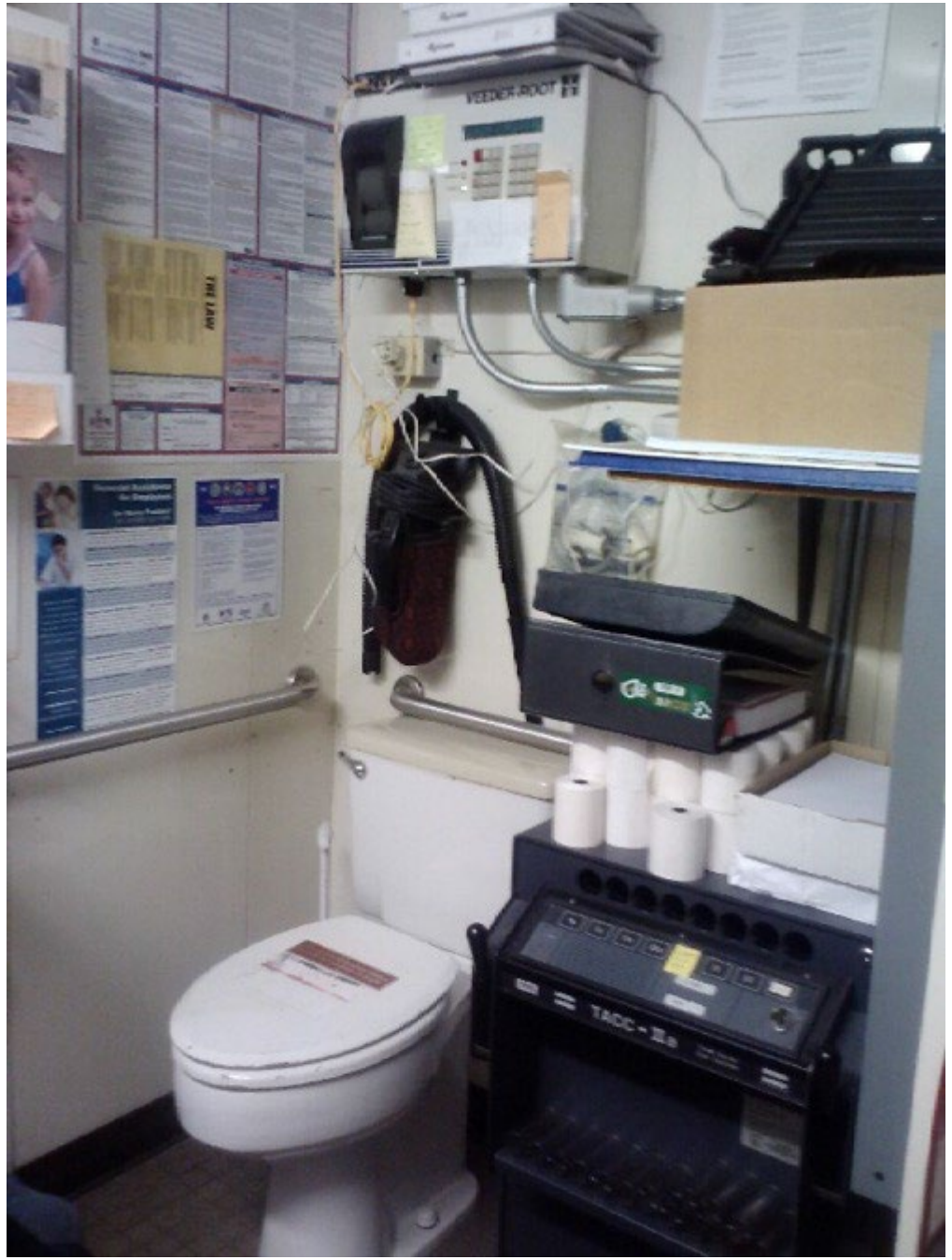
Cyber Attacks on your ATG? Yup.

