NIST Priority Action Plan 2
Wireless standards for Smart Grid

<Insert cool NIST / SGIP Graphic here>

Table of Contents

Revision History iii
Preface ..... - 1 -
Authors ..... - 2 -
1 Overview of the process ..... - 3 -
2 Acronyms and Definitions ..... - 4 -
2.1 Acronyms ..... - 4 -
2.2 Definitions ..... - 7 -
3 Smart grid ..... - 11 -
3.1 Reference Architecture ..... - 11 -
3.2 List of actors ..... - 13 -
3.3 Use Cases ..... - 14 -
3.4 Application requirements ..... - 16 -
3.4.1 Smart grid user applications' quantitative requirements ..... - 16 -
3.4.2 Aggregation of requirements per actor to actor ..... - 16 -
4 Wireless Technology ..... - 20 -
5 Evaluation approach / Modeling approach ..... - 21 -
5.1 Channel Models ..... - 23 -
5.1.1 Indoor-indoor environments ..... - 24 -
5.1.2 Outdoor-outdoor environments ..... - 25 -
5.1.3 Outdoor-indoor environments ..... - 25 -
5.2 Physical Layer ..... - 26 -
5.3 MAC sublayer ..... - 26 -
5.4 Example Modeling Tool ..... - 26 -
5.5 Other Tools ..... - 27 -
6 Findings / Results ..... - 28 -
7 Conclusions ..... - 31 -
8 References ..... - 32 -
9 Bibliography ..... - 32 -

Revision History

Revision Number	Revision Date	Revision By	Summary of Changes	Changes marked
.01	3/31/2010	Matt Gillmore	Initial take on the outline, TOC, ,authors, definitions, acronyms, reference architecture	No
.02	4/28/2010	David Cypher	Added outline numbering for cross reference purposes, added text for 1, 3.3 and 5	No
.03	5/3/2010	David Cypher	Edits and additional material for 3.2, 5 and 6	No
.04	5/4/2010	Nada Golmie	Edits to sections 5	No

Preface

[Joe Hughes]
This guide is the output of the Priority Action Plan number 2 (PAP#2), wireless communications for the smart grid, which is part of the Smart Grid Interoperability Panel (SGIP). PAP#2's work area investigates the strengths, weaknesses, capabilities, and constraints of existing and emerging standards-based physical media for wireless communications. The approach is to work with the appropriate standard development organizations (SDOs) to determine the characteristics of each technology for Smart Grid application areas and types. Results are used to assess the appropriateness of wireless communications technologies for meeting Smart Grid applications' requirements.

This guide contains the smart grid reference architecture, the user applications' requirements, candidate wireless technologies and their capabilities, a methodology to assess the appropriateness of wireless communications technologies along with an example model, and some results.

Authors

Provide feedback and edits to this document to get your name here!

Matthew Gillmore – Consumers Energy

1 Overview of the process

[Nada Golmie / NIST]

The process by which this guide was generated is based on the six tasks for PAP#2.

Task 1: *Segment the smart grid and wireless environments into a minimal set of categories for which individual wireless requirements can be identified*. This was accomplished by the creation of a template (app_matrix_pap_xls) for input to application communication requirements. This template contained two main sheets one for characterizing the user application and the other for characterizing the physical devices that would be used for the user applications. With this template as a basis OpenSG[1] submitted a subset of user application quantitative information (SG Network System Requirements Specification v2.1.xls). See 3 and 3.4.1.

Task 2: *Develop Terminology and definitions*. This was accomplished by combining the terms and definitions from the various input documents to other tasks of PAP#2, as well as using those from the base Smart Grid documents (Second DRAFT NIST IR 7628 Smart Grid Cyber Security Strategy and Requirements and NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0). For Acronyms see 2.1 and definitions see 2.2.

Task 3: *Compile and communicate use cases (see 3.3) and develop requirements for all smart grid domains in terms that all parties can understand*. For the user applications (see 3.4) submitted and the smart grid domains that are applicable to the user requirements, this was done.

Task 4: *Compile and communicate a list of capabilities, performance metrics, etc. in a way that all parties can understand. - Not quantifying any standard, just defining the set of metrics*. This was accomplished by default with the submission for Task 5.

Task 5: *Create an inventory of wireless standards and their associated characteristics (defined in task 4) for the environments identified in task 1*. The Wireless Functionality and Characteristics Matrix for the identification of Smart grid domain application (Consolidated_NIST_Wireless_Characteristics_Matrix-V3.xls.) excel spread sheet captures a list of wireless standards and their associated characteristics. (See 4)

Task 6: *Perform the mapping and conduct an evaluation of the wireless technologies based on the criteria and metrics developed in task 4*. This is the subject of this guide (Evaluation approach / Modeling approach (5), Findings / Results (6), and Conclusions(7)).

[1] The full description of the procedures used in this guide requires the identification of certain commercial products and their suppliers. The inclusion of such information should in no way be construed as indicating that such products or suppliers are endorsed by NIST or are recommended by NIST or that they are necessarily the best materials, instruments, software or suppliers for the purposes described.

2 Acronyms and Definitions

[Matt Gillmore]

The acronyms and definitions provided are used in this guide and in its referenced supporting documentation.

2.1 Acronyms

AC	Alternating Current
AICPA	American Institute of Certified Public Accountants[2]
AMI	Advanced Metering Infrastructure
AMS	Asset Management System
ASAP-SG	Advanced Security Acceleration Project-Smart Grid
B2B	Business to Business
BAN	Business Area Network
CIM	Common Information Model
CIP	Critical Infrastructure Protection
CSWG	Cyber Security Working Group
DA	Distribution Automation
DAP	Data Aggregation Point
DER	Distributed Energy Resources
DHS	Department of Homeland Security[3]
DMS	Distribution Management System
DNA	Deoxyribonucleic acid
DNP	Distributed Network Protocol
DOE	Department of Energy
DOMA	Distribution Operations Model and Analysis
DR	Demand Response
DRMS	Distribution Resource Management System
DSDR	Distribution Systems Demand Response
DSM	Demand Side Management
EMS	Energy Management System
EPRI	Electric Power Research Institute[4]
ES	Electric Storage
ESB	Enterprise Service Bus
ESI	Energy Services Interface
ET	Electric Transportation
EUMD	End Use Measurement Device
EV/PHEV	Electric Vehicle/Plug-in Hybrid Electric Vehicles
EVSE	Electric Vehicle Service Element
FAN	Field Area Network
FEP	Front End Processor

[2] AICPA, 1211 Avenue of the Americas, New York, NY 10036; www.aicpa.org
[3] Department of Homeland Security – www.dhs.gov
[4] Electric Power Research Institute, Inc. (EPRI) 3420 Hillview Avenue, Palo Alto, California 94304

FERC	Federal Energy Regulatory Commission[5]
FIPS	Federal Information Processing Standard Document
FLIR	Fault Location, Isolation, Restoration
G&T	Generations and Transmission
GAPP	Generally Accepted Privacy Principles
GIS	Geographic Information System
GPRS	General Packet Radio Service
HAN	Home Area Network
HMI	Human-Machine Interface
HVAC	Heating, Ventilating, and Air Conditioning
I2G	Industry to Grid
IEC	International Electrotechnical Commission[6]
IED	Intelligent Electronic Device
IHD	In-home Display
ISA	International Society of Automation[7]
ISO	Independent System Operator
	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LMS	Load management System
LMS/DRMS	Load Management System/ Distribution Resource Management System
LV	Low voltage (in definition)
MDMS	Meter Data Management System
MFR	Multi-Feeder Reconnection
MSW	Meter Service Switch
MV	Medium Voltage
NAN	Neighborhood Area Network
NERC	North American Electric Reliability Corporation[8]
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NMS	Network Management System
OMS	Outage Management System
OWASP	Open Web Application Security Project
PAP	Priority Action Plan
PCT	Programmable Communicating Thermostat
PEV	Plug-In Electric Vehicle
PHEV	Plug-in Hybrid Electric Vehicle

[5] Federal Energy Regulatory Commission - www.ferc.gov
[6] International Electrotechnical Commission – www.iec.ch
[7] ISA, 67 Alexander Drive, Research Triangle Park, NC 27709 USA - www.isa.org
[8] www.nerc.com

PI	Process Information
PIA	Privacy Impact Assessment
PII	Personally Identifying Information
R&D	Research and Development
RTO	Regional Transmission Operator
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison[9]
SDO	Standards Development Organization
SGIP	Smart Grid Interoperability Panel
SGIP-CSWG	SGIP – Cyber Security Working Group
SP	Special Publication
SSP	Sector-Specific Plans
T/FLA	Three/Four Letter Acronym
VAR	Volt-Amperes Reactive
VVWS	Volt-VAR-Watt System
WAMS	Wide-Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WLAN	Wireless Local Area Network
WMS	Work Management System

[9] www.sce.com

2.2 Definitions

Actor	A generic name for devices, systems, or programs that make decisions and exchange information necessary for performing applications: smart meters, solar generators, and control systems represent examples of devices and systems.
Anonymize	A process of transformation or elimination of PII for purposes of sharing data
Aggregation	Practice of summarizing certain data and presenting it as a total without any PII identifiers
Aggregator	SEE FERC OPERATION MODEL
Applications	Tasks performed by one or more actors within a domain.
Asset Management System	A system(s) of record for assets managed in the Smart Grid. Management context may change (e.g. financial, network).
Capacitor Bank	This is a device used to add capacitance as needed at strategic points in a distribution grid to better control and manage VARs and thus the Power Factor and they will also affect voltage levels.
Common Information Model	A structured set of definitions that allows different Smart Grid domain representatives to communicate important concepts and exchange information easily and effectively.
Common Web Portal	Web interface for Regional Transmission Operator, customers, retail electric providers and transmission distribution service provider to function as a clearing house for energy information. Commonly used in deregulated markets.
Data Collector	See Substation Controller
Data Aggregation Point	This device is a logical actor that represents a transition in most AMI networks between Wide Area Networks and Neighborhood Area Networks. (e.g. Collector, Cell Relay, Base Station, Access Point, etc)
De-identify	A form of anonymization that does not attempt to control the data once it has had PII identifiers removed, so it is at risk of re-identification.
Demand Side Management	A system that co-ordinates demand response / load shedding messages indirectly to devices (e.g. Set point adjustment)
Distribution Management System	A system that monitors, manages and controls the electric distribution system.
Distribution Systems Demand Response	A system used to reduce load during peak demand. Strictly used for Distribution systems only.
Electric Vehicle/Plug-in Hybrid Electric Vehicles	Cars or other vehicles that draw electricity from batteries to power an electric motor. PHEVs also contain an internal combustion engine.
Energy Services Interface	Provides security and, often, coordination functions that enable secure interactions between relevant Home Area Network Devices and the Utility. Permits applications such as remote load control, monitoring and control of distributed generation, in-home display of customer usage, reading of non-energy meters, and integration with building management systems. Also provides auditing/logging functions that record transactions to and from Home Area Networking Devices.

Enterprise Service Bus	The Enterprise Service Bus consists of a software architecture used to construct integration services for complex event-driven and standards-based messaging to exchange meter or grid data. The ESB is not limited to a specific tool set rather it is a defined set of integration services.
Fault Detector	A device used to sense a fault condition and can be used to provide an indication of the fault.
Field Force	Employee working in the service territory that may be working with Smart Grid devices.
Generally Accepted Privacy Principles	Privacy principles and criteria developed and updated by the AICPA and Canadian Institute of Chartered Accountants to assist organizations in the design and implementation of sound privacy practices and policies.
Home Area Network	A network of energy management devices, digital consumer electronics, signal-controlled or enabled appliances, and applications within a home environment that is on the home side of the electric meter.
Intelligent Fault Detector	A device that can sense a fault and can provide more detailed information on the nature of the fault, such as capturing an oscillography trace.
ISO/IEC27001	An auditable international standard that specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It uses a process approach for protection of critical information
Last Gasp	Concept of an energized device within the Smart Grid detecting power loss and sending a broadcast message of the event.
Load Management System	A system that controls load by sending messages directly to device (e.g. On/Off)
Low Voltage Sensor	A device used to measure and report electrical properties (such as voltage, current, phase angle or power factor, etc.) at a low voltage customer delivery point.
Medium Voltage Sensor	A device used to measure and report electrical properties (such as voltage, current, phase angle or power factor, etc.) on a medium voltage distribution line.
Motorized Switch	A device under remote control that can be used to open or close a circuit.
Neighborhood Area Network	A network comprised of all communicating components within a distribution domain.
Network Management System	A system that manages Fault, Configuration, Auditing/Accounting, Performance and Security of the communication. This system is exclusive from the electrical network.
Outage Management System	A system that receives out power system outage notifications and correlates where the power outage occurred

Personal Information	Information that reveals details, either explicitly or implicitly, about a specific individual's household dwelling or other type of premises. This is expanded beyond the normal "individual" component because there are serious privacy impacts for all individuals living in one dwelling or premise. This can include items such as energy use patterns or other types of activities. The pattern can become unique to a household or premises just as a fingerprint or DNA is unique to an individual.
Phase Measuring Unit	A device capable of measuring the phase of the voltage or current waveform relative to a reference.
Power Factor	A dimensionless quantity that relates to efficiency of the electrical delivery system for delivering real power to the load. Numerically, it is the Cosine of the phase angle between the voltage and current waveforms. The closer the power factor is to unity the better the inductive and capacitive elements of the circuit are balanced and the more efficient the system is for delivering real power to the load(s).
Privacy Impact Assessment	A process used to evaluate the possible privacy risks to personal information, in all forms, collected, transmitted, shared, stored, disposed of, and accessed in any other way, along with the mitigation of those risks at the beginning of and throughout the life cycle of the associated process, program or system
Programmable Communicating Thermostat	A device within the premise that has communication capabilities and controls heating, ventilation and cooling systems.
Recloser (non-Team)	A device used to sense fault conditions on a distribution line and trip open to provide protection. It is typically programmed to automatically close (re-close) after a period of time to test if the fault has cleared. After several attempts of reclosing it can be programmed to trip open and stop trying to reclose until reset either locally or under remote control.
Recloser (Team)	A device that can sense fault conditions on a distribution line and to communicate with other related reclosers (the team) to sectionalize the fault and provide a coordinated open/close arrangement to minimize the effect of the fault.
Regional Transmission Operator	An organization that is established with the purpose of promoting efficiency and reliability in the operation and planning of the electric transmission grid and ensuring non-discrimination in the provision of electric transmission services based on the following required/demonstrable characteristics and functions.
Remote Terminal Unit	Aggregator of multiple serialized devices to a common communications interface
Sub Meter	Premise based meter used for Distributed Energy Resources and PHEV. This device may be revenue grade.
Substation Controller	Distributed processing device that has supervisory control or coordinates information exchanges from devices within a substation from a head end system.
Transformer (MV-to-LV)	A standard point of delivery transformer. In the Smart Grid context is it assumed there will be a need to measure some electrical or physical characteristics of this transformer such as voltage (high and/or low side) current, MV load, temperature, etc.

Use Case	A systems engineering tool for defining a system's behavior from the perspective of users. In effect, a use case is a story told in structure and detailed steps—scenarios for specifying required usages of a system, including how a component, subsystem, or system should respond to a request that originates elsewhere.
Voltage Regulator	This device is in effect an adjustable ratio transformer positioned at strategic points in a distribution grid and is utilized to better manage and control the voltage as it changes along the distribution feeder.
VAR – Volt-Amperes Reactive;	In an AC power system the voltage and current measured at a point along the delivery system will often be out of phase with each other as a result the combined effects of the resistive and reactive (i.e. the capacitance and inductive) characteristics of the delivery system components and the load. The phase angle difference at a point along the delivery system is an indication of how well the inductive and capacitive effects are balanced at that point. The real power passing that point is the product of the magnitude of the Voltage and Current and the Cosine of the angle between the two. The VAR parameter is the product of the magnitude of the Voltage and Current and the Sine of the angle between the two. The magnitude of the VAR parameter is an indication of the phase imbalance between the voltage and current waveforms.
Web Portal	Interface between energy customers and the system provider. Could be the utility or a third party

3 Smart grid

Consists of a reference architecture, list of actors, use cases, and user application requirements.

3.1 Reference Architecture

[Matt Gillmore]

In this section a few illustrative diagrams are included to help the reader of this document to understand the content. These files are also available for reference at the following location:

http://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Interium_Release_2/

The reference architecture models are:

a) SG-NET-diagram-r0.4e-with-Xflows.pdf
b) SG-NET-diagram-r0.4e.pdf

The SG-Network functional requirements spreadsheet is:

c) SG Network System Requirements Specification v2.1.xls

The SG-Network functional requirements spreadsheet companion documentation is:

d) SG Network System Requirements Specification v2.doc

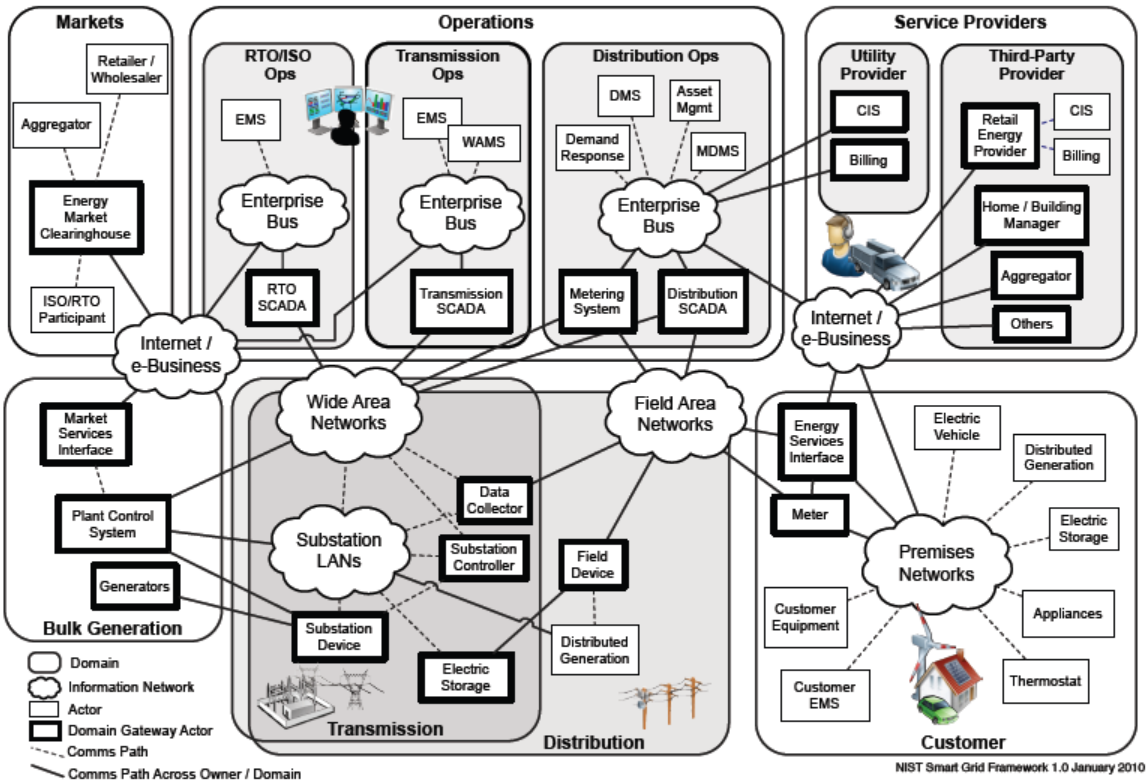

Figure 1 - Baseline Diagram without cross domain and network data flows

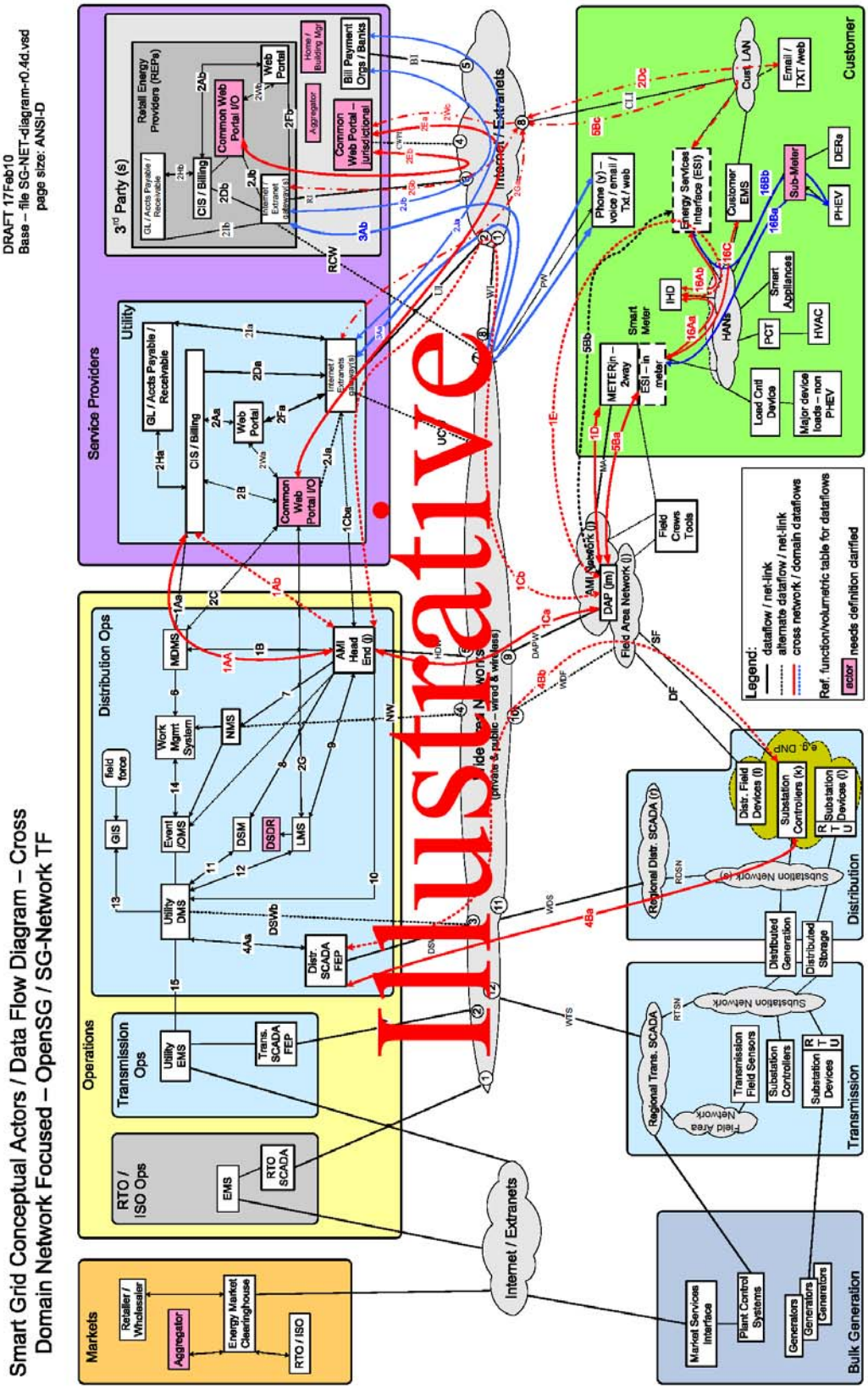

Figure 2: Baseline Diagram With Cross Domain & Network flows

3.2 List of actors

Table 1: List of Actors List of Actors contains a list of actors expanded from the list of actors contained in NIST Special Publication 1108.

