CASE STUDY

Ensuring Safe and Reliable Renewable Energy Production

inflexion point

732-922-6611

info@inflexionpoint.ai

www.inflexionpoint.ai

SECURE REMOTE FACILITIES MANAGEMENT

Delivering on the Promise of Clean Energy

We help South Jersey Industries ensure reliable operation through a holistic approach that includes a combination of software, services, and support.

South Jersey Industries (SJI), a 100-year-old power generator that serves over 700,000 families and businesses across New Jersey, has committed to increasing its supply of clean energy. A primary strategy to fulfill on this commitment is the capture and conversion of methane gas at dairy farms.

This innovative system, which will significantly reduce gasoline usage — up to 25 million gallons annually, equivalent to the consumption of around 50,000 cars — is comprised of dozens of facilities located across the state that collect and refine the waste from dairy cows.

Small Facilities. Big Responsibility.
The process for generating energy from the waste products of dairy cows, strikingly simple in concept but devilishly difficult in practice, requires skilled operators, sophisticated systems, and — because these facilities are regarded as critical infrastructure — impenetrable security.

Each farm is a miniature natural gas facility, with the same risks and requirements as a larger facility, but without the production throughput to support dedicated resources. Operating these renewable energy production facilities safely and productively requires tight control over costs and resources.

Remote Monitoring and Management
Early on SJI realized that remote monitoring and management (RMM) would be key to its business strategy and asked us to include RMM capabilities in the operational technology plans. The need to allow remote access to operational technology (OT) systems triggered concerns about cybersecurity, and we knew we would need to address security as a fundamental part of the plan.

A Holistic Approach
At InflexionPoint we know that effective technology systems act as a seamless extension of the people and processes they are meant to serve. That's why we

Challenge

- SJI collects natural gas across dozens of farms
- Must track operations, for carbon credits
- Each farm is a miniature natural gas factory
- No full-time staff on site

Solution

- 'Single pane of glass' to manage all OEM equipment: controls; MES; cybersecurity
- One common IDC; drop into each facility
- Ability to monitor and manage remotely; no personnel on site
- Patching, asset management of all systems
- Added Ignition MES
- Customer support 24/7

Results

- See all OT equipment in real time
- No breaches; identified a couple CVEs; offered remediation strategy
- 90-100 tickets per site per month
- Savings $40K/month; system pays for itself

A Team Effort

This project for SJI involves a total of 53 sites, 9000 miles of pipeline, and 2 LNG facilities. Our teams coordinate efforts to reduce the time and costs required to plan, build, and manage each facility.

IT/OT

- Design of logical network infrastructure
- Server pre-build and configuration including OS install, Applications, virtualization, data backup, switches and firewalls
- Installation of the server infrastructure at each site

Automation

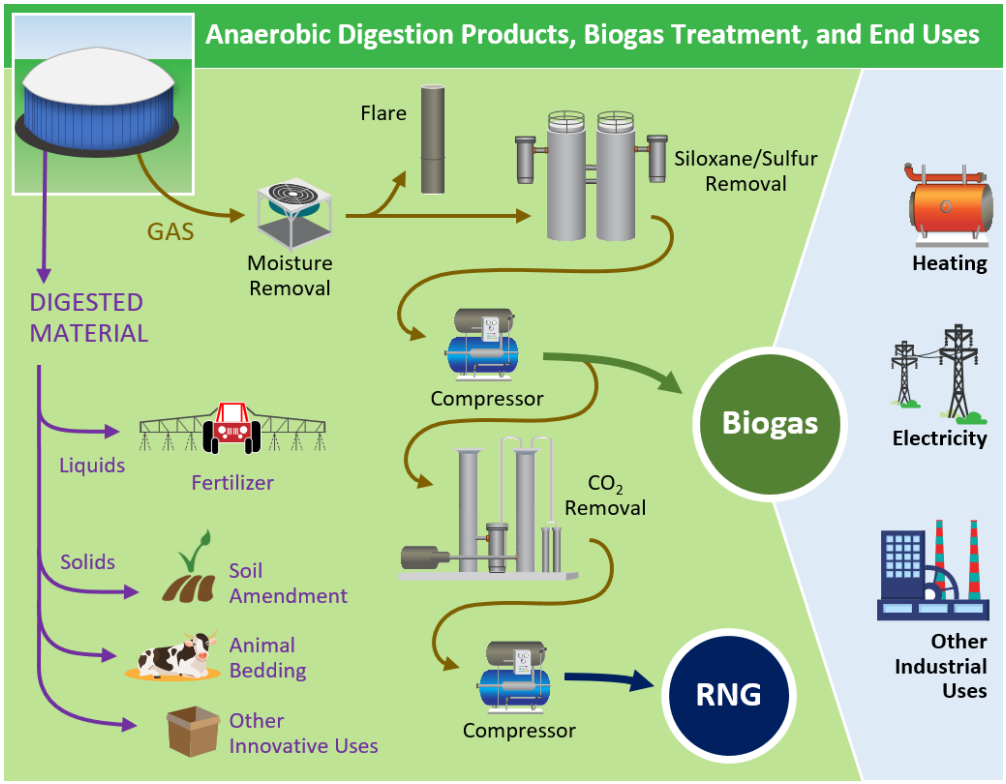
- Design, build of Balance of Plant (BOP) panels
- Integrate controls for each vendor into a BOP Control System and SCADA

Manufacturing Intelligence

- Worked closely with automation team to map required data
- Designed SCADA system using Ignition to provide data such as trailer capacity, gas production volumes, available gas, gas transferred to pipeline, and quality of gas
- RFID to automate trailer detection and loading

Support

- Implementation of ticketing system, help desk and knowledgebase
- Remote monitoring of IT/OT Infrastructure
- Engineering assistance and dispatch
- Boots on the ground engineering



take a holistic approach to IT and OT systems design, and nowhere is this more important than in cybersecurity. A holistic approach means weaving security provisions and technologies into operating plans from the outset, not as an add-on. It means thinking about security as a process, not an end-state; and it means addressing security through a combination of technologies, processes, and training.

Single Pane of Glass, Single Monthly Fee

With RMM at the heart of the operational plans we designed a system that puts everything operators need — equipment controls, MES, cybersecurity — into a 'single pane of glass' accessible via web browser. Each facility received a self-contained integrated data center (IDC) that was pre-configured and tested, ready to run. We also updated and patched all operating systems and assets at each facility and implemented Ignition MES for easier monitoring and management of processes. Last, but certainly not least, as an operating partner to SJI we provide 24/7 support. All software, services and support are included in one monthly fee per facility.

Greater Visibility and Control

Using the RMM system SJI operators and our team can see all OT systems and equipment at a facility in real time, and intervene before problems arise. For additional security we share data between the RMM system and Dragos sensors. Since rolling out the system we have had zero breaches. The system has helped us identify a couple common vulnerabilities and exposures (CVEs) and we were able to quickly develop a remediation strategy. On average we handle 90-100 tickets per site each month, providing triage, routing, and remediation plans.

According to SJI, their savings equal about $40,000 per month, which means the system pays for itself while significantly enhancing security and flexibility.