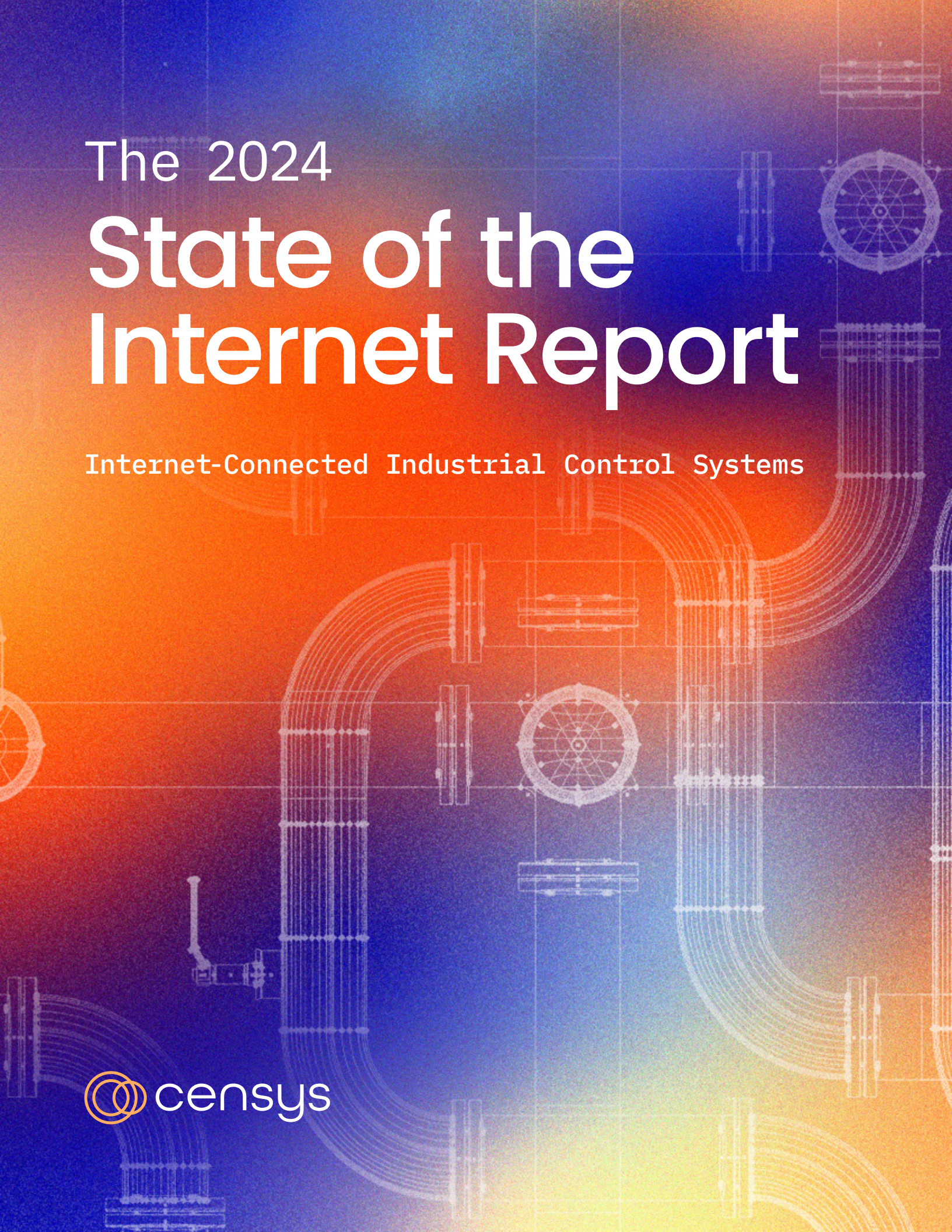
The 2024

State of the Internet Report

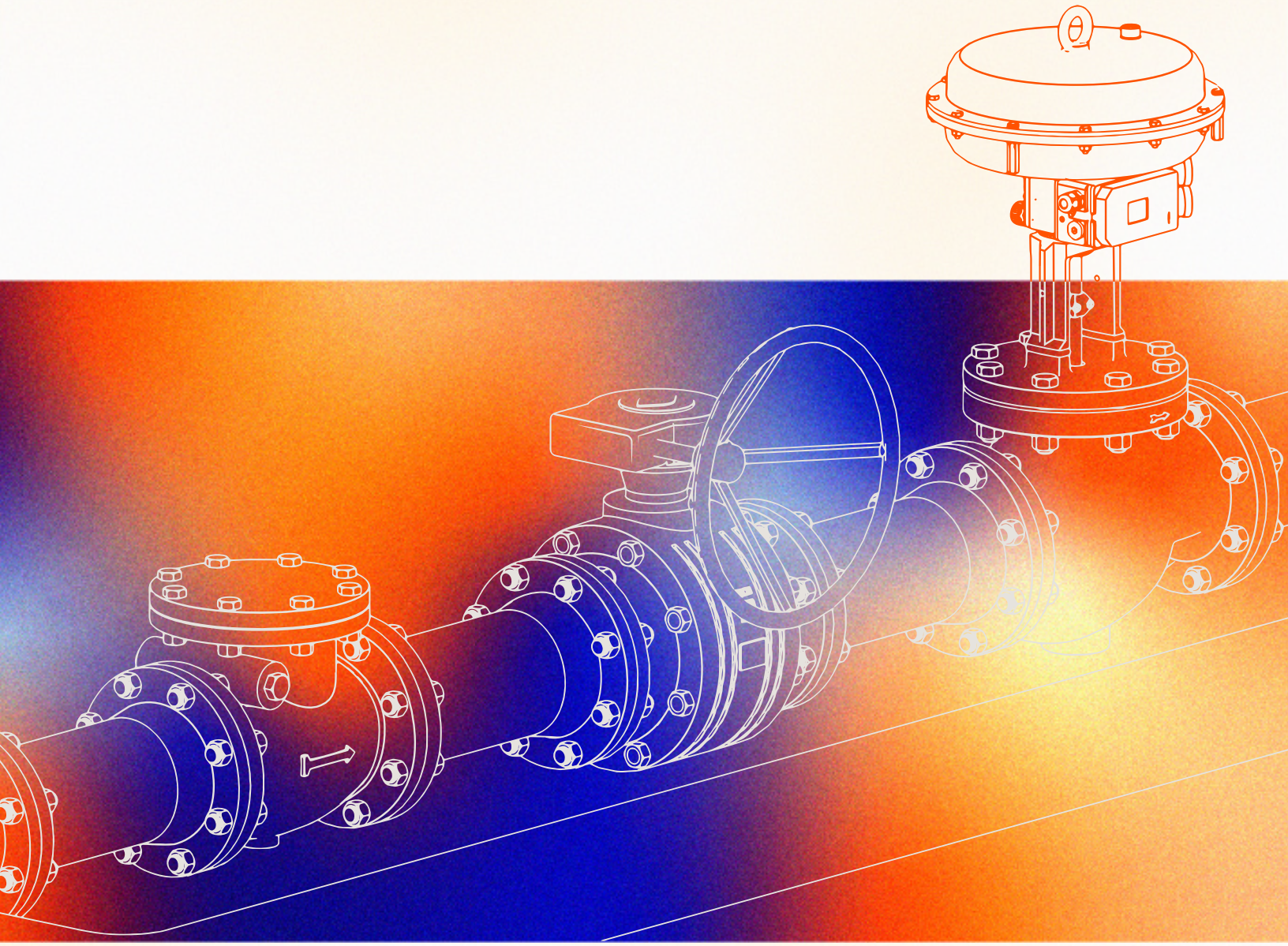
Internet-Connected Industrial Control Systems



censys

Table of Contents

Introduction



Introduction

For years, security researchers have warned about **industrial control systems (ICS)** exposed to the Internet. Reports on the number of devices that speak protocols like Modbus and Siemens S7 are often used to express the severity of the problem, but these protocol exposures are only part of a more nuanced story.

