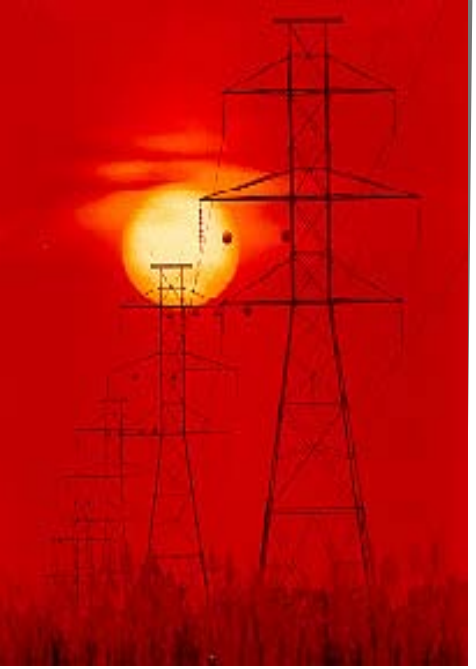


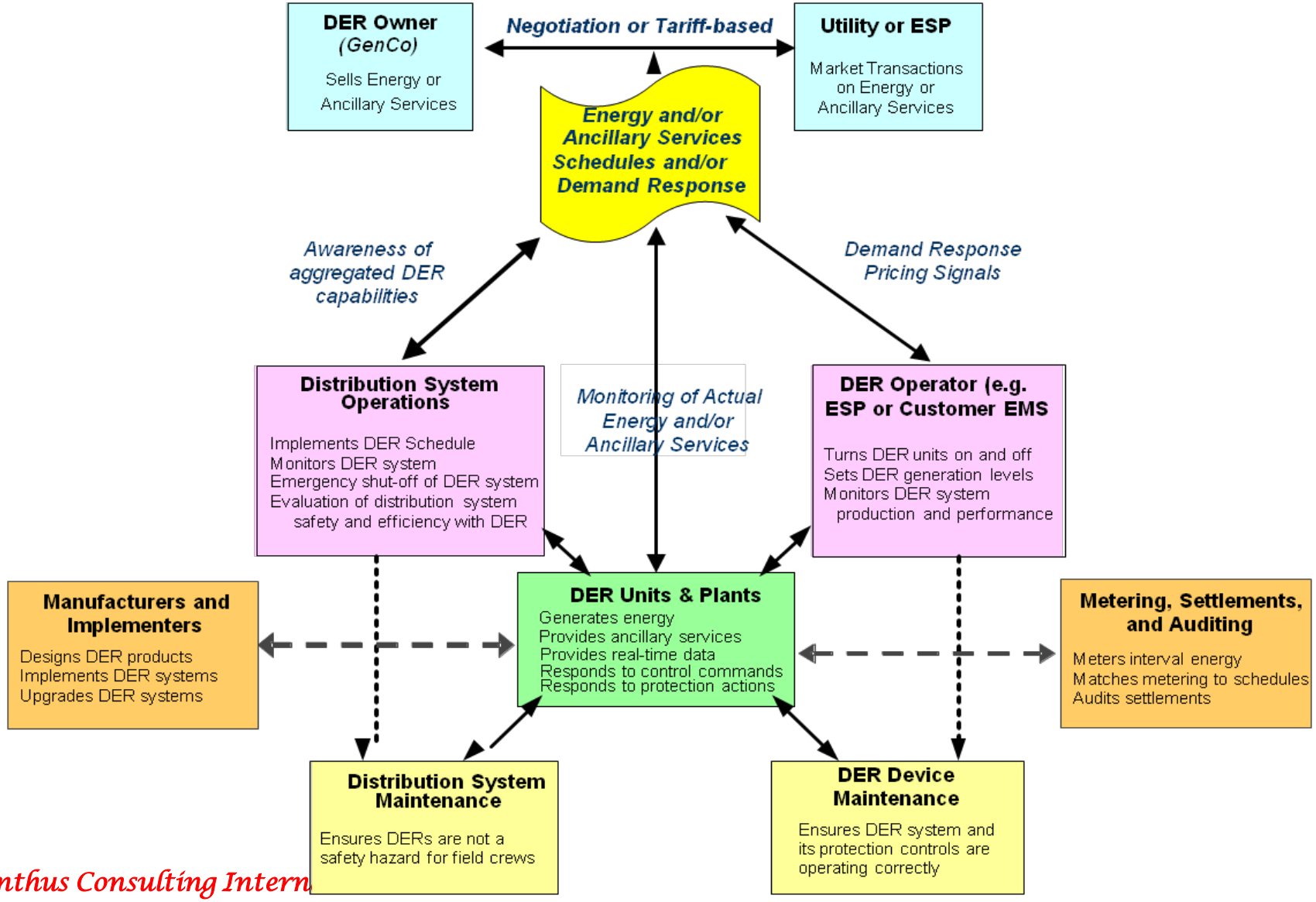
Virtual Power Plant of Distributed Energy Resources (DER) Systems Used for Distribution System Volt/Var Management

