SIXMAP

SIXMAP RESEARCH REPORT

Operational Technology Exposure Report 2026

An analysis of OT exposures around the globe and within the United States.

June 2026

Table of **Contents**

EXECUTIVE SUMMARY

An internet-wide measurement of **exposed OT**

Operational technology (OT) is the digital control layer for physical systems: the programmable controllers, tank gauges, building-automation systems, and telemetry units that run critical infrastructure across industries. When these systems are reachable from the public internet, they become an attack surface that is both unusually fragile and highly consequential: many can be disrupted by a single malformed connection, and a successful manipulation can have physical, not merely digital, effects.

SixMap conducted an internet-wide measurement study across the routable IPv4 address space and, using its proprietary 6Gen technology to discover live hosts in the IPv6 space, across roughly 61 million discovered IPv6 hosts. After scanning 82 of the most common OT protocol ports and systematically filtering out noise, false signals, and non-OT services, we confirmed a verified population of **14,524 internet-exposed OT services worldwide** (14,409 on IPv4 and 115 on IPv6), of which the United States is the single largest source. The U.S. set analyzed in depth comprises **1,537 verified exposures**.

82	14,524	1,537	12%
OT technology ports probed	verified OT exposures worldwide	verified OT exposures in the U.S.	of U.S. OT protocols exposed have a known CVE

Key findings

- **Exposure spans every critical-infrastructure sector.** Verified exposures include industrial controllers (Modbus, EtherNet/IP, Siemens S7, Omron FINS), grid telecontrol (IEC 60870-5-104, DNP3, synchrophasors), and fuel-storage tank gauges (ATG).
- **Fuel-storage gauges are the single largest U.S. category, and the most revealing.** Of the 1,537 U.S. exposures, 755 are tank gauges, and 91% of them broadcast a site name and 48% a full street address in plain text to anyone who connects.
- **Exposed OT is overwhelmingly carrier-hosted, yet still attributable.** Using only passive data, SixMap tied 73% of worldwide exposures and 58% of U.S. exposures to a specific named organization.
- **These systems carry known, fixable vulnerabilities.** Under a strict, version-pinned standard, 179 of the 1,537 U.S. exposures (12%), and 413 of 14,524 worldwide (3%), run firmware whose version falls within a documented CVE's affected range, though none matched a vulnerability in CISA's Known Exploited Vulnerabilities catalog.

INTRODUCTION

Why **OT Exposure** Matters

Most cybersecurity attention is paid to information technology (IT): servers, laptops, web applications, and the data they hold. Operational technology is different in kind. It is the layer of hardware and firmware that senses and controls the physical world, including the programmable logic controllers (PLCs) that drive pumps and motors, the units that operate on the electric grid, the systems that regulate building heating and ventilation, and the gauges that monitor fuel storage.

These exposures also draw a specific and capable class of adversary. Nation-state actors have shown sustained interest in operational environments, not to cause immediate damage but to quietly pre-position inside critical infrastructure and hold persistent access they can exploit at a moment of their choosing.

Exposure is almost always accidental

OT systems are generally designed to run on isolated, trusted networks, not the open internet. When they appear on the public internet it is rarely a deliberate decision. More often a device is connected through a cellular modem or broadband line for remote convenience, a firewall rule is misconfigured, or a system is stood up quickly and never hardened.

Cyber-domain risks, real-world consequences

01 **Disruption and downtime.** Many OT protocols have little or no authentication and were never built to withstand hostile traffic, so a basic flood of requests, or even a single malformed packet, can knock a fragile field device offline.

02 **Exploitation beyond fragility.** These are real software and firmware stacks with publicly documented vulnerabilities, so an exposed, unpatched controller is a candidate for direct compromise, in some cases remote code execution.

03 **Physical worst case.** Because OT is the interface to physical equipment, a compromise can cross from the digital domain into the physical one, where the failure mode is not lost data but a physical event that can put human lives at risk.

The AI inflection point

Until recently, turning an exposed device into a working attack required scarce, specialized expertise. That barrier is eroding: frontier AI systems are increasingly capable at reading unfamiliar code and firmware, finding vulnerabilities, and drafting exploits. An attack surface long protected mainly by obscurity becomes exactly the one AI-assisted attackers are best positioned to open up.

