

# Challenges, Opportunities, and Suggested Processes for FERC's Adoption of 5 Smart Grid IEC Standards

January 31, 2011 Technical Conference

*Frances Cleveland*

***Key question: Do these 5 IEC standards have sufficient consensus for adoption by FERC?***

## Challenges for FERC Adoption of the 5 IEC Standards

- **Lack of functional review.** Although these 5 IEC standards are rightly seen as key in the development of the Smart Grid, “sufficient consensus” can only be based on complete and thorough assessments:
  - The 5 IEC standards were not formally assessed on their functionality, only on their cybersecurity aspects
  - Although all 5 IEC standards are based on state-of-the-art concepts and technologies, they vary tremendously in their scope, maturity, completeness, testing status, and interoperability certification
  - As a participant in the development of all 5 of these IEC standards, I am very aware of many issues that can affect their viability and interoperability in the Smart Grid.
- **FERC’s term “adoption” is unclear in what it implies for stakeholders. For instance:**
  - While "adopt" does not mandate a standard, should stakeholders be urged to use them?
  - Will the “market” feel pressured to use them, regardless of applicability
  - Will utilities feel that it is “safer” to specify these standards, regardless of cost or interoperability?
  - Will vendors feel obligated to implement them prior to full conformance and interoperability testing and certification?
  - Since cybersecurity must reach across multiple users, systems, field equipment and communication interfaces, how can true cybersecurity be achieved if only 5 standards are “adopted”?
- **The 5 IEC standards are just a subset of a larger set of standards.**
  - What is the implication of adopting them without adopting those other standards?

- Will preference be given to these standards, even if other standards are adequate, or possibly better suited to the functional requirements?
- **The cybersecurity reviews identified the lack of cybersecurity in IEC 61968 and IEC 61970, the CIM-based standards. These CIM-based IEC standards do not address cybersecurity because they are primarily abstract information models. However:**
  - Cybersecurity must be required for actual CIM implementations
  - The reviews recommended that cybersecurity guidelines be developed for such implementations, with references to appropriate cybersecurity standards.
  - Therefore, should these standards be adopted before such cybersecurity guidelines are developed?

### Opportunities for Managing “Adoption”

- **A “FERC Adoption Framework” could be developed which describes different *FERC Adoption Categories* to handle the nuances of the differing maturity and scope of the standards**
  - Certain categories of adoption could be used to get recognition of promising standards so that vendors will implement and test them, without pushing the industry to implement them so fast that better solutions are ignored or testing is incomplete
  - **Maturity** would measure:
    - \* Completeness of specification within the standard
    - \* Conformance testing of implementations against the standard
    - \* Interoperability testing of implementations against each other
    - \* Formal certification process has been established
  - **Scope** would cover:
    - \* A standard can be made up of different Parts. If so, identification must be made of which Parts of a standard are to be included in a particular scope. For instance, one Part might be judged to have one scope, while other Parts might be combined into a single separate scope
    - \* Different scopes could be placed in different “adoption” categories, depending upon their status. For instance:
      - Parts still under developed could be identified as potential but not ready for adoption
      - “Informative” Parts (such as introductions and glossaries) could be categorized separately
    - \* Specific profiles of combinations of standards could be adopted, (e.g. requiring the IEC standards to use the IP-based set of standards, or identifying what protocol the abstract information models would be mapped to)

### Possible FERC Adoption Framework with the following Adoption Categories:

- **Adoption Category 0: Information.** These Parts of a standard are information, including introductions, glossaries, and guidelines
- **Adoption Category 1: Potential Adoption.** These Parts of a standard could be of significant value to the Smart Grid, but have not yet been adequately specified or are still under development.
- **Adoption Category 2: Complete Specification.** These Parts of a standard have been completely specified, but have not been implemented or tested.
- **Adoption Category 3: Conformance Testing Certification.** These Parts of a standard have been implemented by at least one vendor and have been tested for conformance with the appropriate Parts of the standard.
- **Adoption Category 4: Interoperability Testing Certification.** These Parts of a standard have been implemented by more than one vendor, and these implementations have been certified to be interoperable.
- **Adoption Category 5: Cybersecurity Certification.** These Parts of a standard have been certified as meeting the interoperability testing and cybersecurity requirements.

### Suggested FERC Adoption Processes

- Before a standard is submitted to FERC for possible adoption, it must go through both functional and cybersecurity assessment.
- During functional assessment, each Part of the standard is reviewed with respect to maturity and scope
  - Each Part would be assessed with respect to which FERC Adoption Category it might fit
  - Additional profile requirements would be included, if necessary
  - Recommendations for next steps to achieve the next Adoption Category could be included
- During cybersecurity assessment, each Part of the standard would be reviewed for its cybersecurity requirements
  - Each Part should be assessed on whether it does include cybersecurity or whether that is provided by another Part or standard
  - If the Part does rely on another standard for cybersecurity, that standard should also be assessed for cybersecurity before the Part could be adopted into the Cybersecurity Certification Category.

- Each Part of the standard should reviewed separately, or in combination with other Parts if they are reliant on each other.
- Once assessed, the standard is submitted to FERC with suggested Adoption Categories for each of the Parts
  - FERC follows normal procedures to determine which, if any, Adoption Category to place a standard or a Part of standard.
  - As the Parts of a standard go through conformance and interoperability testing, and as cybersecurity requirements are provided, FERC can update the Adoption Category of the standard.

## Example Functional Assessment of the 5 IEC Standards

1. **IEC 60870-6 (TASE.2 or ICCP)** is the IEC standard for the exchange of information between control centers, and even between control centers and power plants.
  - ICCP is the most mature standard of the 5 IEC standards, and has been widely implemented for many years.
  - Cybersecurity for ICCP is available through its Bilateral Tables, IEC 62351 (Parts 3 & 4), and typical “IT” security technologies (VPNs, firewalls, role-based access control, etc.), although these security measures are not always implemented.

– *This standard could be placed in the **Adoption Category 4: Interoperability Testing Certification**, with the recommendation that additional testing with the cybersecurity technologies could allow it to reach the **Adoption Category 5: Cybersecurity Certification**.*

2. **IEC 61850** is the IEC standard for communications with field equipment, including monitoring and control of devices. It is first being implemented in substations, but is increasingly being implemented in other domains, such as Phasor Measurement Units, Distributed Energy Resources (DER) generation and storage, wind power plants, and hydro power plants.
  - IEC 61850 standards for **substations** have been implemented by most major substation vendors and have been tested and certified through formal testing procedures. The primary Parts for substations are IEC 61850-5, 6, 7-2, 7-3, 7-4, 8-1, 9-1, & 10.

– *These substation Parts could be placed in the **Adoption Category 4: Interoperability Testing Certification**, with the recommendation that additional testing with the cybersecurity technologies could allow it to reach the **Adoption Category 5: Cybersecurity Certification**.*

- IEC 61850 standards for **hydro power plants** are being implemented in Europe. The primary Part for hydro is IEC 61850-7-410.

– *This hydro power plant Part could be placed in the **Adoption Category 2: Complete Specification**.*

- IEC 61850 standards for **DER** (*originally stemming from the widely utilized IEEE 1547 standards for DER electrical connectivity*) are being implemented by vendors of DER generation and storage, including renewable generation such as wind, photovoltaic systems, combined heat and power, batteries, etc. This is particularly true in Europe where laws and regulations are mandating the rapid response of DER devices to power system conditions. The primary Parts for DER are IEC 61850-7-420 and 90-7 (under development).

– *These DER Parts could be placed in the **Adoption Category 2: Complete Specification**.*

- IEC 61850 standards for **Wind** are being implemented in Europe, but are not yet implemented in North America. The primary Parts for Wind are IEC 61400-25-2 & 25-4.

– *This Wind Part could be placed in the **Adoption Category 2: Complete Specification.***

- The IEC 61850 standard for **PMUs** is under development. The PMU Part is IEC 61850-90-5.

– *This PMU Part could be placed in the **Adoption Category 1: Potential Adoption.***

3. **The IEC 61968 series** of standards provides distribution level “application to application” messaging, typically within a utility’s corporate environment. It covers distribution operations, distribution planning, asset management, meter reading (from the AMI headend into the meter management system), and customer service. It is primarily an abstract model, and is expected to be implemented using XML-based messages. It contains no cybersecurity requirements.

- Part 9, Interfaces for meter reading and control, specifies the exchange of information between a metering system (AMI headend) and other systems within the utility enterprise. This standard recognizes and models the general capabilities that can be potentially provided by advanced and/or legacy meter infrastructures, including two-way communication capabilities such as load control, dynamic pricing, outage detection, distributed energy resource (DER) control signals, and on-request read. An interoperability test is being defined which expects to be carried out in early 2011, while updates to the standard are being developed.