ICS protocols, also known as automation protocols, are communications protocols that enable data exchange between systems in industrial or automated environments. They often lack robust security measures, such as use of TLS or authentication. Initial implementations of some protocols date back to the 1970s, but they remain foundational to industrial processes.

Despite not necessarily having a broad range of functionality, several of these protocols have been leveraged by ICS-specific malware variants. Of the known ICS-specific malware variants, the following in some way leveraged ICS protocols we'll examine in this report:

Industroyer

Year Known/Reported..... **2017**
Protocol(s) Leveraged..... **IEC 60870-5-101, 104; IEC 61850; OPC DA**
Sector(s) Targeted..... **Electric**

Industroyer v2

Year Known/Reported..... **2022**
Protocol(s) Leveraged..... **IEC 60870-5-104**
Sector(s) Targeted..... **Electric**

PIPEDREAM

Year Known/Reported..... **2022**
Protocol(s) Leveraged..... **CODESYS; OPC UA; FINS**
Sector(s) Targeted..... **Unknown**

COSMICENERGY

Year Known/Reported..... **2023**
Protocol(s) Leveraged..... **IEC 60870-5-104**
Sector(s) Targeted..... **Electric**

FrostyGoop

Year Known/Reported..... **2024**
Protocol(s) Leveraged..... **Modbus**
Sector(s) Targeted..... **Energy**

While attacks on ICS are increasingly common, many organizations are attacked via IT vulnerabilities rather than through the ICS systems themselves. Attacks specifically leveraging ICS protocols are often highly targeted and require specialized knowledge and understanding of such environments.

ESET's 2017 report on Industroyer sums it up well:

> **Those behind the Win32/Industroyer malware have a deep knowledge and understanding of industrial control systems and, specifically, the industrial protocols used in electric power systems. Moreover, it seems very unlikely anyone could write and test such malware without access to the specialized equipment used in the specific, targeted industrial environment.**

Although the required knowledge and resources for such an operation are relatively high, this has not prevented actors with limited resources and expertise from discovering ways to attack ICS.

Ecosystem Shift

While there have been attacks on ICS infrastructure for well over a decade, 2023 was a turning point in this space.

On November 25, 2023, the Municipal Water Authority of Aliquippa, Pennsylvania discovered that it had been compromised by an Iranian Islamic Revolutionary Guard Corps (IRGC)-affiliated hacking group. The group, known as the CyberAv3ngers, took control of a water pressure monitoring and regulation system at a remote pumping station, defacing the system's interface with an anti-Israel message.

Image from a defaced HMI during the November 2023 CyberAv3ngers campaign.

Soon after, in January 2024, the Cyber Army of Russia Reborn (CARR), a hacking group purportedly linked to Russia's military intelligence, caused the overflow of water storage tanks and minor, temporary disruption of operations in the small Texas town of Muleshoe. The group later claimed responsibility for manipulating human-machine interfaces (HMIs) at these facilities, taking to Telegram to post a screen recording of unauthorized access and manipulation of the interfaces.

These attacks on ICS were minor, especially in the larger context of ICS attacks such as those involving Industroyer, which resulted in power outages across Ukraine in 2016.

These attacks were also fundamentally different from attacks of years past. Instead of compromising water facilities through IT networks or using highly specialized malware, these attacks were much simpler to execute: they leveraged Internet-connected HMIs for exploitation over the public Internet.

HMIs are graphical interfaces that allow operators to interact with systems and machinery found in industrial settings. Often, HMIs are connected to the Internet to enable operators to remotely manage and monitor systems. HMIs offer user-friendly graphical interfaces that are easy to manipulate, but as with any technology, reducing friction for the intended user also reduces friction for threat actors. Thousands of HMIs are exposed to the Internet globally, many without any form of authentication or other access controls. Though there were no major issues with water quality or supply in these recent attacks on water facilities, with so many ICS devices and HMIs exposed to the public Internet, the implications of such attacks loom large.

In this report, we examine the Internet exposure of ICS services and HMIs. We strive to illustrate the exposure landscape in a measured, non-sensational way to help operators and defenders better understand the true attack surface of industrial control systems around the world.

Executive Summary

1. Censys observes over 145,000 exposed industrial control systems (ICS) services globally. 38% of these services are in North America, 35% are in Europe, and 22% are in Asia. The U.S. alone is responsible for over one third of global ICS service exposures.

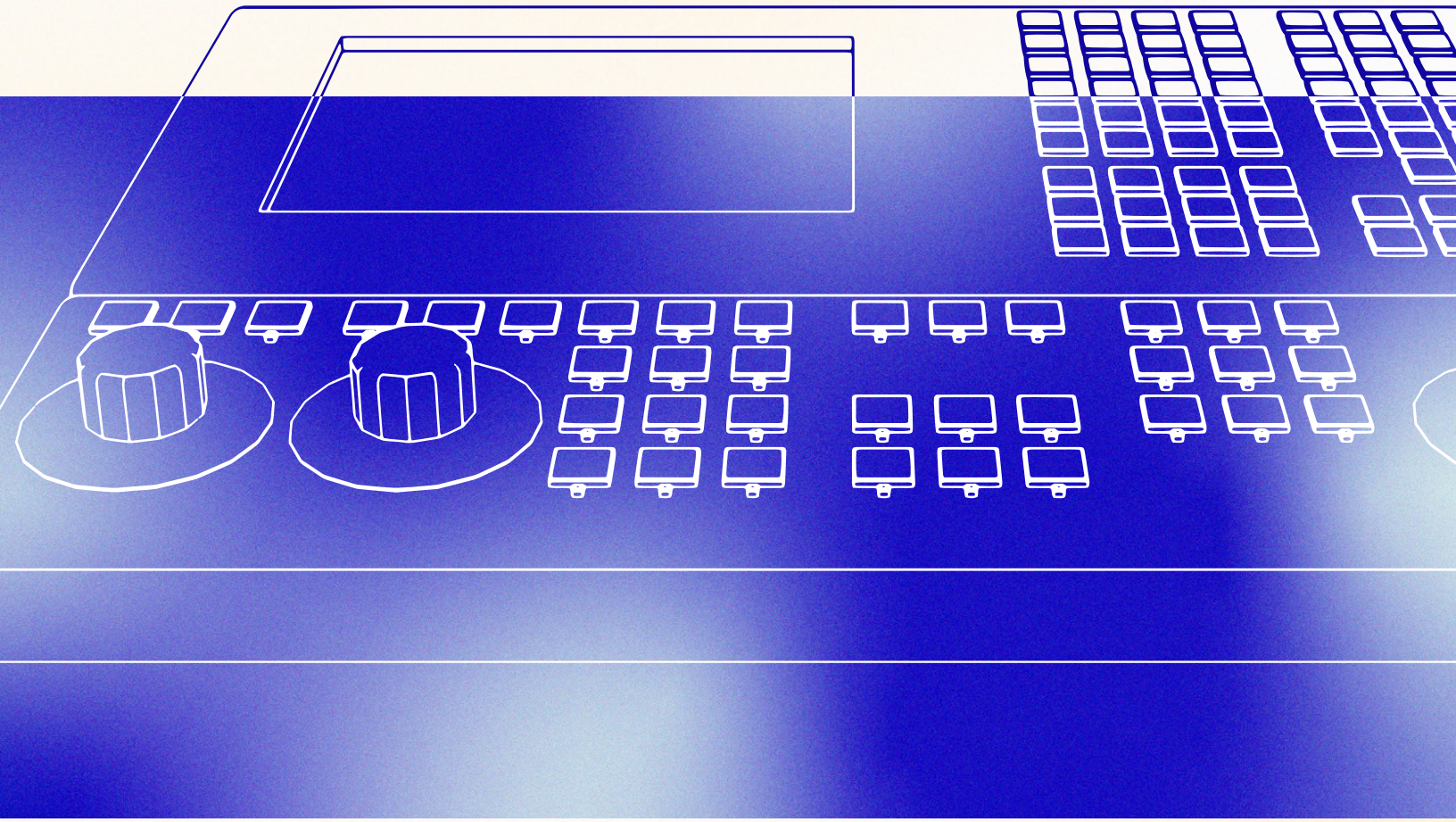
2. ICS attack surfaces are regionally unique. Modbus, S7, and IEC 60870-5-104 are more widely observed in Europe, but Fox, BACnet, ATG, and C-More are more commonly found in North America.