> An attack surface long protected mainly by obscurity becomes exactly the one **AI-assisted attackers are best positioned to open up.**

Why this research matters to SixMap

Discussions of OT risk often rely on narrow-scope research and limited data sets. SixMap set out to open the aperture with global measurement, establishing at internet scale how much OT is exposed, what kinds of systems they are, and what they reveal about themselves. It is the same discipline SixMap applies for its customers every day, pointed at a single organization's external attack surface.

The quality of that measurement depends on infrastructure most security vendors do not control. SixMap operates its own ISP with Tier 1 peering out of two datacenters (one east coast, one west) for fast, reliable internet access and highly accurate results, with no third-party filtering of its traffic.

All discovery is conducted with advanced technology designed to be efficient, quiet, and non-intrusive. Every finding is derived entirely from data exposed systems volunteered in response to benign connection attempts, without ever altering or disrupting any OT system.

METHODOLOGY

How This **Research** Was Conducted

The research began with a complete sweep of the internet rather than a sample. SixMap examined the entire routable IPv4 address space and, using its proprietary 6Gen technology, the roughly 61 million live hosts it discovered in the IPv6 space — then checked each address against 82 ports associated with the most widely deployed OT protocols, asking a simple question of every address-and-port pair: is something listening here? On IPv4, that first pass returned roughly **4.1 million responsive addresses** — a raw map of everywhere on the internet that, at first glance, appeared to be running an OT-associated service. The IPv6 assessment applied the same methodology; its numbers and findings are broken out on page 12.

From open ports to real services

An open port is not proof of an OT system, and the drop from here is dramatic — only about **0.4%** of the responsive IPv4 addresses turned out to be genuine OT. Two filters account for the fall. First, many responses came from ordinary internet infrastructure answering on OT-associated ports: a common alternate-administration port, 2222, was running ordinary SSH on 291,871 hosts, and the alternate web ports 8080 and 8443 were serving standard HTTP/HTTPS on 41,347 and 43,929 hosts — routers, cameras, and web consoles, not industrial devices. Second, of the connections that remained, SixMap actively inspected each one: it collected the data the service returns when contacted and decoded it against the actual structure of each OT protocol, keeping only those whose bytes matched a specific industrial protocol at the correct port. After both filters, **15,368** IPv4 addresses returned a genuine industrial-protocol signature. In every case SixMap relied on the decoded response, not the port label.

Verifying what is genuinely OT

A service was counted only when its decoded response carried the unmistakable byte-level signature of a specific industrial protocol. Two classes of impostor were then removed: promiscuous hosts that answer on many ports at once (honeypots, firewalls, and scanning infrastructure), and research sensors built to imitate industrial protocols. The result is a deliberately conservative count.

From raw IPv4 scan to verified population	COUNT
Responsive addresses evaluated	4,053,274
Genuine protocol-signature candidates	15,368
Less: honeypots, sensors & scanner false signals	−959
Verified OT exposures on IPv4	**14,409**
Verified OT exposures on IPv6 (see p12)	+115
Verified OT exposures worldwide	**14,524**

