Control Systems in the Pipeline Industry - Vulnerabilities and Mitigations

David Sawin – USDOT/Volpe Center, Program Manager
Bob Hoaglund - USDOT/Volpe Center, Modal Lead

Control Systems Security Program / ICS-CERT
Agenda

- Pipeline as a National Infrastructure
- Pipeline networks and systems
- Risks, vulnerabilities and opportunities within the pipeline industry
- Next steps for the pipeline mode
18 Critical Infrastructure Sectors

Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP) identified and categorized U.S. critical infrastructure, which includes **Transportation**.

*Many transportation systems are so automated that they can no longer be operated without control systems.*
Control Systems in Pipeline Are Increasingly Vulnerable to Attack

- Requirements to “connect” operational systems to business systems and the internet
- Adversaries can discover pathways to systems
- Attacks such as Stuxnet proved that connectivity isn’t even necessary in order to launch an attack
- ICS-CERT advisories
Growing Dependencies Can Increase Risk

The pipeline industry uses ICS for:

- Interconnected distribution networks,
- Safety,
- Cost Control/Projection,
- Billing,
- Trending and more!

Automated industry carries risk of potential intentional and unintentional incidents.
Pipeline as a National Infrastructure
Pipeline mode incudes…

Pipeline networks = millions of miles throughout the US

- 3,000 operators
- City gate stations, distribution systems
- Terminals
- 65 percent of the nation’s hazardous liquids & chemicals
Pipeline Networks

Legend
- Interstate Pipelines
- Intrastate Pipelines

Source: Energy Information Administration, Office of Oil & Gas, Natural Gas Division, Gas Transportation Information System
Supply Chain
Vessels Feed Pipeline Distribution Systems at Ports
Typical Natural Gas SCADA Systems

- Control natural gas distribution systems
- Monitor pressure
- Alert and alarm
- Odorant levels
- Flow Control & Pressure Management
- Temperature levels
- Commodities
Pipeline - Critical to US infrastructure

Trans-Alaska Pipeline System
- Critical to US Energy
- Over 15 billion barrels of oil produced
- $8 Billion to build in 1977
- 800 miles long by 48” width
- Control Systems play major roles
- Smart/Dumb Pigs
Infrastructure located in remote areas
Pipeline Mode Progress to Date

- TSA Pipeline Security Division
- API Standards
- Roadmap to Secure Control Systems in Transportation
- Cybersecurity Assessment and Risk Management Approach (CARMA), developed by DHS
- Interstate Natural Gas Association of America (INGAA), Control Systems Cyber Security Working Group
  - Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry
Outreach to Pipeline Partners

- American Gas Association (AGA)
- American Petroleum Institute (API)
- Transportation Security Administration, Pipeline Security Division
- Selected top 100 operators
- Trans-Alaska Pipeline System (TAPS)
Pipeline Strategies

- Cybersecurity requires a lifecycle approach

- Risk assessments
- Standards
- Design practices
- Certification
- Monitoring
- CIA
The Roadmap to Secure Control Systems in Transportation

- A plan for voluntarily improving industrial control systems cybersecurity across all transportation modes:

Socialize Roadmap and Gain Buy-In
Develop Action Plans
Implement Priority Actions
Communicate Results and Sustain Efforts
Next Steps for Pipeline

- Expand CSSP outreach to pipeline operators
- Help industry define cybersecurity strategies
- Transportation Roadmap
- Pipeline standards
Cybersecurity is a Shared Responsibility

Report cyber incidents and vulnerabilities to:

www.us-cert.gov

Or send e-mail to:

soc@us-cert.gov,

ics-cert@dhs.gov

Or call:

877-776-7585 (ICS-CERT)

888-282-0870 (US-CERT)

Get more information at: www.us-cert.gov/control_systems
Questions / Feedback

David Sawin
617.494.2602, david.sawin@dot.gov

Bob Hoaglund
617.494.3653, robert.hoaglund@dot.gov

US Department of Transportation
Volpe National Transportation Systems Center