KEEP YOUR ASSET CYBERSECURE

HyNET and HySEC – The dedicated smart network and security solution for hydropower plants in the digital age

Digital innovations have become an integral part of our world and the energy sector must respond with modern security concepts to keep their operations safe and secure at all times.

Over time, the demands on power plant networks have changed dramatically. Nowadays, a multi-service network is cutting-edge for the hydropower sector and active data exchange between energy producers, distributors, and consumers is making a full spectrum security concept crucial. It must also combine traditional process and control communications systems with modern technology.

"ANDRITZ is offering an all-encompassing cybersecurity tool suite to guarantee hydropower plant systems are able to run in a controlled and secure manner."

ANDRITZ' HyNET network is the basis for secure communications both within a power plant and between geographically separated power plants and the central control room. Based on our long experience, HyNET combines state-of-the-art network and security technology and guarantees smooth and secure operations.

MULTI-SERVICE NETWORK

Networking of all the necessary components for running a power plant takes place on the control and process level. Special attention is given to network availability and redundancy. Even in the case of an interruption, communications between the automation equipment and the control system must be maintained. This is achieved with a comprehensive network design, as well as the use of high-quality components. By integrating voice and video over IP into the existing Ethernet network, additional costs are avoided. However, for security reasons, a strict separation between control systems, process networks, and service networks is required.

CYBERSECURITY

High-performance networks and their connected processes and control equipment must be unconditionally protected against attacks like unauthorized access, data manipulation, and denial of service attacks. ANDRITZ' dedicated cybersecurity solution is known as HySEC. An all-encompassing and fully integrated solution, it meets the extremely high demands required in the energy business.

Technical pictures courtesy of Cisco and Hirschmann/Belden

SYSTEM PATCHING, ANTIVIRUS AND FALSE-POSITIVE PREVENTION

To safeguard the control environment, a comprehensive system patching and anti-malware solution is indispensable. Operating systems must always be kept up to date. The lack of a single patch could endanger the entire environment. However, only patches that have been tested and files that can be clearly identified and processed in the anti-malware system can prevent the occurrence of false positives. With HySEC's false-positive scanning this threat can be prevented.

WHITELISTING

Whitelisting permits only predefined services to be started in a secure environment, preventing the execution of malicious code. A specially fine-tuned malware scanning engine is the basis for ensuring secure and fault-free operation.

MONITORING AND DIGITAL RISK MANAGEMENT

As well as securing the network and all its connected components, monitoring the infrastructure and cyber risk governance are also essential. Behavior of the data streams, vulnerability management, display and monitoring of attacks and the correlation of logging and system information can all be achieved through the system-wide implementation of HySEC orchestration.

ANDRITZ' HyNET and HySEC are innovative and comprehensive cybersecurity solutions that provide a wide range of services, all with top-tier technology, perfectly defined processes, and our long-standing technical experience.

AUTHOR

Michael Ritter
hydronews@andritz.com