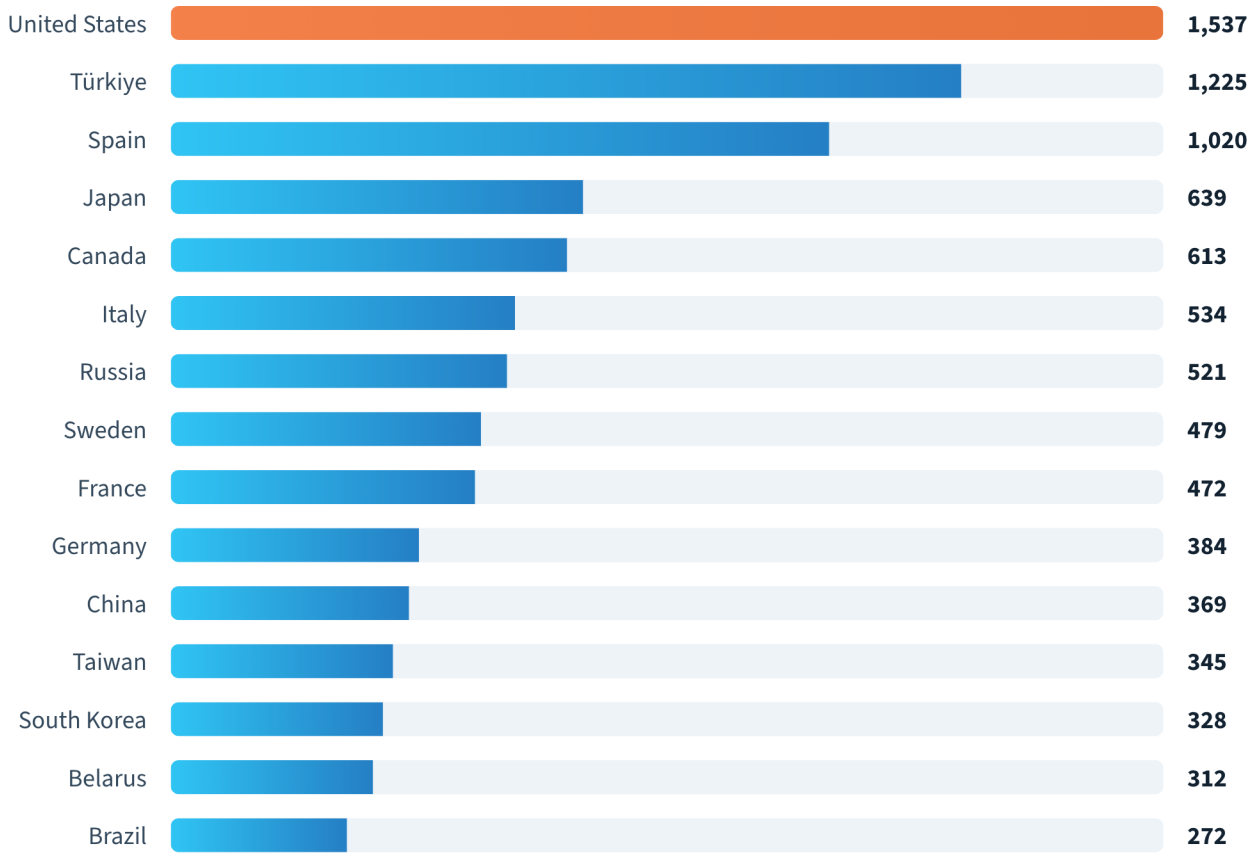
GLOBAL EXPOSURE MAP

Mapping OT Exposures **Around the World**

SixMap resolved the location of each exposure by combining the position a device reports in its own responses with corroborating network geolocation; a location was resolved for **86%** of the verified population. Exposed OT is a global phenomenon, but it is not evenly distributed: it concentrates in industrialized economies with large installed bases of networked control equipment. The United States is the single largest source, followed by a broad mix of European, Asian, and other industrialized nations.

Top 15 countries by verified OT exposures

Geolocated population = 12,550 (86.4% of 14,524). United States highlighted.



