P2030 Smart Grid Standard Text Submittal Form

This text is intended as proposed text for consideration of the P2030 Writing Group to the P2030 Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads.

SUBMITTAL INFORMATION

DATE SUBMITTED: 06/21/2010

SUBMITTED BY: William J. Miller

AFFILIATION: MaCT USA

EMAIL: mact-usa@att.net

TEXT PLACEMENT INFORMATION

IN THE P2030 OUTLINE DRAFT (MENTOR DOC#27-2010):

CLAUSE #: "[Click here and type clause #]"

CLAUSE HEADING: Categorized communications use cases

--OR--

AS A NEW CLAUSE TO THE P2030 OUTLINE:

PROPOSED CLAUSE #: "[Click here and type proposed clause #]"

PROPOSED CLAUSE HEADING: "[Click here and type proposed clause heading]"

PROPOSED TEXT

Include any references (full citation) and provide, if applicable: (a) copyright, trademark, patent, or registration information and (b) related information for figures.

The following is updated information from Subgroup 2 with regard to the Smart Grid Evaluation Criteria (SGEC) for Use Cases.

SMART GRID EVALUAITON CRITERIA (SGEC)

The following information provides an overview of the IEEE P2030 TF3 Use Cases Smart Grid Evaluation Criteria (SGEC). This information was initially used as a means to categorize use cases with respect to protocols and technologies that can be used for the Smart Grid. The process is generic and could have wider use for industry in general since it attempts to capture the understanding of experts in a particular domain and considerations for use in a particular application. The primary purpose is providing a structured guide for engineers and non-engineers to justify their decisions. This also servers to remove bias and vendor preference such that technology can be appropriately use. In the respect the technology chosen or approach taken can offer the best potential degree of success with respect to the knowledge that is known and any gaps or changes needed can be easily identified and remedied prior to implementation. This recursive process continues to be used as subsequent changes are made and over time the same degree of confidence can be maintained if not improved.

It has been subsequently used to evaluate the building of the Architecture and it has been further identified that it could be used as a basis of certification. The actions of evaluation of Use Cases, Architecture linkage, and eventual certification all make use of a recursive risk-based evaluation process. The SGEC makes use of three aspects to make a quantitative and/or qualitative evaluation of the requirements for a particular application. The TIER CLASS relates to the reliability and trustworthiness of the network with respect to services to be provided and the technology chosen must meet the requirements defined under each Tier Class.

TIER CLASS (1, 2, or 3) relates to trustworthiness for potential use based upon the LEVEL OF ASSURANCE, MINIMUM LATENCY, and IMPACT ON OPERATIONS.

- **TIER CLASSIFICATION**

  TIER 1 (CRITICAL) – This is data that are *critical* to the operation, control, and safe operation of the Smart Grid
  TIER 2 (IMPORTANT) - This is data that is *important* with limited control in operations of the Smart Grid
  TIER 3 (INFORMATIVE) – This is data that is *informative* but not necessarily important for operations of the Smart Grid

- TIER CLASS 1 for LOLO (Two Levels), LOW (One Levels) Latency applications, this TIER includes potential for Loss of Life and Damage to Assets and relates to control and safety relevant actions

- TIER CLASS 2 for MEDIUM Latency applications includes potential Damage to Assets and no risk to personnel

- TIER CLASS 3 for HIGH (Two Levels) and HIHI (Two Levels) Latency applications and offer No Damage to Assets and no risk to personnel.

– **LEVEL OF ASSURANCE (LoA) –** this refers to the level of certainty that a service can be provided to meet the Use Case requirements. This would include quantitative and qualitative use related to the direct or indirect impact of actions facilitated by the communications links.

If the Use Case meets has Metrics this is “quantitative” information
If there is no criteria then it may be inferred based upon “qualitative” aspects

The following are rules to determine a Level of Assurance for a particular link:

1) In the event that there are not metric stated then a qualitative assessment would be used.

2) If metrics are stated they shall provide a quantitative basis to assure the packet flow to facilitate the operation of a TIER CLASS.

3) If the quantitative metric is specified for use but it is different then the Level of Assurance which is stated for the metric then sufficient guarantee shall be provided to ensure that it meets the requirements for use at that TIER CLASS.

