THE LANGNER GROUP

Nordic energy giant Fortum selects RIPE Program for fleet of 400 power plants

Fortum rolls out RIPE after successful use in nuclear power plant

In 2014, Fortum selected The Langner Group's RIPE Program to provide a robust, comprehensive program for managing the cyber security of its nuclear power plants. Fortum was so impressed by the positive results they achieved in their most critical facility that they have selected the RIPE Program to be their OT security standard for their nearly 400 power generation facilities in seven countries.

In 2014, Fortum introduced the RIPE OT Security Program at their Loviisa nuclear power plant for two reasons. First, the Finnish nuclear regulatory agency (STUK) was about to introduce tightened cyber security regulation. STUK is already considered among the most rigorous nuclear regulators worldwide and STUK's efforts have catapulted the Baltic state to the leading position in the NTI index.[1] Second, it had always been the company's policy to be a leader in safety and security rather than being the follower of a regulator's requirements.

The decision to incorporate The Langner Group's RIPE Program was made easy because of Langner's outstanding reputation in the Operations Technology (OT) security space. Fortum also appreciated the fact that the RIPE Program's comprehensive instruments could be used with only minor adaptations and therefore be quickly implemented. While other companies spend months or years crafting a custom OT security program, by adopting the RIPE Program, Fortum was ready to implement within weeks.

The case for continuous improvement

Maintaining a cyber security program in a complex operational environment means that one must be able to adapt to an ever evolving situation. One is never truly 'finished'; instead there are always additional actions to take to further improve one's security posture. Fortum was specifically looking for a program that adopted this mindset. Tomas Nyström, Fortum's Cyber Security Manager noted: *"We needed a program to help us measure the current state of our system and to encourage us to implement continuous improvement, along the lines of a Kaizen quality program."*

Tomas Nyström
Cyber Security Manager
Fortum

[1] The 2016 NTI Nuclear Security Index: Threat and Sabotage, 2016

Fortum Use Case Study

After the first months of using RIPE, Fortum management and engineers were pleasantly surprised by an unexpected side effect. *"By implementing the RIPE Program, we created a standardized documentation system with consistently applied solutions, clear policies, standard operating procedures, and training. Most importantly, we had a way to measure our progress on every element. In doing so, we not only identified and corrected configuration issues, we are now able to quickly troubleshoot and perform root cause analyses, saving us hundreds of hours of engineering time."*

Vendors readily adopt RIPE's guidelines

Positive effects were also seen on the vendor front. While many still believe that automation vendors have reservations about adopting cyber security requirements from asset owners, Fortum's experiences were the exact opposite. Major vendors had little problem in providing Fortum with system documentation formatted to the standards provided by the RIPE Program. Prior to this, vendor-sourced components were a 'black-box' and performing root causes analyses or troubleshooting incidents could require extensive staff hours of reverse engineering to resolve.

The RIPE Program's verification and reporting capabilities provided additional benefits. Fortum soon realized that RIPE's reporting delivers fact-based insight on the cost-efficiency of the whole OT security effort and provided actionable information on which areas to improve. This added value was significantly increased after another nuclear operator in Finland also started using RIPE. Now, both asset owners can compare results and learn from each other's experience.

Fortum's nuclear power plant in Loviisa (Finland) has benefited from using the RIPE Program to keep its leadership position in cyber security. Photo Credit: © Fortum

Integrated CMDB program catapults Fortum's results to the next level

The next big step was to incorporate The Langner Group's configuration management system software, myRIPE, into the plant's digital environment myRIPE is a powerful software program specifically designed for OT that provides a full-featured configuration management database. As is often the case, their computerized asset management system was not user-friendly and did not have the capability to model the complex dependencies of modern digital OT systems. Most importantly it did not feature the ability to automatically detect and store system configurations of networked components using software agents and data collectors. Therefore Fortum changed their architecture to use myRIPE as their CMDB powerhouse to serve cyber security and plant maintenance needs and connect to the existing asset management system on the backend.

Fortum looks to RIPE for benefits at all locations worldwide

Two years after introducing RIPE, Fortum felt confident to make RIPE the corporate OT security solution for their impressive fleet of nearly 400 power plants in Europe and Asia. Says Tomas Nyström, *"we are confident that implementing The Langner Group's RIPE program in every facility will yield significant operational and security benefits."*

As a global leader in sustainability, Fortum has expanded into solar and other renewable resources. Now all Fortum facilities will have the cyber security protection of the RIPE Program.
Photo Credit: © Fortum

Fortum's vision is to be the forerunner in clean energy. Already 64% of their electricity generation is CO2 free. They operate nearly 400 facilities generating power and heat from a range of sources including hydro, nuclear, thermal, solar, and wind. They service over three million customers in the Nordic and Baltic countries, Russia, Poland, and India.

The Langner Group is a vendor-neutral cyber defense consultancy specialized in critical infrastructure and large scale industrial facilities. The firm's principals have each accumulated decades of experience in the field and earned their reputation the hard way. Their revelations and insights have changed the way that cyber security, and national security in a larger sense, is seen.

The Langner Group
571.551.2998
info@langner.com
www.langner.com
Washington DC | Hamburg | Munich

Fortum Use Case Study