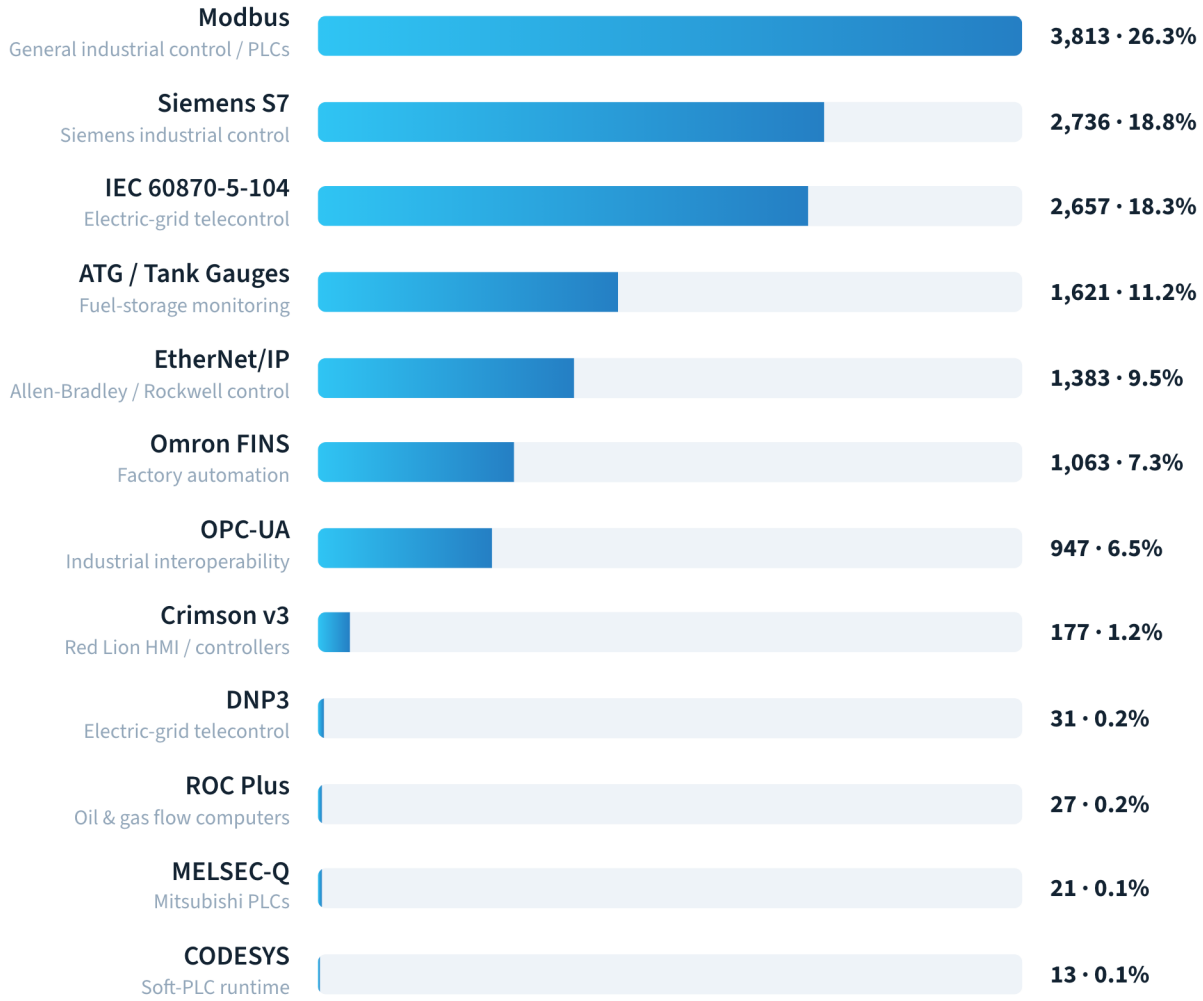
All other countries combined	**3,500** (27.9% of geolocated OT exposures)

PROTOCOLS EXPOSED

A Summary of **Protocols Exposed**

The mix is led by general industrial control and grid telecontrol. Modbus, IEC 60870-5-104, and Siemens S7 together make up well over half of everything found, with fuel-storage tank gauges and factory-automation protocols close behind. The breadth matters as much as the ranking: this is a cross-section of the systems that run physical infrastructure, from factory floors to the electric grid, and no single sector or fix accounts for the problem.

