

HILLSTRONG · THOUGHT LEADERSHIP

The IT Tether

What Actually Stops Your Line

Roger Hill | CEO, Hillstrong Group Security, Inc.

Contents

A five-part executive briefing on the enterprise systems that stop your line, and the one page that maps them.

CHAPTER ONE The Line Stopped and Nobody Touched a PLC

CHAPTER TWO Your ERP Is a Plant Floor Control System. Nobody Scoped It That Way.

CHAPTER THREE The Hypervisor Under Your Plant Floor

CHAPTER FOUR Who Can Still Log Into Your Factory at 2 a.m.

CHAPTER FIVE From Asset Inventories to Stop-the-Line Maps

About the Author

About Hillstrong Group Security



The Line Stopped and Nobody Touched a PLC

Two manufacturers halted production this summer. Neither attack reached a controller.

A plant with every controller online and no order to build is a plant that is down.

On 10 June, Mackay Sugar stopped milling and cane haulage at two of its three Queensland mills. Five weeks later, Coca-Cola told the SEC that fairlife had suspended all US production. The Canadian plants kept running.

Dragos reviewed the Mackay Sugar incident and found no evidence that the attackers reached ICS or manipulated the process. The mills stopped anyway.

I have spent thirty years around control systems, and those two events break a reflex I used to have myself. If the PLCs are clean, the plant is fine.

What your scope leaves out

You scope OT security to the control network. Levels 0 through 3, the assets with firmware versions and rack slots, the things an OT scan can see. That scope produced the asset inventory on your wall and the budget line you defended last year.

The systems that stopped those two producers sit above it, in territory your OT program excludes and your IT team owns on a ticket queue.

Call it the IT tether. Every enterprise system your line cannot finish a shift without, which nobody has counted and which has no single owner.

Three tethers carry most of the load.

Order. ERP and MES decide what the line makes, in what sequence, against which recipe, and whether the pallet leaves with a label it can ship on. Take them away and the line runs through whatever is staged in front of it, then stops with every controller healthy.

Host. Your historian, your HMI servers and your engineering workstations increasingly run as guests on virtualization a data center team administers. The controller keeps running. The screen your operator drives it from is gone.

Access. Identity is the tether with the least documentation: contractor accounts nobody revoked, and the corporate domain your plant inherited during an integration that nobody has revisited since.

What the second quarter looked like

Dragos counted 1,140 industrial ransomware incidents in the second quarter of 2026, up 12 percent on the first quarter. 747 of them hit manufacturing.

Mackay Sugar is the clean case because the forensics are public. The Gentlemen claimed it. Milling and cane haulage stopped at two of three mills. No ICS access, no process manipulation, no controller logic touched. What the attackers took was the enterprise layer those mills schedule and move cane with.

The fairlife disclosure is the more expensive version. Coca-Cola's filing said intruders reached production-related systems and that the company had not yet determined the full scope. US production suspended. Canadian production continued, which tells you the dependency was regional, sitting in something the US plants shared and the Canadian ones did not.

In the plants I have walked, the sequence runs the same way. MES loses ERP. Order release stops. Operators keep building what is already staged, which buys the length of whatever sits in front of them. Then the line runs out of work it is authorized to make, and a plant with every controller online produces nothing.

Why visibility does not answer this

The OT security tools you bought answer one question well: what is on my control network. Ask what stops your line and they go quiet. The answer is not on the network they watch.

Your asset inventory has the same limit. It lists things you own. Production stops come from things you depend on, and those two lists overlap less than the budget assumes.

What the better operators do

They keep a dependency list per line rather than per asset. One line, one page. The enterprise systems that line cannot finish a shift without, each with a named owner and a restoration time somebody has measured with a stopwatch rather than promised in a contract.

It is a short document, and the useful part is the argument it starts. Some of those entries belong to a team that has never been told a production line depends on them.

What you can do this week

If you're a plant or OT leader: Pick your highest-value line and write down what it cannot finish a shift without. Ask the owner of each entry how long a full restoration takes and whether anyone has timed one.

If you're a CISO or enterprise risk lead: Take that list to whoever scoped your OT program and mark which entries fall inside the scope. Report the count of entries outside it instead of a maturity score.

If you're a COO or CFO: Ask for the dependency list before you approve the next OT security capital request. A program scoped to the control network is buying insurance against the smaller of your two exposures.

A final thought

Both of these were IT incidents, and the OT teams involved did nothing wrong. That is accurate, and it restarted nothing. The mills were down, the milk was not made, and the boards asked the question you would expect: why did the plant stop if the plant was secure?