3. Censys researchers analyzed C-More human-machine interfaces (HMIs) and found that 34% are water and wastewater related, while 23% are associated with agricultural processes.

4. Censys researchers discovered nearly 200 hosts running HMIs that were also running products from vendors explicitly prohibited by the U.S.'s National Defense Authorization Act (NDAA) Section 889. While not all of these hosts are critical infrastructure, government-operated, or even located in the U.S., this serves as a reminder that operators should be mindful of what products and software they allow to run alongside industrial processes.

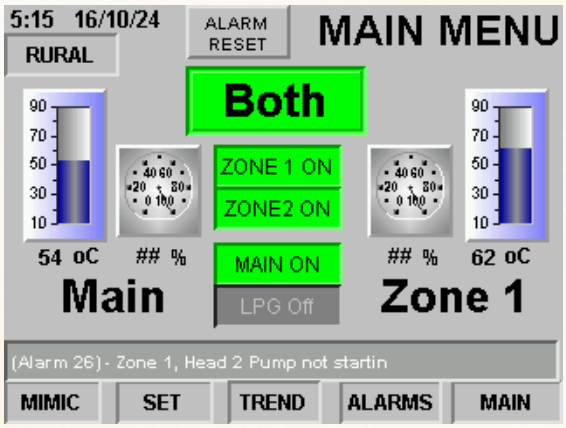
5. Globally, most observed ICS services and HMIs run on mobile or consumer and business-grade ISPs. Given the often remote nature of industrial facilities, a wired Internet connection may not be readily available. 5G or LTE routers, typically provided by mobile service providers, are a common solution to this connectivity issue. However, lack of useful metadata (e.g., DNS) for hosts on these networks can make it nearly impossible to determine a system's owner or intended purpose.

Human-Machine Interface Exposure



Human-Machine Interface Exposure

Human-machine interfaces, or HMIs, are interfaces that operators use to monitor and interact with industrial systems. Such devices are typically physically found in industrial environments but are increasingly connected to the Internet to support remote access.

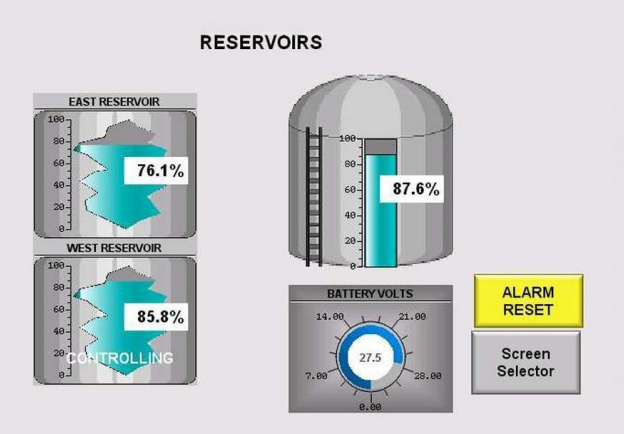


Example HMI accessed over VNC. Operators can monitor pumps for various operation zones from this interface.

While remote access facilitates operations, it also makes threat actors' operations easier. Many of these systems are directly exposed to the Internet without authentication or additional protections such as VPNs. This ease of access and manipulation likely contributed to CARR and CyberAv3ngers' defacement and manipulation of such interfaces in 2023 and 2024.

We examined exposure of over 20 types of HMI software, including Automation Direct C-More HMI, Red Lion Crimson, and Siemens SIMATIC HMI and identified nearly 7,700 hosts across 80 countries running HMIs. We note that our scanning is passive; we never attempt to gain unauthorized access to systems, but rather observe what is publicly exposed on the Internet.

- **AutomationDirect C-More** HMIs run a public web server with a read-only view of each programmed screen. They also run a proprietary protocol built specifically to program the HMIs, which is enabled by default and has weak or no authentication.
- **Red Lion Crimson** is a web-based HMI that is often misconfigured to allow full remote access. An attacker can control automation systems using the web interface and proprietary protocol. Device logs and system information can be obtained using the same interfaces.
- **Siemens SIMATIC HMI** panels can be configured for remote, web-based access. An actor can view system diagnostics over the web and interact with the HMI via Siemens Sm@artClient software.



A C-More HMI monitoring reservoir and tank levels.

