

IEEE STANDARDS CORNER

FOCUS ON THE IEC TC 57 STANDARDS

By: John Gillerman
Herb Falk
Ralph Mackiewicz
SISCO, Inc.
www.sisconet.com

Introduction

It is often said that electrical grids represent the world's most complex machines. However, one can argue that this analogy understates the problem. For example, how many airliners or factories are operated by a team whose members are employed by different companies with competing interests or whose members don't traditionally talk to each other much? While the grid has been run with remarkable reliability in the past, it is likely that business and operating constraint pressures will only increase in the future. The pressure to operate "closer to the edge" combined with the graying of the power system engineers (not to mention all those mature power transformers out there) surely must lead to greater continuity and efficiencies if we are to continue our track record. But how can we increase continuity and efficiency in such a way that does not require overly centralized bureaucracy and where the drive for profitability can be used as the "unseen hand" that rewards success. This issue of the Standards Corner marks the start of a biannual column two years in length devoted to the discussion of International Electrotechnical Commission (IEC) Technical Committee (TC) 57 standards. The intention of this technical series is to discuss the how standards can be used to address the needs related to power system reliability and profitability.

The IEC, like the IEEE is a global standards organization focused on electricity, electronics and related technologies. The IEC consists of a set of Technical Committees (TC's). TC 57 is focused on Power Systems Management and Associated Information Exchange and is divided up into a series of working groups. Each working group is comprised of members of national standards committees from the countries that participate in the IEC. Each working group is responsible for the development of standards within its domain. The current working groups are:

- WG 3: Telecontrol protocols
- WG 7: Telecontrol protocols compatible with ISO Standards and ITU-T recommendations

- WG 9: Distribution automation using distribution line carrier systems
- WG 10: Power system IED communication and associated data models
- WG 13: Energy management system application program interface
- WG 14: System interfaces for distribution management
- WG 15: Data and communication security
- WG 16: Deregulated energy market communications
- WG 17: Communications systems for distributed energy resources
- WG 18: Hydroelectric power plants – communication for monitoring and control
- WG 19: Interoperability within TC 57 in the long term

In general, these working groups attempt to define standards that govern the interaction between components and not the internal design of components. Here the word component is used to denote an Intelligent Electronic Device (IED), software application, or group of applications that interact with other components as a whole.

There is a high degree of technology reuse across TC 57. For example, there are shared communication protocols specified within WG's 7, 10, 17, and 18. WG's 13, 14, and 16 all use the Unified Modeling Language (UML) to describe their aspect of a unified data model for power systems. WG 15 and 19 are focused on looking across the other working groups to address end to end security and interoperability.

Many of the TC57 standards share a common structure (see diagram). This structure implements what is called a “model driven” architecture. This model driven approach defines the power system aspects of the standard in a technology neutral way that is decoupled from the technology specific implementation profiles that implementers use to build conformant systems. Separating the abstract (or virtual) information models and services from the technology specific details of how to build an actual implementation enables the standards to be migrated as technologies improve and also enables the virtual part of the standard to be used in other applications outside the scope of the official standard. For instance, a protocol standard that includes abstract object models and point naming convention enables those naming conventions to be used in other applications even if the protocols are not used (e.g. using the standardized point names in a SCADA system). This significantly increases the applicability of the standard in existing systems without necessarily requiring new equipment and system purchases.

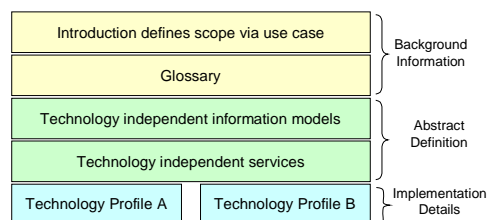


Figure 1: Typical structure of a TC 57 standard

In order to precisely define a power system management or information exchange function, the standards will define an abstract *information model* or *object model*. The terms “Information model” and “object model” have the same meaning and this column treats these terms as synonyms. An information model describes a collection of related real world objects in terms of their classes (or types), attributes, their relationships with other objects, and provides unique names and definitions for each object type. An information model is also sometimes referred to as a “schema”.

Once the meaning of the data has been defined, an abstract definition of services is then defined to specify how information about those objects can be accessed, exchanged, and controlled. This abstract service model specifies how users interact with the standardized objects of the information model in a standardized way to implement the business processes (i.e. power system management and information exchange) defined in the introduction to the standard.