Your turn

Take your highest-value line. Which enterprise system, dark on a Sunday night, stops it before the next shift ends? And can you name the person who owns that system's recovery time?



Your ERP Is a Plant Floor Control System. Nobody Scoped It That Way.

SAP shipped a 9.9 in August for the software sitting between your plant floor and your order book. Whose patch window owns it?

Your line does not stop when a controller fails. It stops when nothing tells the controller what to build.

On 11 August, SAP released a fix for CVE-2026-44772, scored 9.9, in SAP Manufacturing Integration and Intelligence. MII is the translation layer between plant floor assets and ERP business logic. The flaw allows remote code execution through malicious transformation logic, and Onapsis notes that a low-privilege service account is enough to reach it. That describes most of the accounts living in a plant network.

Ask who owns that patch at your company. The answer is usually a Basis team working an enterprise calendar, and your OT risk register has no line for it.

The systems that stop a line are not on the control network. Order is the first of them.

Order release is a control function wearing a business label

Sequencing decides which order runs next, and recipe selection decides what the equipment is set to when it runs. Both determine the physical behavior of your plant. Shipment authorization decides whether the finished pallet is allowed to leave. Those are control decisions. They carry a business label because they run on a server in a data center rather than in a panel on the floor, and your scope followed the label.

Call it the order tether, the first strand of the IT tether. It decides whether work exists.

The failure you should worry about is release, not production

The obvious version is a line with nothing to build. Most plant managers I talk to have already argued their way past it, and they are right to. MES caches recipes. Operators keep going on staged work. A well-run site absorbs a few hours of this without an alarm reaching anyone senior.

Quality is where it stops being survivable. Batch records, recipe versions and electronic signatures live in the same systems. A food or pharmaceutical plant that cannot produce a batch record cannot release product it has already made. The line runs. The warehouse fills. Nothing ships, and every hour of production adds inventory you are not yet allowed to sell.

What it cost the one company that had to file about it

Clorox disclosed a cyberattack on 14 August 2023 and moved to manual order processing. Manufacturing came back at most sites within weeks. The company was still warning about product outages a month later, on 18 September.

In its SEC filing, Clorox reported 49 million dollars in costs as of 31 December 2023, covering forensics, IT recovery and incremental operating expenses, and told investors the disruption had a material impact on the quarter ended 30 September 2023.

No attacker touched a controller in that sequence. The plants could make product. The company could not decide what to make, or ship what it had made.

Two calendars, one system, no owner

An enterprise patch window gets scheduled around month end and financial close. A production patch window gets scheduled around a changeover or a shutdown. Those calendars share nothing, and MII sits inside both.

What happens next is predictable. The OT team assumes the SAP estate is covered because it is a corporate application. The Basis team assumes anything touching production needs plant approval they have not been asked for. A 9.9 waits for a window neither group believes they own.

How the good ones triage a 9.9 they do not own

They rate the order path by production impact rather than by CVSS. A vulnerability in the system that authorizes shipment gets triaged against tonnes and orders, not against a severity score that knows nothing about your plant.

They also rehearse the shift. One site, one changeover, order release unavailable, and somebody times how long the plant keeps producing sellable product. The number that comes out of that exercise is the only honest input to the recovery conversation.

What you can do this week

If you're a plant or OT leader: List the production decisions your site cannot make without ERP or MES, separating what stops the line from what stops the shipment. Name which of the two arrives first at your site.

If you're a CISO or enterprise risk lead: Find out who patched CVE-2026-44772 and when. If nobody can answer inside a day, you have found the ownership gap rather than a patching problem.

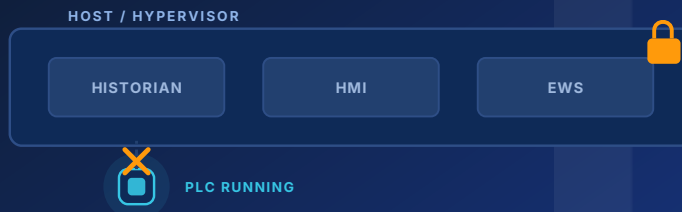
If you're a COO or CFO: Ask what your plants can produce and release with the order systems down, and for how long. Then ask who has tested that answer rather than estimated it.

A final thought

The comfortable reading is that ERP is an IT system with an IT owner and an IT recovery plan. That reading survived until the quarter Clorox had to describe to investors. Your ERP decides what your factory does with its day, and a system that decides what a factory does is a control system whatever the org chart calls it.