DISTRIBUTION BY PROTOCOL FAMILY · SHARE OF 14,524 VERIFIED EXPOSURES

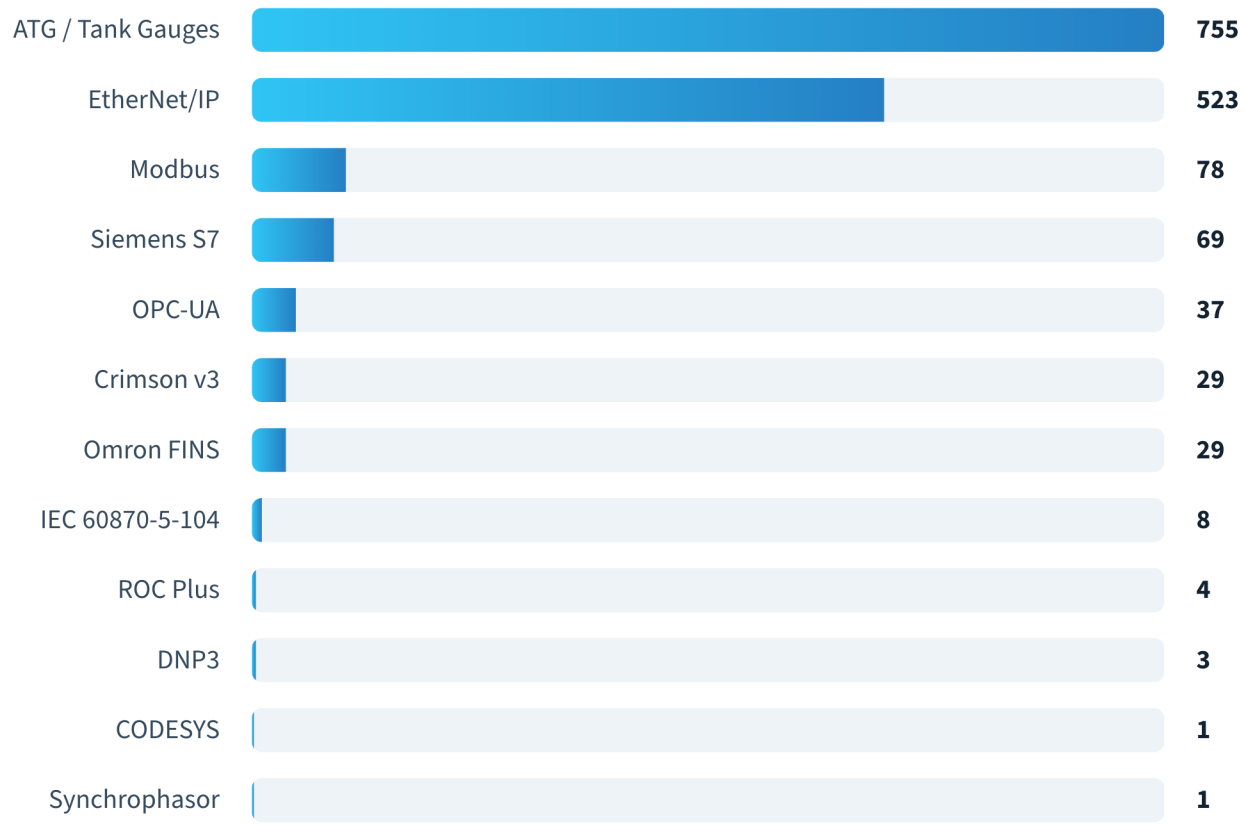


UNITED STATES

OT Exposures Within the **United States**

The United States is the largest single source of verified exposures, with **1,537 verified U.S. exposures**. Its profile is more concentrated than the global one: fuel-storage tank gauges and Allen-Bradley / Rockwell industrial controllers together account for the large majority of domestic exposure, with Modbus, Siemens S7, and OPC-UA making up most of the remainder.

