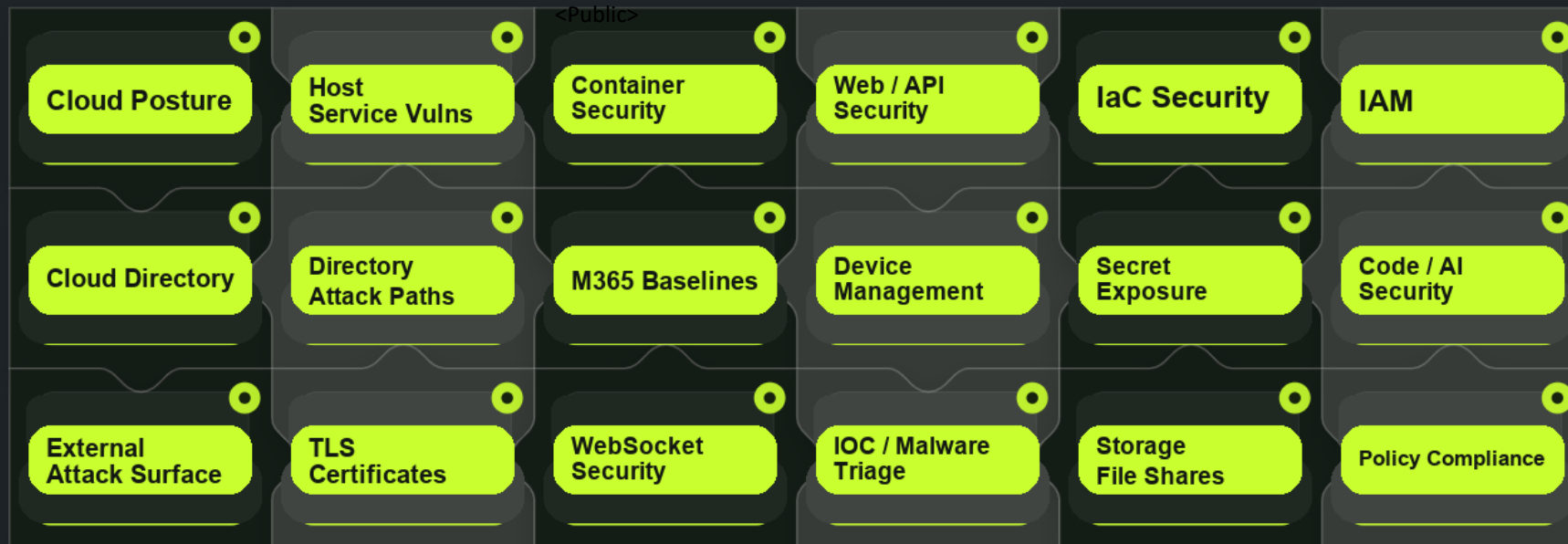
AUTOMATE

ICC automates tasks, risks monitoring, and follow-through workflows before decisions are made.

Bottom Line:

The point is not another dashboard. It is one operating model that keeps the engagement current by moving from signal to judgment to action in one system.

Collect



Intelligence

INTELLIGENCE LAYER

OCR

Extracts text and structure from source material



RAG

Retrieves grounded evidence, context, and prior knowledge



AI

Reasons over the evidence and generates usable insight

Automate

AUTOMATION LAYER

Trigger

Schedule, threshold, event, or analyst action



Workflow Engine

Rules, orchestration, branching, approvals



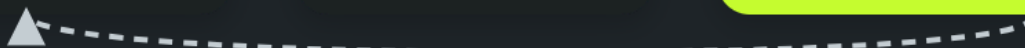
Actions

Tickets, alerts, assignments, evidence moves



Continuous Follow-through

Recheck status, notify owners, update reports



Some Example Use Cases

1

Automated Facility Ratings Change Tracking and Compliance

2

Automated Ports and Services Justification Workflow

3

Automated Patch Identification, Assessment and Mitigation Plan Development

4

Automated Vendor System Hardening Validation Process

5

Automated Maintenance Task Optimization and Scheduling

6

Automated Asset Onboarding Workflow

7

Automated Protection System Test Validation Reporting

8

Automated Vulnerability Identification Triage

<Public>

Chris Luras
Partner
Chris.luras@guidehouse.com

Keshav Sarin
Director
Keshav.sarin@guidehouse.com

Thank You