Your turn

Take your highest-volume site. With order release unavailable, how many hours until it produces something it cannot ship? And is that number measured, or is it the one somebody offered in a meeting?



The Hypervisor Under Your Plant Floor

Your controllers survive this. The people who run them do not.

A controller nobody can see is a controller nobody can run.

The PLC is fine. It is executing the logic it executed yesterday, holding the same setpoints, and it will keep doing that until somebody changes it or the power goes.

Nobody can see it. The HMI servers, the historian and both engineering workstations were guests on the same virtualization cluster, and that cluster is encrypted. Your operators are running a live process from memory and a clipboard. Your controls engineer cannot open the project file to check what the logic says.

Order decides whether work exists. The host is the second strand of the IT tether, the one that decides whether anyone can watch the work happen.

The consolidation nobody logged as an OT change

Over the last several years your OT servers moved. It happened one server at a time, as a data center efficiency project, and every step had a defensible business case. The historian hit end of life. The HMI server needed more memory. A virtual instance cost less than another rack in a cabinet on the floor.

Your asset inventory recorded the guests. It did not record the host, and it did not record that a team outside the plant now holds the power button for all of them.

What changed in the second half of last year

Hypervisor involvement in ransomware encryption went from 3 percent of cases in the first half of 2025 to 25 percent in the second half, on Huntress case data reported in December. That is roughly an eightfold move inside six months.

The economics explain the shift. CVE-2024-37085 hands an attacker full administrative control of an ESXi host and mass encryption of every virtual machine on it in seconds. One credential, one host, and everything that host was carrying stops at the same instant. Akira has driven much of the pattern. Given a choice between encrypting guests one at a time and encrypting the floor they all stand on, an attacker picks the floor.

The hosts also sit in a monitoring blind spot. An ESXi host does not run the endpoint agent your guests run, and the tooling watching those guests cannot see the layer holding them up. An attacker who reaches the host works underneath everything your SOC has been told to look at.

Consolidation did to your OT servers what it did to everyone's, and it built a single point of failure your Purdue diagram does not show. That diagram has your historian at Level 3 and your HMI at Level 2. Both are on the same host, and the diagram has no box for the host.

Recovery is a sequencing problem, and your process is still running

Restoring a virtualized estate is an ordering exercise. Domain controller, then the historian, then the HMI servers, in a sequence somebody has to already know. CISA published recovery guidance for ESXiArgs in February 2023 because organizations were restoring virtual disk files without a working order and getting inconsistent results.

A plant carries a constraint that guidance does not address. Your process does not pause while you sequence. Operators are holding a live process on manual control for the entire restoration, and the length of that window is a safety question before it is an availability one.

The one machine that stays off the cluster

They put the host in the OT asset inventory with the guests, and they read the admin group. Not the team name. The list of accounts, including the service accounts and the ones belonging to people who left.

They also keep one viewing path that does not depend on the cluster. A physical engineering workstation holding current project files, or an HMI that boots from local storage

and talks to the controllers without passing through the virtual estate. It costs one machine per site and it is the difference between running blind and running degraded.

What you can do this week

If you're a plant or OT leader: Find which host your HMI servers and historian run on. Then ask who can power that host off, and get a person's name rather than a team's.

If you're a CISO or enterprise risk lead: Pull the admin group for every host carrying plant guests and read it line by line. Report the count of accounts on it, not the count of hosts you have.

If you're a COO or CFO: Ask how long your operators would hold a live process on manual control during a full restoration of the plant's virtual servers. If the answer arrives as a range rather than a measured number, the recovery plan has not been run.

A final thought

Every controller stayed up. That sentence gets said in incident reviews as though it settles something. It settles the question about your control network, which was the question nobody needed answered, and leaves untouched the reason the site sat idle.

Your turn

Which host carries your HMI servers? And when you pull its administrator group, how many of those accounts belong to somebody who still works on your plant floor?

SSL VPN

JUMP HOST

VENDOR MODEM

OEM TOOL

PLANT



2:00

Who Can Still Log Into Your Factory at 2 a.m.

Your access review counts names. An attacker counts paths.

An account nobody revoked is a vendor relationship that outlived the contract.

Ask your team how many accounts can reach the plant network from outside the building. You will get a number. It comes from VPN group membership, and it is low enough to sound managed.

Now count paths instead. The SSL VPN. The remote access tool the OEM installed during commissioning and still supports on their own licence. The jump host with a shared local account the integrator uses, because provisioning named accounts took longer than the last outage did. The cellular modem the vendor builds into every skid they ship.