HMIs By the Numbers

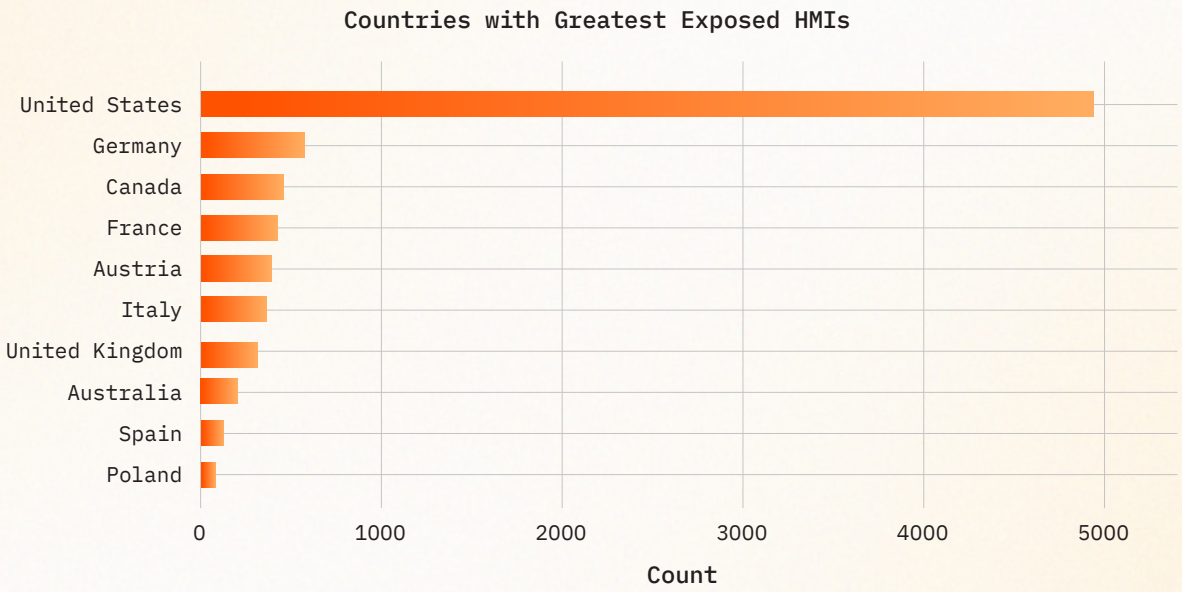
COMMONLY OBSERVED HMI SOFTWARE

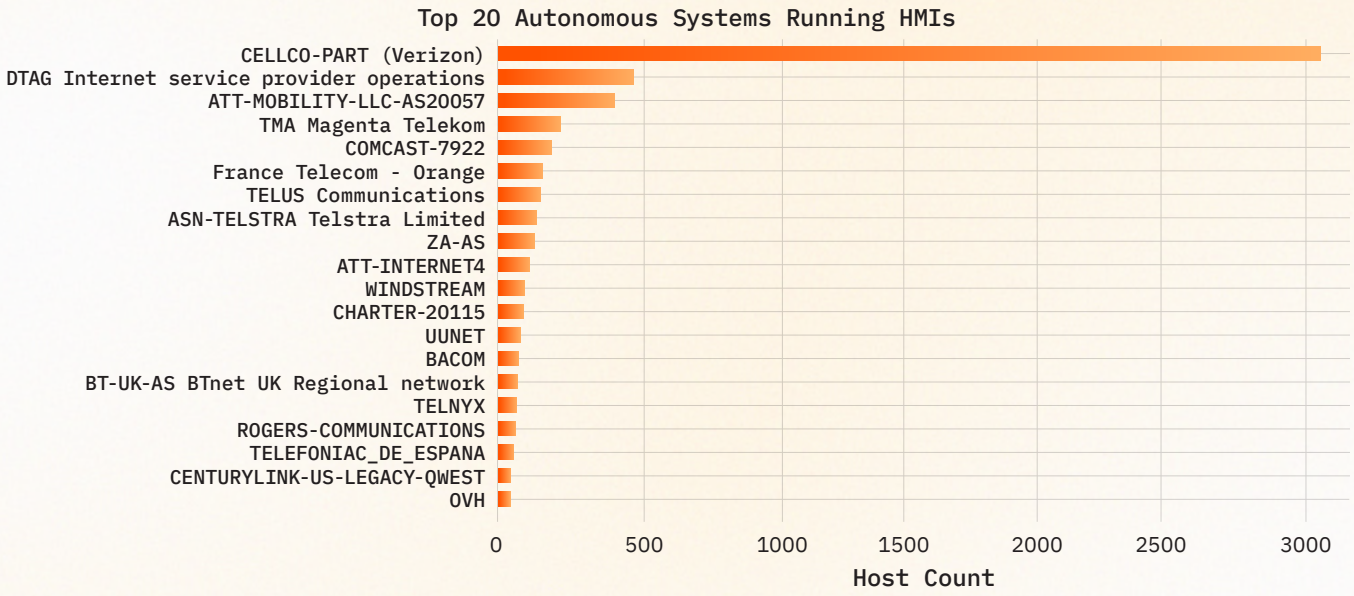
HMI Software	Host Count
AutomationDirect C-More HMI	2,823
Red Lion Crimson	2,726
Siemens SIMATIC Miniweb	973
Siemens SIMATIC HMI Comfort Panels	873
Siemens Sm@rtClient	827
atvise	351
Industrial Control Links ScadaFlex II	82
Siemens Fieldpanel Web	60
Rockwell Automation PanelView	42

REGIONAL DIFFERENCES

Continent	% of Observed HMIs
North America	69.43
Europe	26.94
Oceania	2.27
Asia	0.96
South America	0.23
Africa	0.15

Nearly 70% of the exposed HMIs we observe are located in North America, while nearly 27% are found in Europe. The majority of exposed HMIs are located in the U.S.





NETWORKS

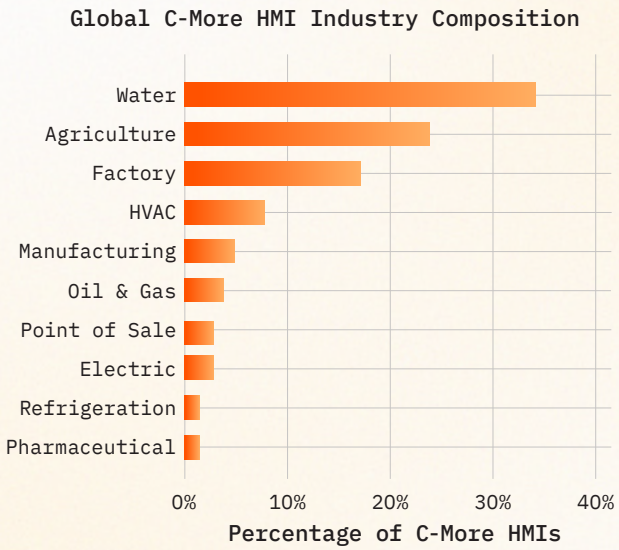
Globally, most HMIs run not in the cloud or on organization-owned ASes, but on mobile or business-grade ISPs. Given the often remote nature of substations, power plants, or other industrial facilities, a wired Internet connection may not be readily available. 5G or LTE routers, typically provided by mobile service providers, are a common solution to this connectivity issue.

While useful for connectivity, this can present challenges when attempting to determine ownership of a given HMI; there is rarely useful host or network metadata that indicates who might be responsible for a system. However, many HMIs contain company logos, plant names, addresses, and other clues that can be helpful in determining ownership.

CELLCO-PART, where we observe the majority of HMIs, is the formal business name of Verizon Wireless, a leading mobile provider in the U.S. Similarly, DTAG, or Deutsche Telekom, is a major mobile and telecommunications provider headquartered in Germany.

INDUSTRIES

We collected and analyzed 4,137 screenshots from over 200 C-More HMIs across multiple dates to better understand global industry impacts of such exposures. Through a combination of machine learning and manual review, we were able to determine industry for C-More HMIs on 125 hosts.



Of those we could confidently classify by industry, we find that 34% of C-More HMIs are water and wastewater related, including water treatment facilities and reservoir level monitoring. 23% are related to agriculture, including crop management and greenhouses.

While the above data reflects global C-More exposure, we note that C-More is most prominent in North America.

ADDITIONAL FINDINGS

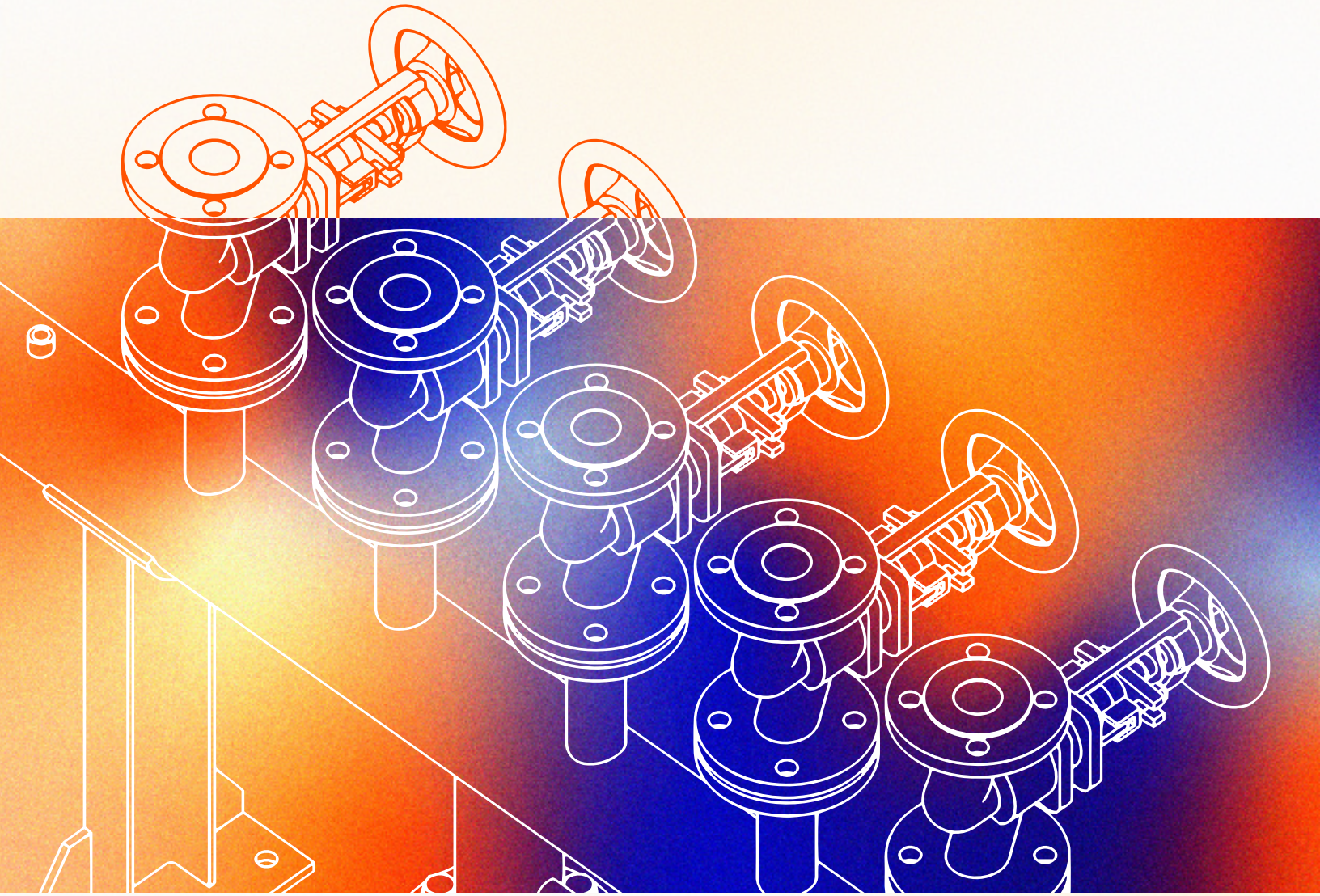
In addition to running HMIs, nearly 200 of these hosts were also running products from vendors explicitly prohibited by the U.S.'s National Defense Authorization Act (NDAA) Section 889. While not all of these hosts are critical infrastructure, government-operated, or even located in the U.S., this serves as a reminder that operators should be mindful of what products and software they allow to run alongside industrial processes.

We also identified an HMI whose router appeared to be infected with the 7777 botnet for several weeks throughout September and October 2024 (at minimum). We were unable to determine the likely industry of this HMI, and at the time of writing, the host no longer appears to be infected.

HMI CLOSING THOUGHTS

HMI exposures represent the most concerning and compelling exposures in the ICS space. While remote access and ease of use facilitate operators' jobs, these same attributes lower the bar for threat actors seeking to disrupt industrial processes. Moreover, it's often possible to determine the owner or operator of the HMI, making targeting of specific organizations much easier.

ICS Protocol Exposure

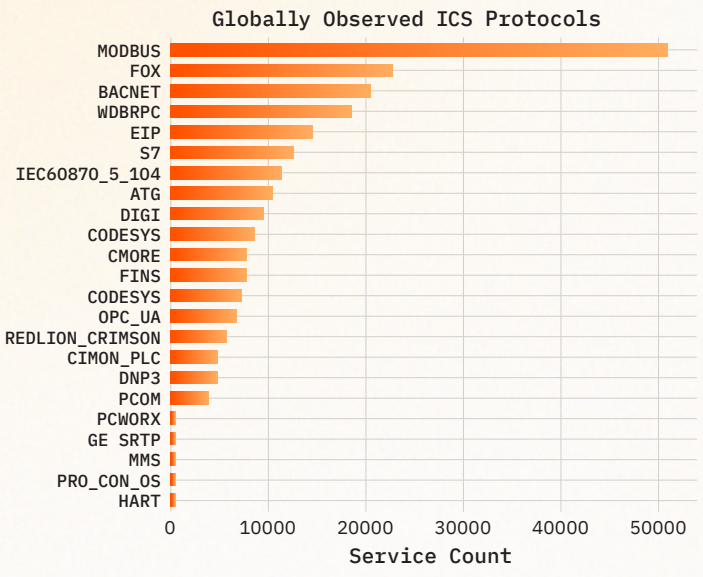


ICS Protocol Exposure

ICS protocol exposure has historically been the focus of both academic and industry reporting on Internet-exposed ICS, but it's only part of the story. As explored previously, HMIs offer a low barrier to entry for ICS attacks–once discovered, they're easily manipulated, even without ICS-specific expertise.

The risk of ICS protocol exposure is a bit different. While several protocols have been leveraged by ICS-specific malware, manipulating and interacting with these protocols typically requires knowledge and expertise about the underlying systems. That said, even if a threat actor isn't planning to carry out an attack directly leveraging one of these protocols, an organization's exposure of them could be an indication of other lax security practices.

Globally, Censys observes over 148,000 exposed ICS services across 175 countries.



Several are known to have been incorporated into ICS-specific malware or attacks, including:

- **Modbus**, initially developed in 1979, is a communications protocol used to "establish client-server communication between intelligent devices." It is the most commonly observed service globally, and boasts a wide variety of applications across sectors like facility management, telecommunications, and manufacturing.
- **IEC 60870-5-104** is an extension of the IEC 60870-5-101 protocol, enabling network access and communications for 101, which is widely used in power system operations. This protocol is more commonly observed in Europe, while North America primarily uses DNP3.
- **CODESYS**, initially released in 1994, is used to program PLCs and is often used across manufacturing, energy, and building automation.
- **OPC UA (Open Platform Communications Unified Architecture)**, initially released in 2006, is a cross-platform communications protocol used in multiple industries, including manufacturing, oil and gas, and energy.