Frances Cleveland

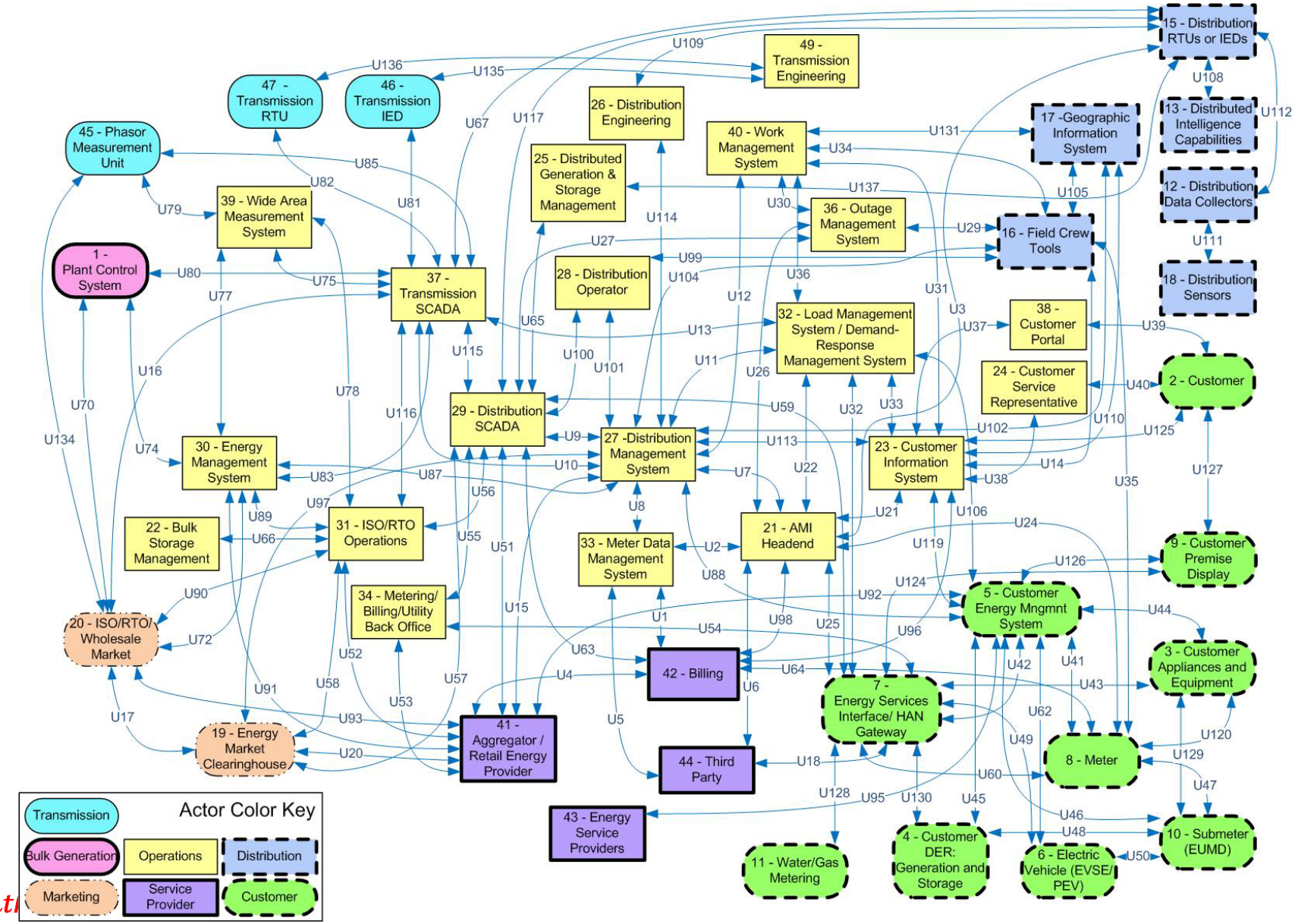
fcleve@xanthus-consulting.com

Xanthus
Consulting International

DER Stakeholders / Actors
(In California, 12,000 MW must be added by 2020)



NISTIR 7628 “Spaghetti” Diagram



Xanti

Policies, procedures, and technologies

Goals for Electric Sector Cybersecurity:

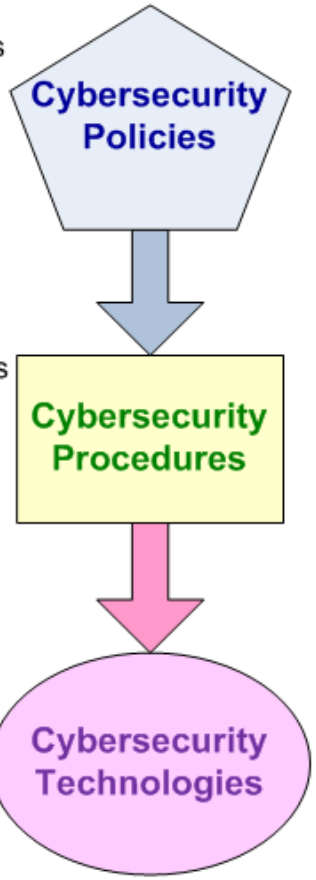
- ***Availability/Reliability*** of the Power System
- ***Integrity*** of Critical Information
- ***Confidentiality*** of Sensitive Data

IT Cybersecurity Tools

- Personnel screening policies
- Access control policies
- Defense in depth policies
- Privacy policies
- Risk assessment policies
- Cross Power-IT training

Power System Cybersecurity Tools

- Power system outage management
- Power system operations policies
- Power system planning policies
- Power system maintenance policies
- n-x contingency policies
- Safety policies
- Cross IT-Power training



- Risk assessment procedures
- Privacy management
- Password procedures
- Personnel security training
- IT audit logging procedures

- Power system operations procedures
- Outage management procedures
- Metering data handling procedures
- Testing procedures
- Maintenance procedures
- Power system audit logging procedures

- Role-based access control
- Password protection
- Information authentication
- Key management
- Firewalls
- Network management
- Security audit logs

- Protective relaying
- Phasor measurements
- Redundant equipment
- SCADA monitoring and control
- Contingency analysis
- Fault location, isolation, service restoration
- Power system alarm and event logs