By Ben Thomas
President
UST Training

National Tanks Conference
Spokane, WA
Sep. 22-25, 2025

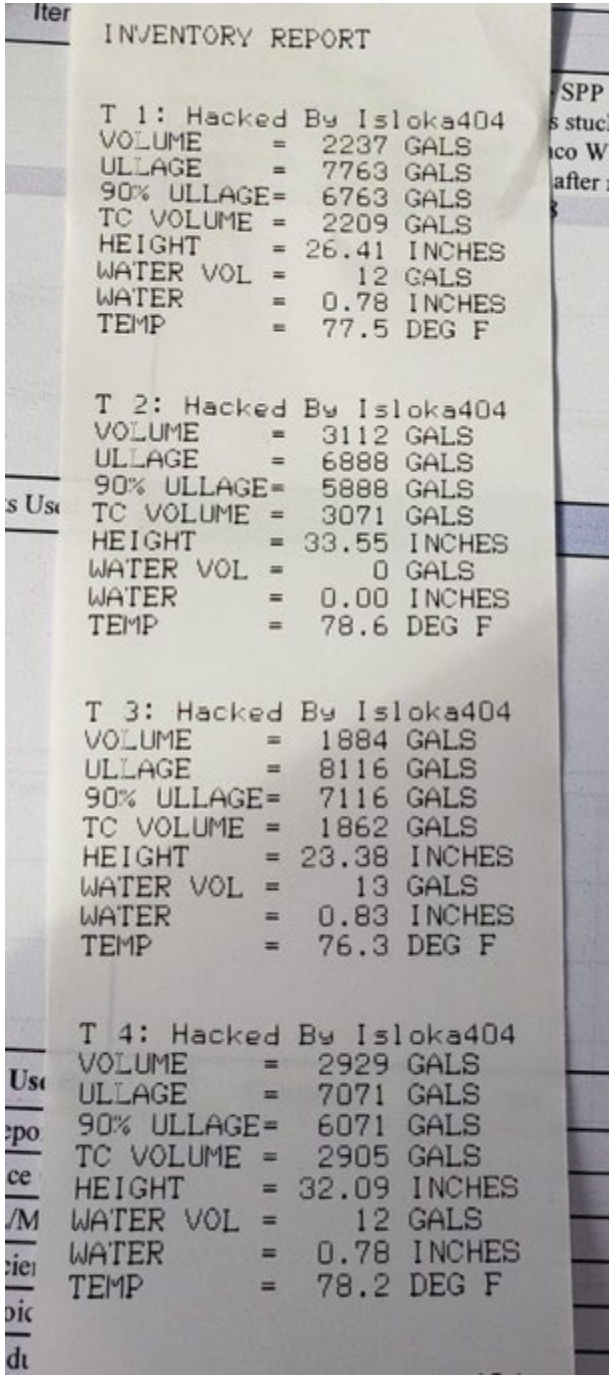


How many of you

- Are regulators, owner/operators, service providers?
- Any network security folks?
- Have never heard about security breaches with ATGs?
- Have been the victim of or know about an ATG hack?
- Have been the victim of a cyber attack either, you or your organization?
- Have said it is not possible?

Is your automatic tank gauge (ATG) potentially subject to a cyber security breach?

The short answer is yes.



Critical Vulnerabilities Discovered in Automated Tank Gauge Systems

September 24, 2024

Written by Pedro Umbelino
Principal Research Scientist

From Sept. 2024 report by Bitsight

Bitsight strongly believes in responsible disclosure of vulnerabilities.

For the past six months, Bitsight has been collaborating closely with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), as well as with affected vendors, in order to mitigate these vulnerabilities.

This coordinated effort aims to safeguard critical infrastructure and prevent the dire consequences that could result from successful attacks.

Overview

Recent investigation by Bitsight TRACE has discovered multiple critical 0-day vulnerabilities across six ATG systems from five different vendors.

These vulnerabilities pose significant real-world risks, as they could be exploited by malicious actors to cause widespread damage, including physical damage, environmental hazards, and economic losses.

Thousands of ATGs are still currently online and directly accessible over the Internet, making them prime targets for cyberattacks, especially in sabotage or cyberwarfare scenarios.

“What can happen if you do not take ownership of your network?”

Rename Tank Information: On consoles using Telnet, hackers find the MAC address, determine whether it is a TLS-350 or TLS-450PLUS and simply change the tank names to something inappropriate.