VERIFIED U.S. EXPOSURES BY PROTOCOL FAMILY

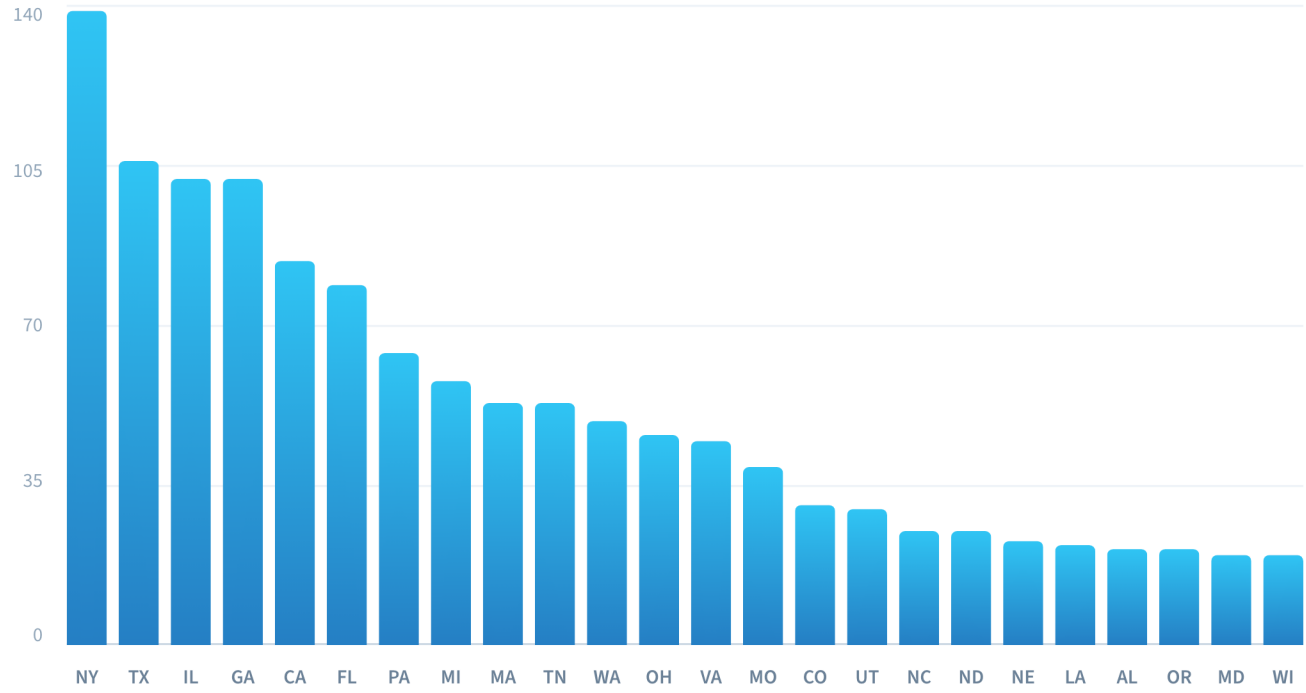


> Tank gauges and Allen-Bradley / Rockwell controllers alone account for **over 80% of U.S. OT exposures.**

Geographic distribution

Exposed OT is national in footprint, spanning 50 states and territories. The distribution combines the location a device reports in its own responses with corroborating geolocation; fuel-storage gauges, which print their physical location in plain text, anchor the picture.

VERIFIED U.S. EXPOSURES BY STATE · TOP 24



Exposure concentrates in a few states

Top 4 states (NY, TX, IL, GA) — 29% of all U.S. OT exposures

ATTRIBUTION

Who Owns the Exposure, **and What It Reveals**

Counting exposures is only half the picture; the more useful question is whose systems these are, and what they give away. Using only passive, externally observable signals (internet-registry records, reverse-DNS and domain ownership, the equipment's own self-disclosed site identity, and physical-address geocoding), SixMap tied a large share of exposures to a specific operating organization, without ever contacting a device.

73%
of worldwide exposures attributed to an org

58%
of U.S. exposures attributed to an org

687
U.S. exposures that disclosed a site name

362
U.S. exposures that leaked a street address

The single richest source of attribution is the equipment itself. Fuel-storage tank gauges, the largest U.S. category, respond to an unauthenticated connection with a plain-text status report that often names the site and prints its street address: **687 U.S. exposures disclosed a site name and 362 a full street address**, effectively handing anyone who connects a business card for a piece of critical infrastructure. In all, SixMap resolved a named organization for **10,621 of 14,524 exposures worldwide (73%)** and 893 of 1,537 in the United States; the unattributed remainder sit behind broadband providers whose records name only the carrier.

How U.S. owners were identified

Attribution method	What it draws on	U.S. owners named
Device self-identification	Tank-gauge site name printed by the device	**705**
Registry sub-allocation	Registry records naming a business customer	**93**
Independent enrichment	Corroborating org from independent observation	**87**
Domain & registry ownership	Reverse-DNS domain and registrant records	**8**

DOCUMENTED VULNERABILITIES

From Exposure to **Vulnerability**

SixMap took every exposure that disclosed an exact make, model, and firmware version and mapped it to its Common Platform Enumeration (CPE) identity, then looked each up in the U.S. National Vulnerability Database (NVD) and enriched every CVE with its CVSS base score and EPSS exploit-probability. Under a strict, version-pinned standard, **413 of 14,524 worldwide (3%) — 179 of them in the United States (12%)** — run firmware that falls within a documented CVE's affected-version range. None of the matched CVEs appears in CISA's Known Exploited Vulnerabilities catalog.

1,624 (11%)
fingerprinted to an exact firmware version & CPE

5,346 (37%)
resolved only to vendor & product (mostly tank gauges)

Version-confirmed CVEs · OT exposures where only a product name, but no precise version number, were excluded.

CVE ID	Product	Affected	CVSS	EPSS	Count	Top countries
CVE-2017-16740	MicroLogix 1400	≤ 21.0	10.0	7.3%	312	US, CA, TW
CVE-2017-7901	MicroLogix 1100 / 1400	≤ 16.0	8.6	6.6%	316	US, CA, ES
CVE-2017-7898	MicroLogix 1100 / 1400	≤ 16.0	9.8	5.1%	316	US, CA, ES
CVE-2017-7899	MicroLogix 1100 / 1400	≤ 16.0	9.8	4.6%	316	US, CA, ES
CVE-2016-9334	MicroLogix 1100 / 1400	≤ 15.0	7.3	4.0%	258	US, CA, ES
CVE-2017-7903	MicroLogix 1100 / 1400	≤ 16.0	9.8	2.7%	316	US, CA, ES
CVE-2017-7902	MicroLogix 1100 / 1400	≤ 16.0	9.8	2.6%	316	US, CA, ES
CVE-2016-9338	MicroLogix 1100 / 1400	≤ 15.0	2.7	2.4%	258	US, CA, ES