Table 1: List of Actors

Descriptor Diagram	DomainName	Related NIST Actor
Energy Market Clearinghouse	Markets	Energy Market Clearinghouse
Retailer/Wholesaler	Markets	Aggregator/Retail Energy Provider
Market Aggregator	Markets	Aggregator/Retail Energy Provider
RTO/ISO	Markets	RTO/ISO
EMS	Operations	Utility EMS
RTO SCADA	Operations	SCADA
Utility EMS	Operations	Utility EMS
Trans. SCADA FEP	Operations	SCADA
LMS/DRMS	Operations	LMS/DRMS
MDMS	Operations	MDMS
GIS	Operations	GIS
Event/OMS	Operations	OMS
Distr. SCADA FEP	Operations	SCADA
AMI Head End	Operations	AMI Head-End
Work Management System	Operations	Workforce Tool
Utility DMS	Operations	DMS Applications
DSDR	Operations	
NMS	Operations	Power System Control Center
DSM	Operations	
Third Party ODW	Service Provider	
Utility CIS/Billing	Service Provider	CIS
Distributed Energy Resource	Service Provider	
Utility ODW	Service Provider	Web Site
Utility Web Portal	Service Provider	Web Site
Retail Energy Providers Web Portal	Service Provider	Web Site
Bill Payment Orgs/Banks	Service Provider	Billing
Retail Energy Providers CIS/Billing	Service Provider	Billing
Third Party Aggregator	Service Provider	Aggregator/Retail Energy Provider
Home/Building Manager	Service Provider	Monitoring/Billing/Utility Back Office
Common Web Portal-Jurisdictional	Service Provider	Web Site
Internet/Extranet Gateway	Service Provider	
Utility Internet/Extranet Gateway	Service Provider	
Smart Meter	Customer	Meter
ESI (In Meter)	Customer	Energy Services Interface
ESI (Broadband)	Customer	Energy Services Interface
In Home Device (IHD)	Customer	Customer Equipment
Load Control Device	Customer	
Major Device Loads (Non-PHEV)	Customer	
PCT	Customer	
HVAC	Customer	
Smart Appliances	Customer	Customer Appliances

Descriptor Diagram	DomainName	Related NIST Actor
Sub-Meter	Customer	Sub-Meter
PHEV	Customer	Electric Vehicle
DERs	Customer	
Public Communications Interface	Customer	
Customer EMS	Customer	Customer EMS
Phone/Email/Txt/Web	Customer	
Meter Switch	Customer	
Two Way Meter	Customer	Meter
Market Services Interface	Bulk Generation	
Plant Control Systems	Bulk Generation	MDMS
Generators Bulk	Generation	
Transmission Field Sensors	Transmission	Field Devices
Distributed Application Controller (	Transmission	Field Devices
Transmission Substation Devices	Transmission	Field Devices
Transmission RTU	Transmission	SCADA
Transmission FAN Gateway	Transmission	
Distribution Field Sensors	Distribution	Field Devices
Distribution RTU	Distribution	Distribution SCADA
DistributionSubstation Devices	Distribution	Field Devices
Capacitor Bank (shunt Capacitor)	Distribution	SCADA
Voltage Regulator	Distribution	Field Devices
Distributed Generation	Distribution	Distributed Generation
Distributed Storage	Distribution	Storage System
Distribution FAN Gateway	Distribution	
Sectionalizer	Distribution	Field Devices
Circuit Breaker	Distribution	Field Devices
Medium Voltage Sensor	Distribution	Field Devices
Low Voltage Sensor	Distribution	Field Devices
Recloser (non-Team)	Distribution	Field Devices
Recloser (Team) Server to Remote	Distribution	Field Devices
Recloser (Team) Peer-to-Peer Inter	Distribution	Field Devices
Motorized Switch	Distribution	Field Devices
Fault Detectors	Distribution	Field Devices
Intelligent Fault detector (with Oscil	Distribution	Field Devices
Phase Measuring Unit (PMU)	Distribution	Field Devices
Transformer (MV-to-LV)	Distribution	Field Devices

3.3 Use Cases

[Matt to find an SG-Network volunteer]
Three levels of describing use cases.

The following table lists the smart grid use cases (or applications)

Smart Grid Use Case Name
Accounting Management
Configuration Management
Demand Response

Distribution Automation Support
Fault Management
Independent Power Producers
Load Management
Meter Events
Meter Reading
Meter Service Switch
Outage Events
Performance Management
PHEV
Pre-Pay Metering
Real Time Pricing
Security Management
System Updates
Tamper Events
Transmission Automation Support
Volt/VAR Management
Wind Solar Storage
Work Force Automation

From the Interoperability Knowledge Base (IKB)
http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/InteroperabilityKnowledgeBase#Use_Cases

Use Cases come in many shapes and sizes. With respect to the IKB, fairly comprehensive Use Case descriptions are used to expose functional requirements for applications of the Smart Grid. In order to provide this depth, these Use Cases contain the following:

Narrative -- a description in prose of the application represented including all important details and participants described in the context of their activities.
Actors -- identification of all the persons, devices, subsystems, software applications that collaborate to make the Use Case work
Information Objects -- defines the specific aggregates of information exchanged between Actors to implement the Use Case
Activities/Services -- description of the activities and services this Use Case relies on or implements
Contracts/Regulations -- what contractual or regulatory constraints govern this Use Case
Steps -- the step by step sequence of activities and messaging exchanges required to implement the Use Case

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/IKBUseCases
Contains use cases following this description

3.4 Application requirements

There are many smart grid user applications (use case). Many have text describing the user applications (see IKB) , but few contain quantitative requirements, which are necessary to design communications protocols.

3.4.1 Smart grid user applications' quantitative requirements

Some smart grid user applications' quantitative requirements were submitted to PAP#2 (See "SG Network System Requirements Specification v2.1 (March 12, 2010)). This version contained three user applications: meter reading, PHEV, and service switching along with their quantitative requirements.

3.4.2 Aggregation of requirements per actor to actor

[NIST to work on it]

Some links between actors carry aggregated traffic. For these links a method for creating an aggregated traffic load from individual events is needed. This section describes a method and contains an example for creating an aggregate traffic load. The aggregate traffic load can then be used as input to the model in **Error! Reference source not found.**.

As of April 12, 2010 there were three user applications provided (meter reading, PHEV, and service switching) in the SG Network System Requirements Specification v2.1. The events from these three user applications are used for this example.

Method:

Step 1 - Select a link between two actors.
Step 2 - Identify the events that cross this link.
Step 3 - Use the information from these events (and perhaps others) to calculate the individual contribution of frequency of event and size of application payload.
Step 4 - Select one value for each.
Step 5 - Assume (and document) values for missing information.
Step 6 - Calculate the aggregate traffic using selections and assumptions.

Example use of the method

Step 1 - Select a link between two actors.

1D, which is the link between the Data Aggregation Point (DAP) and a Smart Meter.

Step 2 - Identify the events that cross this link.

Five events are present in the DAP to Smart Meter direction

- 2 for meter reading,
  - multiple interval meter reading request and
  - on-demand meter read requests.
- 3 for Service Switch
  - cancel service switch operate request,
  - service switch operate request, and
  - service switch state request.

Ten events are present in the Smart Meter to DAP direction

- 6 for meter reading,
    - multiple interval meter read data
        - Commercial / Industrial Gas smart meters,
        - Commercial / Industrial Electric meters,
        - Residential gas smart meters, and
        - Residential electric smart meters.
    - on-demand read request app errors, and
    - on-demand meter read data.
- 4 for Service Switch
    - send service switch operate acknowledgment,
    - send service switch operate failure,
    - send metrology information after a successful service switch operate, and
    - send service switch state data.

Step 3 - Use the information from these events (and perhaps others) to calculate the individual contribution of frequency of event and size of application payload.
For some of these events there are ranges of values or scalar values. An example of the range of values is the multiple interval meter read data (Commercial / Industrial Gas smart meters) where the frequency is 1 – 6 transactions per day and the size of the data is 1600 bytes – 2400 bytes. An example of the scalar values is the send service switch operate failure to DAP where the frequency is 1 trans per 1000 switch operate per day. Since this is an error based on the original number of switch operate commands, we must obtain that events' frequency information, which is 1 - 50 transactions per 1000 meters per day.

Step 4 - Select one value for each
For each of the possible range of values select a value that is meaningful to your particular scenario. The following tables give an example selection of values.

Table 2: Selected values for DAP to Smart meter direction

Event	How often	Size (bytes)
multiple interval meter reading request	25 transactions /1000 smart meters	25
on-demand meter read requests	25 transactions /1000 smart meters	25
cancel service switch operate request	2 transactions /1000 smart meters	25
service switch operate request	50 transactions /1000 smart meters	25
service switch state request	50 transactions /1000 smart meters	25

Table 3: Selected values for Smart meter to DAP direction

Event	How often	Size (bytes)
multiple interval meter read data (Commercial / Industrial Gas smart meters)	6 transactions / 24 hours	2400
multiple interval meter read data (Commercial / Industrial Electric	24 transactions / 24 hours (i.e., one per	1600

meters)	hour)	
multiple interval meter read data (Residential gas smart meters)	6 transactions / 24 hours	2400
multiple interval meter read data (Residential electric smart meters)	6 transactions / 24 hours	2400
on-demand read request app errors	(25/1000+10)1000	50
on-demand meter read data	25 transactions /1000 smart meters	100
send service switch operate acknowledgment	2 transactions /1000 smart meters	25
send service switch operate failure	1/1000 * 50/1000	50
send metrology information after a successful service switch operate	2 transactions /1000 smart meters	100
send service switch state data	50 transactions /1000 smart meters	100

Step 5 - Assume (and document) values for missing information
There is still some information not available from the user applications matrix. For example to calculate the aggregate traffic from a single smart meter to a DAP, the type of smart meter is needed, also the number of smart meters that will be sending their data to a single DAP is needed.

- How many Smart Meters?
    - What proportion of types of smart meters?
        - Commercial / Industrial Gas smart meters,
        - Commercial / Industrial Electric meters,
        - Residential gas smart meters, and
        - Residential electric smart meters.

Assume 1000 smart meters attached to a DAP
Assume the following proportions of types of smart meters:

Commercial / Industrial Gas smart meters	6.5%
Commercial / Industrial Electric meters	17.4%
Residential gas smart meters	6.5%
Residential electric smart meters	69.6%
Total	100%

Step 6 - Calculate the aggregate traffic using selections and assumptions
Using the selected values from **step 4** and the assumed values from **step 5,** the aggregate traffic for each direction is calculated below each of the following tables.

Table 4: DAP to Smart Meter direction

Event	How often	Size (bytes)	
multiple interval meter reading request	25 transactions /1000 smart meters	25	0.625
on-demand meter read requests	25 transactions /1000 smart meters	25	0.625
cancel service switch operate request	2 transactions /1000 smart meters	25	0.05

service switch operate request	50 transactions /1000 smart meters	25	1.25
service switch state request	50 transactions /1000 smart meters	25	1.25
Total	0.152 events / smart meter	N/A	3.8

Mean message size in bytes = 3.8 / 0.152 = 25
Number of events per meter per second = 0.152 / 86400 = 1.76×10^{-6}

Table 5: Smart Meter to DAP direction

Event	How often	proportion	Size (bytes)	
multiple interval meter read data (Commercial / Industrial Gas smart meters)	6 transactions / 24 hours	0.065	2400	936
multiple interval meter read data (Commercial / Industrial Electric meters)	24 transactions / 24 hours (i.e., one per hour)	0.174	1600	6681.6
multiple interval meter read data (Residential gas smart meters)	6 transactions / 24 hours	0.065	2400	936
multiple interval meter read data (Residential electric smart meters)	6 transactions / 24 hours	0.696	2400	10022.4
Subtotal	Frequency * proportion =	9.132	Frequency * Size * proportion =	18576
on-demand read request app errors	(25/1000+10)1000		50	0.50125
on-demand meter read data	25/1000		100	2.5
send service switch operate acknowledgment	2/1000		25	0.05
send service switch operate failure	1/1000 * 50/1000		50	0.0025
send metrology information after a successful service switch operate	2/1000		100	0.2
send service switch state data	50/1000		100	5
Total	9.221075		N/A	18584.25

Mean message size in bytes = 18584.25 / 9.221075 = 2015.411
Number of events per meter per second = 9.221075 / 86400 = 1.07×10^{-4}

4 Wireless Technology

[Bruce will generate an example for everyone else to follow]

See wireless spreadsheet

Create narratives for the content of the contents of the spreadsheet

DSSS vs FHSS vs OFDM

security

5 Evaluation approach / Modeling approach

[David Cypher / NIST]
Determining an assessment method for evaluating whether a wireless technology can satisfy the smart grid user applications' requirements is a daunting case, especially given that there are so many possibilities for the actual physical deployment of the smart grid devices and facilities, the option laden wireless technology standards, and the uncertainty in planning for future needs.

Some wireless technologies are a part of a larger system, while others are complete communication networks. For example wireless technologies developed by the IEEE 802 consider mostly the Media Access Control (MAC) sublayer and Physical Layer (PHY), while the Universal Mobile Telecommunications System (UMTS) is a complete mobile (and wireless) network system. This makes comparing wireless technologies impractical. For this reason, an individual wireless technology is assessed on whether it can satisfy the smart grid user applications requirements and not a ranking of how well the various wireless technologies compare with each other for the smart grid.

The initial assessment is based on the smart grid user applications' requirements provided in 3.4 and the wireless functionality and characteristics provided in 4. For example a user application's requirement (performance metric) of a reliability needs to be somehow related to the wireless technology's link availability (ability to reliably establish an appropriate device link and ability to maintain an appropriate connection). This initial assessment may be used to determine whether a candidate wireless technology should be considered further.

The next step is to refine the assessment using other methods (i.e., mathematical models, event-driven simulation models, or experimental measurements). Mathematical models usually take less time to produce results than event-driven simulation models. However simulation models may provide more realistic results than mathematical models since they model the details of the protocol behavior. The major problem that both of these models suffer from is how to model a realistic situation (e.g., accurate channel model). This is where the use of a testbed can provide better results. However, this method requires the most time to produce results.

