NIST Workshop on Applying NIST SP 800-53 to Industrial Control Systems

Team Reports

8/17/2007

Red font indicates Red Team

Green Font indicates Green Team

Blue Font indicates Blue Team

Q: What is meant by convergence?

Note: This question posed and answered only by Red Team

- Only 1 standards for all ICS (i.e., no NERC, ISA, etc.)
- Only one standard **from NIST** for all ICS (i.e., covers SCADA, DCS, water, power, etc.)
- Only one standard from NIST **that converges ICS & IT into SP 800-53**
- Answer (from NIST): all three of the above are correct in NIST's concept of convergence

Q: Do you think that convergence of standards is important? Why? (1/3)

- Pros:
  - Easier to implement one standard
  - Eliminates conflicting requirements
- Cons:
  - Dilutes intentions/requirements of specific groups
  - May lose some original ideas
  - Difficult to achieve

Q: Do you think that convergence of standards is important? Why? (2/3)

- Convergence is good thing™ because:
  - Common baseline
  - One standard to comply with. Examples: Government Power (NERC/FIPS 200) and Vendors
  - Having to comply to several standards is labor intensive, redundant
  - Better products sooner
- Convergence is bad thing™ because:
  - Sector support - Is there support from other groups?
  - Who will take these on? i.e.: without regulation

Q: Do you think that convergence of standards is important? Why? (3/3)

- Yes but convergence to what level?
  - US?
  - North America?
  - Global?
- Why
  - Diverse standards increase costs
  - Establishes baselines
  - Source mapping to other standards
  - Who is the convergence good for?
    - Venders
    - Suppliers

Ideas/questions
(posed by the Red Team)

- Has anyone published & updated a cross-reference for all the different standards?
- Government mandated standards have negative connotations
- Quantify cost of an incident and consider that in the context of the cost of insurance (or other risk transfer vehicles).

Issues/Challenges (1/2)
(posed by Green Team)

- Standards that add complexity or additional configuration/management should also include requirements for policies. The policies would ensure that adequate technical knowledge is available to operate or use equipment in an emergency.
  - Example: if Network Access Control is enforced, during an emergency (say at 3am) a procedure and possible technical skills may be required to enable timely replacement of a critical hardware component.
- Standards may not be detailed enough

Issues/Challenges (2/2)
(posed by Green Team)

- How to adequately audit?
  - Check boxes – don’t provide an adequate analysis
  - Testing requirements
  - Training auditors in cyber/control systems
- Politics – leave your emotions at the door
  - Ensure participation from all stakeholders
  - "I didn't write this/not invented here“
- Lack of authority by government organization
  - Need a law to allow gov. organization to dictate coordinated compliance across sectors
- Small Entities
  - How to support

Q: Based on prior knowledge and what you heard here, are the NIST RMF and the ICS augmentation of SP 800-53, Revision 1 a good basis for convergence?

- Yes
- Yes
- Best starting point for US convergence
- Probably the best starting point for North American convergence
- Probably a big challenge for global convergence
- But we have to start somewhere!

Q: What can be done to accelerate convergence? (1/3)

- Legal means (policy, mandates, legislation, regulations)
- Encourage end users/asset owners to drive convergence
- Increase outreach/awareness/promotion

Q: What can be done to accelerate convergence? (2/3)

- Government Regulation or Incentives
  - Sector leads have the authority for cyber security standards
  - Format for sector specific plan to be in 800-53
- Shared mission
  - Require users to participate
- Provide tools/examples of how to apply
  - Sector examples of how to implement
- Exposure/Training (e.g., using CS2SAT)
- Simple
- Expansion/revision of 800-53 to include requirements for all sectors – make it relevant
- Align “groups” to use common framework (e.g., 800-53)

Q: What can be done to accelerate convergence? (3/3)

- Examine examples in other areas where this has happened to see how they can be applied
  - UL Standards
  - Power outlets in US (ANSI?)
  - Fire Hydrants (pipe thread standards)
  - UCA→IEC-61850
- Identify the Benefits/Drivers
  - Economics
  - Safety
- Increase emphasis/pressure on compliance and enforcement

Q: What mechanisms, approaches, & venues should be considered for achieving convergence? (1/3)

- Committee collaborations (e.g., standards committees)
- Subcommittees (e.g., Board of Governors, FCC)
- Websites, road shows, publicity
- Describe link between security & safety
- Entertainment & Media (not Fear, uncertainty, and doubt)
- Find a champion (well known, respected, committed, aggressive, knowledgeable)

Q: What mechanisms, approaches, & venues should be considered for achieving convergence? (2/3)

- Regulation
- Certification for Vendor products
- Management/Industry buy-in
- Training
- Government/CIO door knocking program
- Business case/mission explained when vulnerability testing is done instead of purely detailed technical content.

Q: What mechanisms, approaches, & venues should be considered for achieving convergence? (3/3)

- Venues
  - Expand out to the international community using 800-53 as an input into ISA, IEEE, ANSI
    - IEEE may be a good start due to North American attention to NERC CIP (Many utilities still looking for answers)
  - Get the sector specific organizations to participate in the national standards effort
- Approaches/Drivers/Incentives
  - Market Forces
    - Economies of scale leading to reduced product costs
    - Larger Markets for products
    - Insurance
  - Liability
    - Limits on liability/Insurance discounts
    - Lack of “Due Diligence” (Both Criminal and Civil)

Q: What changes to SP 800-53 and other NIST documents would help catalyze convergence?

- Develop use cases (i.e., examples)
- Use cross reference to the related but non-NIST standards to highlight commonality
- Include requirements for all sectors
- Get SP 800-53 included into industry standards (SP99) so they are used
- Standards and specifications covering minimum security feature set for end devices and components
- More emphasis on forensics and prosecution
- Privacy