CYBERSECURITY COMPLIANCE
GAS TURBINE CONTROL SYSTEMS

Options to Consider

Presented by: David Donnaruma

TURBINE TECHNOLOGY SERVICES CORPORATION

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.

Agenda

Situation

Compliance Standards

Cybersecurity Control Systems

Multiple Options

Closing Remarks and References

Situation

Need for Cybersecurity has grown dramatically

Many operators are not in compliance

Multiple options are available

- 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.
- There are options available for owners and operators to bring their obsolete systems into compliance. The first steps are to asses the system as a whole and distribute resources to best meet the needs of the overall objective. Note: Compliance cannot happen overnight.

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.

Critical Infrastructure Protection

- Began with the U.S. Energy Policy Act of 2005
- Gave the Federal Energy Regulatory Commission (Commission or FERC) authority to oversee the reliability of the power grid.
- NERC developed CIP reliability standards that were issued in 2008.
- Reliability Standards include CIP standards 001 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid.

Critical Infrastructure Protection (CIP)

CIP-002-5: Bulk Electric System (BES) Cyber Asset and BES Cyber System Categorization

CIP-003-5: Requires that responsible entities have minimum security management controls in place to protect Critical Cyber Assets

CIP-004-5: Requires that personnel with authorized cyber or unescorted physical access to BES Assets have appropriate levels of personnel risk assessment, training, and security awareness

CIP-005-5: Requires the identification and protection of the Electronic Security Perimeters inside which all Critical Cyber Assets reside, as well as all access points on the perimeter

CIP-006-5: Addresses implementation of a physical security program for the protection of BES Assets

CIP-007-5: Requires responsible entities to define methods, processes, and procedures for securing BES Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeters

CIP-008-5: Identification, classification, response, and reporting of cybersecurity incidents related to BES Assets

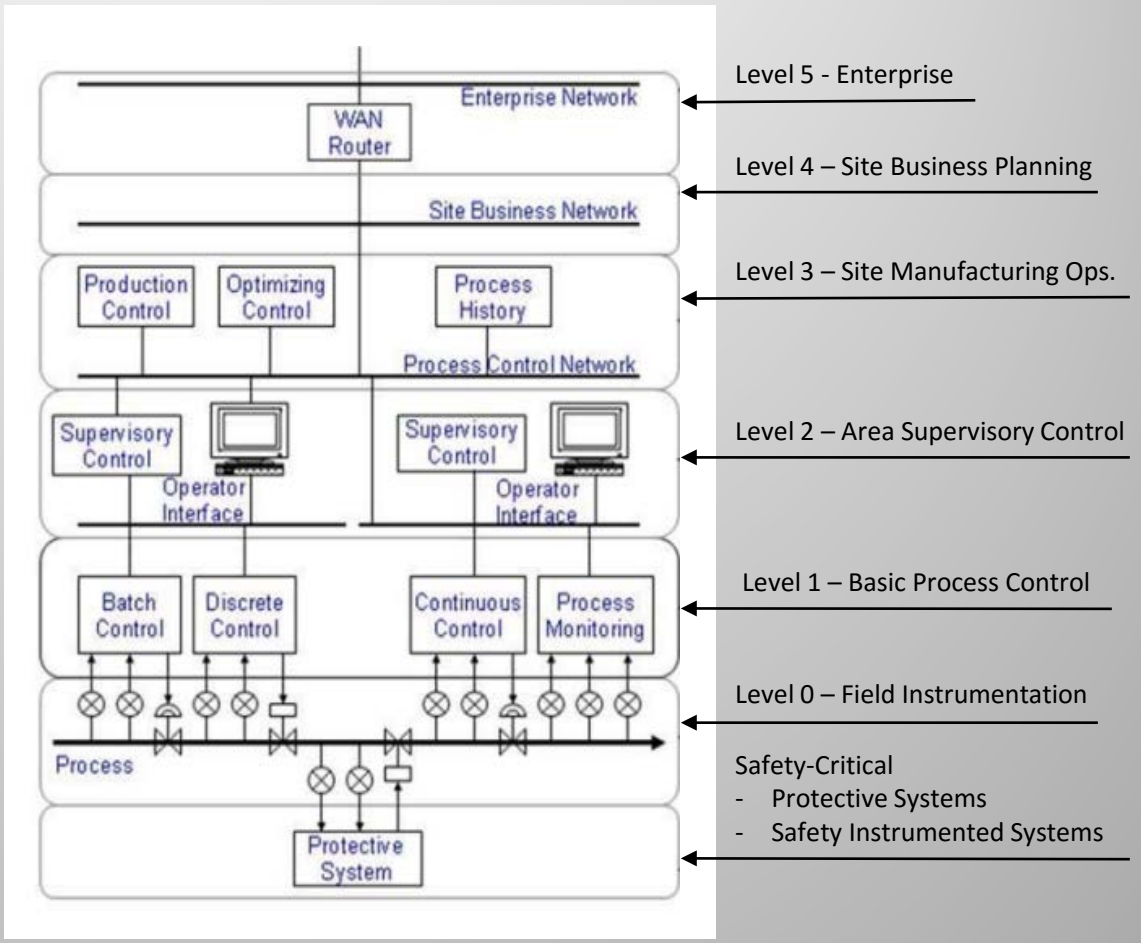
CIP-009-5: Ensures that recovery plans are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices

CIP-010-5: Configuration Management and Vulnerability Assessments

CIP-011-5: Information Protection

ISA/IEC 62443 Compliance Standards

- ISA/IEC 62443 Standards were developed to meet the regulations set forth by NERC-CIP by the ISA99 committee.
- These standards apply to cybersecurity for manufacturing and industrial control systems.
- The goal is to divide the plant-wide control system into functional levels of control
- This includes: PLC's, HMI PC Devices, Network Devices and Software



Cyber Emergency Response Team (ISC-CERT)

- 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.
- Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.
- Advisories are posted continually throughout the year warning and advising about current security issues and reports on what steps the manufacturer of the affected equipment is taking to resolve the vulnerability.
- Sign up for the newsletter! https://ics-cert.us-cert.gov/monitors

CYBER SECURITY CONTROL SYSTEMS

Homeland Security Recommended Practice…

Improving Industrial Control Systems CyberSecurity with Defense-In-Depth Strategies.

A recent report indicated that 27% of the organizations in the Energy/Utilities industry had advanced malware in their systems and 98% of these companies have experienced a breach.

Obsolescence of Vintage Speedtronic™ Systems

- **Lifecycle**
  - Phase 1 – Product Release
  - Phase 2 – Mature Product
  - Phase 3 – End of Production – Product is no longer available for new installations
  - Phase 4 – After Market – New spare parts are no longer available and support is limited to repair, exchange or remanufacture
  - Phase 5 – Obsolete – The product is no longer supported.
- **Parts**
  - High cost for replacement parts
  - Can be difficult to find
  - Reliability in question

Obsolescence of HMI Hardware

- **ARCNet Communications**
  - 2 Types of cards provided by GE:
    - ISA Slot - Rare! Extremely hard to find
  - PCI
    - Off-the-shelf replacements available
- **HMI Hardware**
  - Typically Dell workstations
  - Not up to today's standards
    - Obsolete components
    - Virus-prone operating systems: Windows XP/NT

Termination of HMI Computer Operating Systems (NT, XP)

- **Windows XP**
  - End of support date: April 8, 2014
- **Windows NT**
  - Workstation versions support ended on June 30 2002, extended until June 30 2004
- **What does this mean?**
  - Microsoft end of support means no further security patches
  - Large OEM manufacturers will discontinue support
  - These devices cannot remain connected to the corporate network

Multiple Options

The guardians of your company's cyber security should be encouraged to network within the industry to swap information on the latest hacker tricks and most effective defenses.

NERC Compliance

- Whether driven by obsolescence or other factors, upgrading is an opportunity to achieve NERC compliance.
- Considerations:
  - Retain existing controls
  - HMI strategic upgrades
  - Complete controls upgrade

Retain Existing Controls

PROS	CONS
Longer product life cycle results in less costs associated with product retrofit, and operational staff training.	Spare parts become harder to find and costs increase with demand.
Less risk of forced outages, and compliance issues as trusted system is in place.	Connected interfaces such as Human Machine Interfaces need to maintain compliance. (GAP options)
No risk from cascading costs incurred due to outdated instrumentation, connected control interfaces, and networked devices.	Potential security weaknesses.

HMI GAP – Strategic Upgrades Options

- **Non-OEM:**
  - 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 gas and steam 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
    - Newly manufactured hardware is available that is compatible with previous versions of Windows. This allows the customer to extend the life of the system and does not require any additional operator training – straight hardware upgrade means that the software is left untouched.
- **OEM Options:**
  - No direct replacements for HMI's – typically an entire new control system is quoted.

Complete System Upgrades Options

- 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.
  - Avoids penalties for non-compliance
  - System can be designed around compliance requirements
- Non-OEM options are extensive!
  - Allen Bradley (ControlLogix, CompactLogix), Siemens (S7), GE PLC (RX3i), Mitsubishi (iQ-R), Modicon
  - Industrial PLC's are much more powerful and feature-rich than in the past
    - Isolated analog cards, direct speed inputs
    - Vast communications abilities – OPC, Modbus, DNP, Profibus, DeviceNet, Ethernet/IP etc.
- OEM options typically mean high price tag and limited customization.

Closing Statements

- Security is an ever-evolving process of determining where, when and how attackers will strike.
- The key aspects to protecting an asset lie within the organization's processes and employee's personal responsibility for following the rules.
- The options available differ per the individual corporate policy – this will determine the level of compliance necessary.
- The benefits of an open (non-OEM) system are clear – primarily lower cost, agile response to new threats, including integration of the latest available security hardware and software, and enhanced exposure to new non-OEM technologies.
- Breaking away from the OEM allows for options for strategically replacing assets in a manner that is still in line with corporate IT policy.

References

- **“Helping Power Plant Control Systems Achieve NERC CIP Compliance”** 03/01/2009 | Jonathan Pollet and Walter Sikora
- http://www.ferc.gov
- http://www.nerc.com
- “An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity” https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf