



NIST Smart Grid Framework

*Harnessing value; securing
interfaces*

Avi Gopstein

Smart Grid Program Manager
February 24, 2021

1. NISTIR 7628 Logical Interfaces

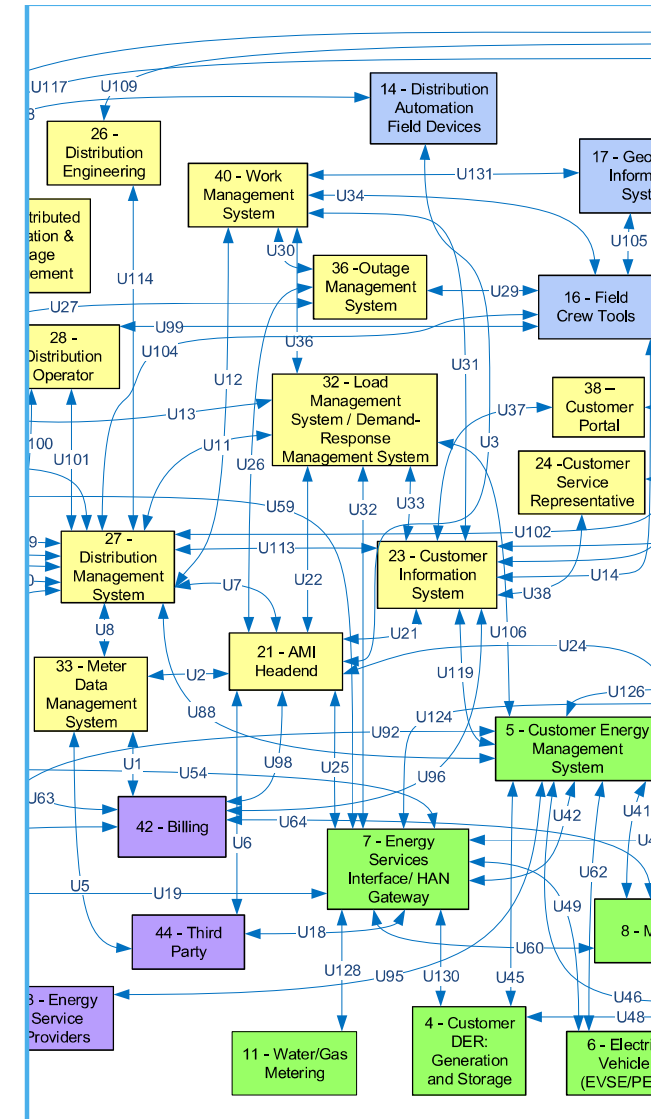
In 2014 NIST defined a set of 21 logical interface categories (LICs) based on smart grid communications

2. High-DER Scenario

In the Interoperability Framework V4 we reexamined the required communications for the High-DER scenario

3. Categories and Next steps

New communications interfaces in the High-DER scenario were mapped to the LICs from NISTIR 7628



A. Empowered consumers

Customers at the heart of many value propositions

B. Technology adoption & new applications

New technologies change how we interact with the system

C. Market access

Interoperability reduces barriers to market entry

D. Transaction costs

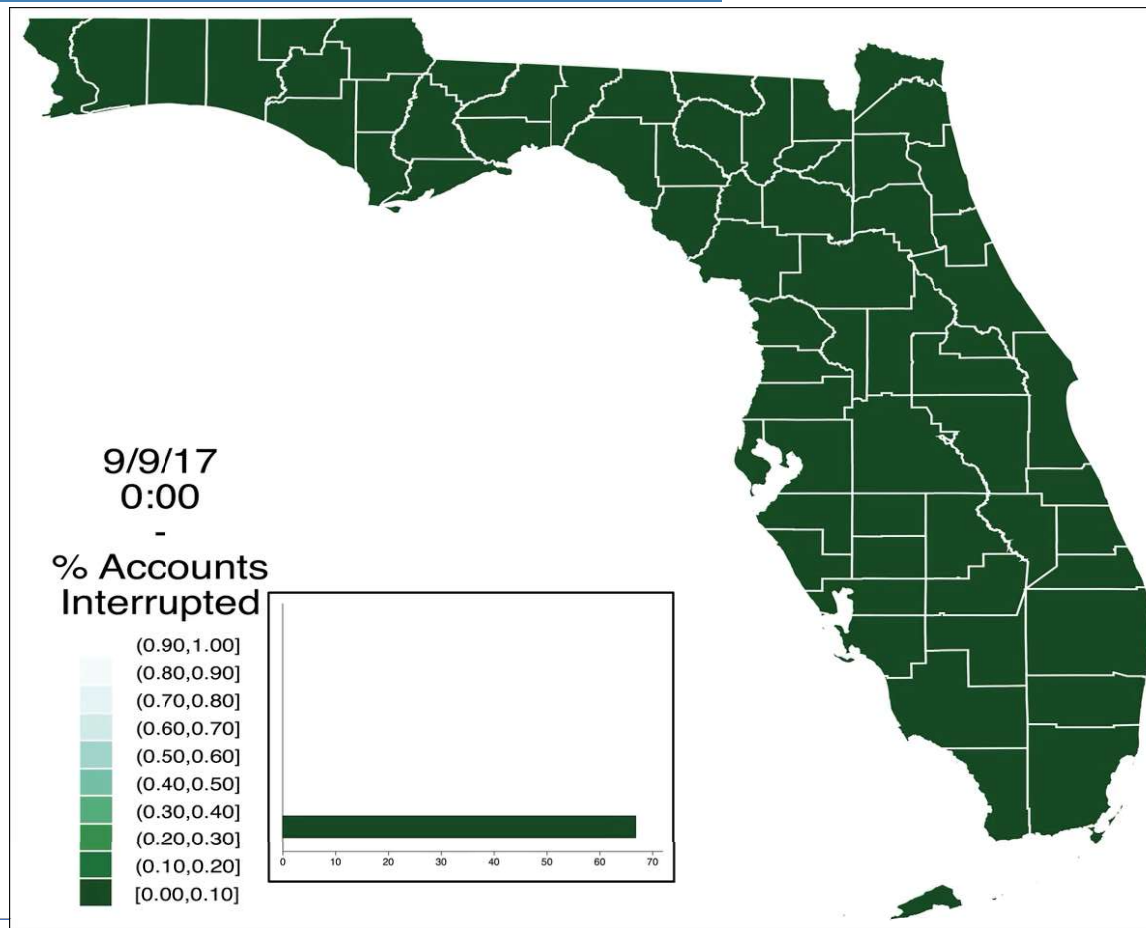
Full interoperability eliminates transaction costs

E. Resilience

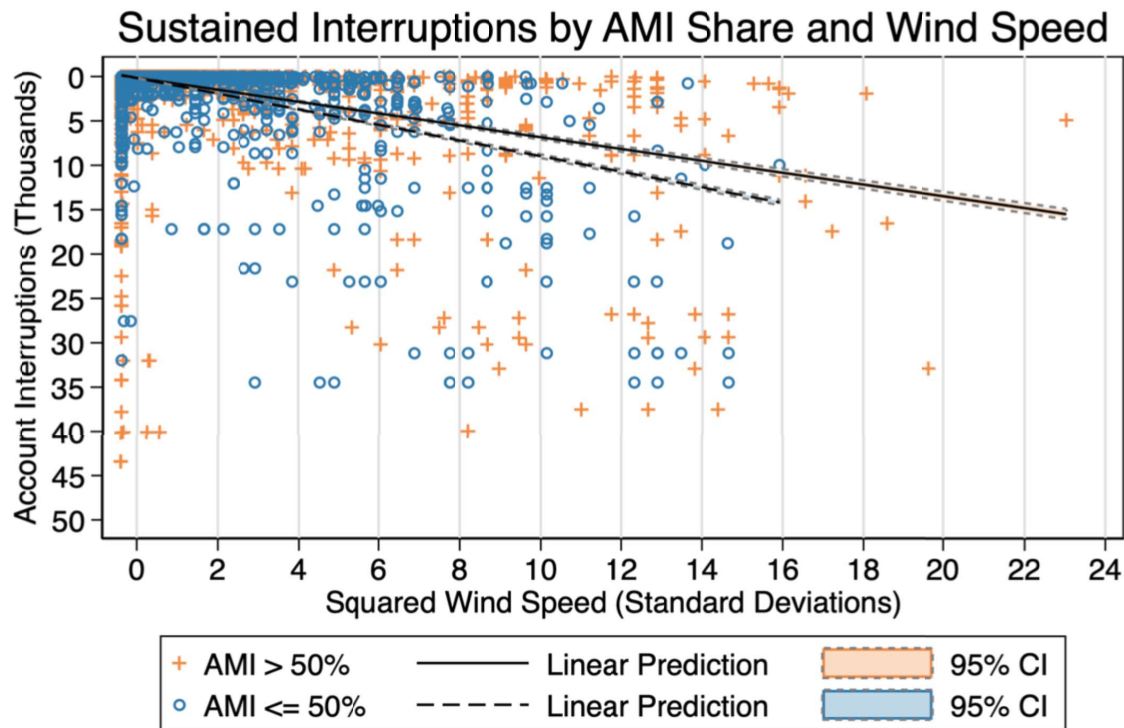
Interoperability can improve system operations under stress