Each row is version-confirmed: the affected-version range shown is NVD's, and Count is the number of fingerprinted exposures whose firmware falls within that range. CVEs whose applicability is an unbounded "all versions" wildcard are excluded. This standard limits the published set to Rockwell Allen-Bradley controller families whose firmware revision maps unambiguously onto NVD's versioning; families such as Siemens S7 are excluded rather than over-claimed. All 413 matched exposures sit on IPv4.

EXTENDING THE SCAN

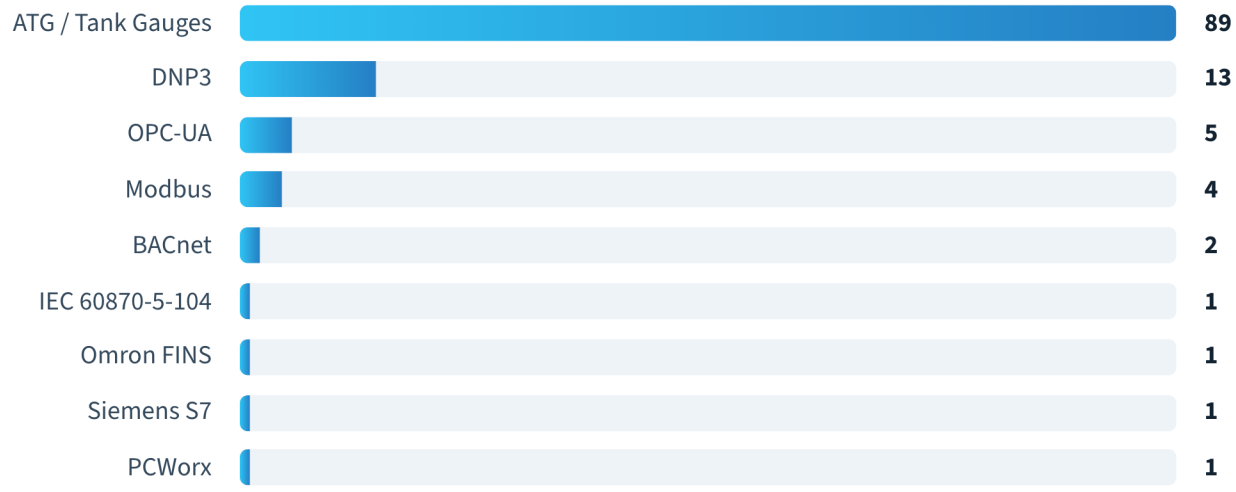
Extending the Scan to **IPv6**

The routable IPv4 space is finite; once scanned in full it gives a complete picture of what is exposed there. IPv6 is not. The address space is astronomically large and mostly unallocated, so finding the small fraction that carries live hosts is a research problem of its own, and the reason nearly every internet-wide OT study to date has been IPv4-only. SixMap's proprietary 6Gen technology maps the global IPv6 space and identifies live hosts with high precision (about 61 million worldwide, more than any comparable public dataset), then runs them through the same pipeline used for IPv4: the same 82 ports, protocol-level verification, and conservative filtering.

~61M	82	510	115
live IPv6 hosts discovered	operational-technology ports probed	genuine protocol-signature candidates	verified OT exposures on IPv6

The population is small by design. Of the 510 IPv6 hosts that returned a valid industrial-protocol signature, 395 were removed for cross-protocol behavior consistent with research honeypots, templated single-service clusters on cloud infrastructure, or explicit hosting-provider tenancy (Hostinger, OVH, Hetzner, Scaleway, Linode, and others). Under that strict standard, the final verified count is **115**.

VERIFIED IPV6 EXPOSURES BY PROTOCOL FAMILY



Attribution is weaker on IPv6: a country resolved for only 30% of the 115, clustering in China (13), Hong Kong (6), Switzerland (4), and Brazil (4), and firmware fingerprints were too sparse to yield version-pinned CVE matches, which is why page 11's table draws exclusively from IPv4. The takeaway: IPv6 is not, today, a significant OT attack surface, but it can now be measured on the same basis as IPv4 with SixMap's technology.