The second number is the one an attacker works from.

Order decides whether work exists, and the host decides whether anyone can see it. Access is the third strand of the IT tether, and it decides who else is standing at your controls.

Your access review counts the wrong noun

The annual review takes the list you already hold and asks whether each name still needs what it has. It has no way of asking what never reached the list. An OEM engineer connecting to a machine they support under warranty does not generate a row in your identity system, and the commissioning project that created their path closed three years ago.

Vendor sprawl is the shape this takes at scale. Secomea's 2026 industrial remote access research put it plainly: confidence in access control runs ahead of actual control, and the gap widens with every vendor added.

The part where having MFA stops being an answer

Akira has been reaching organizations through SonicWall SSL VPN appliances, and Rapid7 documented the combination that made it work. An unpatched CVE-2024-0015, disclosed in August 2024, sat alongside a group default that over-provisioned access to SSLVPN services.

The piece worth your attention is the third one. The Virtual Office Portal was reachable from the internet in default configurations, and an attacker already holding a valid username and password could use it to enroll their own MFA token. The second factor became something the attacker issued to themselves.

"We have MFA" answers a question about your architecture. It does not answer whether the enrollment path is exposed, and those are different questions with different owners.

How long a door stays open once nobody is watching it

Black Kite's third-party breach report, published 5 March 2026, put unauthorized network access at 47.06 percent of verified breaches in 2025. Ransomware accounted for 13.24 percent and stolen credentials for 6.62 percent. The same work found an average of 5.28 downstream victims for every third-party breach, the highest figure they have recorded, and an average of 730 days to detect an advanced persistent threat.

Two years. Set that against the standing vendor account nobody revoked and the question stops being whether a door is open. It becomes what has already been done through it, by someone who had no reason to hurry.

Inventory paths, and give every one an expiry date

They inventory paths rather than people. One row per way in, with the vendor, the purpose, the owner inside the company, and a date it stops working.

That last field does the work. Vendor access expires by default, and somebody has to ask for it back. An OEM who needs standing access to support a warranty will ask, which turns an invisible permission into a conversation with a renewal date on it.

What you can do this week

If you're a plant or OT leader: Walk one line and write down every way a person outside the building could reach something on it, including the modems and the vendor tools. Compare that against the access review you signed.

If you're a CISO or enterprise risk lead: Run the 2 a.m. list at one site. Every account and path that could authenticate to plant systems tonight. Report the count that was not on the access review, because that number is the finding.

If you're a COO or CFO: Ask what happens to a vendor's access when their contract ends. If the answer describes a process rather than an expiry date, the access is still live at sites you stopped paying for years ago.

A final thought

None of this reads as a security failure while it is happening. It reads as a plant that gets support quickly, an integrator who can fix a line at midnight without a ticket, and an uptime number your board likes. The access built to protect production is the access most likely to end it, and the reason it survives every review is that it works.

Your turn

Pick your last commissioning project. Whose remote access did it create, and is that access still live tonight? If you cannot answer without calling the integrator, they are holding a key to your factory and the record of who has used it.

ORDER

HOST

ACCESS

STOP-THE-LINE MAP



From Asset Inventories to Stop-the-Line Maps

Your renewal questionnaire is asking for the pieces of a document you have never built.

A list of people is not a list of ways in, and a list of assets is not a list of stoppages.

Read your cyber insurance renewal questionnaire. Underwriters covering industrial risk in 2026 ask for asset inventories, software bills of materials, and your IT and OT architecture with the segmentation drawn in. They also want an end-of-life systems inventory, mapping to IEC 62443 or NIST SP 800-82, patch cadence or the compensating controls where there is none, and the honest reach of your multi-factor authentication.

Those are fragments of one document. Nobody has asked you for the document, so nobody has built it, and the questionnaire gets answered field by field from eight different systems by whoever has capacity that week.

Three strands of the IT tether have run through this series, each with a different owner and a different failure. What follows is what happens when you stop arguing them one at a time and put them on a single page.

What your two existing documents actually answer

The asset inventory answers ownership. The maturity score answers conformance. Both are honest documents and neither was built to answer the question a board asks after a stoppage, which is why the plant stopped when the plant was secure.

Filling that gap does not require a new framework. It requires a different unit of analysis. Stop organizing by asset and organize by line.

The stop-the-line map

One production line, one page, six columns.