Regardless of the method used, any evaluation model needs to consider the following components, which are: the network topology and traffic characteristics, the channel propagation and the network consisting of the various protocol layers, for example, MAC and PHY.

Figure 3: Evaluation Building Blocks provides an illustration of this.

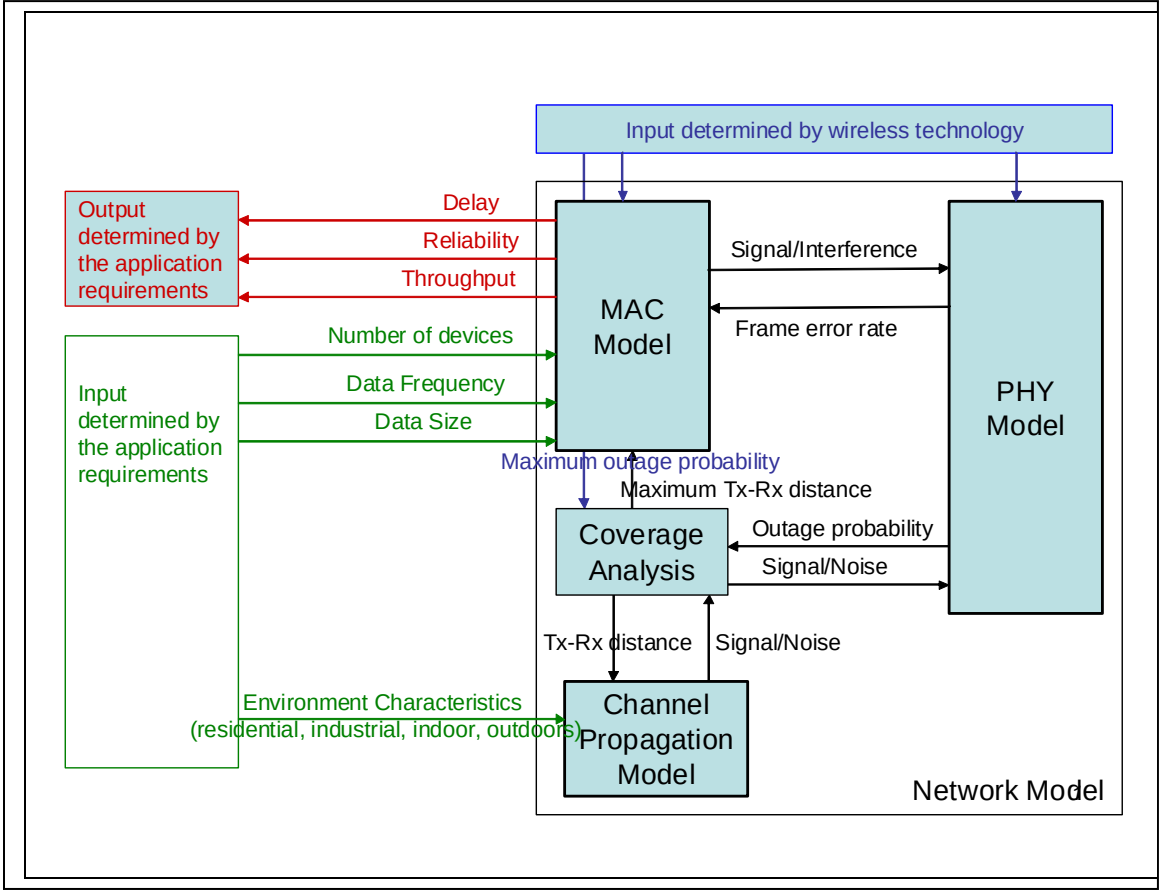

Figure 3: Evaluation Building Blocks
Note: Replace signal/noise in figure with path loss.

5.1 Channel Models

[Mostofa to provide input on this section with help from NIST]

Channel models describe the signal propagation through the wireless environment and the impairments imposed by the environment including noise, fading, shadowing, and interference.

The environments considered are categorized according to the placement of the transmitter-receiver pair as indoor-indoor, outdoor-outdoor, and outdoor-indoor. The channel propagation path between the pair is characterized by the dual-slope path loss model. It is more flexible than the single-slope model and so can reflect a wider range of environments. The deterministic component of the path loss *PL* (dB) is a function of the distance *d* (m) between the transmitter and receiver and is defined as follows:

$$PL(d) = PL_0 + \begin{cases} 10n_0 \log_{10}(d/d_0), & d \le d_1 \\ 10n_0 \log_{10}(d_1/d_0) + 10n_1 \log_{10}(d/d_1), & d > d_1 \end{cases}$$

where PL_0 (dB) is the reference path loss at $d_0 = 1$ m and d_1 (m) is the breakpoint where the path loss exponent adjusts from n_0 to n_1.

The path loss model with shadowing PL_S (dB) includes the stochastic shadowing parameter *S* (dB) which varies according to a zero-mean Normal distribution with standard deviation σ:

$$PL_S(d) = PL(d) + S,$$
$$S \sim N(0, \sigma)$$

Figure 4: shows the extraction procedure of the model from the data points. The PL in red is fit to the blue data points collected in an indoor-indoor residential environment at $f_c = 5$ GHz. The deviation of the data points from the line represents the shadowing effect.

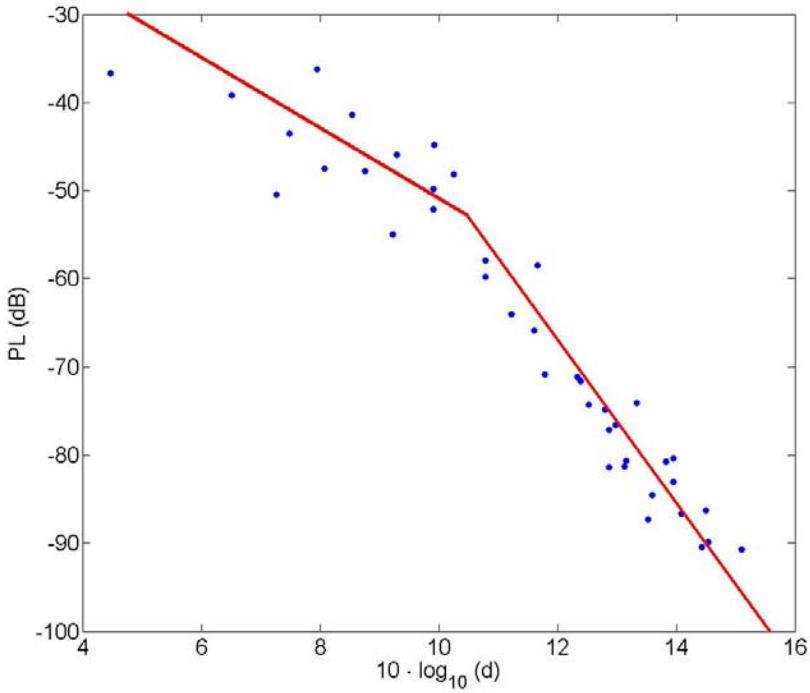

Figure 4: The dual-slope path loss model in an indoor-indoor residential environment at f_c = 5 GHz

In the next subsections channel propagation model parameters are presented for a host of environments, which may be representative of several smart grid domains. The model parameters were extracted from data collected in a series of measurement campaigns conducted by the Radio Frequency (RF) Fields Group in the Electronics and Electrical Engineering Laboratory at NIST. The measurements were conducted in the 2.4 GHz and 5 GHz unlicensed bands common to many technologies.

5.1.1 Indoor-indoor environments

Indoor-indoor data has been gathered for *residential*, *office*, *industrial*, and *cinder block* environments. The details of the measurement system, procedure, and campaign are described in [1,2]. The five model parameters are listed in Table 6: Indoor-indoor environments. Each environment is further differentiated into line-of-sight (LOS) and non-line-of-sight (NLOS) conditions. Note that in some environments the dual-slope model simply collapses to the single-slope model by setting $n_1 = n_0$ and arbitrarily choosing $d_1 = d_0$.

Table 6: Indoor-indoor environments

environment		f_c = 2.4 GHz					f_c = 5 GHz				
		PL_0	n_0	D_1	n_1	σ	PL_0	N_0	d_1	n_1	σ
LOS	*residential*	16.3	2.2	1	2.2	2.4	17.9	1.7	1	1.7	1.5
	office	22.8	1.2	1	1.2	1.7	17.5	1.9	1	1.9	1.1
	industrial	22.4	1.1	1	1.1	2.1	15.2	1.8	1	1.8	1.2
	cinder block	24.2	1.5	1	1.5	2.8	12.7	2.5	1	2.5	1.6
NLOS	*residential*	12.5	2.2	11	5.6	3.0	20.2	2.4	11	5.4	3.3
	office	26.8	2.2	10	6.7	3.7	26.0	2.3	10	8.1	4.0
	industrial	29.4	1.4	1	1.4	6.3	27.5	1.7	1	1.7	6.7
	cinder block	9.1	4.9	1	4.9	6.7	7.8	5.3	1	5.3	7.7

5.1.2 Outdoor-outdoor environments

Outdoor-outdoor data has been gathered for *oil refinery* and *urban-canyon* environments. The details of the measurement system, procedure, and campaign are described in [3,4]. The model parameters are listed in Table 7: Outdoor-outdoor environments. In the *oil refinery* environment, the propagation paths before the breakpoint were in LOS, while those after the breakpoint traversed dense metal piping. This explains the large discrepancy between n_0 and n_1 there.

Table 7: Outdoor-outdoor environments

environment	f_c = 2.4 GHz					f_c = 5 GHz				
	PL_0	n_0	D_1	n_1	σ	PL_0	n_0	d_1	n_1	σ
urban-canyon / LOS	6.9	1.7	1	1.7	2.4	15.2	1.6	1	1.6	2.7
urban-canyon / NLOS	21.3	1.6	1	1.6	7.4	20.7	2.1	1	2.1	7.5
oil refinery	16.8	0.4	87	12.2	2.3	3.0	1.3	87	12.9	3.3

5.1.3 Outdoor-indoor environments

Outdoor-indoor data has been obtained for *office*, *high-rise building*, *convention center*, and the *Greathouse mine tunnel* environments. The details of the measurement system, procedure, and campaign are described in [3]. The model parameters are listed in Table 8: Outdoor-indoor environments. By virtue of the outdoor-indoor environment, all parameters are for non-line-of-sight conditions. In the *office* environment, measurements were not available at 5 GHz. Also, since no data points were collected there before d_1 = 70 m, we just assumed free space (n_0 = 2.0) for distances before the breakpoint. In the *mine-tunnel* environment, the propagation paths before the breakpoint were in LOS, while those after were in NLOS where penetration is difficult given the thickness and density of the mine walls. This explains the very large discrepancy between n_0 and n_1 there.

Alternatively, an outdoor-indoor environment can be composed from an indoor-indoor segment, an outdoor-outdoor segment, and a fixed penetration loss to account for the transition through the building material. Reference [5] provides an extensive list of penetration losses at a number of center frequencies.

Table 8: Outdoor-indoor environments

environment	f_c = 2.4 GHz					f_c = 5 GHz				
	PL_0	n_0	D_1	n_1	σ	PL_0	n_0	d_1	n_1	σ
office	0.2	2.0	70	4.2	3.3	NA	NA	NA	NA	NA
high-rise	8.8	2.2	1	2.2	5.6	9.2	3.3	1	3.3	4.8
convention center	4.2	0.6	100	3.7	4.6	15.5	0.8	100	7.6	3.6
mine tunnel	5.7	0.7	70	18.3	5.8	1.3	0.2	70	23.4	4.3

5.2 Physical Layer

The main purpose of the physical layer is to provide a coverage analysis and to predict the maximum range of a wireless technology for a given outage probability and a specified set of operating parameters. The range of a wireless technology can help to determine its suitability for linking a particular pair of actors, the number of actors it can support in a point-to-multipoint arrangement, and the resulting network topology.

The outage criterion is the probability that the wireless transmitter-receiver link is not operational. It is expressed in terms of a probability because of the unpredictable behavior of RF propagation, which is often modeled as a stochastic process when accounting for the possible losses due to obstructions (shadowing) and reflections (multipath fading).

In the context of a point-to-multipoint wireless technology, coverage is often analyzed in terms of the maximum cell radius that a base station (BS) or access point (AP) can support. Within the cell, the outage probability varies, generally increasing as a terminal approaches the cell edge. In the analysis below, the outage criterion is expressed in terms of the average outage probability, averaged over all locations in the coverage area. Thus, a reported outage probability of 1%, for example, means that a terminal located at a random point in the cell has a 1% chance of being in outage.

We define the outage probability as the probability that the received signal-to-noise-ratio (SNR) is below the required SNR to operate the link. The required SNR depends on the wireless technology under consideration and serves as an input to the analysis. The received SNR is modeled as a deterministic component, based on transmitter-receiver separation distance, attenuated by random components due to shadowing and fading. For the distance-based component, we assume a dual slope model of path loss with distance. For the shadowing, we assume a lognormal distribution, and for the fading, we assume a Nakagami distribution of the fading envelope.

5.3 MAC sublayer

The MAC model describes the behavior of the medium access control protocol as it receives data from the higher layers and presents them on the shared medium.

5.4 Example Modeling Tool

[NIST]

An example modeling tool implementing this evaluation approach was developed at NIST. The MAC model developed by NIST is specifically designed for the 802.11 (baseline), as an example. However the PHY model is not specific to 802.11.
Our model of the IEEE 802.11 MAC layer is derived from Bianchi's seminal model [8], which developed a Markov chain representation for the state of a given station's backoff

counter but which assumes that all stations were in saturation. Stations are allowed up to α retransmissions of a frame if the first attempt fails. If a transmission attempt fails, which occurs with probability P_{fail}, the station chooses a random backoff if it has retransmission attempts remaining. If, after α +1 attempts, the station fails to send the frame, it drops the frame.

To account for both the non-saturated state of a typical station and the effect of a finite buffer in each station, we use the enhancements to the Bianchi model that were developed by Zhai et al. in [9]. The extensions in this model include the use of probability generating functions (PGFs) to obtain expressions for the various contributions to the MAC-layer delay and the use of a queuing model to obtain performance metrics such as the probability that a station is idle, the expected time that a frame spends in the buffer, and the probability that a frame is dropped because the buffer is full.

Daneshgaran et al. [10] developed an extension to the Bianchi model that also eliminated the saturated station assumption. In addition, their model considered the possibility that a station could capture the channel and successfully transmit its frame, even during a collision event, provided that its power as received by the access point (AP) was sufficiently greater than that of the other stations. Our model also incorporates this capture effect, however rather than decouple the collision and channel capture from a frame loss due to channel effects, we consider them as statistically dependent events.

