21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2017 Grid of the Future Symposium

Cybersecurity Good Practice: Not Just NERC CIP Compliance

A. WEST
SUBNET Solutions Inc.
Canada

SUMMARY

This paper discusses a selection of practical cybersecurity guidelines from NIST's Special Publication 800 82 "Guide to Industrial Control Systems (ICS) Security" that may be adopted by electric utilities to improve the cybersecurity posture of a control system. Whether or not you are required to comply with NERC's rules, the NIST guidelines provide prompts for considering how to make a grid control system more secure, not just compliant.

KEYWORDS

Cybersecurity, risk management, system engineering

andrew.west@subnet.com

Introduction

Many ICSs are required to comply with legislation related to safety and environmental protection and industry specific rules. In some regions, the electricity industry must comply with market regulations relating to quality of supply and operating practices, with financial penalties imposed for failure to meet specified compliance levels. Engineering design practices have been developed to comply with these requirements. Even where no specific cybersecurity regulations are imposed, many facets of good ICS cybersecurity practice can support systems to meet their contractual and legislative obligations. In this regard, many areas of good cybersecurity practice should be viewed as an aid to good engineering design.

The US National Institute of Standards and Technology (NIST) has published a number of cybersecurity guidelines targeted at various sectors. It has on-going programs to develop cybersecurity frameworks, methodologies, standards and guidelines applicable to many specific application domains.

This paper is focused on guidelines published in NIST SP 800-82[1], which address the specific requirements of industrial control systems. This guideline document is freely downloadable from NIST (see references for URLs). SP 800 82 does not define legal requirements, but provides guidance that may be applicable to many types of ICSs. Implementation of selected guidelines may bring specific benefits in the operation or maintainability of an ICS.

Many North American electric utilities are required to comply with cybersecurity requirements established by NERC for some or all of their infrastructure. The guidelines from SP 800-82 can complement the NERC CIP requirements and may provide for functional cybersecurity that is superior to merely complying with NERC CIP. Consequently, SP 800 82 should be considered when creating or reviewing cybersecurity policy or implementation, irrespective of whether the utility is also required to comply with NERC CIP requirements.

Guidelines that support electric utility design and operation

The primary security objectives raised in SP 800 82 are intended to support the correct and reliable operation of the control system. Many recommendations relate to enacting policies and procedures to ensure or enforce good engineering practices for system design and operation.

The electricity grid may be characterized as being a continuously-operating, highly-distributed system of independently acting subsystems (e.g. substation protection, automation and control systems) overlaid with a supervisory network. Some aspects of the automation systems must operate at high speed and irrespective of the availability of the supervisory and communication systems. The interactions between the various subsystems are often complex. When considering cybersecurity implications, all interactions between the various automation systems could be affected and these effects should be considered. This review may require contribution from a multi-disciplinary team who are knowledgeable about the behavior of the various subsystems and aware of the regulatory framework within which the utility operates.

Cybersecurity should be considered as part of an organization's risk management procedures. In this regard, cybersecurity may be considered as one more possible source of alteration of some aspect of the system's operation. The potential impacts on the system operation from

cyber sources should be considered and the mitigating capabilities of the system considered in conjunction with these. Operational staff are often best placed to assist in evaluating risks: The experienced operator is often aware of many ways that system operation may be impacted through cyber means. They should be involved to participate in risk reviews. One useful question to an operator might be: "What is the most significant damage that you could cause from your keyboard?" It may be found that the potential risks from cyber means are mitigated by fundamental physical design constraints. For example: Even if an operator closes the valves in a power station steam plant boiler and sets the fuel feed rate to maximum, they cannot cause a catastrophic explosion of the boiler if it is fitted with pressure-relief rupture disks that will release pressure before it reaches critical levels. Look for mitigations that cannot be circumvented through cyber means.

Design the system to operate in a resilient manner during unexpected conditions. Various factors can reduce system capability, such as the loss of communications networks, excess load due to high rates of data change, etc. Cyber events may also cause unexpected outage or reduction of performance and should be included as part of system resilience design. One possible strategy is to separate critical and non-critical functions and provide additional resources for the critical functions.

Disaster recovery: Software executables and configuration data may be lost or damaged by many causes ranging from failure of hardware to inadvertent or malicious corruption or deletion. Create a disaster recovery plan that describes how to restore a system to normal operation. Have up-to-date backups of software, configuration, etc. Have plans describing how those backups are used to recover or rebuild a system. Check that the backups work. Ensure that staff are trained to execute the restoration plan. Run periodic exercises to restore a system from backups: This verifies the integrity of the backups, the correctness of the recovery plan and the training, knowledge and ability of the staff to implement the plan. Most importantly: Do all these things before you need them.

