A Forward-Looking Approach to CIP

Stanley A. Klein
Open Secure Energy Control Systems, LLC
(301) 565-4025
stan@osecs.com

Agenda

- Backward-looking comments from meetings and articles
- Background of the comments
- A look ahead
- A forward looking principle
- IEC-61850 as a forward looking example
- Conclusions

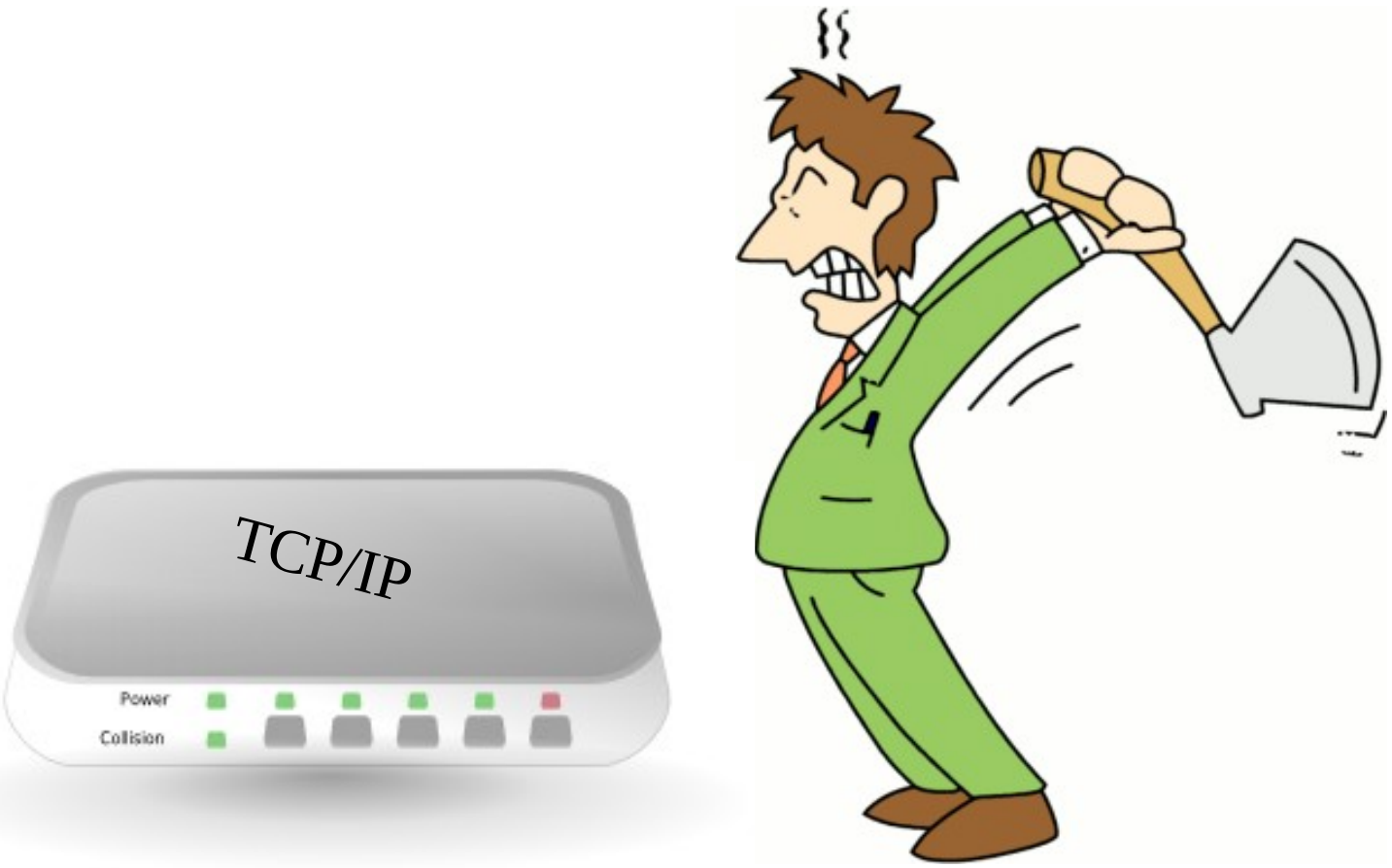
What I've been hearing

- "I told my boss what it would cost to protect our distribution SCADA and he said he would rather shut it down than spend the money"
  - Remark at a NERC CSSWG meeting 4 years ago
- "The CIP standards outlaw routable protocols. We are planning to get rid of them and use non-routable protocols"
  - Remark at a recent PSRC meeting

What I've been hearing (continued)

- "We operate the largest transmission system in our state and we may wind up with the smallest number of critical cyber assets. That's because our substations are not IP (Internet Protocol) or dial-up accessible."
  - Utility executive quoted in Public Utilities Fortnightly

Is this the answer to the CIP standards?



Where do these ideas come from?

- "..... For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
  - R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
    R3.2. The Cyber Asset uses a routable protocol within a control center; or,
  - R3.3. The Cyber Asset is dial-up accessible."