4) If no proof is provided then the application may require further guarantees that additional provisions can be provided without change to the latency metric.

5) In all cases the Impact on Operations (IoO) shall be assured to guarantee the expected operation for that TIER CLASS.

In practice and if available the packets shall be assigned a priority at the packet level based upon the following:

- Priority 1 = High
- Priority 2 = Moderate
- Priority 3 = Low

NOTE – High, Moderate, and Low are used from the FIPS 199 Impact on Operations matrix which is used as the basis of NISTIR 7648 Cyber Security Strategy for the Smart

NOTE – In the event that packet level classification is not available then a Service level classification can be used such that if Priority 1 traffic is used then it shall have a higher Class of Service (CoS) versus Priority 2 or 3 data traffic. This shall apply to Priority 2 traffic as well that it shall be assured over Priority 3 data traffic. This shall be a function of traffic flow and all related actions shall be handled at that Priority level**.**

The following section discusses the requirements to differentiate latency requirements such that if a primary service is provided that it can be assured that it can meet the TIER (CLASS) requirement. If the service is provided over higher TIER (CLASS) as a converged service that the primary service be given priority. This may make use of a Quality of Service (QoS) mechanism to provide this service. Quality of service (QoS) refers to resource reservation control mechanisms rather than the achieved service quality. QoS is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow with respect to its bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as Voice over IP, online games and IPTV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. The use of QoS is to mitigate problems with congestion that would significantly delay traffic. QoS may be a consideration to guarantee operation of converged services over a common link.

- **LATENCY AND ITS INTERPREATION**

Latency in a packet-switched network is measured either *one-way* (the time from the source sending a packet to the destination receiving it), or *round-trip* (the one-way latency from source to destination plus the one-way latency from the destination back to the source). Round-trip latency is more often quoted, because it can be measured from a single point. Note that round trip latency excludes the amount of time that a destination system spends processing the packet. Where precision is important, one-way latency for a link can be more strictly defined as the time from the *start* of packet *transmission* to the *start* of packet *reception*.

The time from the *start* of packet *reception* to the *end* of packet *reception* is measured separately and called "Serialization Delay". This definition of latency is independent of the link's throughput and the size of the packet, and is the absolute minimum delay possible with that link. However, a typical packet will be forwarded over many links via many gateways, each of which will not begin to forward the packet until it has been completely received. In such a network, the minimal latency is the sum of the minimum latency of each link, plus the transmission delay of each link except the final one, plus the forwarding latency of each gateway.

In practice, this minimal latency is further augmented by queuing and processing delays. Queuing delay occurs when a gateway receives multiple packets from different sources heading towards the same destination. Since typically only one packet can be transmitted at a time, some of the packets must queue for transmission, incurring additional delay.

Processing delays are incurred while a gateway determines what to do with a newly received packet. The combination of propagation, serialization, queuing, and processing delays often produces a complex and variable network latency profile. The Aggregate Latency shall meet the total of all latency expected between the sender and the receiver and may represent the accumulated latency of multiple latency actions.

For the purposes here-in the stated table relates the total aggregate latency:

- **LATENCY**

LOLO 2	**< 3 ms**
LOLO 1	**3 ms - 20 ms**
LOW	**20 ms <> 100 ms**
MEDIUM	**100 ms <> 1 sec**
HIGH 1	**1 sec <> 5 sec**
HIGH 2	**5 sec <> 1 min**
HIHI 1	**> 1 min to 1 hour**
HIHI 2	**> 1 hour to 1 day**

- **IMPACT ON OPERATIONS (IoO) (PRIORITY LEVEL)**

POTENTIAL IMPACT			
Security Objective	**1 = LOW**	**2 = MODERATE**	**3 = HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

FIPS PUB 199 – Standards for Security Categorization

The use of FIPS 199 plays an important pot in that to assure availability for operations, personnel, and assets are not put at risk. This is a starting point of what is a risk-based approach for the evolution of the system though out its life cycle. The Impact on Operation is related to the TIER CLASS. However, the degree may vary depending up the organizational requirements.

In FIPS 199, confidentiality, integrity, and availability are defined as Security Objectives:

- **Confidentiality:** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** "Ensuring timely and reliable access to and use of information…" A loss of availability is the disruption of access to or use of information or an information system.