ICS Services By the Numbers

REGIONAL DIFFERENCES

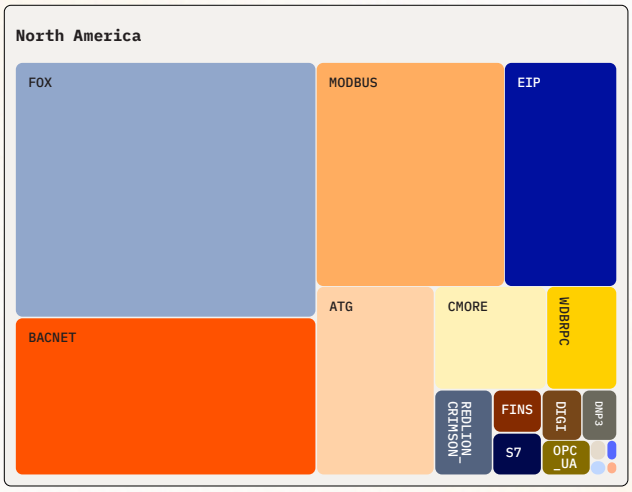
Nearly three quarters of the world's exposed ICS services are found in North America and Europe, with 38% of these services in North America and 35% in Europe.

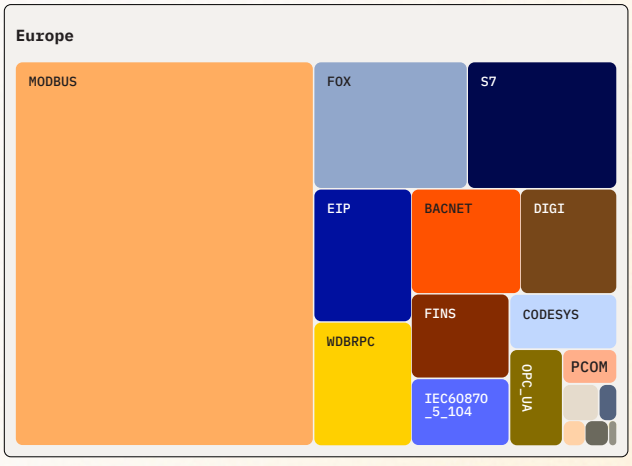
Continent	% of Global ICS Services
North America	38.07
Europe	35.47
Asia	22.93
Oceania	1.71
South America	1.22
Africa	0.57

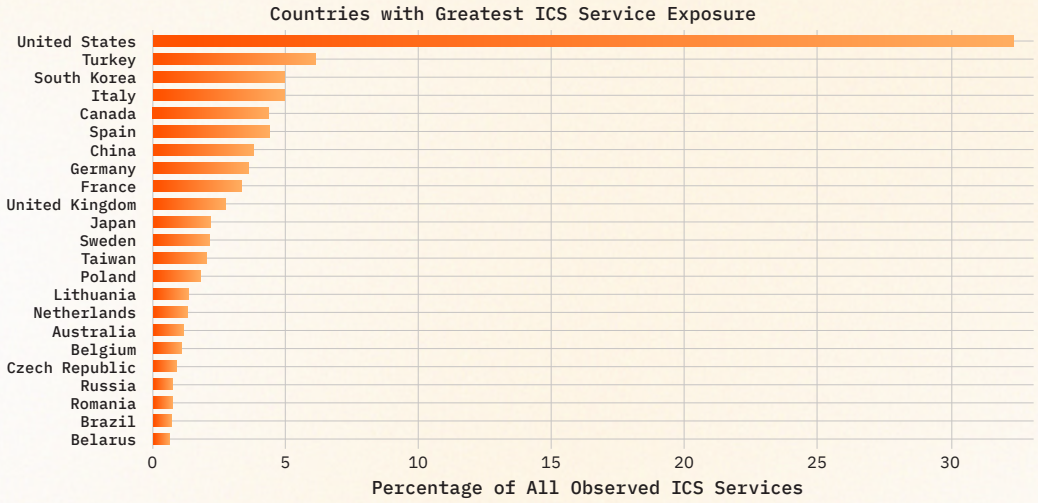
REGIONAL ICS SERVICE EXPOSURE

While North America and Europe have similar percentages of total ICS service exposure, there are differences in composition of these percentages. Modbus, S7, and IEC 60870-5-104 are more widely observed in Europe, while Fox, BACnet, C-More, and DNP3 are more commonly found in North America.

Service Comparison, North America and Europe (pictured right)



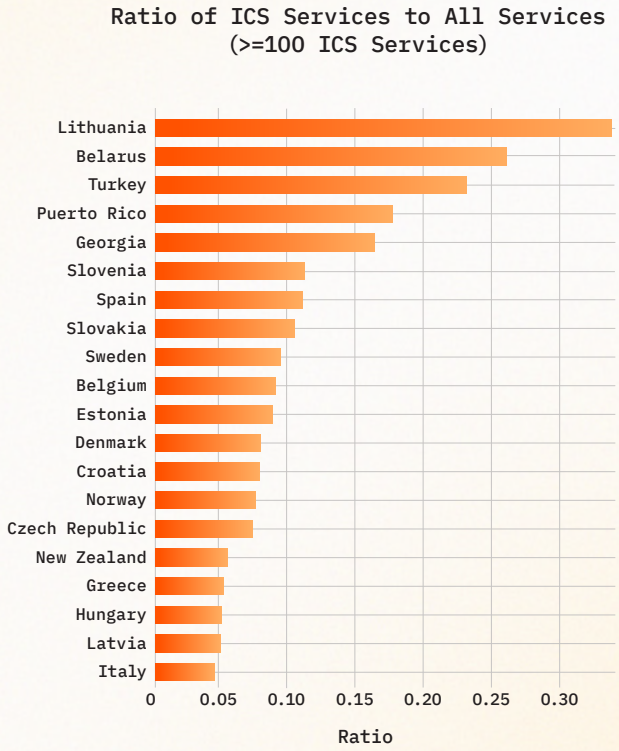




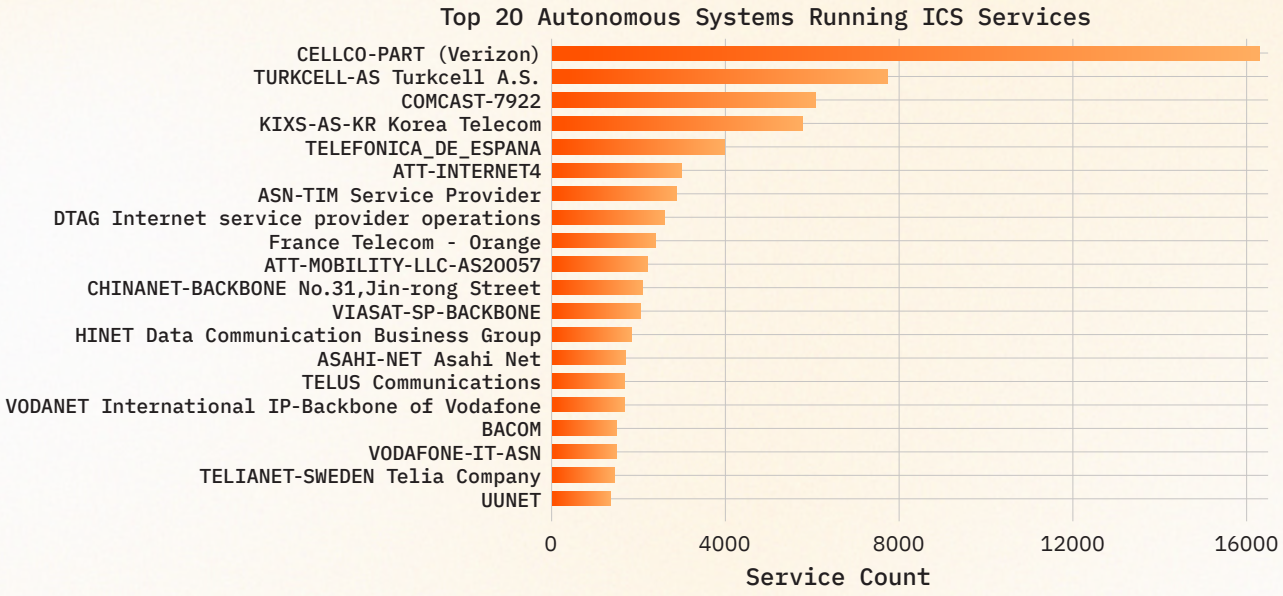
The U.S. hosts over a third of all the ICS services observed globally, with over 48,000 exposures. The country with the next largest number of exposed ICS services is Turkey, with just under 10,000 services exposed. The U.S. has the greatest number of allocated IPv4 addresses, which may in part explain the outsized number of exposed ICS services found there.