Resize Tanks (From 10K to 20K Gallons): It is possible to change the tank size, so it appears the tank can hold more than it really can. The thresholds could also be changed so that overflow alarms appear at a higher level. The potential would be to overfill the tank causing an environmental leak.

Shutdown Dispensing (PLLD and Relay Settings): The relays could be deprogrammed so that the pump wouldn’t be activated on a hook signal. Additionally, PLLD could be turned off so catastrophic leaks may not be detected.

“What can happen if you do not take ownership of your network?”

Capture Sensitive Corporate Data: By monitoring insecure Telnet connections, observers can gather operations data (delivery, inventory, alarms, etc.) for sale to third parties.

Shutdown IP Cards / Networking Services: Hackers could alter TLS-350 Ethernet cards lacking passwords; changing configurations and rendering systems ineffective. Critical operations could be impacted (hospitals, 911, cell service, power plants, etc.).

Loss of Compliance Data: Reprogramming the console could result in the loss of compliance data translating to potential regulatory fines.

Past Security Research

ATGs were already mentioned in the past as vulnerable systems, as far back as 2015. In January that year, H.D.Moore published in the Rapid7 blog an article titled: “The Internet of Gas Station Tank Gauges” based on Jack Chadowitz research on ATGs. The article stated:

*"Approximately **5,800 ATGs** were found to be exposed to the internet **without a password.** Over 5,300 of these ATGs are located in the United States, which works out to about 3% of the approximately 150,000 fueling stations in the country.”*

These are some of the actions that could be performed by an attacker via the protocol:

General configurations

- Delete/change automatic events
- Change product labels (ex. switch diesel for gasoline)

Physical related configurations

- Change tank volume/diameter/tilt/limits/other parameters (spillage)
- Change pump control devices and parameters
- Change relay, relay types and configurations (potential physical impact)

These are some of the actions that could be performed by an attacker via the protocol:

Network related configurations (DoS, traffic monitoring, firmware updates, etc)	Other actions
• Change DNS server / gateway • Change contact numbers and alarms destination (silent alarms, trigger alarms to paid numbers)	• Start/stop In-Tank Leak Detection Test • Start/stop pressure line leak detection test • Remote reboot (and DoS by looping the reboot command)

Recommendations to Safeguard ATG Systems: for Security Leaders

Identify any ATG deployed by your organization or 3rd-party business partners & promptly assess security of these systems.

1

Remove any ATG from the public internet.

2

Employ safeguards like firewalls to protect against unauthorized access to your ATG systems.

3

Security leaders must acknowledge the unique control needs that apply to OT including industrial control systems rather than just apply a traditional IT risk model to this infrastructure.

Recommendations to Safeguard ATG Systems:

For Manufacturers

- ATG manufacturers must take action to increase the cybersecurity of their devices, not only in their internal software development life-cycle, but also throughout their supply chain.
- Also, should work with their customers to ensure the proper configuration and security of already deployed devices.

Recommendations to Safeguard ATG Systems:

For Manufacturers

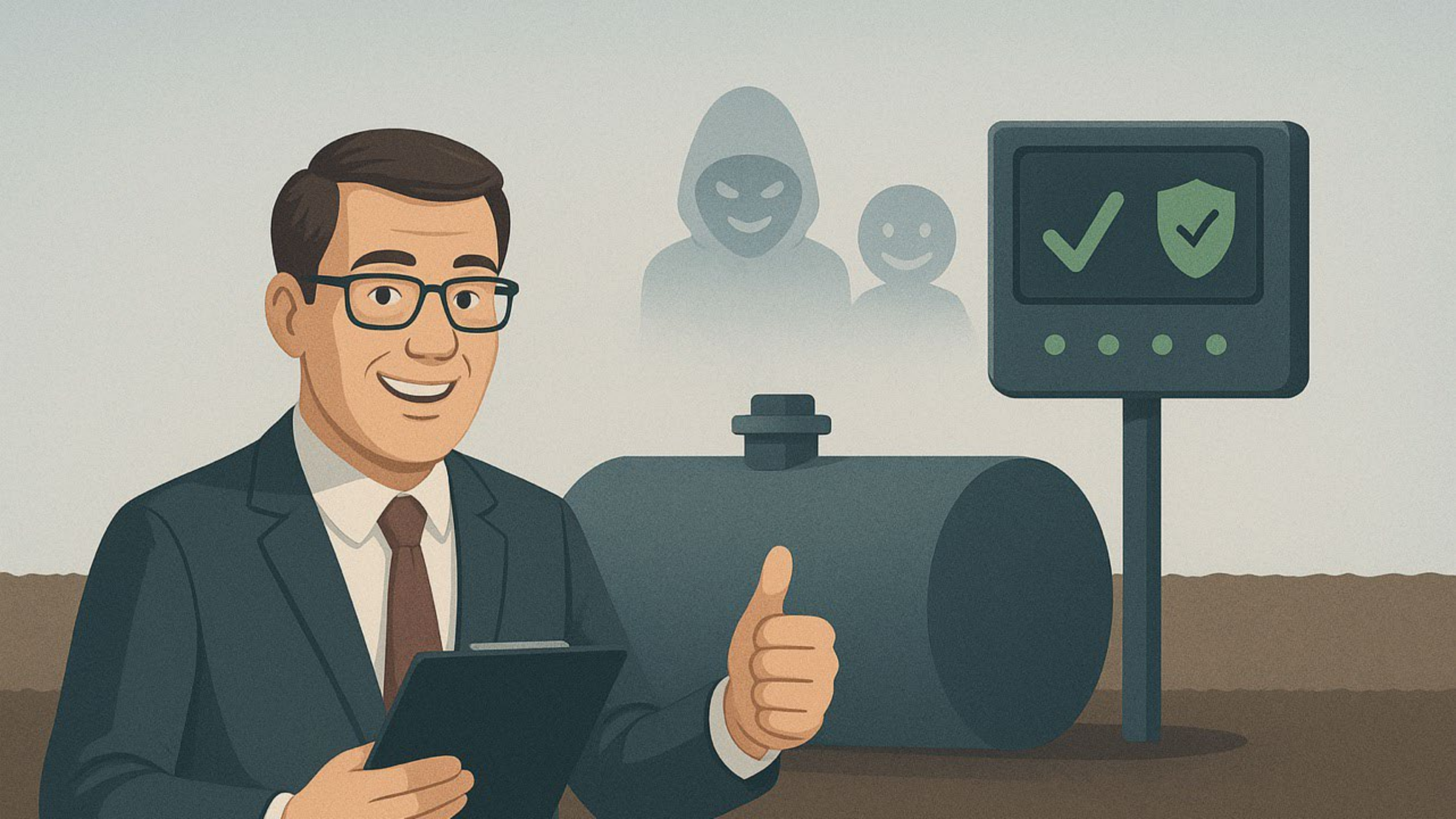
- Use secure-by-design principles to develop more secure technology.
- Improve the security posture of deployed equipment and machinery by leveraging data and insights.
- Promote the importance of end users securing their operations, thereby reducing their exposure.
- Build programs to accurately and swiftly detect misconfigured or otherwise exposed systems.

Recommendations to Safeguard ATG Systems: For Government Policymakers

The exposed ATG systems identified in this research should alert policymakers to the current state of ICS — and more broadly, OT — security. Due to the potentially serious consequences resulting from incidents involving industrial systems, policymakers should:

Understand the risks of exposed industrial control systems, including ATGs, particularly those involving critical infrastructure.

Inform national security strategies and programs to include adversarial threats targeting operational technology, and how an industrial cyber attack could impact national security and human safety.



Recommendations to Safeguard ATG Systems:

For Government Policymakers

- Quantify the impact — financial and otherwise — that a cyber attack targeting industrial infrastructure could inflict on national, regional, and local economies as well as diplomatic relationships.
- If you believe you may have an issue, please contact Bitsight so we can help.

SUMMARY: ATG CYBER ATTACKS

Federal DoD study showed ATGs subject to critical security vulnerabilities

Ensure your business network is safe

Another reason to get the latest ATG model

Pro Tip: Never use admin for password

Use Technology wisely...

but have some fun too