TURBINE TECHNOLOGY SERVICES CORPORATION

CYBERSECURITY

"The single biggest threat out there, is cyber."

Cybersecurity has become an increasingly important issue for turbine operators, with concerns about the vulnerability of industrial control systems to malicious hackers. This has led to requirements from both the North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC) to assess existing plant systems and improve their protection from attacks.

Over the last 2 decades cybersecurity has grown to be one of the nation's most important issues. Dealing with cyber crime has proven to be a difficult challenge necessitating the need for new laws and new ways of enforcement.

Cybersecurity, as it pertains to industrial control systems (ICS) has been a particularly unique challenge: Many owners and operators have, in the past, focused very little on security and staying current with their cyber assets. This means that a large portion of the control systems and HMI's in use today are non-compliant with standards set forth by NERC-CIP.

Cyber Emergency Response Team

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

Why should I care about Malware?

Malware attackers receive direction and support from a national government. Whether their mission is to steal data, disrupt operations, or destroy infrastructure, these threat actors tenaciously pursue their goal using a wide range of tools and tactics.

Malware breaches in the energy and utilities Industry...

27%

Compliance Standards

Cybersecurity has been a concern for several years, but from a compliance and regulation point of view, it is still very new. And, hackers are becoming well funded and very creative. As a result, the governing entities and the rules are sometimes vague and unclear. Consultants are often engaged to make the standards more clear and create strategic plans for upgrades and compliance.

Governing Entities

NERC North American Electric Reliability Council
- Originally Formed in 1968 and reformed in 2006 under the same name as a nonprofit corporation.
- Mission: "ensure the reliability of the North American bulk power system".
- Certified by FERC as the US's Energy Reliability Organization.

FERC Federal Energy Regulatory Commission
- Independent agency that regulates the interstate transmission of electricity, natural gas, and oil.

NERC Compliance and Options to Consider

Whether driven by obsolescence or other factors, upgrading is an opportunity to achieve NERC compliance. Considerations:

- Retain existing controls:
  - Spare parts become harder to find and costs increase with demand.
  - Connected interfaces such as Human Machine Interfaces need to maintain compliance. (GAP options)
  - Potential significant security weaknesses.
- HMI strategic upgrades:
  - Server/client configured HMI systems compatible with MK IV, MKV, and MKVI controllers.
  - Plug and play replacement systems are available such as Turbine Monitoring Systems (TMOS). Designed to replace existing OEM and aftermarket turbine and BOP control system interfaces on most turbine applications.
  - Provides a direct replacement for OEM supplied HMI and offers all OEM functionality and in some instances more.
  - Easily configured to meet NERC requirements as well as satisfy customer's unique cybersecurity needs.
  - Hardware Replacement
- Complete controls upgrade:
  - While expensive initially, the benefits of a complete system upgrade will pay off over time.
  - As a whole, the benefits are regulatory compliance, reliability and availability.
  - Extensive non-OEM options are available.
  - OEM options typically mean high price tag and limited customization.