New Smart Grid Interfaces Categories Assessment (Discussion DRAFT)

November 9, 2018

Information cybersecurity is primarily associated with information exchange interactions[1] between entities[2] and is a critical aspect of power system operations and security. The impacts of cybersecurity breaches—whether deliberate or inadvertent—may affect both physical and cyber operations of the grid.

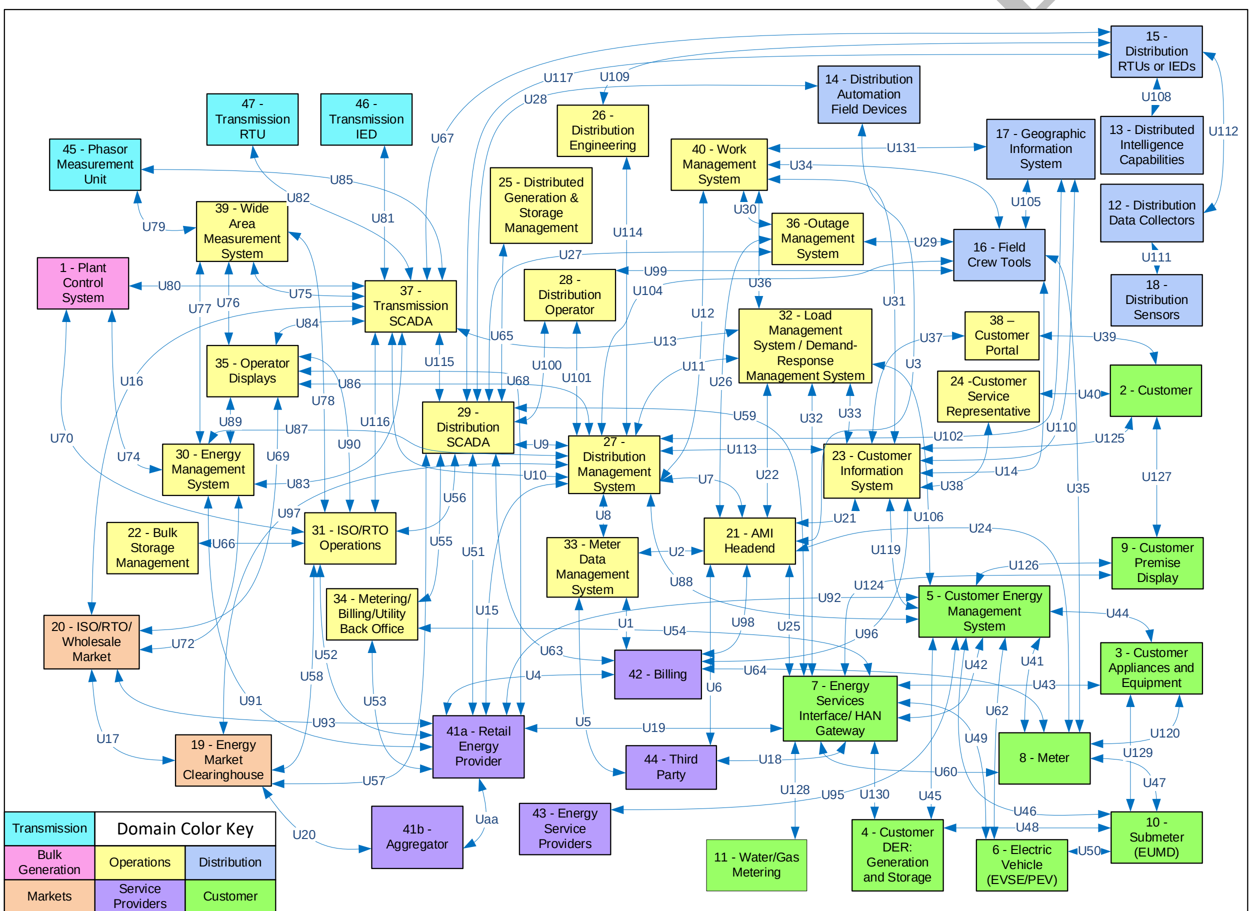

Figure 1- Logical Interface Reference Model "Spaghetti Diagram" from NISTIR 7628[3]

Identifying the entities[2] involved with information exchanges in power system operations is the first step towards understanding cybersecurity issues for the grid. To facilitate this understanding, the 2014 NIST publication *Guidelines for Smart Grid Cybersecurity*[3] included a composite diagram of grid entities that exchange information within and across each of the seven

---

[1] Although information cybersecurity also addresses stored data, NIST's focus is on interoperability and the security of associated information exchanges.

[2] Entities could be users, systems, devices, network or communications nodes, etcetera.

[3] NISTIR 7628 Rev 1, available here: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

smart grid conceptual model domains.[4] By mapping these information exchanges—called logical interfaces—to the composite diagram of grid entities, the NIST Guidelines publication described where, at a high level, the smart grid would need to provide security (see **Figure 1**).

Yet knowing *where* security is needed is of limited value, as locational information alone does not provide details on the requirements of *what* needs to be done to enhance security. To understand the latter, the NIST *Guidelines* document (NISTIR 7628) defined a set of logical interface categories (LICs) based on attributes that could affect grid cybersecurity requirements. Because many of the individual logical interfaces are similar in their security-related characteristics, grouping interfaces into LICs with similar characteristics is a means to simplify the identification of appropriate security requirements. In that way, the hundreds of individual interfaces drawn in **Figure 1** can be grouped into 22 representative categories, or LICs, from which broadly applicable cybersecurity requirements can be derived (see **Table 1** at the end of this document).

New System Interfaces

The modern grid will be more heavily dependent on information exchange than the legacy grid. As distributed energy resources (DERs) and other innovations are used more extensively across the grid, the set of entities involved with information exchanges in power system operations will expand and new communications interfaces will evolve. It is useful, therefore, to explore how portions of the **Figure 1** logical interface diagram—which contains high-level representations of current power system operations domains—can be expanded to provide more detailed cybersecurity requirements for emerging interfaces.

To explore the cybersecurity implications introducing new technologies and architectures to the grid, we updated the NISTIR 7628 logical interface diagram (**Figure 1**) to include examples of the new equipment and information exchanges that could be expected for future high-DER penetration grids. A representation of the new power system entities and logical interfaces for a high-DER architecture is shown in **Figure 2**, where Uxx labeled blue interface arrows are the same as those originally shown in NISTIR 7628 (**Figure 1**), and Dxx labeled red interface arrows are new to the high-DER example.

From this example (**Figure 2**), we understand that a modernized grid would likely have to accommodate at least three new types of communications interfaces, including:

> **New interfaces for new entities:** As new systems are introduced to the grid the number of communications interfaces and pathways will increase dramatically. In this example, extensive penetration of distributed resources requires introduction of a Distributed Energy Resources Management System (DERMS) into the grid operations domain. This DERMS would likely have different data and communications requirements than legacy systems, and new communications linkages are required throughout the rest of the system.

[4] See companion pre-read document, *Update of the NIST Smart Grid Conceptual Model: Discussion DRAFT*, available here: https://www.nist.gov/document/draftsmartgridconceptualmodelupdatev2pdf

New interfaces between subsystems: As the physical capabilities of grid-connected systems advance, logical interface requirements between equipment subsystems will evolve. In this example, the customer sited DER asset, electric vehicle asset, and the utility-scale DER or cogeneration asset have been split to reflect the different logical interface requirements between asset controllers and the equipment that is connected to the grid and physically consuming or supplying electrons.

New interfaces for legacy systems: As new capabilities are introduced to conventional grid assets, information will have to be exchanged with and between legacy systems. In this example, both the utility-scale DER or cogeneration asset and the facility energy management system interface directly with the utility supervisory control and data acquisition (SCADA) system via a new logical interface.

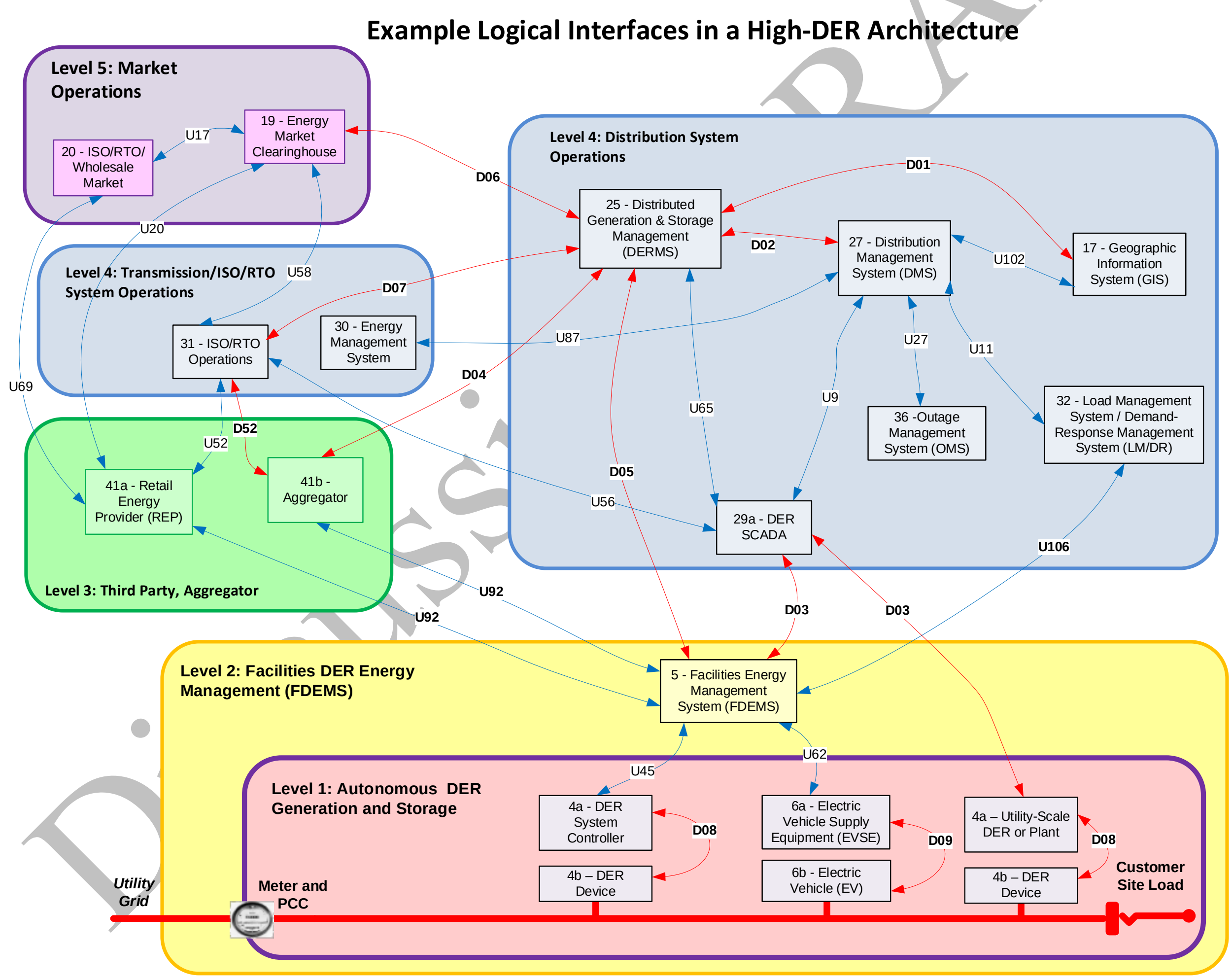

Figure 2 - Example Logical Interfaces in a High-DER Architecture. Note that to ease examination, this figure includes only those entities requiring new logical interfaces for this high-DER example.

Assessing Security Requirements of New Interfaces

New or changed logical interfaces may require new cybersecurity precautions. The high-DER example in **Figure 2** identifies nearly a dozen new interfaces, and the changing characteristics of the system itself may alter the communications and cybersecurity requirements for previously established interfaces.

To assess the cybersecurity requirements for the high-DER example, the new and updated interfaces shown in **Figure 2** were evaluated against the LICs of the earlier NIST *Guidelines* document. Each of the high-DER example interfaces could be mapped to an existing LIC, meaning the cybersecurity requirements for protecting communications interfaces within this new architecture are not substantially different than those described in the original NISTIR 7628 *Guidelines*. This mapping is shown graphically in **Figure 3**. The complete evaluation of each information exchange is provided in **Table 2** at the end of this document.

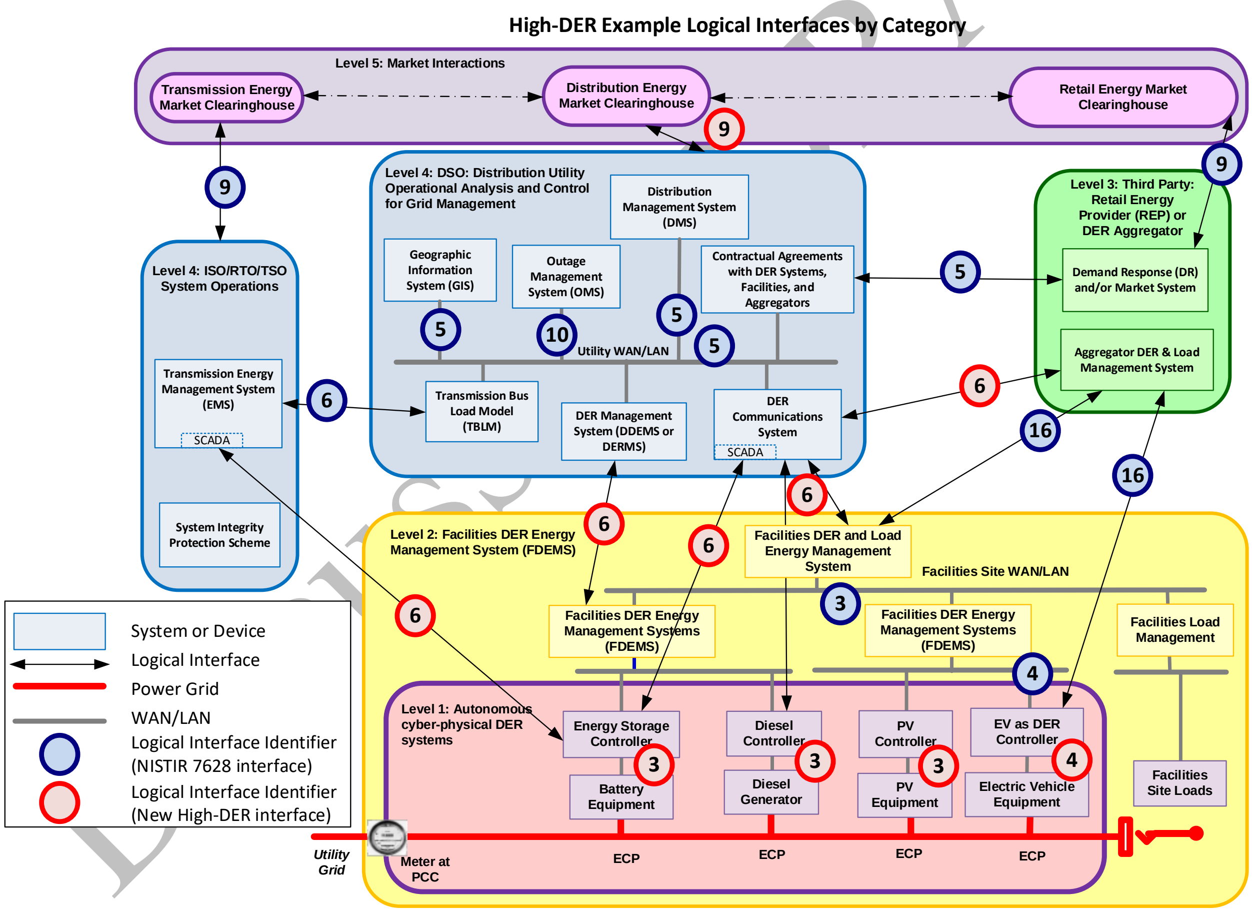

Figure 3 - Logical Interface Categories (LICs) for the High-DER Example

Conclusion

The smart grid brings new information technology capabilities to electric infrastructure, and as this occurs the number of communications interfaces will grow substantially. Even so, the fundamental cybersecurity requirements for each interface are likely to be consistent with known requirements, as described by existing LICs. Mapping new interfaces to existing LICs should facilitate the effective application of category-driven protection schemes to the evolving grid.

Appendix A – Table 1: Logical Interface Categories from NISTIR 7628

Table 1 - Logical Interface Categories from NISTIR 7628

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • 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 • (NOTE: LICs 1-4 are separate due to the architecturally significant differences between the availability and constraints, which impact mitigations such as encryption.)	U67, U79, U81, U82, U85, U102, U117, U137
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	U67, U79, U81, U82, U85, U102, U117, U137
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	U67, U79, U81, U82, U85, U102, U117, U137
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	U67, U79, U81, U82, U85, U102, U117, U137
5. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	U7, U9, U11, U13, U27, U65, U67, U83, U87, U115, Ux2
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U10, U56, U66, U70, U74, U80, U83, U87, U89, U90, U115, U116, Ux3
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U2, U4, U21, U22, U26, U31, U53, U96, U98, U110, Ux4
8. Interface between back office systems not under common management authority, for example: • Between a third party billing system and a utility meter data management system	U1, U4, U6, U15, U52, U53, Ux4, Ux6

Logical Interface Category	Logical Interfaces
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U4, U9, U17, U20, U51, U52, U53, U55, U57, U58, U72, U90, U93, U97
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U12, U30, U33, U36, U52, U59, U75, U91, U106, U113, U114, U131
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	U111
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	U108, U112
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U2, U6, U7, U8, U21, U24, U25, U32, U95, U119, U130
14. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	U2, U6, U7, U8, U21, U24, U25, U32, U95, U119, U130
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U42, U43, U44, U45, U49, U62, U120, U124, U126, U127
16. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U18, U37, U38, U39, U40, U42, U88, U92, U125
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	U14, U29, U34, U35, U99, U101, U104, U105
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U25, U41, U46, U47, U48, U50, U54, U60, U95, U128, U129, Ux5

Logical Interface Category	Logical Interfaces
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	U77, U78
20. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	U109, U114, U135, U136, U137
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	U5
22. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	U133 (includes interfaces to actors 17-Geographic Information System, 12 – Distribution Data Collector, 38 – Customer Portal, 24 – Customer Service Representative, 23 – Customer Information System, 21 – AMI Headend, 42 – Billing, 44 – Third Party, 43 – Energy Service Provider, 41 – Aggregator / Retail Energy Provider, 19 – Energy Market Clearinghouse, 34 – Metering / Billing / Utility Back Office)

Appendix B – Table 2: Types of Information Exchange Between Entities in the High-DER Example

Table 2 - Types of Information Exchange Between Entities in the High-DER Example

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
Level 1: Autonomous Cyber-Physical Systems							
D08	4a: DER Controller of DER Devices (single or in aggregate)	4b: DER Device or Unit (e.g. PV, Storage, Diesel, Turbine)	LIC #3: Interface between control systems and equipment with high availability, without compute nor bandwidth constraints	Communications between DER components and their DER controller typically uses ModBus. Cybersecurity protection of this protocol is not feasible, so physical security, such as locked rooms or cabinets should be used. If necessary, a VPN can be used to secure the transport of ModBus messages.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks	Responses to attacks may depend on the type and criticality of the DER, but most likely will require aborting communications. The DER may or may not continue to operate.	The controller and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D08	4a: Utility-Scale DER System or Plant (e.g. large storage system)	4b: DER Device or Unit (e.g. PV, Storage, Diesel, Turbine)	LIC #3: Interface between control systems and equipment with high availability, without compute nor bandwidth constraints	Communications between DER components and their DER controller typically uses ModBus. Cybersecurity of this protocol is not feasible, so physical security, such as locked rooms or cabinets should be used. If necessary, a VPN can be used to secure the transport of ModBus messages.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks	Responses to attacks may depend on the type and criticality of the DER, but most likely will require aborting communications. The DER may or may not continue to operate.	The controller and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D09	6a: EVSE Charging Stations	6b: Electric Vehicles	LIC #4: Interface between control systems and equipment without high availability, without compute nor bandwidth constraints	Most communications between EV Service Elements (charging stations) and EVs use the ISO/IEC 15118 standard, while the actual charging standards vary among different countries and for different levels (Levels 1-3, fast charging) and types of charging (AC vs. DC charging). Cybersecurity for these standards are partially developed.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks	Responses to attacks would most likely require aborting communications. The EVSE may or may not continue to charge EVs, using local default charging functions.	The EVSE and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
Level 2: Facilities DER Energy Management Systems (FDEMS)							
U45	#5: Facility EMS (DER and Load) or Plant EMS	4a: DER Controller of DER Devices (single or in aggregate)	LIC #3: Interface between control systems and equipment with high availability, without compute nor bandwidth constraints	Communications between DERs and the Energy Management System within their facility could use many different protocols, including IEC 61850, IEEE 2030.5, and Modbus. Cybersecurity would be the responsibility of the facility, and could range from none to very sophisticated, depending upon the facility requirements.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U62	#5: EV Fleet EMS	6a: EVSE Charging Stations	LIC #4: Interface between control systems and equipment without high availability, without compute nor bandwidth constraints	Communications between EVSEs and the EV fleet Energy Management System could use many different protocols including IEC 61850, IEEE 2030.5, and OCPP. Cybersecurity would be the responsibility of the facility, and could range from none to very sophisticated, depending upon the facility requirements.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
Level 3: Third Party, Aggregators							
U92	#5: FDEMS	#41a: Retail Energy Provider (REP)	LIC#16: Interface between external systems and the customer site	Communications would most likely use the Internet with proprietary protocols established by the Retail Energy Provider. Cybersecurity would most likely be minimal or use traditional IT techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U92	#5: FDEMS	#41b: Aggregator	LIC#16: Interface between external systems and the customer site	Communications would most likely use the Internet with proprietary protocols established by the Retail Energy Provider. Cybersecurity would most likely be minimal or use traditional IT techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U69	#41a: Retail Energy Provider (REP)	#20: Wholesale Market	LIC#9. Interface with B2B connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary protocols established by the Retail Energy Provider. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U20	#41a: Retail Energy Provider (REP)	#19: Energy Market Clearing-house	LIC#9: Interface with B2B connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
D52	41b: Aggregator	#31: ISO/RTO Operations	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D04	41b: Aggregator	#25: DERMS	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
Level 4: Utility Operations							
D03	#5: FDEMS	#29a: DER SCADA	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
D03	#4a: Utility Scale DER or Plant	#29a: DER SCADA	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D05	#5: FDEMS	#25: DERMS	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U106	#5: FDEMS	#32: Load Manageme nt System	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U56	#29a: DER SCADA	#31: ISO/RTO Operations	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U65	#29a: DER SCADA	#25: DERMS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter (ESP). Cybersecurity authentication and authorization would reflect the organization's policies.	ESP techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the ESP, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules, including any ESP routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.
U09	#29a: DER SCADA	#27: DMS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter (ESP). Cybersecurity authentication and authorization would reflect the organization's policies.	ESP techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the ESP, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules, including any ESP routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
D07	#31: ISO/RTO Operations	#25: DERMS	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U27	#27: DMS	#36: OMS	LIC#10: Interface between control systems and non-control/corporate systems	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U11	#32: Load Manageme nt	#27: DMS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter (ESP). Cybersecurity authentication and authorization would reflect the organization's policies.	ESP techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the ESP, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules, including any ESP routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U102	#27: DMS	#17: GIS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter (ESP). Cybersecurity authentication and authorization would reflect the organization's policies.	ESP techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the ESP, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules, including any ESP routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.
D02	#27: DMS	#25: DERMS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter (ESP). Cybersecurity authentication and authorization would reflect the organization's policies.	ESP techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the ESP, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules, including any ESP routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.
D01	#25: DERMS	#17: GIS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter (ESP). Cybersecurity authentication and authorization would reflect the organization's policies.	ESP techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the ESP, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules, including any ESP routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U87	#27: DMS	#30: EMS	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
Level 5: Market Operations							
U58	#31: ISO/RTO Operations	#19: Energy Market Clearinghouse	LIC#9: Interface with B2B connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U17	#20: Wholesale Market	#19: Energy Market Clearinghouse	LIC#9: Interface with B2B connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
D06	#19: Energy Market Clearinghouse	#25: DERMS	LIC#9: Interface with B2B connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, systems would require their removal.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.