The use of technology a neutral information model and services do not, by themselves, completely provide what is needed for interoperability of heterogeneous systems. For example, the issues of lower level communication capabilities such as TCP/IP, serial links, radios and different technology platforms such as Java, Web Services, and .Net must also be addressed in order to build a real world implementation of the standard. For this, the standards define a set of mappings, or technology profiles, that specify how to implement the abstract models using a particular set of technologies.

One motivation for the abstract structuring of the standards is that the requirements for the *what* (data models) and the *how* (services) power systems components interact seems to change more slowly than the technology used to implement these interactions. A case in point is the rapid rise of Web Services technology that enables data exchange using the protocols and technology widely used on the Internet compared with a standardized abstract definition of *transformers* that has changed much more slowly over the years. With the TC57 approach to standards, the abstract definitions for power system components and their services can be applied to the new technology profiles without having to completely start a new standard from scratch.

Brief summary of TC 57 WG activity

This section briefly describes the work of the TC 57 working groups. A more detailed discussion of general areas of secure substation/field device integration, secure control center/operations integration as well as secure generation/energy market integration will appear in future columns.

WG 3 has focused on the development of traditional remote terminal unit (RTU) device communications. A traditional RTU is a general purpose device capable of collecting I/O signals in a variety of formats (digital, analog, state, etc.) and communicating those I/O signals typically over a serial link to a SCADA Front End Processor. WG 3's IEC 60870-5 RTU protocol specifies a broad set of data objects and device types sufficient to provide interoperability for a large number of applications and device types in power systems. Additional profiles are added as needed by the user community. Furthermore, the use of small 8-bit numbers to represent object and variation types and compact index numbers provided a very byte-efficient mechanism for specifying a data point. This allows 60870-5 to maximize the number of data points that could be fit into a single 60870-5 data frame. This byte efficiency is critical to the effectiveness of 60870-5 as a solution for low-bandwidth serial links.

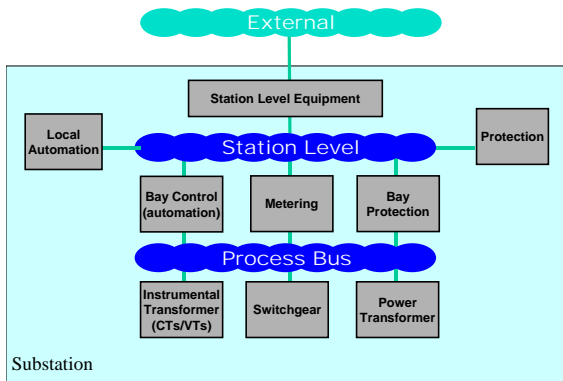
Newer technology profiles have allowed IEC60870-5 to run over the TCP/IP Protocol stack. This permits networking of the communications for monitoring and controlling field devices through a SCADA Wide Area Networks (WAN).

WG 7 has focused on data exchange over WAN's between a utility control center and other control centers, other utilities, power plants and substations. WG 7's IEC60870-6 Telecontrol Application Service Element 2 (TASE.2) protocol (informally known as the InterControl Center Communications Protocol (ICCP)) is supported by most vendors of SCADA and Energy Management Systems (EMS).

TASE.2 provides support for SCADA measurement values, device control, general messaging and control of programs at a remote control center. Since it was first developed in the mid 1990's before object models had been developed for SCADA applications, TASE.2 (ICCP) was not designed to support the transfer of an extensible set of types of objects beyond those defined in the standard.

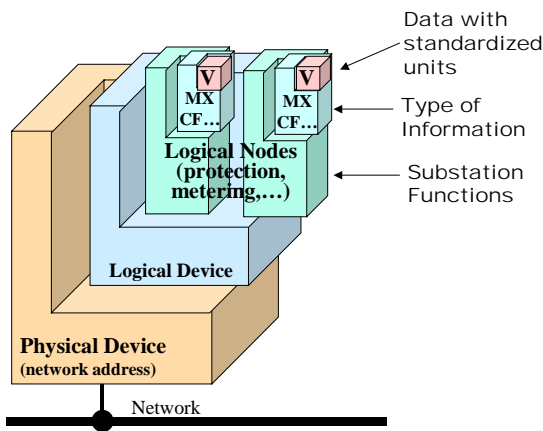
WG 9 has developed IEC 61334, a distribution Power Line Carrier (PLC) communication standard called Distribution Line Message Specification (DLMS). DLMS provides two-way communications and can be used on medium and low voltage networks. While DLMS can be used to access a wide variety of devices (switches, meters, lighting control, and other load controlling devices), currently it is primarily used for retrieving metering information using the IEC 62056 metering standard. WG 9 standards also define requirements for safe interconnection of distribution PLC with medium voltage networks.

WG 10 has focused on substation automation and integration standards that provide capabilities in that go beyond traditional point-to-point protocol solutions. Some of the major innovations have been the development of a substation automation/integration architecture, adoption and standardization of substation function oriented objects, and the development of a standardized Substation Configuration Language (SCL).



A three tier substation architecture, based upon Ethernet, has been developed. The Process Bus level allows for digital current transformer (CT) and voltage transformer (VT) measurements to be streamed to multiple receiving units, thereby reducing costs and allowing leveraging of optical CTs and VTs in a standardized manner. The Station Level/Bus allows for peer-to-peer communications to be used for distributed automation and protection schemes. The third level is for external communications to

remote control centers or remote substations/devices. The functional requirements for each level can be met through the use of appropriate protocols and communication profiles as specified in IEC 61850.



The function oriented, as opposed to data oriented, objects definitions allow a great deal of flexibility and extensibility. The basic hierarchy starts with the communication address that allows access to a Logical Device. A single physical device may contain multiple Logical Devices (LDs) thereby allowing easier information aggregation and creation of communication gateways. Within any particular LD multiple substation functions are exposed. These substation functions are known as by

Logical Nodes (LNs). LNs consist of the information needed to configure, control, perform SCADA reporting functions, settings group control, and measurement/status exchanges. Each LN decomposes into data whose elements are objects and are typically standardized in type and semantics (conveyed through standardized naming). It is the standardized use of the hierarchy, semantic, type, and use of SI units that allow multiple vendors' implementations to expose similar and interoperable object models.

Focusing on decreasing the integration and lifecycle costs of substation automation and integration has been a major focus of IEC 61850. To that end, a set of standardized file formats has been defined to allow exchange of device and substation information to be exchanged. This is known as the Substation Configuration Language (SCL). SCL defines the mechanism for exchanging communication connectivity and device information in a vendor neutral format. This allows vendor substation-engineering tools to exchange this type of information and to drive down the overall engineering and integration costs. A side benefit is that users can use SCL to unambiguously specify the device requirements as part of procurement specifications.

IEC 61850 is being used as the foundation for the work IEC TC57 WG17 and WG18. Additionally, IEC TC57 WG15 is addressing the security needs of IEC 61850. Further descriptions of this work can be found within this article.

WG 13 has focused on interoperability between control center/operations oriented applications including but not limited to:

- Energy, Distribution System, and Outage Management
- Geographic Information Systems
- Network Analysis Applications
- SCADA

WG 13 has defined a Common Information Model (CIM) that describes data typically used in these utility's operational systems. WG 13 is also in the process of adopting a series of technology neutral services called the Generic Interface Definition (GID) IEC61970-4 as well as a set of technology profiles for deployment. The GID is an umbrella term for four interfaces:

- Generic Data Access (GDA) – A generic request/reply oriented interface.
- Generic Eventing and Subscription (GES) – A publish/subscribe oriented interface.
- High Speed Data Access (HSDA) – A request/reply and publish/subscribe oriented interface typically used for measurements.
- Time Series Data Access (TSDA) – – A request/reply and publish/subscribe oriented interface for time-series data.

The table below organizes the GID functionality into a simple matrix:

	Generic (Name/Value Pairs)	High Speed	Time Series
Request/Reply	GDA	HSDA	TSDA
Publish/Subscribe	GES	HSDA	TSDA

Table 1 Matrix of GID Functionality

The GID interfaces are generic. That is they can be applied to any application because they don't specify any data content. The payload or actual data that is exchange between specific application will also be specified in 61970-4 ,

WG 14 focuses on the area of distribution related systems.

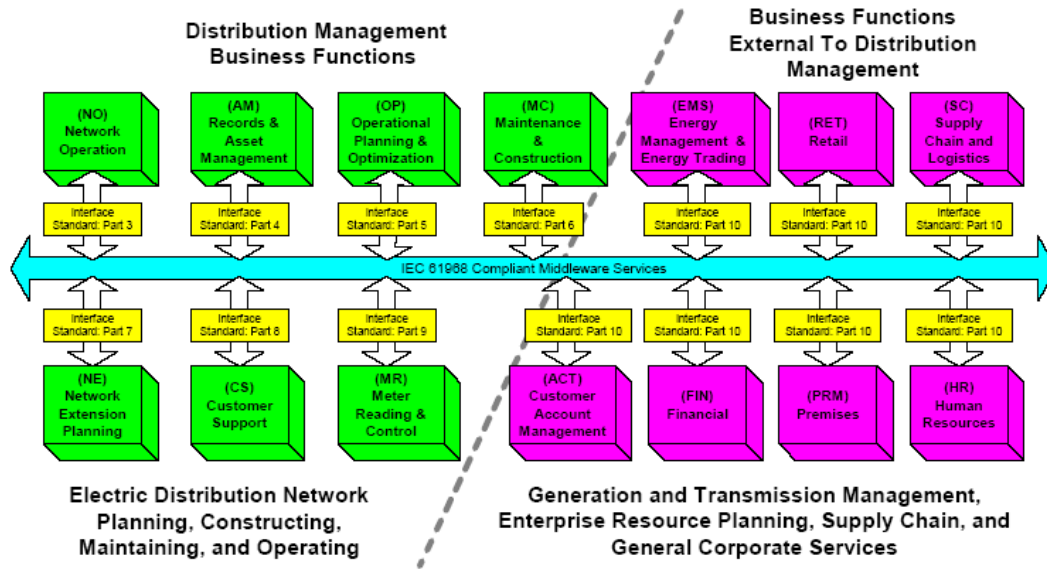
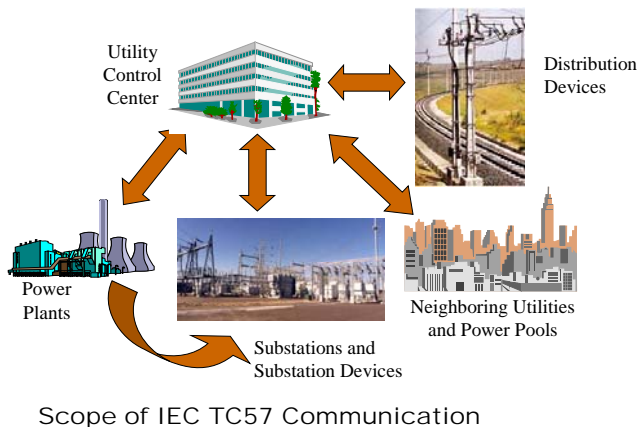


Figure 2: Operations Application Integration

WG 13’s IEC 61970 and WG 14’s IEC 61968 are complementary in that both standards have defined utility data semantics for the IEC Common Information Model (IEC61970-3). The difference between the two is that WG 13 has chose to define a set of application independent interfaces for exchanging data (IEC61970-4) first and then focus on the actual data to be exchanged, WG 14 has solely focused on the data exchanged. WG 14 standards define the nouns (e.g. “Work Order”) and verbs (e.g. “Create”) for messages exchanged between systems (IEC61968-1-11). IEC61968 messages are independent of data exchange mechanisms. 61970 includes a mapping of WG 14 verbs to WG 13 services.

WG15 is chartered to supply security analysis and expertise to the other IEC TC57 working groups and to recommend or supply standardized security enhancements as needed.