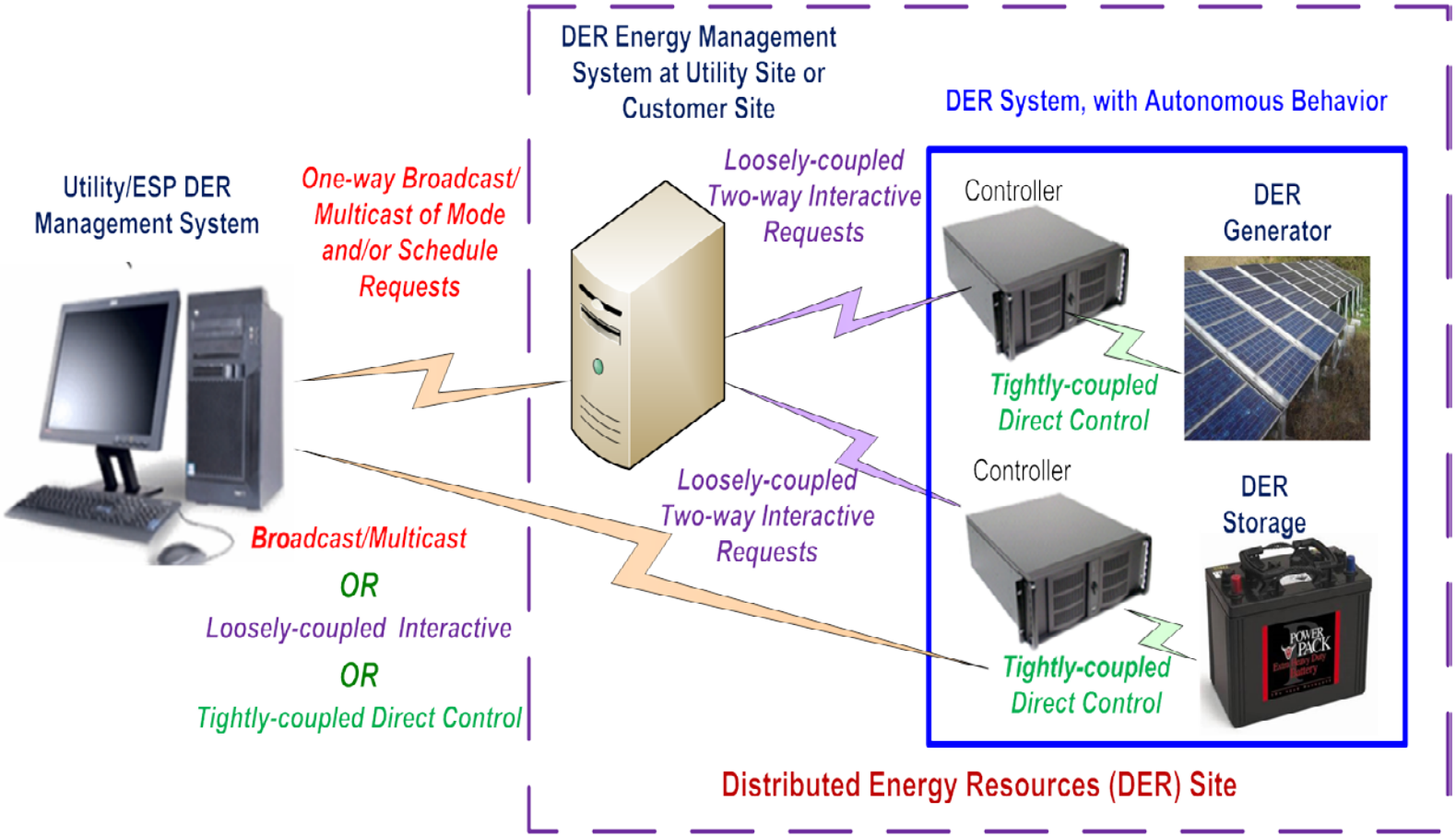
NISTIR 7628 Interface Categories to Identify Security Catalog Requirements (copied from NISTIR)

Logical Interface Categories		Logical Interfaces		Security			NIST Catalog of Security Requirements									
#	Interface Category Description	Interface	#	C	I	A	SG.PE	SG.SA	SG.CM	SG.SC	SG.MA	SG-IR	SG.SI	SG.AC	SG.AU	SG.RA
1	Interface between control systems and equipment with high availability requirements, and with compute and/or bandwidth constraints, for example: • Between distribution protective relays and protected equipment • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	Distribution protective relaying Trans. SCADA & substation IEDs	U108a U67	L	H	H	PE-2 PE-3 PE-4 PE-21 PE-22	SA-12 SA-13	CM-3 CM-4 CM-5 CM-6 CM-7 CM-9 CM-11	SC-2 SC-3 SC-5 SC-6 SC-7 SC-8 SC-11 SC-12 SC-14 SC-15 SC-20 SC-22	MA-2 MA-4 MA-10	IR-8 IR-9 IR-15 IR-18	SI-4 SI-7 SI-8 SI-9 SI-10 SI-11	AC-9 AC-10 AC-11 AC-12 AC-13 AC-14 AC-15 AC-24 AC-25	AU-2 AU-3 AU-4 AU-8 AU-16	RA-5

Use Case Narrative – Background

- A university campus has many buildings with photovoltaic arrays on their roofs.
- Each PV array has an associated controller located within the building.
- Some of these buildings also have
  - large battery systems,
  - while a couple of diesel generators are available for backup for some critical laboratories, but may be used occasionally for additional generation.
  - Many professors and students have Electric Vehicles that are available for energy management
- The university has a customer energy management system (CEMS) that manages these DER systems, with a contract to respond to an energy service provider's (ESP) signals for providing energy and ancillary services to the utility grid.
- These ancillary services include volt/var management.

Virtual Power Plant 3-Lever Configuration



DER Management: Interactions between Components

Scenario

- On a hot afternoon:
  - the utility determines that the transmission system needs more vars,
  - broadcasts a signal (using IEC 61850 over the DNP3 protocol over a cellphone wireless data channel, similar to Amazon's Kindle) to the ESP (and many other entities) to "go into volt/var mode 3".
- The ESP in turn sends this request to the CEMS,
  - including some additional information based on their contractual relationship with the university,
  - (using IEC 61850 over web services through a virtual private network over the Internet).
- The CEMS commands some of the building PV systems and one battery storage system to provide the volt/var mode 3,
  - while also commanding one diesel generator to run for an hour to help charge up the other battery systems
  - (using IEC 61850 over SEP 2.0 over the campus LAN).
- Responses from the controllers to these commands allow the CEMS to determine if additional steps need to be taken.

Use Case Steps (1-3)

Use Case Step							
#	**Triggering Event**	**Information Producer**	**Information Receiver**	**Description of Process/Activity**	**Information Exchanged**	**Interface, Category, & Standards**	**Security Focus**
1	Transmission system needs vars	Utility DMS	ESP	Request for volt/var mode 3	• Request for volt/var mode 3	IEC 61850 DNP3 Cellphone systems	**Authentication** **Integrity** **Provenance** **Non-repudiation**
2	ESP receives request	ESP	CEMS	Request for volt/var mode 3	• Request for volt/var mode 3 • Maintain same energy output • Ensure battery storage is full by 6 pm	IEC 61850 Web services Internet	**Authentication** **Integrity** **Confidentiality** **Non-repudiation** **Timeliness** **Guaranteed delivery** **Time accuracy** **Logging**
3	CEMS receives request	CEMS	Some PV systems	Command for volt/var mode 3	• Command to go into volt/var mode 3 within 5 minutes	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Confidentiality** **Availability** **Non-repudiation** **Time accuracy** **Alarm reporting** **Logging**

Use Case Steps (4-6)

Use Case Step							
#	**Triggering Event**	**Information Producer**	**Information Receiver**	**Description of Process/Activity**	**Information Exchanged**	**Interface, Category, & Standards**	**Security Focus**
4	CEMS receives request	CEMS	One battery system and some EVs	Command for volt/var mode 3	• Command to go into volt/var mode 3 within 5 minutes	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Confidentiality** **Availability** **Non-repudiation** **Time accuracy** **Alarm reporting** **Logging**
5	CEMS receives request	CEMS	One diesel generator	Command to turn on and provide x kW of energy for 2 hours	• Command to turn on and generate x kW	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Confidentiality** **Availability** **Non-repudiation** **Time accuracy** **Alarm reporting** **Logging**
6	Upon mode change	PV systems	CEMS	Acknowledging going into volt/var mode 3	• Ack	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Alarm reporting** **Logging**

Use Case Steps (7-8)

Use Case Step							
#	**Triggering Event**	**Information Producer**	**Information Receiver**	**Description of Process/Activity**	**Information Exchanged**	**Interface, Category, & Standards**	**Security Focus**
7	Upon mode change	Battery systems	CEMS	Error going into volt/var mode 3	• Error message	IEC 61850 SEP 2.0 LAN	**Authentication** **Integrity** **Alarm reporting** **Logging**
8	Continuously	Monitoring devices at the connection between the campus and the grid	CEMS	Using report by exception, monitor the energy, vars, and other electrical parameters	• Measurements of watts, vars, voltage, frequency, etc.	IEC 61850 Web services LAN	**Authentication** **Availability** **Alarm reporting** **Logging**