CONCLUSION

What can be measured **can be managed**

Internet-exposed operational technology is not a rare edge case. Measured rigorously, at internet scale across both the IPv4 and IPv6 address spaces, it is a standing population of 14,524 verified systems worldwide, with the United States the largest single source at 1,537 verified exposures: controllers, grid devices, and fuel-storage gauges that were almost never meant to be reachable from the open internet.

The significance lies in the combination of factors: these systems are fragile and frequently disruptable; many run software with publicly known vulnerabilities; they sit at the boundary between the digital and physical worlds; and a meaningful share disclose their own identity and location to anyone who asks. The arrival of capable, AI-assisted vulnerability discovery steadily lowers the barrier to turning any one of these exposures into an incident.

The encouraging part is that this is a knowable, measurable problem. Every exposure here was found using only externally observable data, which means defenders can find their own exposed OT the same way, before an adversary does. The essential first step is visibility: knowing what an organization actually presents to the internet, across its entire address space (both IPv4 and IPv6) and every port, rather than what it believes it presents.

Key takeaways from this report

Internet-exposed OT is a large, standing population, not an edge case. SixMap verified thousands of exposed industrial controllers, grid devices, and fuel-storage gauges worldwide using a strict, protocol-level standard, and the United States is the single largest source.

Exposure plus disclosure plus known CVEs equals actionable risk. These systems are fragile and trivially disruptable, a meaningful share run firmware with publicly documented vulnerabilities, and many broadcast their own site name and street address, turning an anonymous exposure into a targeted one.

Most attack surface management tools do not detect OT exposures. They focus on web and IT assets on standard ports and miss industrial protocols entirely. Confirm that OT discovery is in scope, not assumed.

Visibility is the first and decisive step. Every exposure here was found with externally observable data alone, so defenders can find their own exposed OT the same way an adversary would, across the entire address space and every port, and remediate the connectivity, segmentation, or configuration that put it online before it is exploited.

SIXMAP

PREPARING FOR THE ERA OF AI

Cyber Fundamentals, **Delivered at Machine Speed**

With frontier AI models changing the dynamics of the cyber threat landscape, the most effective response is to double down on the foundations that now matter more than ever: complete asset inventories, fast and effective risk detection, and agile vulnerability management.

THE SIXMAP PLATFORM

A continuous, four-step view of **everything you expose**

The SixMap platform delivers cyber fundamentals continuously and with high precision: mapping an organization, discovering all assets across both IPv4 and IPv6, and inspecting all 65,535 ports on each host to surface IT and OT exposures, then enriching each CVE finding with threat intelligence so teams know what to fix first.

MAP

Organization Mapping

Map your organization's structure and identify all entities, so every asset is automatically assigned to the responsible entity.

DISCOVER

Across IPv4 & IPv6

Discover hosts with high precision across both the IPv4 and IPv6 address spaces, continuously rather than point-in-time.

ASSESS

All 65,535 Ports

Inspect all 65,535 ports on each asset, every week, to uncover IT and OT exposures on the non-standard ports other tools miss.

PRIORITIZE

Risk-Based Prioritization

Detect hidden CVEs and prioritize them with threat intelligence (which CVEs are exploited in the wild and by whom) for faster mitigation.

SixMap continuously maps, discovers, and monitors all aspects of an organization's digital estate, revealing all IT and OT exposures visible from the public internet. These capabilities support whole-of-state cyber initiatives, helping state-level security teams protect all entities across the state from cyber attacks.

ABOUT SIXMAP

Know thyself. **Preemptively reduce risk.**

SixMap delivers the most complete and accurate external view of any public or private organization, showing security teams who they are, what they own, and what they must protect. By closing the gap between what security teams monitor and what adversaries find through reconnaissance, SixMap helps customers mitigate risks before attacks occur. Its strategic mapping ensures no assets are overlooked, while advanced technology pinpoints hosts, exposures, and risks with precision. Born out of national defense and deployed to protect some of the nation's most sensitive networks, SixMap now brings military-grade capabilities to public and private organizations to preemptively stop cyberattacks.

BOOK A DEMO

6731 Columbia Gateway Dr, Suite 100, Columbia, MD 21046
sixmap.io

SIXMAP