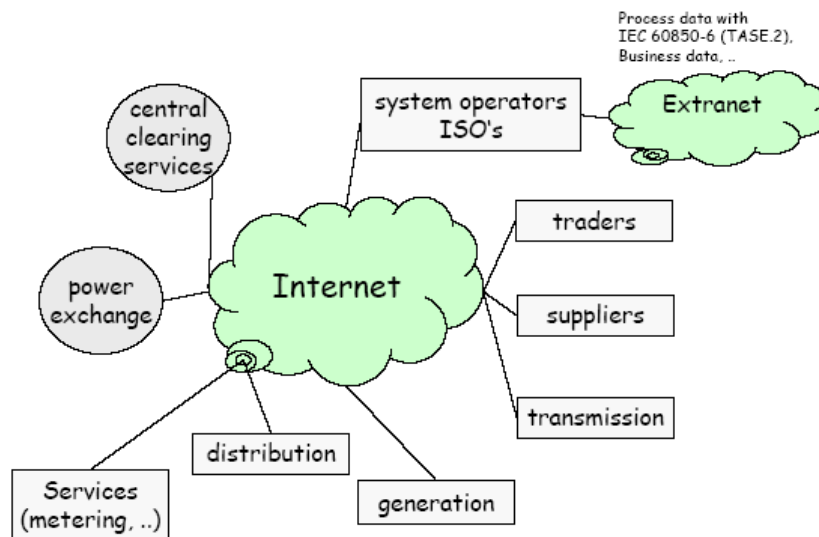


The scope of the IEC TC57 work is broad and encompasses tele-control used between control centers, substations, generation facilities, and distribution devices. The exchange is accomplished through different applications, protocols, transmission media, and communication paths. The focus of WG15 is to secure the application-to-application information exchange through

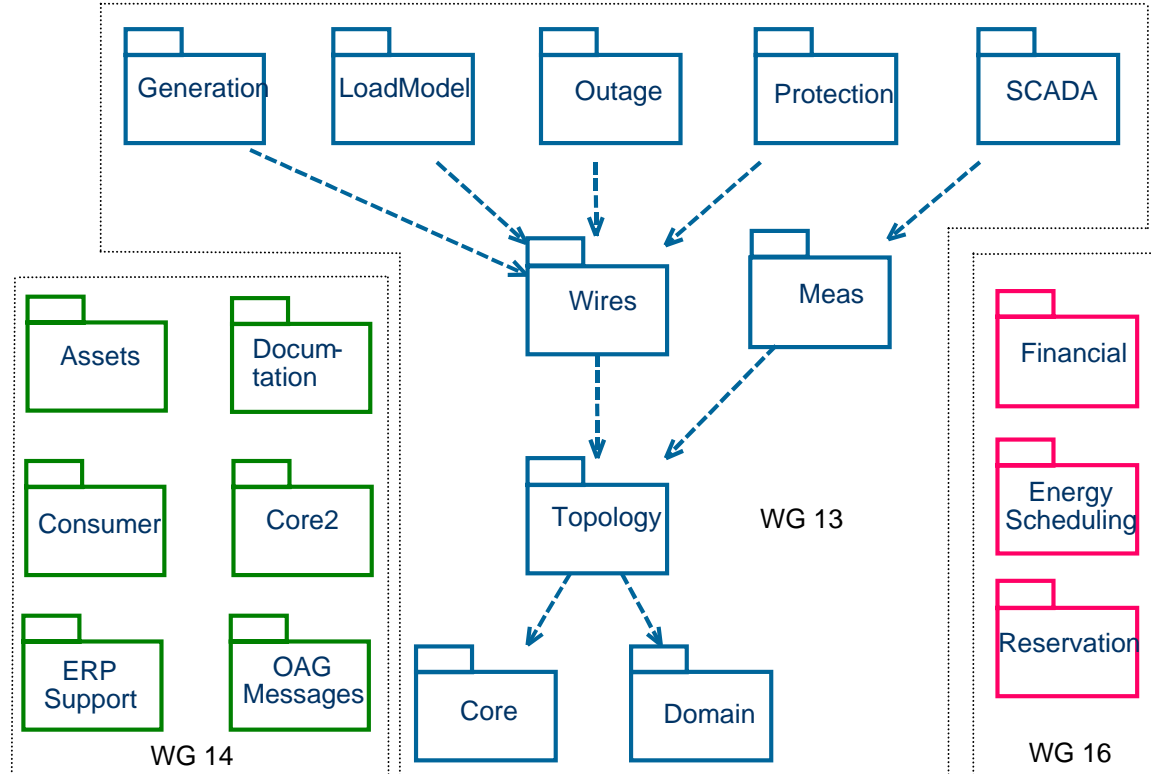
supplying strong authentication and confidentiality enhancements to the IEC TC57 protocols. The protocols, currently being addressed, are IEC 60870-5 and its derivatives (e.g. DNP), IEC 60870-6 TASE.2 (a.k.a. IEC 61850), and IEC 61850.