– *IEC 61968-9 could be placed in the **Adoption Category 1: Potential Adoption.***

- Part 13, the CIM RDF Model exchange format for distribution, specifies the format and rules for exchanging modeling information based upon the CIM (Common Information Model) and related to distribution network data. The intention of this part of IEC 61968 is to allow the exchange of instance data in bulk. It describes only differences with IEC 61970-452.

– *IEC 61968-13 could be placed in the **Adoption Category 2: Complete Specification.***

4. **The IEC 61970 series** of standards consists primarily of an abstract Common Information Model (CIM) specified in the Unified Modeling Language (UML) in the Enterprise Architect tool, with additional standards to define the rules and format for exchanging this modeling information. The purpose of these standards is to define an application program interface (API) for an energy management system (EMS). The common information model (CIM) specifies the semantics for this API. The component interface specifications (CIS), which are contained in other parts of the IEC 61970 standards,

specify the content of the messages exchanged. It contains no cybersecurity requirements.

- The CIM UML model is an abstract power system model that is used as a base for extracting subsets of the model to be used for specific implementations. It is continuously being updated and expanded to meet new requirements. Only the extracted snapshots, such as IEC 61970-301, are standardized.

– *IEC 61970-301 could be placed in the Adoption Category 1: Potential Adoption.*

- IEC 61970-4xx series describes Component Interface Specifications (CIS) that are Platform Independent Models (PIMs), that are independent of the underlying technology used to implement them. IEC 61970-4XX CISs specify the functional requirements for interfaces that a component (or application) should implement to exchange information with other components (or applications) and/or to access publicly available data in a standard way. The component interfaces describe the specific event types and message contents that can be used by applications for this purpose.

– *IEC 61970-4xx series could be placed in the Adoption Category 2: Complete Specification.*

- The IEC 61970-501 specifies the format and rules for producing a machine readable form of the Common Information Model (CIM) as specified in the IEC 61970-301 standard. It describes a CIM vocabulary to support the data access facility and associated CIM semantics.

– *IEC 61970-501 could be placed in the Adoption Category 2: Complete Specification.*

5. **IEC 62351 series**, Parts 1-7, *Information Security for Power System Control Operations*, are explicitly security standards for the IEC communication standards based on TCP/IP, the Manufacturing Messaging Specification (MMS), IEC 61850, IEC 60870-6, and IEC 60870-5 (not included in this set of 5 IEC standards), and Network & System Management. Although vendors are starting to implement these standards, none of the standards have yet gone through formal conformance testing or interoperability testing.

- **Part 3** of the IEC 62351 series provides technical specifications on ensuring the confidentiality, tamper detection, and message level authentication for SCADA and other telecontrol protocols which use TCP/IP as a message transport layer between communicating entities. TCP/IP-based protocols are secured through specification of the messages, procedures, and algorithms of Transport Layer Security (TLS).

– *Part 3 could be placed in the Adoption Category 2: Complete Specification.*

- **Part 4** of the IEC 62351 series provides specifications to secure information transferred when using ISO 9506, Manufacturing Message Specification (MMS)-

based applications; specifying which procedures, protocol extensions, and algorithms to use in MMS to provide security.

– *Part 4 could be placed in the **Adoption Category 2: Complete Specification.***

- **Part 5** of the IEC 62351 series specifies messages, procedures, and algorithms that apply to the operation of all protocols based on/derived from IEC 60870-5, *Telecontrol equipment and systems-Part 5: Transmission protocols*. The focus of this 62351-5 is on the application layer authentication and security-issues that are a result of application layer authentication. While authentication of sources and receivers is considered the most important requirement and confidentiality is not considered important, encryption can be included by combining this standard with other security standards, such as IEC 62351-3, TLS.

– *Part 5 could be placed in the **Adoption Category 2: Complete Specification.***

- **Part 6** of the IEC 62351 series addresses security for IEC 61850 profiles through specification of messages, procedures, and algorithms. IEC 61850 specifies a number of different profiles which have different constraints, performance requirements, and security needs, but the primary requirement is for authentication of sources of data, receivers of data, and data integrity.

– *Part 6 could be placed in the **Adoption Category 2: Complete Specification.***

- **Part 7** of the IEC 62351 series provides an abstract model of network and system data elements that should be monitored and controlled. Its focus is network and system management, one area among many possible areas of end-to-end information security. The primary focus is the enhancement of overall management of the communications networks supporting power system operations, by specifying monitoring and control of communication networks and systems. Intrusion detection and intrusion prevention are addressed.

– *Part 7 could be placed in the **Adoption Category 2: Complete Specification.***