Why does CIP-002 say that? My "educated guess":

- NERC had to produce a standard that can be met
  - Asset owners will be audited
  - There are penalties for non-compliance
  - The cyber-security standards are part of the reliability standards, and must use the same overall rules
- Some of the non-routable protocols and the equipments that use them are difficult to cyber-secure
  - Example: CIP 005 R2.2 requires turning off ports and services in cyber-critical assets not needed for operations or for security monitoring. In some older equipment, this is difficult or may break something else if tried.

Is retreating in technology the answer? No!

- The non-routable protocol exclusion could disappear
  - FERC received comments from the ISA99 Team that non-routable protocols are critical to operations and "have been shown to be vulnerable – by testing and experience."
  - FERC's response in Order 706 was: "... we direct the ERO [NERC] to consider the comment from ISA99 Team."
- If the exclusion does eventually disappear, a decision now to move back to non-routable protocols could wind up being the worst possible choice.

Additional factors

- FERC Order 706 also calls for “defense-in-depth” subject to technical feasibility considerations with NERC/ISO/RTO oversight.
- Defense-in-depth is defined as two or more defensive measures used in constructing a security perimeter.
- Technologies that are difficult to protect also have difficulty providing defense-in-depth.

And look what is right around the corner

- Title XIII (Smart Grid) of the Energy Independence and Security Act of 2007:
  - Establishes a policy of advancing the technology of power grid communications, control, and automation standards
  - Mandates state regulators to consider requiring that when a utility makes investments in nonadvanced technology, it justify to the regulators why it didn't choose advanced technology

A forward looking principle

Embrace the new technology

It offers better cyber-security than the old

And it offers benefits in cost and improved operations

IEC 61850 is a forward-looking example

- It provides advanced technology for utility automation
- It has features that facilitate security protection
  - Named objects
  - Routable protocols
  - Configuration information that can support security
- It facilitates using off-the-shelf technology to provide defense-in-depth
- And it also provides cost and operational benefits

IEC 61850 provides advanced technology for utility automation

- Defines data models that represent monitor/control IEDs
  - Hierarchy of named objects with specified naming rules
  - Defines services for data object types
- Includes XML-based Substation Configuration Language
- Provides layered communication protocol framework
  - Uses existing standards: TCP/IP, SSL/TLS, MMS, ASN.1, others
  - Maps data model and services to MMS
  - Can support mappings to other protocols
- Plug and play self-description
- Companion to several other IEC standards

Overview of 61850 modeling and naming

- Intelligent Electronic Devices (IED's) include Logical Devices (LD) modeled using Logical Nodes (LN) composed of common data classes (CDC) and attributes (CDA) that use Basic Types
- Part of name is utility-defined, remainder is standard
- Naming illustration:
  - **Roanoke_238KV_LB99A_CTRL/MMXU1.PhV.phsB.CVal.mag.f**
  - Roanoke_238KV_LB99A_CTRL is a utility defined LD name
  - MMXU1.PhV.phsB.CVal.mag.f is the 61850 standard name for the floating point magnitude of the complex value of the Phase B voltage measured by measurement unit (MMXU) number 1 of the IED/LD

61850 is a benefit enabler

- Planned for implementation in 17% of North American utilities but 55% elsewhere (Newton-Evans survey)
- Immediate benefit: Substation wiring.
- Other benefits captured only with additional tools
  - More extensive operational information
    - Maintenance, configuration settings, condition monitoring, renewable energy regulatory reporting
  - Reduced cost
    - Upgrade, meeting new challenges, CIP documentation
  - Improved cybersecurity
    - Enables conventional security protections

Issues caused by IEC standards process

- The IEC standards process is unlike the IETF process
  - IETF requires demonstrating interoperability of two differently coded reference implementations before standardization
  - IEC (and ISO) often adopt first and address problems later
- The “Tissues” process addresses 61850 problems
  - Numerous issues and ambiguities identified
  - Process suspended/preempted by Edition 2 balloting
- Harmonization among companion standards is a continuing issue

Secure 61850 SCADA Toolkit Project

- Phase I and II SBIR from Department of Homeland Security
  - Focus on security issues
  - Open source software implementation
  - Produced initial benchtop prototype
  - Pioneering use of W3C SOAP/XML Web Services in 61850
- Phase I SBIR from Department of Energy
  - Extend to wind power (61400-25)
  - Further development
  - Adjusted focus to tools/products for capturing benefits

Lessons Learned from Toolkit Project

- Routable protocols enable a wide range of off-the-shelf security tools and functions
  - Encryption
  - Firewalls
  - Intrusion Detection
- Other off-the-shelf tools provide defense-in-depth
  - Secure operating system
  - Change control and surveillance for device settings
  - Individual control center user login without rebuilding displays

Lessons Learned from Toolkit Project (Continued)

- SCL supports critical cyber asset identification
  - Can start from definition of critical lines (supported in Toolkit)
  - Automated SCL object naming can provide information for relating critical lines to critical equipment assets
  - SCL information relates critical equipment assets to critical cyber assets
  - Need not implement 61850 to use this capability
- Named objects support access control on individual data objects
  - Ease of definition
  - Ease of enforcement

Conclusions

- Treat the non-routable exclusion as providing time for transition to advanced automation technology
- There are ways to begin transitioning to advanced technology (such as 61850) before fully implementing it. Take advantage of them.
- Take a serious look at the security and other benefits of 61850 and related advanced technology. Even if you choose not to implement it, you will probably need to eventually explain in detail why you didn't.