To account for each country's Internet footprint, we examined the ratio of ICS services to all services in that country, and different patterns emerged. Lithuania, Belarus, and Turkey top this list, and the U.S. falls out of the top twenty. Compared with raw numbers in the figure above, we observe a greater number of eastern European countries among the top twenty using this metric.

Even for countries with the highest ratio of ICS services to all services, ICS services represent less than 1% of all services observed for that country. While this measure provides a different perspective, countries with the highest raw numbers of exposures still likely have the largest ICS service-related attack surfaces.



Countries with the highest ratios shown here.



NETWORKS

We noted previously that many HMIs run on mobile or consumer and business-grade ISPs, and we find the same to be true of ICS protocols. CELLCO-PART (Verizon) and TURKCELL, a major mobile telecommunications provider in Turkey, are where we observe the greatest number of ICS services. This is unsurprising based on where we geographically observe most ICS services.

However, unlike HMIs, hosts running these services often lack useful metadata for determining ownership. They don't have graphical interfaces and are often the only or one of a few services running on the host. Moreover, all network information points back to the telco rather than an organization that might be responsible for the service. There are tens of thousands of these services online, most of which are impossible to attribute to an industry, let alone an owner or operator.

ICS PROTOCOL CLOSING THOUGHTS

While the exposure of ICS protocols has been a significant focus in discussions regarding Internet-exposed ICS, it represents only part of the broader ICS exposure landscape. Globally, the U.S. stands out with orders of magnitude more ICS service exposures than any other country, and it's challenging to understand who owns these devices. While exposure of ICS services may indicate poor security posture, they aren't as likely to be directly attacked as HMIs, or even other vulnerable services running on the same hosts.

Conclusions

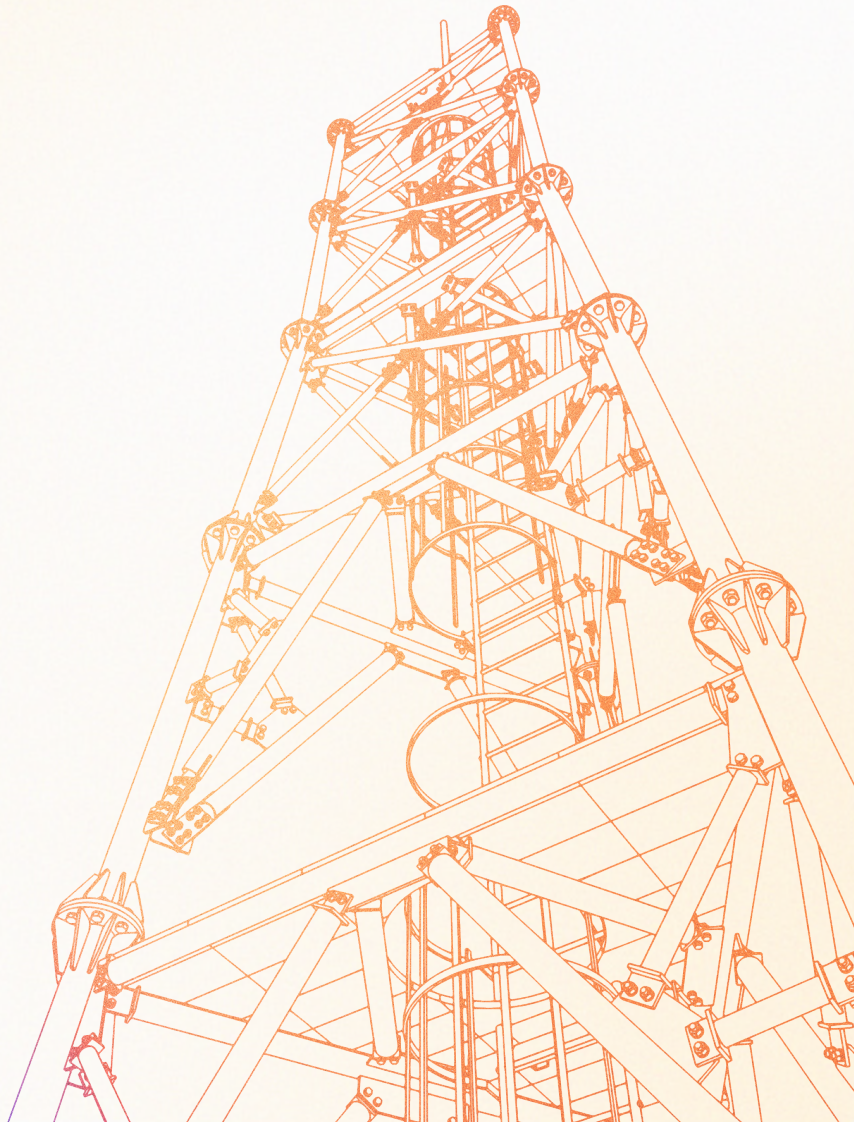
Historically, ICS protocol exposure has garnered the most attention in discussions of ICS security, while the risk of exposed HMIs is often overlooked. Recent attacks on Internet-exposed HMIs emphasize the importance of identifying and securing these interfaces.

Remotely accessible HMIs offer convenience for operators, but without proper safeguards such as authentication or protection behind a VPN, they also provide a low-complexity potential target for threat actors. The interfaces are intentionally easy to use, and unlike ICS protocols, require no specialized expertise to manipulate. Despite often being hosted on 5G or LTE networks that provide little useful metadata, the interfaces themselves typically offer clues about ownership and sector.

Water and wastewater systems represent 34% of the C-More HMIs for which we were able to determine industry. Over the last year, the water and wastewater sector has increasingly become a target for threat actors. C-More is widely found in the U.S., and our findings suggest that still more work is needed to harden systems in this sector. This is particularly challenging, as many small utilities are underresourced and may not have dedicated IT or security staff. However, a recent SANS ICS/OT report found that nearly 53% of ICS cybersecurity staff have worked in the field for five years or less, which may suggest recently increased interest in working in this critical space.

Similar to HMIs, ICS protocols typically reside on 5G or LTE networks that provide little useful metadata about who is responsible for the system. HMIs often contain company logos or plant names that can aid in identification of the owner and sector. ICS protocols rarely offer this same information, making it nearly impossible to identify and notify owners of exposures. Cooperation from major telcos hosting these services is likely necessary to solve this problem.

