Safeguarding Cybersecurity with EOSi's Virtual Nitrack®:

Ultra-secure Biological Nutrient Removal Optimization with Cloud-based Process Automation

| EOSi's cloud-based Virtual Nitrack® carbon-source dosing control system for biological nutrient removal optimization offers enterprise-grade cybersecurity for resisting hacking efforts of the most determined "bad actors."

Virtual Nitrack® Cloud-based MicroC® Optimization

EOSi's Virtual Nitrack software-based system frees wastewater treatment plant operators from the high cost and technology constraints of older hardware-based biological nutrient removal optimization systems and adds advanced multilayered security, access control, encryption, and other safeguards to deter the increasing threats of hacking and cyberattacks.

Like EOSi's hardware-based predecessors, the Virtual Nitrack system enables automating, monitoring, and optimizing biological nutrient removal dosing of MicroC supplemental carbon sources widely used in denitrification, enhanced biological phosphorus removal (EBPR), and biochemical oxygen demand (BOD) addition applications.

In contrast, the Virtual Nitrack software exists and operates "in the cloud," migrating processes and processing formerly handled by onsite computer hardware to a "virtualized" cloud-computing environment that enables plant operators to achieve consistent permit compliance with a new lower-cost, rapidly deployable, and ultra-secure solution.

Powerful Enterprise-Grade System Security

The Virtual Nitrack system was designed from the ground-up to deliver powerful enterprise-grade security. End-to-end TLS/SSL encryption (TLS (Transport Layer Security) and SSL (Secure Sockets Layer) ensures application access and all communications from local nodes to the cloud is secure and encrypted to deny unauthorized access, data monitoring, or configuration changes. All sensors and devices communicating with the Nitrack system are secured with authentication and access control. IIoT (Industrial internet of things) gateway and cellular probes feed data to the cloud through encrypted channels, safeguarded by stateful firewalls and certified security protocols.

Supporting the Virtual Nitrack system are several enterprise-grade technologies maintained with up-to-date firewalls, full cybersecurity implementations, and full daily backups stored offline, including Microsoft's Azure cloud-computing platform, Microsoft SQL Server database management, a specialized data broker service for monitoring business-critical data traffic, and Inductive Automation's Ignition industrial application platform using Cirrus Link's MQTT Engine encrypted data pathways.

In the field, SignalFire cellular transmitters deliver process data values to Moxa industrial networking and communications units installed onsite at the treatment plant, providing secure “pull and push” data communications between the plant’s PLC network and the Virtual Nitrack system.

Firewalls allow VPN-only (virtual private network) access to Moxa devices, and physically separate “air gapped” networking connectivity ensures no active connections exist between the subnet used for the PLCs, the cellular network, or the network subnet used internally by Cirrus Link’s MQTT gateways. Further, the MQTT protocol defeats data interception or hacking by transmitting only tiny amounts of non-contextual numerical data on a third cellular connection also encrypted and linked to secure CA digital certificates.

System Monitoring and Operational Security

The Virtual Nitrack system also offers built-in operational safeguards, including active system monitoring, change logs, notifications, alerts, and optional layers of automated security. If a Virtual Nitrack system starts performing abnormally because of user error, system misconfiguration, or even an unauthorized “bad actor,” EOSi’s active monitoring enables reacting quickly and decisively within minutes of detection.

Virtual Nitrack logs all actions of any user who uses the system, monitoring remotely and recording what they are doing, all actions taken, or any changes made to the system settings. If a user activates or stops a particular pump, Virtual Nitrack creates a log entry revealing who did it, what time they did it, and what action was performed. System administrators can review any changes or modifications to the system, and either remedy the situation or establish safeguards to prevent a reoccurrence.

Login “timeouts” are an example of automated security measures to prevent unauthorized persons from accessing and making changes to Virtual Nitrack system programming values using unattended plant workstations still actively logged into the application. Other automated security measures include intelligent safeguards preventing excessive or nonstandard system values from being entered into the software, automatic notifications or alerts if the system detects improper levels of MicroC are being applied for wastewater treatment, automatic user lockouts to prevent certain system values from being configured, and more.

EOSi is evaluating using AI functionality limited to assisting plant operators and users achieve more efficient operation with their Virtual Nitrack-driven nutrient removal system, including AI tools programmed to provide training assistance or system status updates. But future iterations will focus on incorporating operational improvements and strengthened safeguards to ensure a more reliable, available, and ultra-secure Virtual Nitrack system that enables plant operators to comply quickly with new wastewater treatment regulations or permit restrictions.