Geothermal Sector Cybersecurity Vulnerability Assessment

Tony Markel (tony.markel@nrel.gov),

Konrad Hauck, and Ian Warren, National Renewable Energy Laboratory

Patrick Dobson, Lawrence Berkeley National Laboratory

Kevin Kitz, Kitzworks, LLC

2020 GRC Annual Meeting, October 18-23, 2020

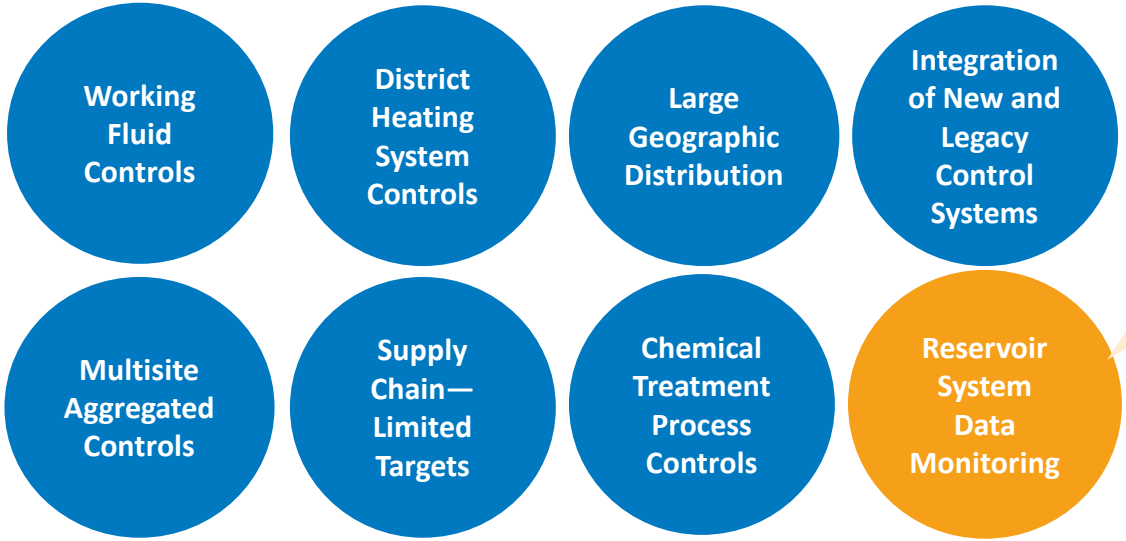
Geothermal Technologies Office (GTO) Cybersecurity Study Goals

- Fill a critical information gap: cybersecurity assessment specific to the geothermal sector.
- Focus on the aspects unique to geothermal development, production, and operations.
- Initiate thought process and raise awareness among industry members, leading to active improvements.

Congressional Guidance

Cybersecurity of energy technologies are a priority for the U.S. Department of Energy (DOE). In 2018, congressional guidance directed the Office of Energy Efficiency and Renewable Energy (EERE) to deliver a multiyear program plan addressing cybersecurity for all EERE programs.

Cybersecurity Vulnerabilities Identified for Review



Unique Vulnerability

Of the vulnerabilities reviewed, only one is unique to geothermal operations: a potential attack to the reservoir system data monitoring systems that could potentially cause seismic disturbances.

Assessment Study Methods

Geothermal Cyber Workshop w/SMEs

- Landscape of systems and technology
- Brainstorming cyber scenarios

Industry Inputs

- Literature Review
- Dialogs on key topics

Field Observations

- Understanding practice
- Raising awareness

VULNERABILITY: Reservoir System Data Monitoring

- During development of a geothermal resource, electronic monitoring equipment provides significant data to be used within models of the subsurface (e.g., reactions to pressure, flow, and thermal attributes).
- Modeling insights guide system design, operational plans, and financial decisions unique to the geological resource.
- Future enhanced geothermal systems (EGS) technology will similarly use data sets to engineer a viable energy resource. These data are critical to maximizing production while limiting induced seismicity.

Potential Consequences

In rare instances, seismic impacts from mis-operation of geothermal systems have been observed (Kim 2018, Grigoli 2018, Nature 2019). Proximity to population would increase the consequences of malicious sensor data manipulation and associated digital controls. Public perception of benefits and risks could be influenced.

Mitigations

Use measures that protect critical data transmission and storage, enhance access control practices, and provide redundancy for measurement validation. Consider GTO prior work “Protocol for Addressing Induced Seismicity Associated with Enhanced Geothermal Systems” (Majer et al., 2012) for cybersecurity purposes.

Unique to Geothermal

YES – Though similar in nature to oil and gas operations with injection and production wells, the risks of geothermal reservoir monitoring, model development, and operation in this scenario are unique to the geothermal industry.

Opportunities to Leverage Best Practices from Other Sectors

Relevant Sectors to Geothermal Systems Technologies

- Oil and gas
- Chemical processing
- Electricity industry.

Common Topics and Protections

- Supply chain risks
- Supervisory control and data acquisition system protections
- Staff cyber-hygiene (e.g., practices and steps that users of computers and other devices take to maintain system health and improve network security)
- General physical and business systems security.

Cross-Sector Resources

- National Institute of Standards and Technology (NIST) 800 Series – Computer Security
- NIST 1800 Series – Cybersecurity Practice Guides Department of Homeland Security Industrial Control Systems Recommended Practices.

Conclusion

The study represents a proactive effort to fill an information gap, with an intended outcome to identify unique cybersecurity consequences and vulnerabilities within the geothermal sector. While not an exhaustive study, eight potential cybersecurity vulnerabilities were reviewed.

Unique to geothermal:

- Results indicate that **reservoir data system monitoring** is a unique vulnerability to geothermal; consequences have the potential to induce seismicity with significant impact.

Not unique to geothermal:

- A further review of challenges and solutions from other sectors should be considered for potential implementation to other topics.

As geothermal resource contributions to the energy sector grow, cybersecurity will be increasingly important to ensure resilient, reliable, and secure clean energy for years to come.

Thank you

www.nrel.gov

NREL/PR-5R00-77674

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Geothermal Technologies Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

We acknowledge Geothermal Technologies Office member support, specifically Susan Hamm for initiating, sponsoring, and monitoring this research effort. Guidance from Arlene Anderson (Geothermal Technologies Office), Jeff Winick (Boston Government Services), along with Avinash Nayak, Dipankar Dwivedi, and Sean Peisert (Lawrence Berkeley National Laboratory) were critical to the project's success. We appreciate the willingness to participate from the various industry contacts we connected with for insights on geothermal-relevant cybersecurity challenges.

NREL
Transforming ENERGY