Asset management: Know what you have. Ensure that engineering drawings and equipment registers are kept up to date and reviewed periodically for accuracy. Whenever a system change is made, all relevant drawings should be updated to show the current state of the system. Implement procedures to ensure that this is done and staff trained to ensure awareness of the procedure. Keep a register of all control system equipment: Manufacturer and model, software versions and configuration revision. If the vendor releases a software patch, having an accurate equipment register simplifies the process of knowing if and where the patch may be needed. Keeping an up to date record of approved configuration revisions allows verification that the correct configuration is loaded (technology solutions may help automate this verification) and assists with disaster recovery. The system should also be periodically reviewed to verify that the actual system matches the records. This can identify unauthorized additions to the system. Again, some technology solutions can assist in automating this work by verifying all equipment connected to the system; verify the network connectivity, logging all MAC and IP addresses, etc. In systems that monitor all connections to all network ports, unexpected modifications to a system's hardware can be quickly identified.

Control access to equipment, both physically and "logically". Implement ways to manage equipment access. Only allow authorized staff to manipulate the equipment. This may involve procedures such as locking cubicle doors and controlling access to keys or implementing access control procedures so that only authorized users can log into the network that access the control equipment. Keep a log of who has access (e.g. was issued a key or logged in) and

what work they performed. If they made a change, this change should be archived (as described for asset management and disaster recovery). If equipment permits multiple levels of access (e.g. “view-only”, “operator” or “engineer”), then the equipment should always be accessed with the least amount of privilege required to perform the task. This helps prevent inadvertent changes. Prevent all access to equipment other than through the approved methods. This may necessitate network redesign to separate critical segment from non-critical segments, introduction of DMZs, firewalls, etc. Where possible, monitor, verify and restrict communication between segments to ensure that only expected and approved traffic crosses between segments. SP 800 82 discusses many network topologies and techniques for managing connectivity. Where possible, support the access procedures with tools that automatically enforce the procedure (e.g. role-based access controls that only permit an authorized user to perform permitted functions) or to maintain the logs, records of changes, etc. that allow tracking of all changes.

Appendix G: ICS Overlay

Appendix G of SP 800 82 provides a summary of cybersecurity-related characteristics that should be considered for a control system. This can be considered as a checklist that can be used as an aid to creating a security policy and reviewing the cyber-security readiness of a system. For each item listed in this appendix, a system owner’s cybersecurity team should consider if that item is applicable for the system and what policy, procedure or technology is appropriate to address that item. This may be an iterative process whereby a system’s cyber resilience can be progressively improved by periodic review and reassessment. The standardized form of this checklist also supports the ability to compare results of equivalent reviews in different organizations or industries.

Consideration of the items in Appendix G is recommended for all ICS owners, including electric utilities. If nothing else, it can lead to collecting an understanding of the control system cyber security preparedness. This is then useful to assist management prioritize further work. A side-effect of many of the review activities is to bring people from different segments of the business together to share information. This can lead to a better understanding of other parts of the organization and improved internal communication and cooperation.

Summary

Cybersecurity awareness and considerations should be included as part of normal system design and ongoing operation and review. SP 800 82 provides guidelines for introducing cybersecurity aspects into normal engineering processes. In particular, Appendix G provides a comprehensive list of cybersecurity considerations for industrial control systems.

As with other areas such as operational performance and risk management, cybersecurity is an on-going process that requires periodic reassessment and review. When viewed in isolation, this may appear an unwelcome burden. However, the adoption of well-designed procedures with appropriate technological support to automate them can lead to improved performance in asset management and system integrity. This is especially the case where the correct deployment of all software and configuration can be verified and the system topology and device operation continuously monitored in real time. Instead of a burden, good cybersecurity practices lead to better engineering outcomes, reducing risk and improving system performance. This may be a route to simplifying compliance with other regulations, a case of good cybersecurity practices actually saving money.

The reader is encouraged to obtain a copy of SP 800 82 and consider the applicability of its recommendations to their system.

Reference

[1] NIST Special Publication 800-82, Revision 2, Guide to Industrial Control Systems (ICS) Security, May 2015, available from
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
Or
http://dx.doi.org/10.6028/NIST.SP.800-82r2

Glossary

CIP Critical Infrastructure Protection
ICS Industrial Control System
NERC North American Electric Reliability (www.nerc.com)
NIST National Institute of Standards and Technology (United States) (www.nist.gov)