Resilience (Hurricane Irma)



<https://doi.org/10.6028/NIST.TN.2137>



For clarity of exposition, 14 observations with greater than 50 000 interruptions are not plotted. Lines of best fit are estimated using all data points including those not plotted.

<https://doi.org/10.6028/NIST.TN.2137>

Sustained Outages

When comparing counties with high and low AMI penetration, it appears sustained account outages increase more quickly for those counties with low AMI penetration

TABLE II
ALTERNATIVE REGRESSION MODEL SPECIFICATIONS (COUNTY-UTILITY)

Dependent Variable: Δ Interruptions	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Squared Wind Speed (W^2)	1.588*** (0.0000)	1.475*** (0.0000)	1.542*** (0.0000)	1.532*** (0.0000)	1.591*** (0.0000)	1.613*** (0.0000)	1.621*** (0.0000)	1.623*** (0.0000)	1.647*** (0.0000)	1.499*** (0.0000)
$W^2 \times$ AMI-Share	0.905* (0.0120)				0.904 (0.0721)	0.920* (0.0494)	0.905* (0.0190)	0.863** (0.0015)	0.888* (0.0232)	1.082 (0.4796)
$W^2 \times$ Population Density		1.011 (0.0588)			0.999 (0.9493)			0.991 (0.1762)		
$W^2 \times$ Median Household Income			0.956** (0.0025)			0.964** (0.0037)			0.921* (0.0211)	
$W^2 \times$ New Building Share (Since 2000)				0.900 (0.5745)			0.911 (0.6218)			1.405* (0.0473)
$W^2 \times$ Population Density \times AMI-Share								1.037 (0.3914)		
$W^2 \times$ Median Household Income \times AMI-Share									1.069 (0.1826)	
$W^2 \times$ New Building Share (Since 2000) \times AMI-Share										0.395* (0.0486)
Observations	144,065	144,065	144,065	144,065	144,065	144,065	144,065	144,065	144,065	144,065
BIC	4.744e+07	4.764e+07	4.747e+07	4.768e+07	4.744e+07	4.729e+07	4.743e+07	4.739e+07	4.726e+07	4.728e+07

Exponentiated coefficients. *p*-values in parentheses. * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

<https://doi.org/10.6028/NIST.TN.2137>

10% Fewer Outages

Counties with full AMI penetration should experience 9.5% fewer sustained outages for each standard deviation increase in wind speed

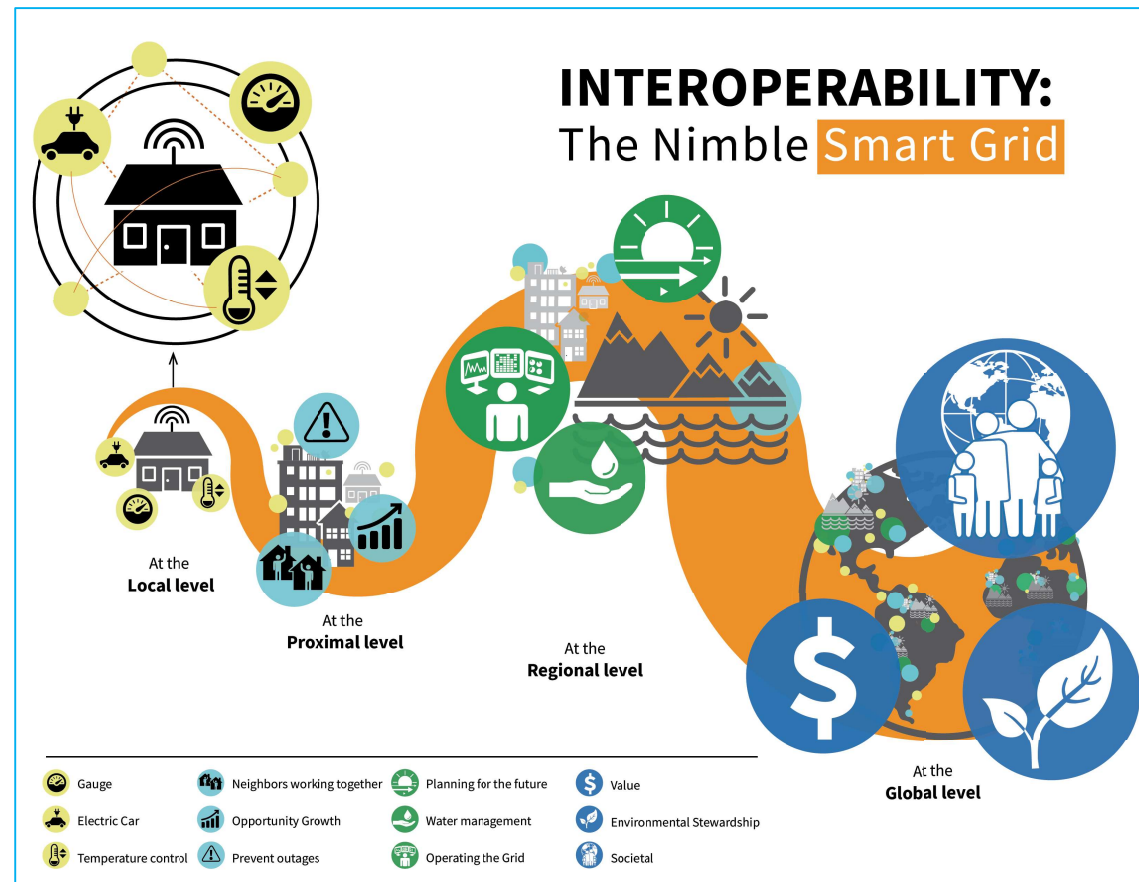
Interoperability & physical function

Actions have a physical context

- Where in the system is the action performed?
- What action is performed?
- How does that action interact with others?

Communications must accommodate that context

- Is the goal local, proximal, regional, or other?
- Can the action be performed without violating physical or economic constraints?



