Use of ICS standards within Vattenfall

NIST Workshop on Applying NIST Special Publication 800-53 to Industrial Control Systems

August 16, Knoxville

Erik Hjelmvik, Vattenfall Research and Development

VATTENFALL

Our information security policy

- Vattenfall doesn’t use any specific standard
- We have our own security policy which is valid within the whole Vattenfall Group
  - Group Instruction 26, Information Security (GI26)
- GI26 Structure
  - One top level document (short)
  - Appendix 1 Organisational Security
  - Appendix 2 Communications and Operations Management
  - Appendix 3 Access and Authorisation Control
  - Appendix 4 IT Operations and IT Maintenance
  - Appendix 5 Asset Classification and Control
  - Appendix 6 Malicious Code Handling
  - Appendix 7 Computer Network Security
  - Appendix 8 Secure Software Development
  - **Appendix 9 Technical Systems**
  - Appendix 10 Audit Checklists

We do use standards

- GI26 is based on several standards and guidelines
  - ISO 17799 (ISO 27001)
  - We have a mapping GI26 ←→ ISO 17799
- In Germany we have BSI
  - German Federal Office for Information Security
- Swedish Nuclear Power Inspectorate (SKI)
  - SKIFS
  - Almost no Cyber aspects
  - Swedish nuclear power plants Forsmark and Ringhals interpreted cyber requirements
  - They interpreted it completely different!

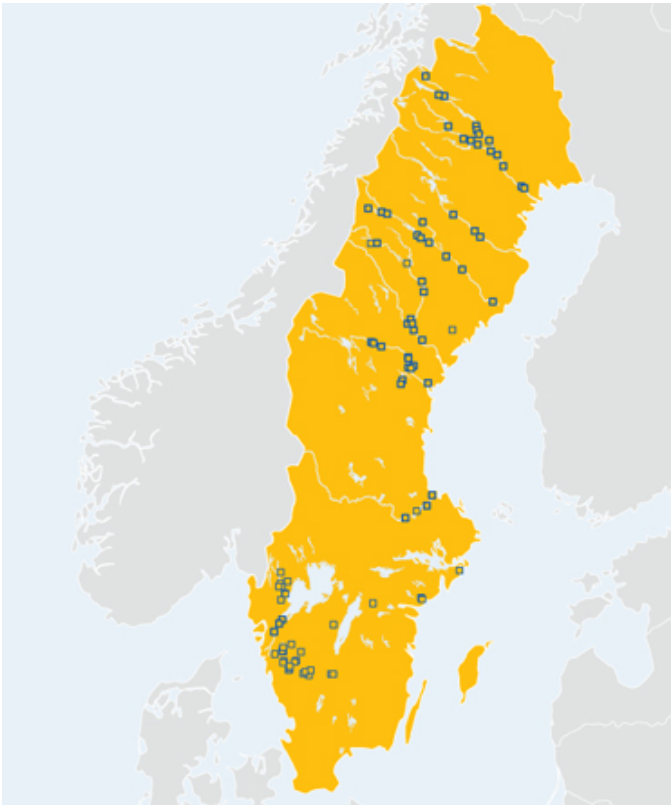
Forsmark

Ringhals

VATTENFALL

Problems with GI26

- Business units have problems with GI26
  - GI26 requirements can be interpreted differently
  - Need for more hands-on how-to guidelines
  - Different needs for different business units
    - Stand-alone cole plants (CHP)
    - Distributed SCADA-like hydropower plants
    - Electric transmission and distribution networks
- Business Units are recommended to crate their own security policy on top of GI26



VATTENFALL

Updating GI26

- GI26 needs to be updated
- More focus needed for ICS issues!
- Questions
  - Separate or joint document for Business and “Technical” IT?
  - Referencing to or copying from standards?
  - What standards to use?
    - ISO 27001
    - NIST 800-53
    - NERC CIP
    - ISA-SP99
  - Nuclear will be handled separately, but how about energy production vs. energy transmission?