While the ICS security landscape continues to evolve, Censys remains committed to providing the best visibility to help operators and defenders protect the world's most critical infrastructure.



Appendix

Recommendations for Operators

CISA provides guidance for securing and defending ICS environments, but we make the following suggestions for defenders and operators based on our observations:

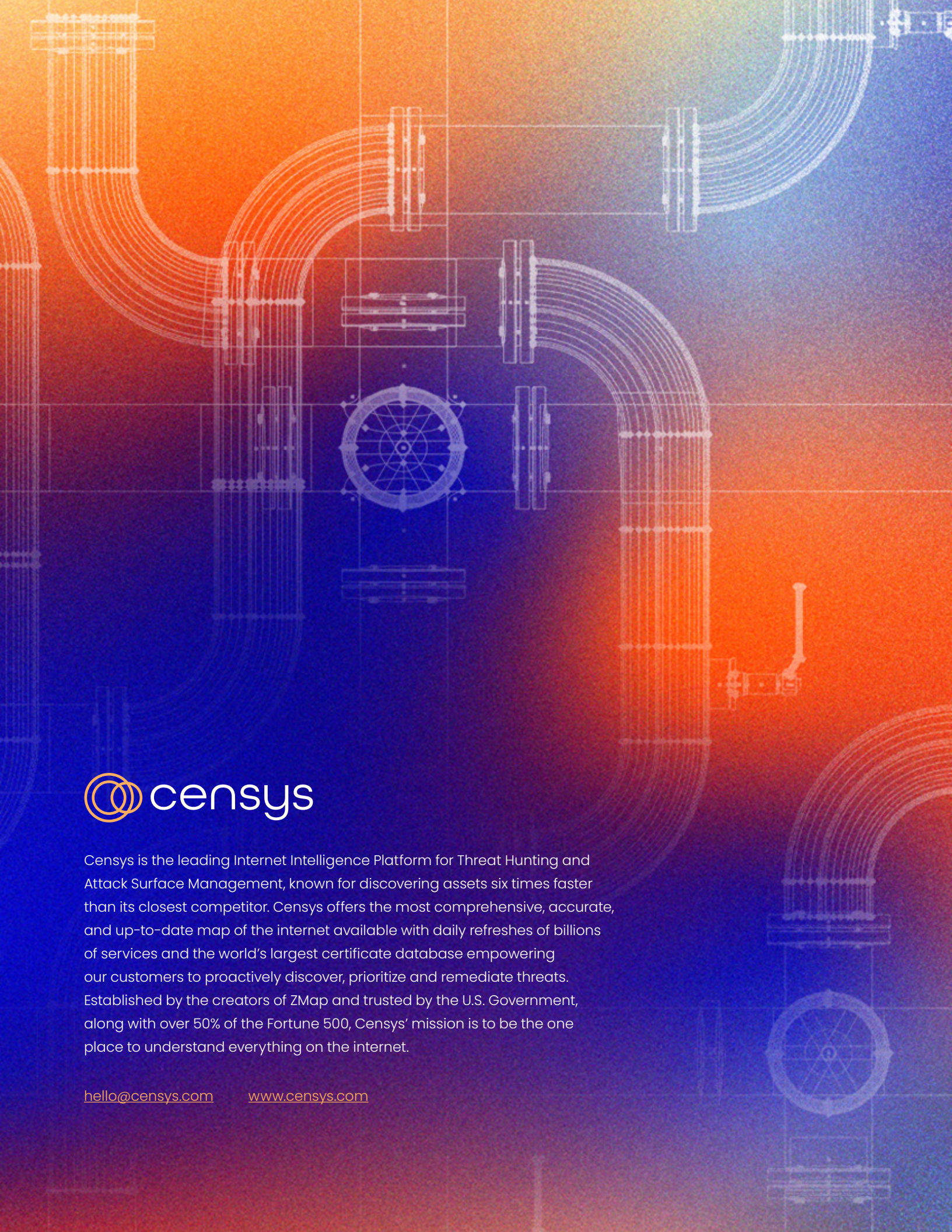
1. Perform a comprehensive asset inventory and understand your public Internet attack surface. It's impossible to defend systems you don't know about, and it's useful to understand what your external perimeter looks like from a threat actor's perspective.
2. If possible, avoid connecting any ICS service or HMI directly to the public Internet. Protecting these assets with a VPN or a firewall is ideal, but for services that offer it, authentication should be enabled at minimum.
3. Avoid using weak or default credentials, as these are trivial for threat actors to guess or crack.

Glossary

- **ATG (Automated Tank Gauge)** is used to monitor and track levels of tank contents (often fuel) over time.
- **BACnet** is primarily used for building automation and control, such as HVAC, lighting, and building access controls.
- **CIMON PLC** facilitates communications for the CIMON programmable logic controller.
- **C-more** serves the C-more HMI, which allows operators to monitor and interact with industrial control systems.
- **CODESYS** is hardware-independent automation software used to program and debug PLCs.
- **DIGI** is used to discover networked devices, often in industrial settings.
- **DNP3 (Distributed Network Protocol 3)** is a communications protocol widely used in electric utility systems in North America.
- **E/IP (Ethernet Industrial Protocol)**, was designed for use in various automation systems. Encapsulated inside CIP (Common Industrial Protocol), this protocol exchanges data between various device types, such as PLCs, HMIs, and controllers.
- **FINS (Factory Interface Network Service)** is a proprietary protocol for Omron industrial automation devices, particularly Omron-manufactured PLCs and HMIs.

Glossary (Continued)

- **FOX** is used for building automation and control, such as HVAC and other facilities management processes.
- **GE SRTP (General Electric Service Request Transfer Protocol)** facilitates communications between GE PLCs and other devices.
- **HART (Highway Addressable Remote Transducer)** is an open source protocol that combines analog and digital communication for industrial systems.
- **IEC 60870-5-104** is part of the IEC 60870 series of standards designed for applications in electrical engineering.
- **MMS (Manufacturing Message Specification)** transfers process information among networked devices in industrial settings.
- **Modbus** enables communications between PLCs, sensors, and other devices in industrial environments.
- **OPC UA (Open Platform Communications Unified Architecture)** is a communications protocol that emphasizes interoperability among devices from different manufacturers.
- **PCOM** is a proprietary communications protocol used by Unitronics PLCs.
- **PCWORX** is a proprietary protocol for communicating with Phoenix Contact PLCs.
- **ProConOS** is a proprietary communications protocol used by systems running the ProCon operating system.
- **Red Lion Crimson** is a software and communications protocol used for Red Lion HMI configuration.
- **S7** is a proprietary Siemens protocol used in communications between HMIs and PLCs in an automated or industrial environment.
- **WDBRPC (Wind River Debug)** is a protocol for Wind River's VxWorks real-time operating system (RTOS).



censys

Censys is the leading Internet Intelligence Platform for Threat Hunting and Attack Surface Management, known for discovering assets six times faster than its closest competitor. Censys offers the most comprehensive, accurate, and up-to-date map of the internet available with daily refreshes of billions of services and the world's largest certificate database empowering our customers to proactively discover, prioritize and remediate threats. Established by the creators of ZMap and trusted by the U.S. Government, along with over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the internet.

hello@censys.com www.censys.com