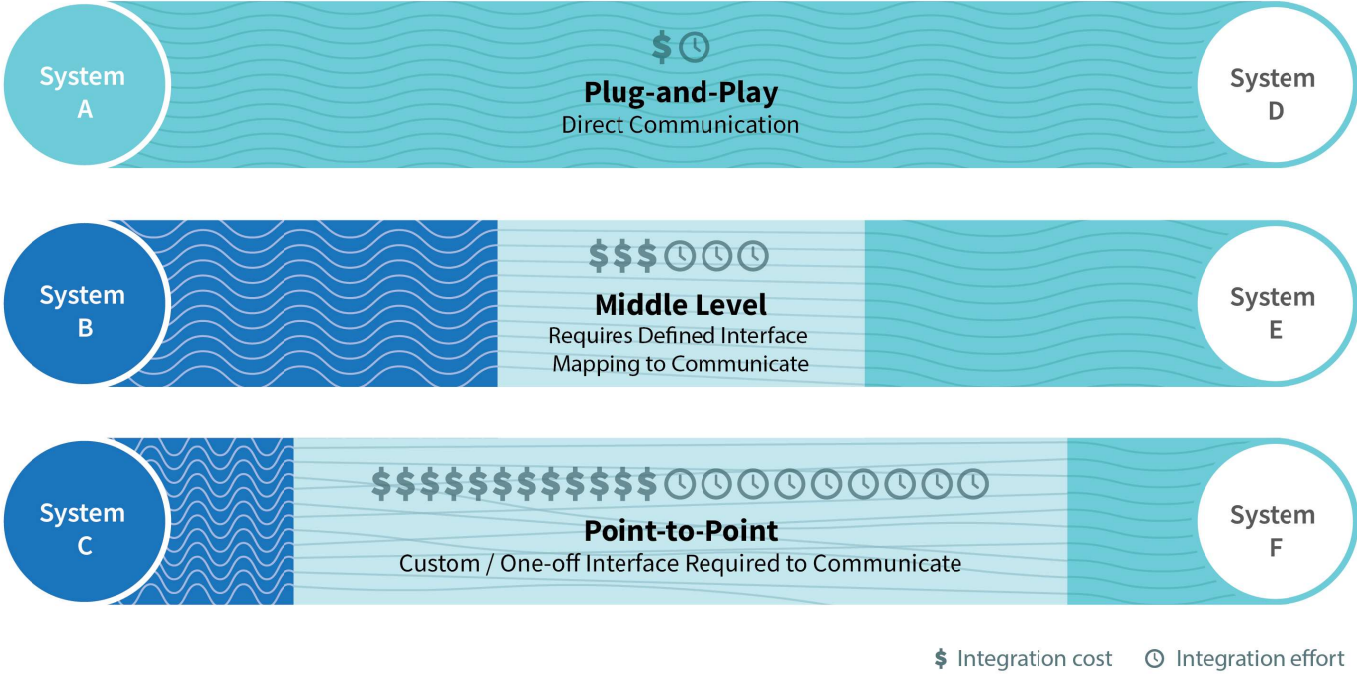
The Interoperability Feature Space

Hardware Functional Requirements

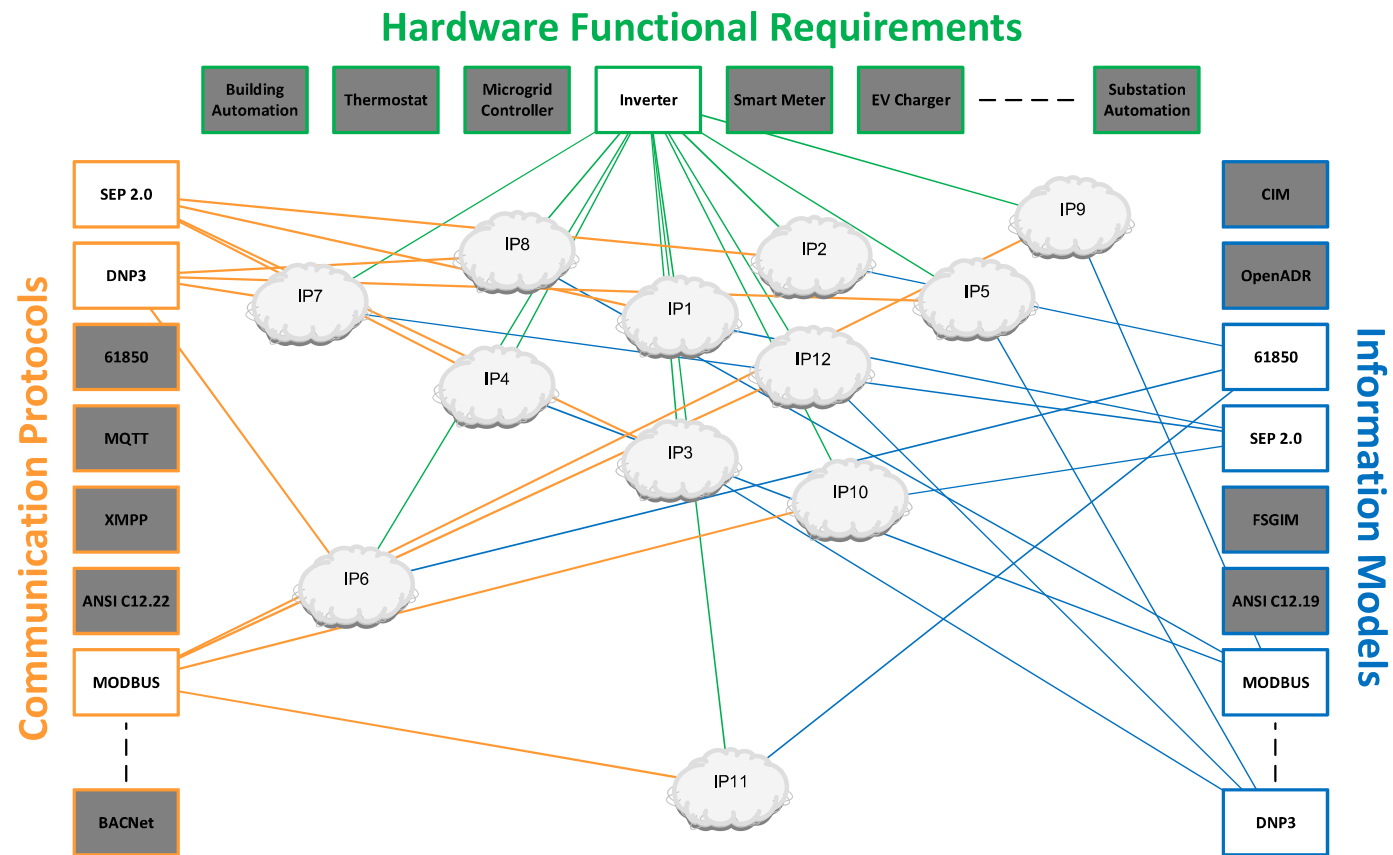


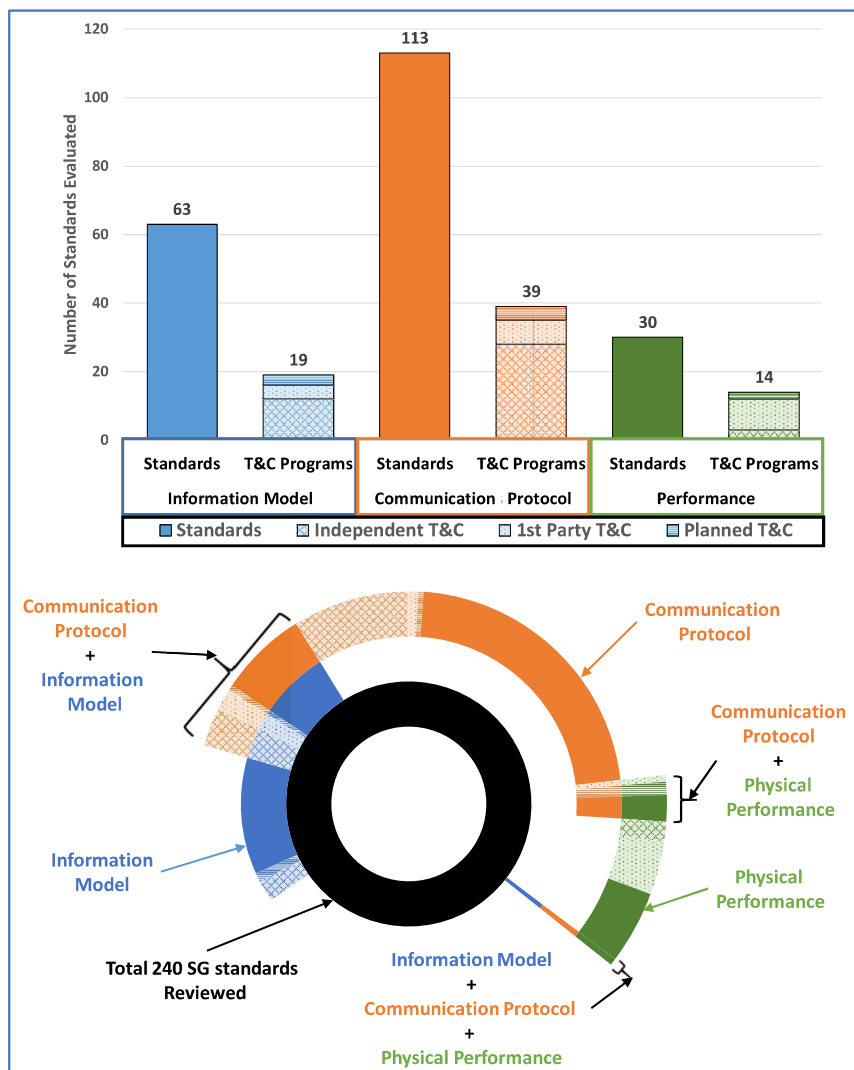
The Importance of Standardization

LEVELS OF INTEROPERABILITY



Interoperability Profile: IEEE 1547 Case Study





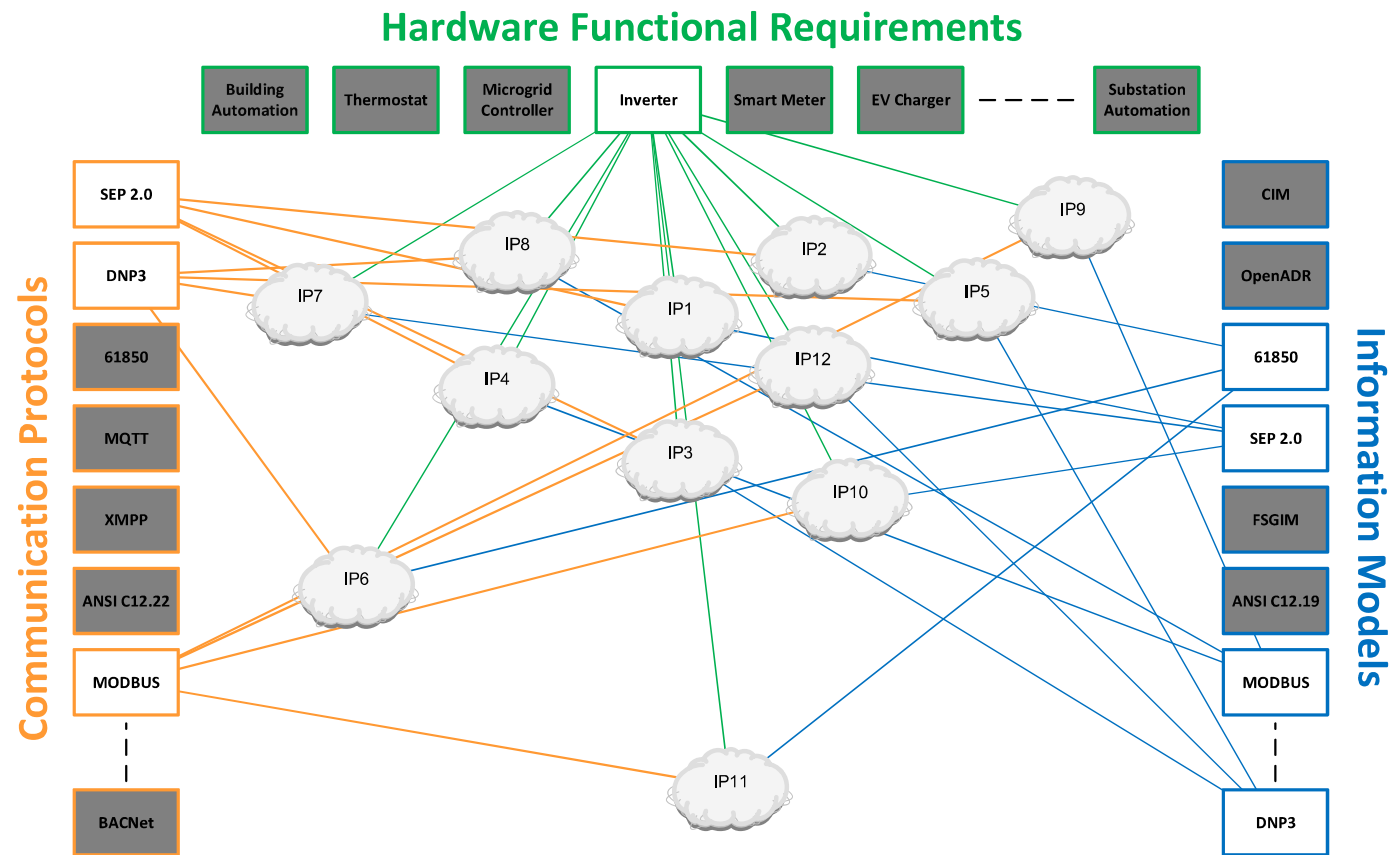
Sources: NIST Draft Interoperability Framework v4 and NIST Tech Note 2042

21% T&C Availability

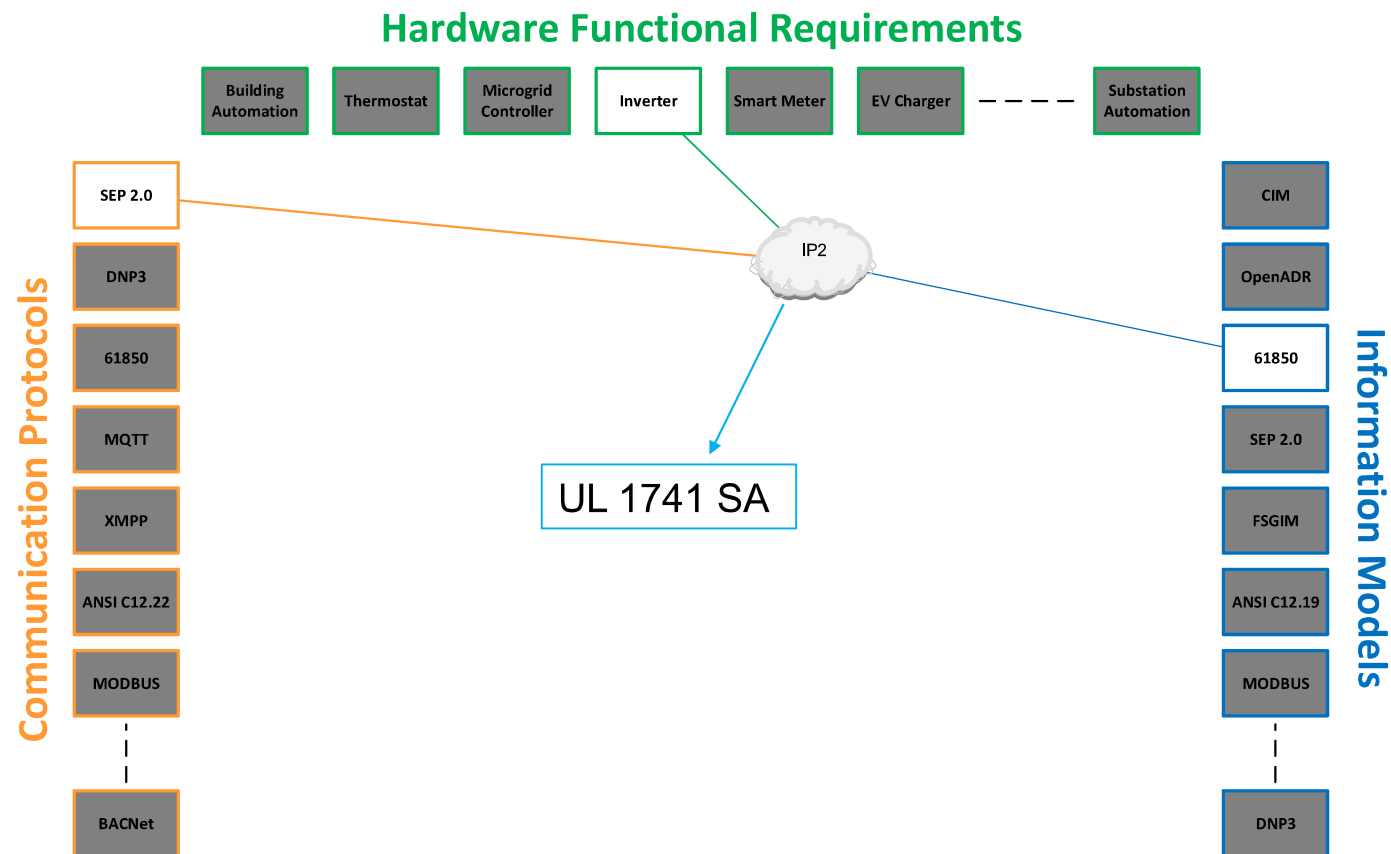
Independent testing & certification (T&C) is available for about 1 in 5 standards

Most T&C is available for Communications Protocols, but even that is only 27%

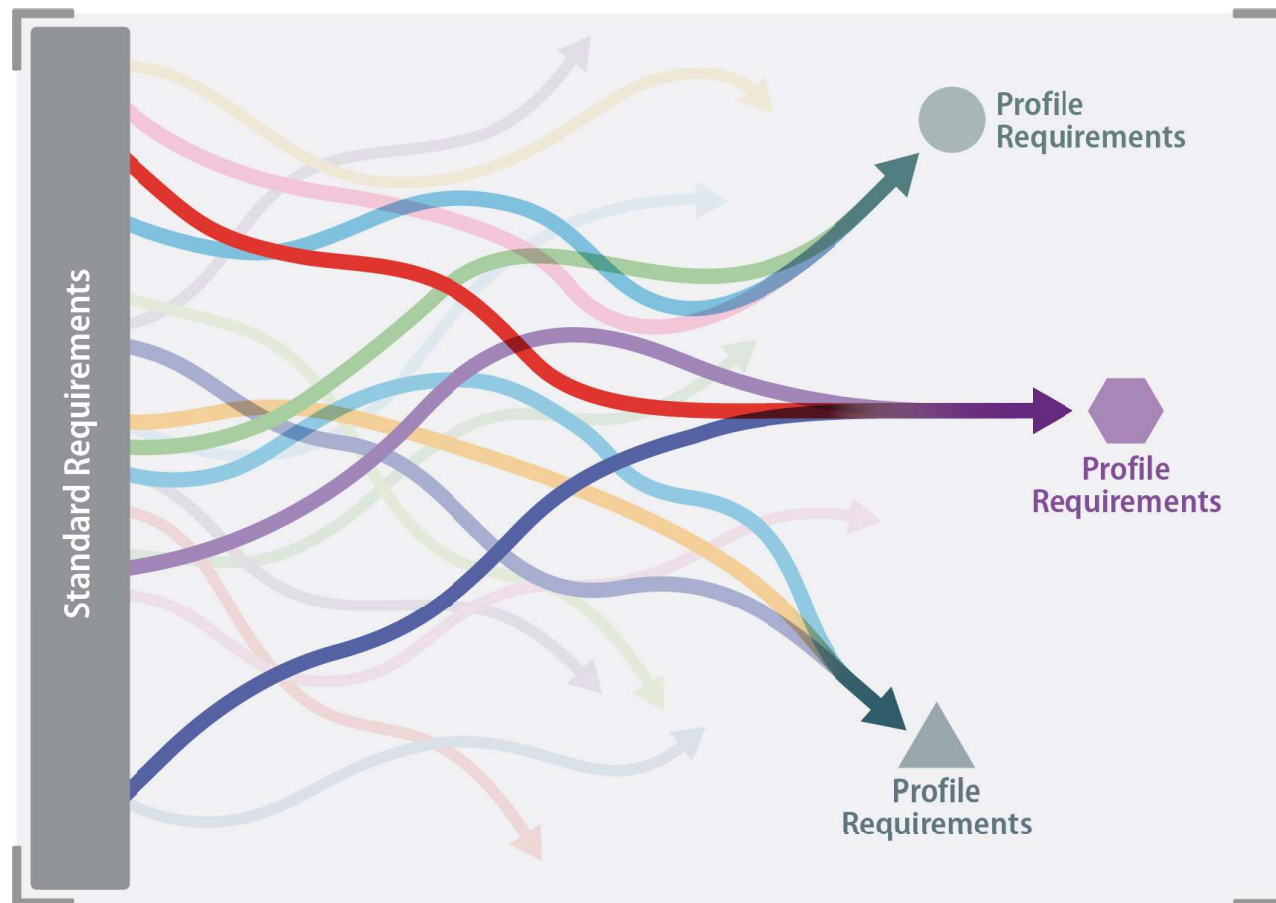
Interoperability Profile: IEEE 1547 Case Study



Interoperability Profile: CA Rule 21 Case Study



Interoperability Profiles



1. NISTIR 7628 Logical Interfaces

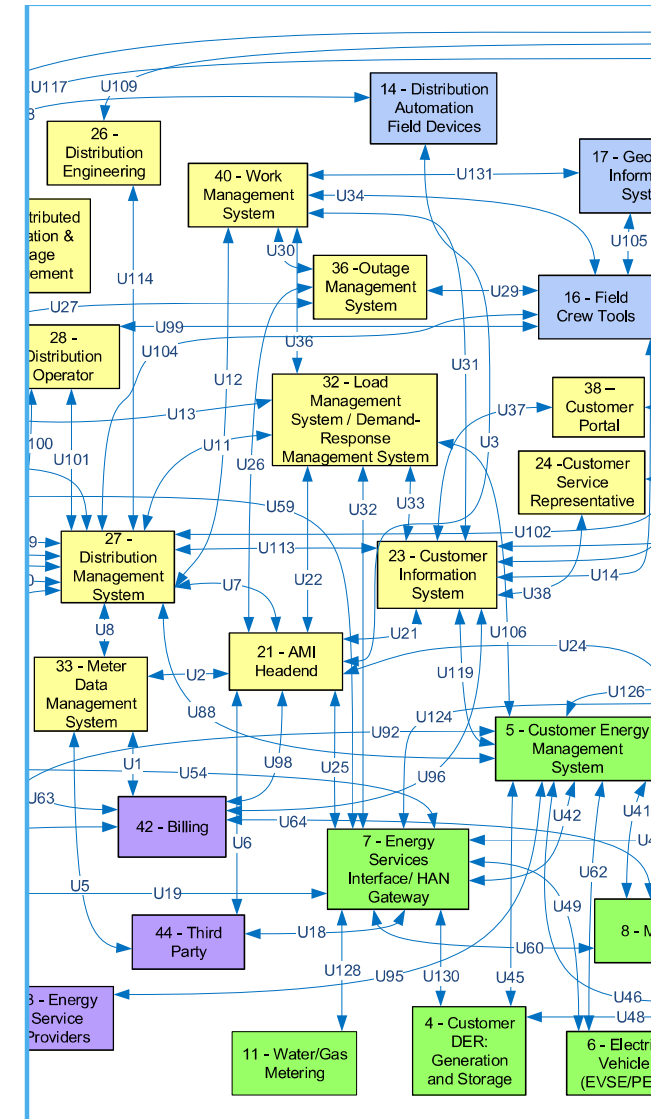
In 2014 NIST defined a set of 21 logical interface categories (LICs) based on smart grid communications

2. High-DER Scenario

In the Interoperability Framework V4 we reexamined the required communications for the High-DER scenario

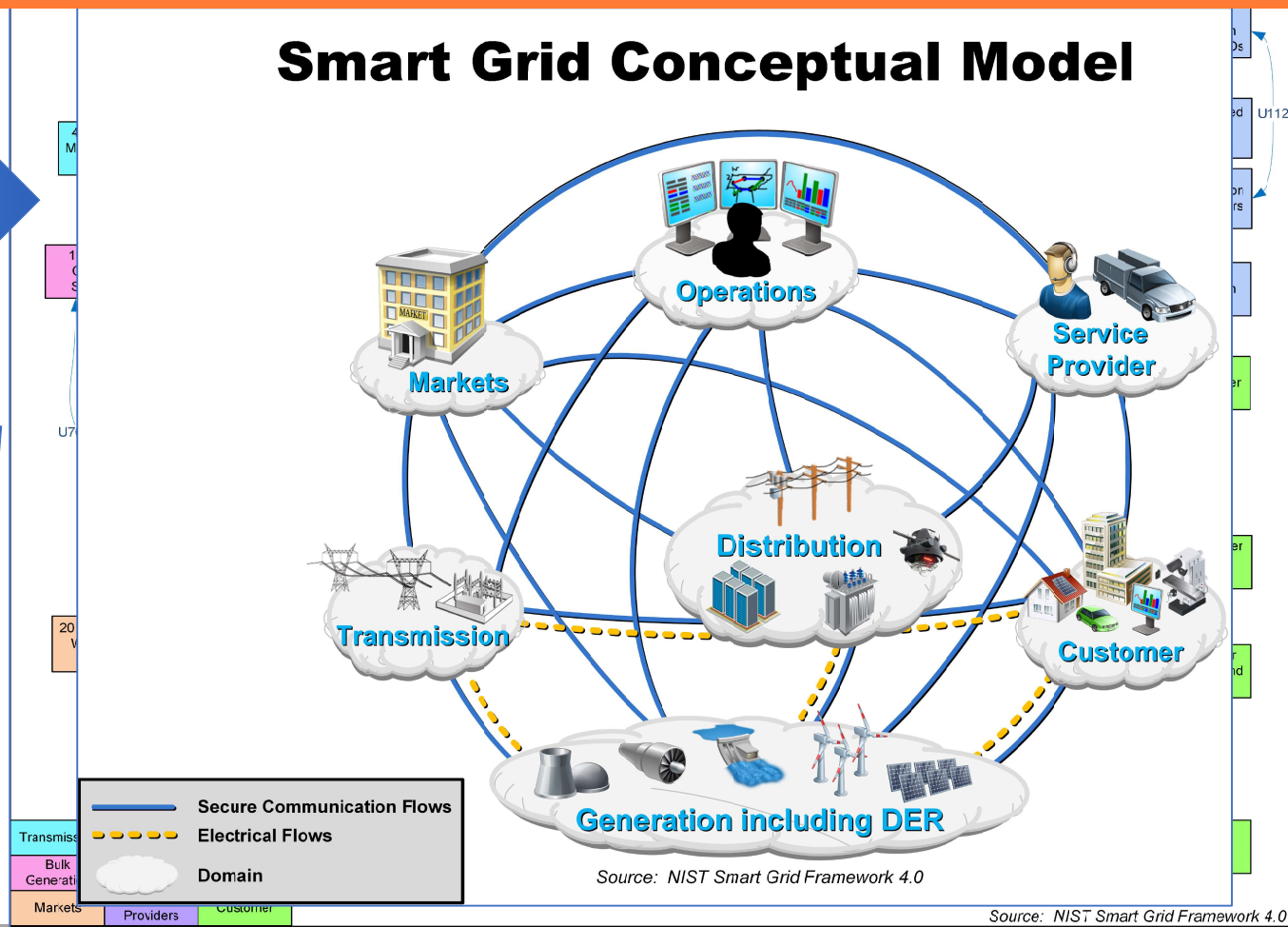
3. Categories and Next steps

New communications interfaces in the High-DER scenario were mapped to the LICs from NISTIR 7628



NISTIR 7628 – Cybersecurity guide built on interfaces

Smart Grid Conceptual Model



NISTIR 7628 – Logical Interface Categories

Table 2-2 Logical Interfaces by Category

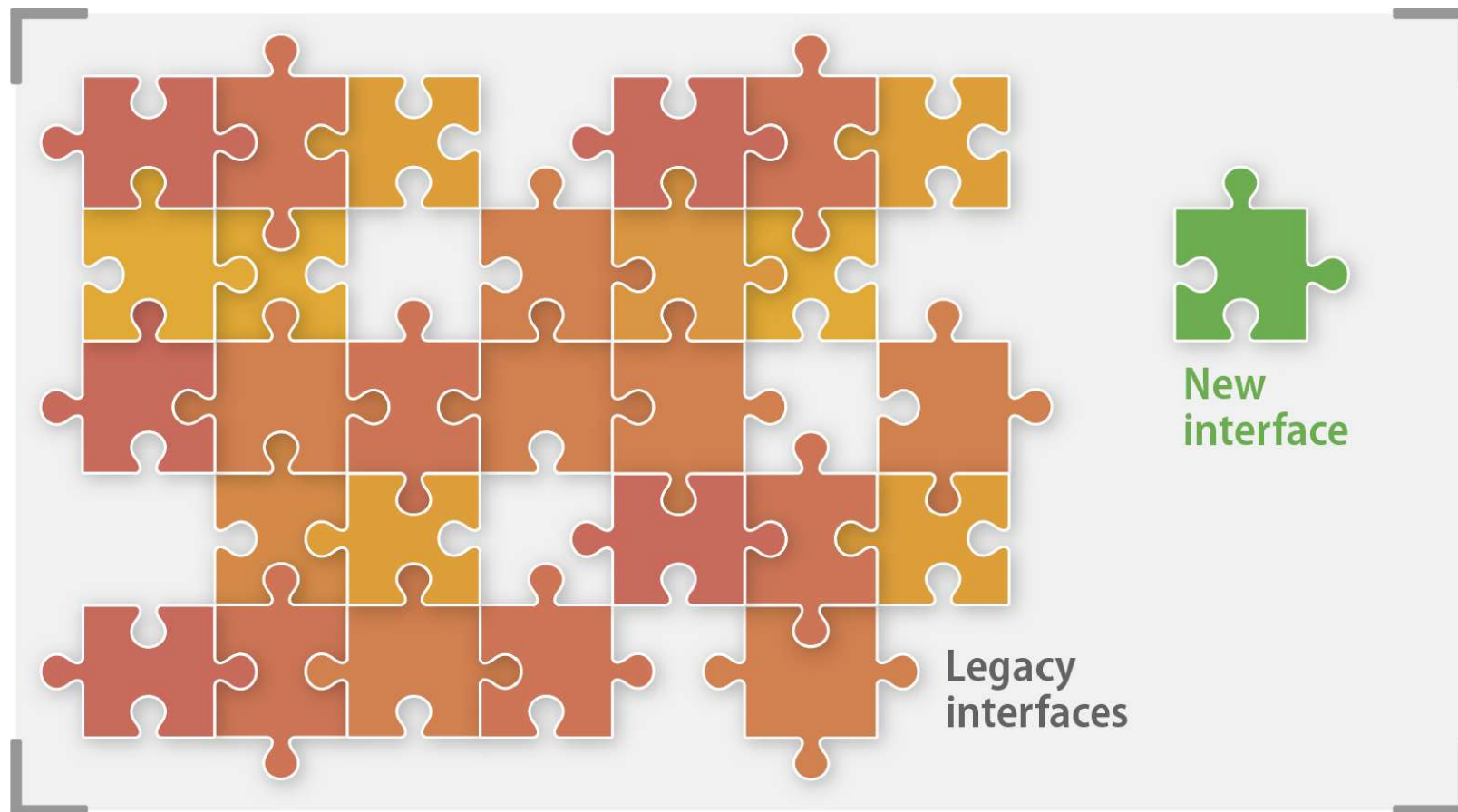
Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: <ul style="list-style-type: none"> Between transmission SCADA and substation equipment Between distribution SCADA and high 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Between an RTO/ISO EMS and a utility energy management system 	U10, U56, U66, U70, U74, U80, U83, U87, U89, U90, U115, U116, Ux3

Logical Interface Category	Logical Interfaces
7. Interface between back office systems under common management authority, for example: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Between a third party billing system and a utility meter data management system 	U1, U4, U6, U15, U52, U53, Ux4, Ux6
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Between a temperature sensor on a transformer and its receiver 	U111
12. Interface between sensor networks and control systems, for example: <ul style="list-style-type: none"> Between a sensor receiver and the substation master 	U108, U112
13. Interface between systems that use the AMI network, for example: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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

Logical Interface Category	Logical Interfaces
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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
19. Interface between operations decision support systems, for example: <ul style="list-style-type: none"> Between VAMS and ISO/RTO 	U77, U78
20. Interface between engineering/maintenance systems and control equipment, for example: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Between SCADA system and its vendor 	U5
Logical Interface Category	Logical Interfaces
22. Interface between security/network/system management consoles and all networks and systems, for example: <ul style="list-style-type: none"> 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)

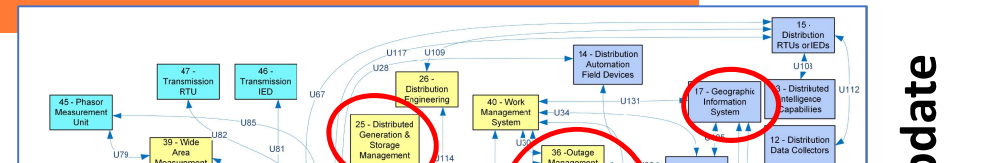
Source: NISTIR 7628r1, Table 2-2 (2014)

New Interfaces



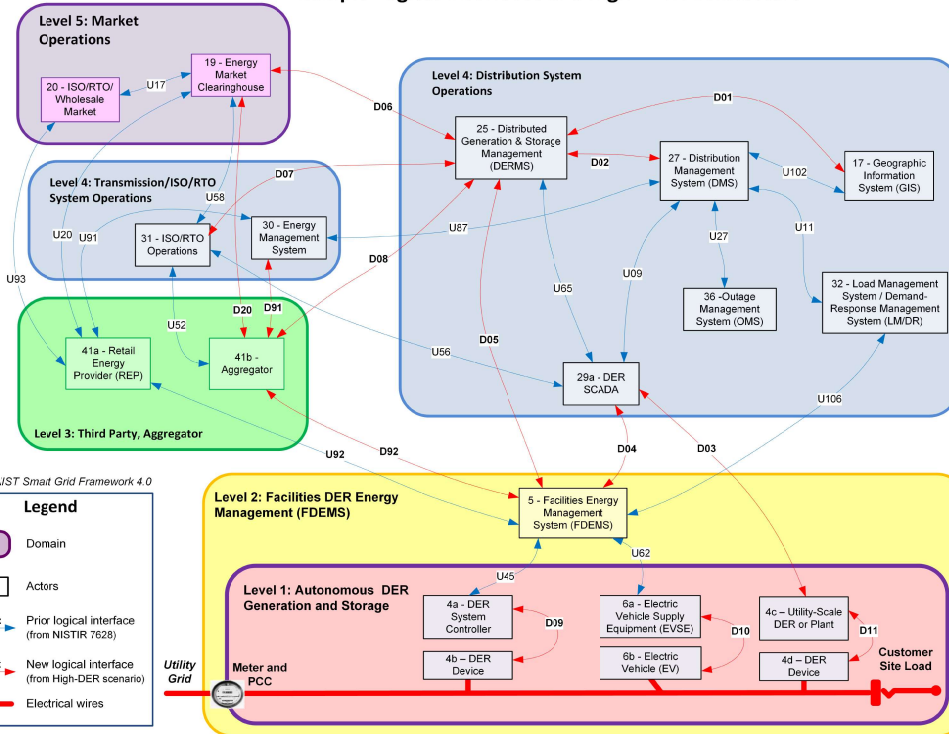
Framework V4 – High—DER Scenario LICs

New Interfaces, known challenges

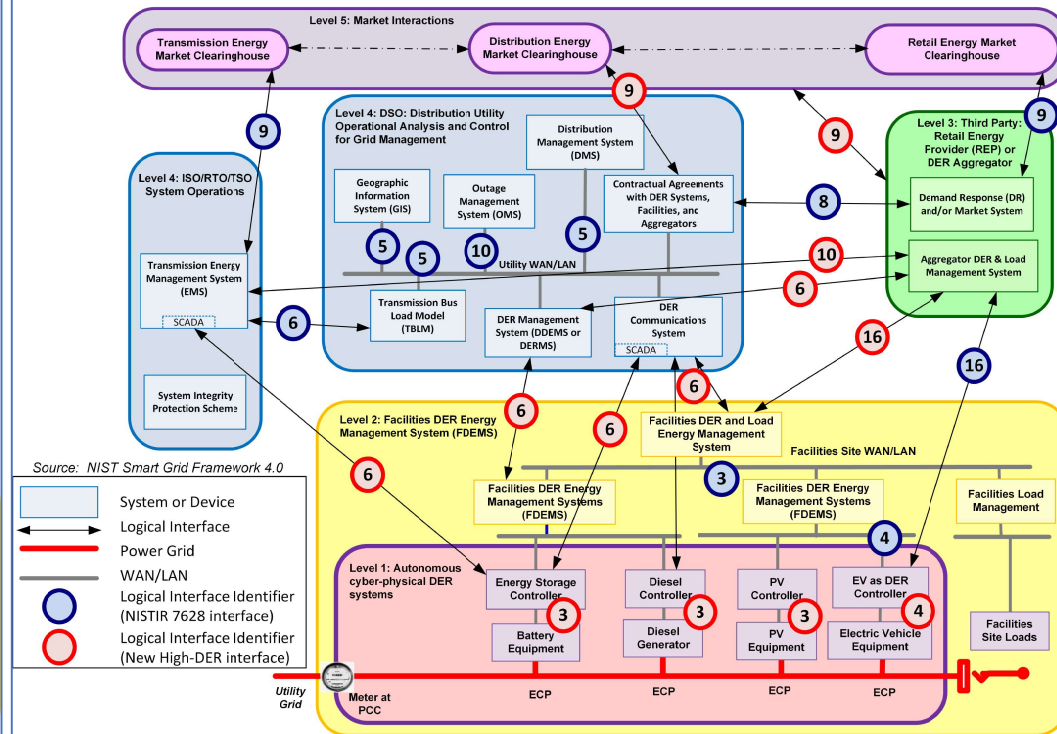


update

Example Logical Interfaces in a High-DER Architecture



High-DER Example Logical Interfaces by Category



Framework 4.0: New High-DER Interfaces

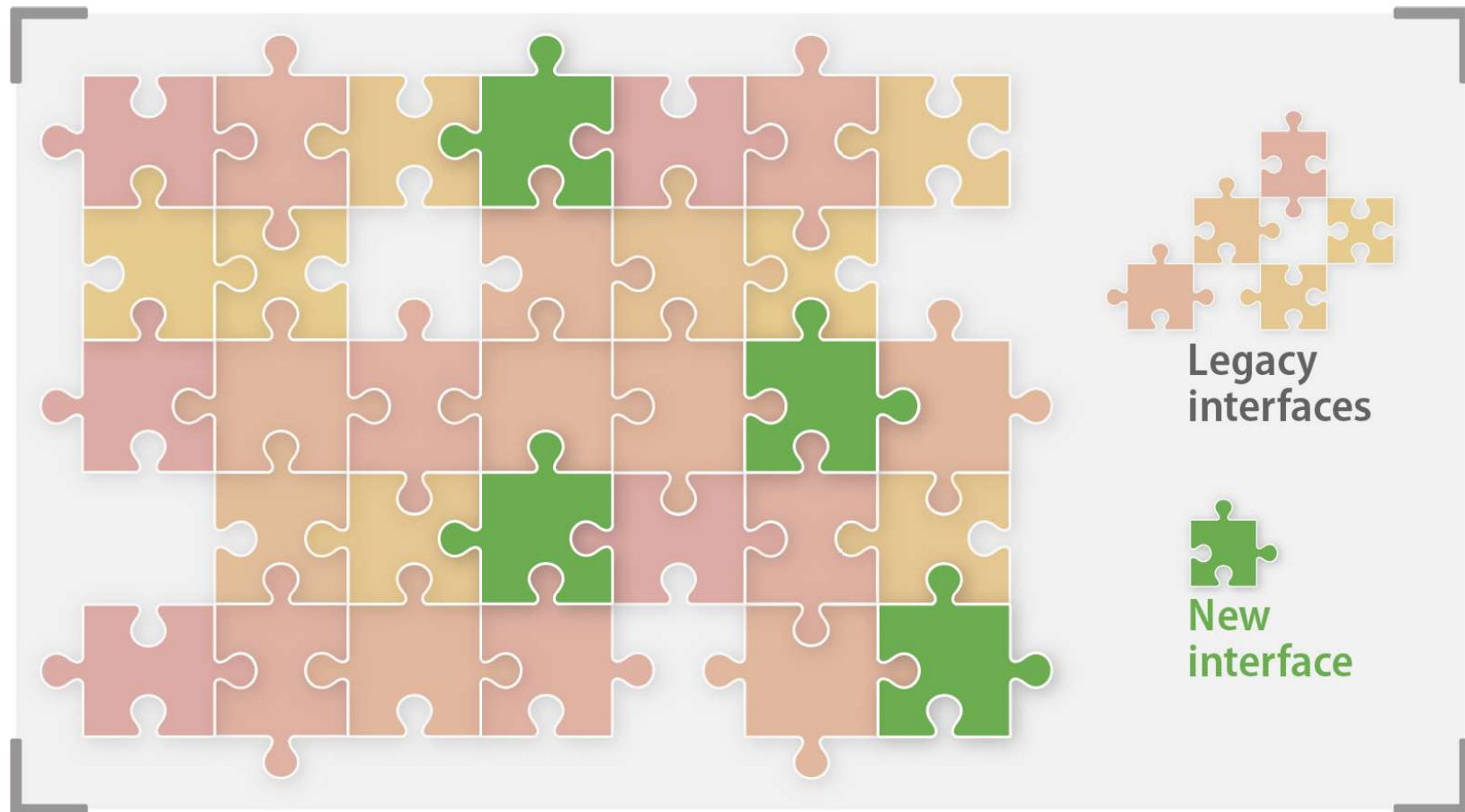
Framework 4.0: Existing Logical Interface Categories

Framework v4 – Logical Interface Categories

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
D11	4c: Utility-Scale DER System or Plant (e.g. large storage system)	4d: 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.
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.

Source: NIST Smart Grid Interoperability Framework, v4

New Interfaces



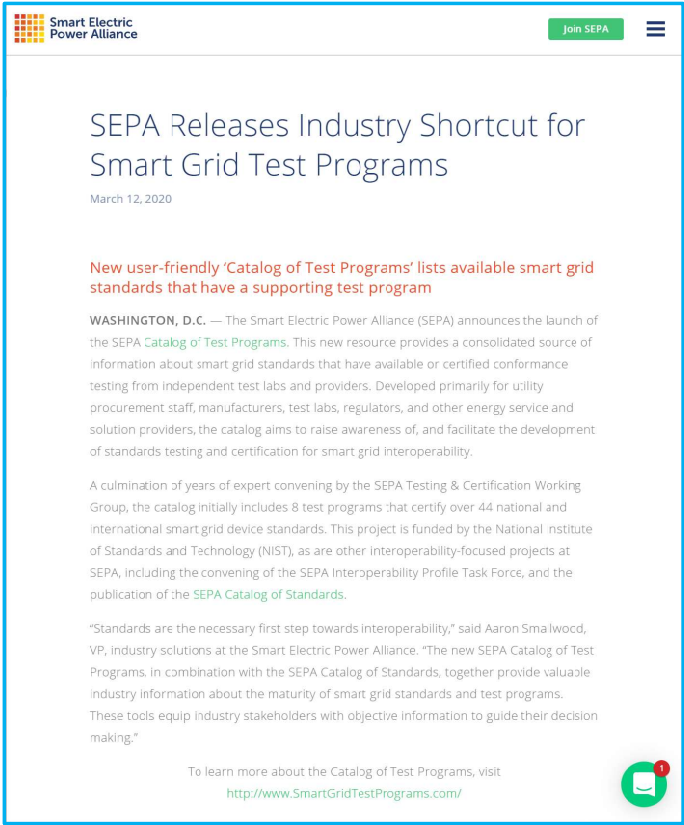
Working with SEPA: Catalog of Test Programs

Catalog of Standards

Built from the SGIP database, and continuing to expand through member engagement.

Catalog of Test Programs

Built upon NIST research, intended to help utility procurement staff, manufacturers, regulators, and energy service providers easily identify opportunities for certified standards conformance testing.



Working with SEPA: Interoperability Profiles

Beyond standards conformance

Standards conformance is inadequate to ensure interoperability, so SEPA and NIST are collaborating on a better way forward.

Interoperability Profiles: Managed charging of EV Fleets



Supporting a standard information exchange between DSO, EV Fleet, and Charge Point Operators to provide collective visibility to the constraints, availability, and responsive capacity of EV fleet facilities to enhance system reliability and power quality.

Interoperability Profiles: Distributed Energy Resources

Facilitating safe and efficient integration of DER into the electric power grid at multiple scales, DER profiles will map IEEE 1547 physical capabilities to relevant operational and communications strategies for different scale systems tied into primary and secondary distribution systems.

Interoperability Profiles: products and outputs

Use case, application guide, and interoperability profiles.

 [Join SEPA](#) 

Interoperability Profiles – A Better Way to Buy Grid Technology

April 2, 2020 | By Daisy Chung

Imagine browsing online for a new computer app. Once you have located the app, you swiftly hit the 'download' button – and immediately realize you've purchased the Windows version, which is incompatible with your Apple device. You have become a victim of technology tribalism.

If your device represents a utility's service territory, and the app represents new technology being connected to the grid, then this example demonstrates the device interoperability failures possible with today's smart grid. As newer and more complex technologies connect to the grid, opportunities for failure increase.

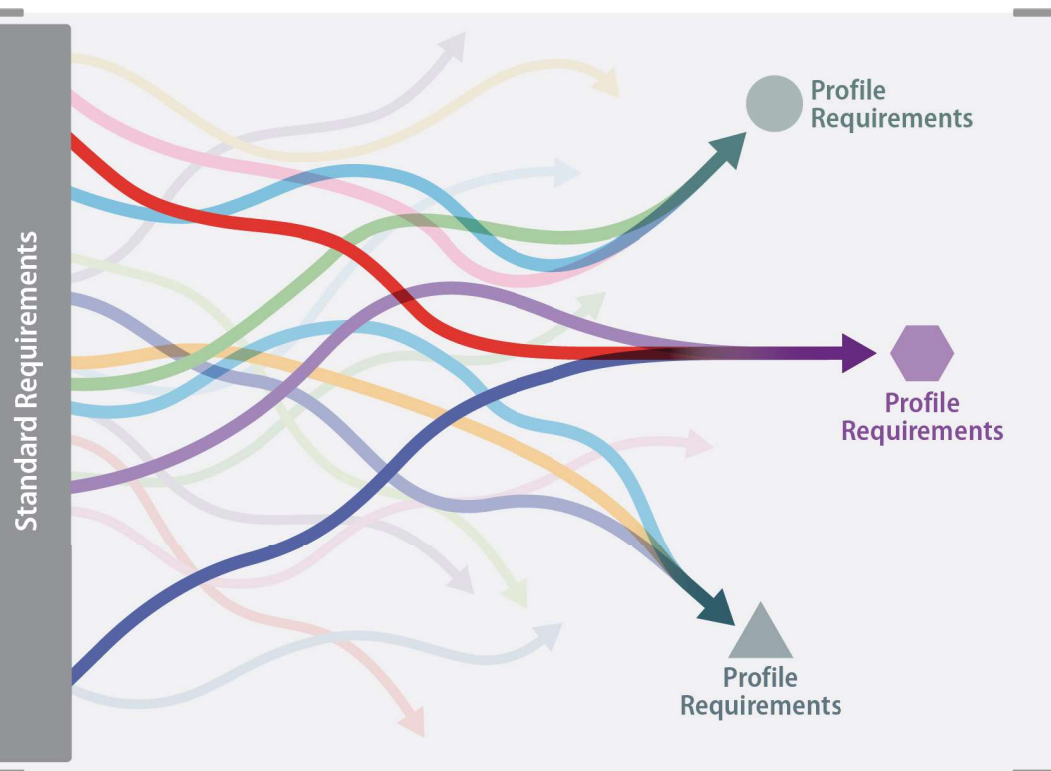
Why Can't All Devices and Systems Get Along?

As manufacturers develop new devices, smart grid standards and conformance tests should ensure interoperability — the ability to exchange actionable information between two or more systems. However, the industry remains encumbered by a lack of interoperability at the device/interface level. Without time consuming and often expensive software and hardware integration, adding new smart grid devices, supported by multiple different standards, onto a distribution system will likely result in systems that aren't interoperable.

Current smart grid standards exhibit three characteristics that may present interoperability issues. The first is the **wide range of applicable standards** that can pertain to a smart grid device. For example, over 30 international standards could apply to a customer smart meter.

The second is the wide range of configuration options allowed within the

Questions?



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1108r4

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0

Avi Gopstein, Cuong Nguyen, Cheyney O'Fallon, and David Wollman
*Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory*

Nelson Hasting
*Applied Security Division
Information Technology Laboratory*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.1108r4>

February 2021



U.S. Department of Commerce
Wynn Coggins, Acting Secretary

National Institute of Standards and Technology
James K. Olthoff, Acting NIST Director and Acting Undersecretary of Commerce for Standards and Technology

<https://doi.org/10.6028/NIST.SP.1108r4>