For each type of data flow within a communications system or for the system itself, requires the assignment of s security category consisting of an impact level for the link or the particular system. This may relate to a general area of use and that area classified stated in the same manner. The security category consists of an impact level for each of the three security objectives of confidentiality, integrity, and availability. An impact level of low (L), moderate (M), or high (H) represents the impact on operations, assets, or individuals should there be a breach in security objective areas (i.e., for each security objective area, the impact level could be L, M, or H). The assignment of security categories must take place within the context can be used in the preliminary evaluation of use cases, architecture building, or even potential certification for use by an organization or may be in recognition of protection of critical infrastructure.

Impact levels are defined in FIPS 199 as follows:

The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on operations, assets, or individuals. A limited adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause degradation in operational capabilities to an extent and duration that the functional operations are not able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- Result in minor damage to assets, minor financial loss, or minor harm to individuals.

The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause a significant degradation in operational capability to an extent and duration that the functional operations is not able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- Result in significant damage to assets, significant financial loss, or significant harm to individuals, but not loss of life or serious life threatening injuries.

The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a *severe* or *catastrophic* adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause a severe degradation in or loss of operational capability to an extent and duration that the functional operation is not able to perform one or more of its primary functions;
- Result in major damage to assets, major financial loss, or severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Security Categorization Applied to the Communication

The security categorization drives the requirements for the communications for trustworthiness including resiliency, reliability, and fault tolerance. In establishing the appropriate security categorization with respect to the TIER CLASS it set a baseline for a target for a potential impact that can define the goal for the designer to use in selection of the appropriate components. It also provides a means for those defining the architecture for example to relate this information to others in a common and meaningful way.

The following summarizes the attributes of the SGEC in the form of a hierarchy:

TIER CLASSIFICATIONS HEIRARCHY

TIER CLASS 1
- HIGH LoA, PRIORITY 1
  - Control, or Safety relevant
  - Loss of life, or injury, and damage to assets
  - (1A) LOW, LOLO Latency (Relaying)
  - (1B) MEDIUM, HIGH (Distribution)

TIER CLASS 2
- MEDIUM LoA, PRIORITY 2
  - Control (ex. “Slow” SCADA), Important
  - Damage to assets
  - MEDIUM, HIGH 1 or 2 Latency

TIER CLASS 3
- LOW LoA, PRIORITY 3
  - Informative
  - No damage to assets
  - HIGH 1 or 2, HIHI 1 or 2 Latency

EXAMPLE OF USE OF SGEC

The following are examples related to the conditions for a particular service:

HAN	Important	Energy Management Systems (EMS) may require control actions.
AMI	Important	Informational but important, privacy concerns
DR	Important, Limited Control	Control of devices is required
EV	Important, Limited Control	Control of charging equipment is required, rate information and customer profiles are confidential.
WAN	Critical	Micro Grid, Substations, Generation, Distribution
INTERNET	Important, Informative	Privacy Concerns but multiple informational Services can be provided.

Evaluation of SG Protocols and their TIER Classification

Standard	Application	TIER CLASS
AMI-SEC System Security Requirements	Advanced metering infrastructure (AMI) and Smart Grid end-to-end security	2
ANSI C12.19/MC1219	Revenue metering information model	2
BACnet ANSI ASHRAE 135-2008/ISO 16484-5	Building automation	2
DNP3	Substation and feeder device automation	2
IEC 60870-6 / TASE.2	Inter-control center communications	1
IEC 61850	Substation automation and protection	1
IEC 61968/61970	Application level energy management system interfaces	1
IEC 62351 Parts 1-8	Information security for power system control operations	1
IEEE C37.118	Phasor measurement unit (PMU)communications	1
IEEE 1547	Physical and electrical interconnections between utility and distributed generation (DG)	1
IEEE 1686-2007	Security for intelligent electronic devices (IEDs)	1
NERC CIP 002-009	Cyber security standards for the bulk power system	1
Open Automated Demand Response (Open ADR)	Price responsive and direct load control	2
OpenHAN	Home Area Network device communication, measurement, and control	2, 3
ZigBee/HomePlug Smart Energy Profile	Home Area Network (HAN) Device Communications and Information Model	2, 3