Column	What goes in it
The line	The physical line or cell, named the way the plant names it
What it cannot finish a shift without	The enterprise system, not the category
Which strand	Order, host or access
Owner	A person, with a phone number. Not a team, not a queue
Restoration time	Measured with a stopwatch, with the date it was measured
Last tested	Blank is an answer, and it is the most useful entry on the page

Five columns can be filled in from a desk. The restoration time cannot, which is why it is the column that decides whether the document is real. A map with an empty restoration column is a list, and you already have one of those.

Two controls that pay across all three strands

Privileged access review is the first. The administrator group on your ERP, the administrator group on the host carrying your HMI servers, and the accounts that can authenticate through your remote access path are three instances of one control. Most manufacturers run it three times, on separate calendars and against separate standards. Run it once, against the map, by line.

Restoration sequencing is the second. Every strand fails into the same question: what comes back first, and who decides. A plant that has sequenced its restart once has answered it for ransomware, for a failed migration, and for the afternoon a vendor pushes a bad update.

The self-assessment

Three questions. Answer them out loud, at your highest-value site.

Order. Name the person who decides your plant can ship without an electronic batch record.

Host. Name every account in the administrator group of the host carrying your HMI servers.

Access. Name what causes an integrator's access to stop working, without anyone deciding to revoke it.

The one you cannot answer cleanly is the strand you have left exposed. In most of the plants I walk, it is the third.

The full argument, in one paragraph

Two producers stopped production this summer and neither attacker reached a controller. Order is what decides whether work exists, and it lives in systems your OT scope files as business applications. The host underneath your HMI servers decides whether anyone can see the work happening, and your Purdue diagram has no box for it. Access is the strand your annual review already covers, badly, because a list of people is not a list of ways in. Put all three on one page per line, with a person against every entry and a restoration time somebody has held a stopwatch on, and you have the only document that answers what stops your plant.

What you can do this week

If you're a plant or OT leader: Build the map for one line. One page, six columns, and no entries you cannot name a person for.

If you're a CISO or enterprise risk lead: Take the completed page to your next renewal or customer security review and answer from it. Then count how many questionnaire fields it covered.

If you're a COO or CFO: Fund the map before you fund the next platform, and sequence the capital plan against the empty restoration times rather than against the severity scores.

A final thought

Standard cyber policies exclude physical damage, Lloyd's mandated the nation-state exclusion in 2023, and roughly 25 percent of claims are denied on exclusions or policy limits. The market has decided that industrial buyers should be able to describe what stops them and how fast they come back. Your insurer will get that document out of you eventually, on

their schedule and in their format. Building it first is cheaper, and it is worth more to you than to them.

Your turn

Which line would you map first, and what stops you from having a measured restoration time in that column by the end of the month? If the answer is that nobody will approve the downtime to test it, you have found the decision this whole series has been about.

About the Author



Roger Hill

CEO, Hillstrong Group Security, Inc.

Roger brings over 30 years of experience in industrial automation and cybersecurity. His extensive background in OT security has positioned him as a trusted advisor to CISOs across various industries. His expertise lies in developing and implementing robust OT GRC programs that address the unique challenges faced by global manufacturing operations.

Throughout his career, he has been dedicated to helping organizations achieve operational resilience through strategic security initiatives and pragmatic solutions. His commitment to excellence and deep understanding of the intricacies of OT systems have earned him a reputation as a pioneer in the field. Roger's methodologies continue to drive the development of secure and compliant OT environments for leading manufacturing companies worldwide.



About Hillstrong Group Security, Inc.

Hillstrong Group Security, Inc. is an operational-technology cybersecurity consultancy helping industrial and critical-infrastructure operators build security programs that hold up across their regulatory, product, service, and grid obligations. Blending OT, IoT, and ICS expertise, Hillstrong partners with companies in energy, manufacturing, water, chemicals, food and beverage, automotive, and other essential sectors to achieve operational resilience. Every engagement starts on the plant floor, hands-on and on-site, not on a remote scan.

Our Core Services

- OT Security Maturity Assessments
- OT Risk & Vulnerability Analysis
- OT Program Design & Governance
- Expert-Level OT Security Engineering
- Fractional CISO & Advisory Support
- OT Governance, Risk & Compliance (GRC) as a Service
- OT Staff Augmentation & Contract Specialists
- Resilion.io, AI Execution Engine for OT Cybersecurity

Resilion.io is Hillstrong's AI-powered OT cybersecurity platform, delivering continuous visibility, risk quantification, and program execution (build, execute, manage), so assessment findings translate into measurable resilience.

www.hillstrongsecurity.com · Based in Atlanta, GA · Solving cybersecurity challenges globally