The working group is also analyzing the different transmission media and paths in order to standardize a security monitoring infrastructure that is protocol independent yet capable of detecting intrusions and attacks. The working group is also attempting to standardize the global process for reporting detected attacks and vulnerabilities.

WG 16 is chartered with developing standards related to energy market communications. As illustrated below, the scope of this work includes many actors including suppliers, consumers, traders, and managers of transmission or distribution system capacity and related services. The diagram below illustrates



While this working group has yet to release any standards, this group is currently considering several general areas. The first general area is how an international standard can accommodate differences in regional markets. The discussion has focused on extending the CIM to include market information and the creation of an adaptable architecture. The second general area is how non-utility specific eCommerce standards can be applied to create energy trading technology profiles. The latter conversation has focused on two standards: ebXML and Web Services.



WG17 and WG18 have worked together with IEC TC88 WG25 to adopt and extend IEC 61850 into functional areas not considered as substation functionality and are concentrated on the distributed generation. These working groups specialize in different types Distributed Energy Resources (DERs). WG17 is attempting to address the general needs of DER whereas WG18 is addressing hydroelectric generation and WG25 is addressing wind power. All of these working groups are using IEC 61850 as the basis of their work, but developing generation specific standardized functions. This is being done through the reuse, extension, or creation of IEC 61850 Logical Nodes.

The newest working group, WG 19 is chartered with looking across all other working groups to harmonize standards and facilitate end to end interoperability. The following figure illustrates this concept using a substation example. In this situation, information from field devices that use various low level protocols is exposed using the common information model and services approach. This permits data derived from these various devices to be integrated. In addition to device data, substation related applications need power system topology and asset management information. Similar to device data, power system topology and asset data can be accessed via a common information model and access methods. Only when all of the related information is fused together can an operator (human or cyber) have a clear picture of what the state of the system is before initiating an action in a cost effective and safe manner that is consistent with the higher-level mission of the overall enterprise.

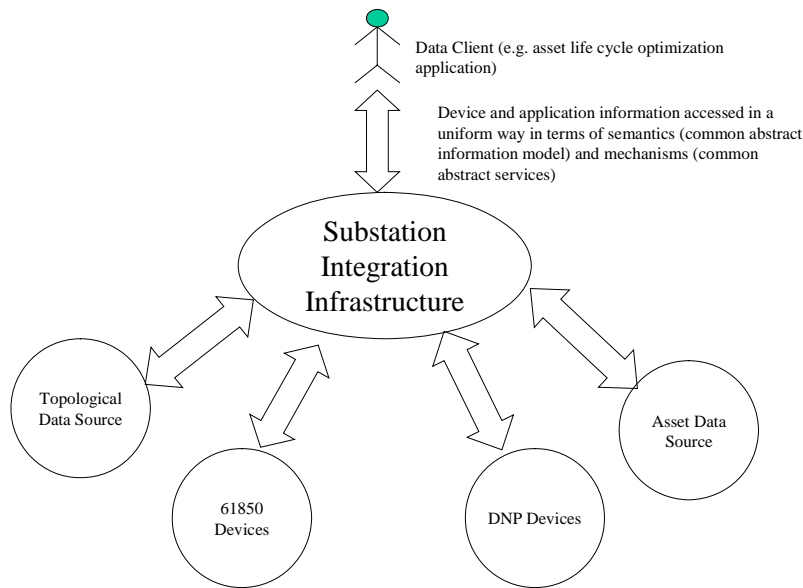


Figure 0-2 Integration of Device and Application Data

The primary benefit of accessing substation data in this way is that it enables higher level applications to interact with devices and other applications in an efficient, structured, and unambiguous fashion independent of the application interfaces or the device's physical attributes and communications interfaces. This approach allows data to be gathered and fused together to accomplish a higher-level mission without requiring detailed knowledge of the inner workings of each device and application. The ultimate benefit is the ability to change out individual devices and applications as technology and functional requirements change with little or no impact at the application level thereby providing higher reliability at lower cost (implementation and maintenance). The reliability issue is actually addressed here on two fronts – the inherent reliability of the device and application integration itself and the ability to take advantage of device and application integration to implement system reliability analysis and management applications at the inter-substation level.

For more information about WG 10 activity see: www.ucausersgroup.org

For more information about WG 13, 14, 16, and 19 see: www.cimusers.org