Finally, because the applications which we are considering result in traffic flows in both directions on every link in the network, we extended the model to account for the effect of traffic on the downlink, i.e., from the AP to the stations. Because IEEE 802.11 is typically implemented as a half duplex link, our model now accounts for the fact that a network entity can be in either transmit or receive mode, but cannot perform both functions simultaneously. Thus, an AP that is transmitting to a station will not receive any frames that are being sent on the uplink, i.e., from a station to the AP; this will result in unacknowledged frames that the stations will treat as collisions. A version of the half-duplex link model was developed by Jin et al. [11], but this model assumes that the stations and the access point are all in saturation. The complete description of our model can be found in [12].

5.5 Other Tools

6 Findings / Results

Does wireless technology X meet SG-Network requirements
Performance Metrics
- Reliability
- Latency
- Scalability
- meets throughput needs
- handles the number of devices needed
- range
- interference immunity

By actor to actor / Link by link which is the best to use

How does its work in urban, sub-urban, rural
How well does it propagate (e.g. walls, basements, vaults, clutter, hills)
scalability over a quantity of end points

Equipment required to operate
Include processing time between actor to actor

Figure 5: Sample Outage results at 2.4 GHz plots sample results for the average outage probability

$$\overline{P_{\text{out}}} = \frac{1}{R_{\text{max}}^2 - R_{\text{min}}^2} \int_{R_{\text{min}}}^{R_{\text{max}}} P_{\text{out}}(r)\, 2r\, dr \,. \tag{6}$$

as a function of the maximum coverage radius, R_{max}, and for R_{min} = 10 m. Outage curves for three cases are shown, all at 2.4 GHz: (i) the indoor residential non-line-of-sight (NLOS) environment (row 2 of Table II) at typical transmit power, (ii) the outdoor urban NLOS environment (row 4 of Table II) at typical transmit power, and (iii) the same outdoor environment but operating at the maximum permitted EIRP for the unlicensed 2.4 GHz band. In each case, the fading is Rayleigh (i.e., Nakagami fading parameter m = 1). The values for the remaining technology-specific parameters used in this example are listed in Table III and generally correspond to the IEEE 802.11 standard operating at 1 Mb/s.

Environment	PL_0 (dB)	n_0	d_1 (m)	n_1	σ (dB)
Indoor residential LOS	16.3	4.2	N/A	N/A	2.4
Indoor residential NLOS	12.5	4.2	11	7.6	3.0
Indoor industrial NLOS	29.4	3.4	N/A	N/A	6.3
Outdoor urban-canyon NLOS	21.3	3.6	N/A	N/A	7.4
Indoor-outdoor convention center NLOS	4.2	2.6	100	5.7	4.6

TABLE II
PATH LOSS PARAMETERS AT 2.4 GHZ FOR SEVERAL ENVIRONMENTS

TABLE III
PHY PARAMETER VALUES USED FOR FIG. 4

PHY Model Parameter	Symbol	Value
PHY data rate	R_b	10^6 b/s
Required E_b/N_0	$(E_b/N_0)_{\mathrm{req,dB}}$	10.4 dB
Receiver noise figure	F	5 dB
Temperature	T_0	293 K
System losses	$L_{\mathrm{s,dB}}$	1.5 dB

Figure 5: Sample Outage results at 2.4 GHz shows that, for this example, the outdoor coverage radius corresponding to a 1% outage probability is 220 m at moderate transmission power and nearly 500 m at maximum transmission power. Furthermore, the indoor range is clearly sufficient for most indoor residential environments.

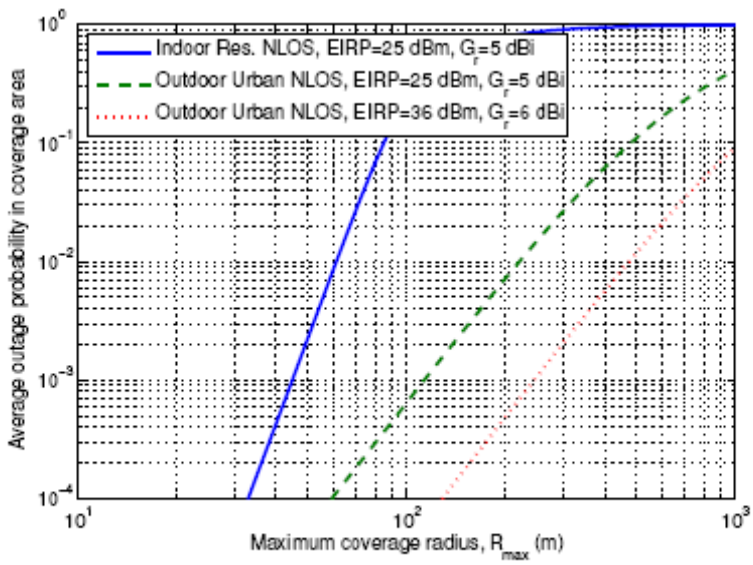

Fig. 4. Sample outage results at 2.4 GHz

Figure 5: Sample Outage results at 2.4 GHz

Consider again the example physical link topology of the Smart Grid network illustrated in Figure 6: Example physical link topology. The 12 actors are grouped into Operations and Customer domains connected through Data Aggregation Points (DAP). The network contains a total of 1000 smart meters (SM), each logging data from the IHD, PHEV, and Customer EMS actors of the Customer domain. The latter three contend for the same channel so that their combined mean arrival rate is 4.8 x 10^{-4} messages/s and their combined mean message size is 61.3 bytes. Further, each DAP serves 25 meters for a total of 40 DAPs in the network. This makes for additional contention between the SMs for access to the DAP and between the DAPs for access to the AMI Head End. All other actors in the network are represented singularly.

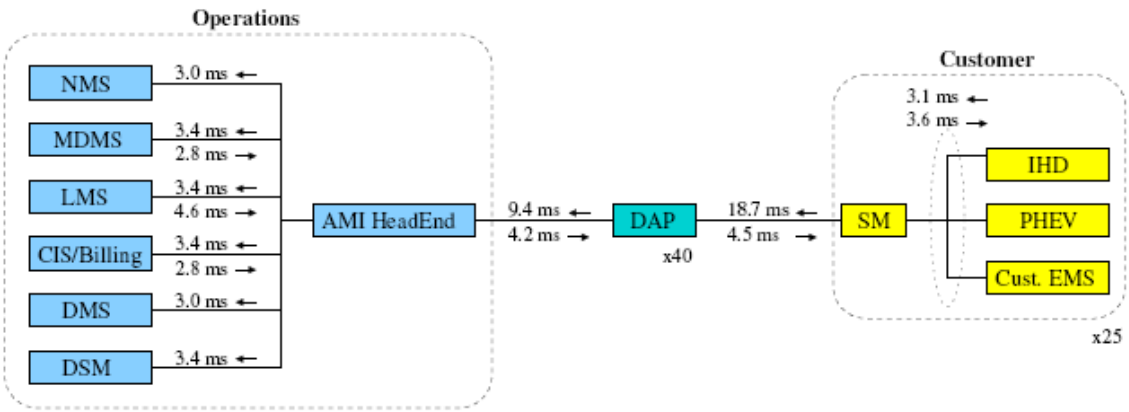

Fig. 3. Example physical link topology

Figure 6: Example physical link topology

For illustrative purposes only, the network was analyzed assuming that all the actors communicate through an 802.11 wireless link[3]. Under this assumption, our 802.11 analysis tool processed the traffic parameters of each link and returned its reliability and mean delay. The reliability is defined as the probability that once the message is generated or relayed by actor j, it is successfully transmitted and received by actor k. The mean delay is the time required to complete this sequence of events.

Since network loading was very light, the reliability for all link flows was essentially 1. The mean delay is shown on each link in Figure 6: Example physical link topology. Note that the messages between the AMI Head End and NMS, DMS, and the DSM flow only in one direction.

7 Conclusions

1) Smart Grid Standards are Smart Business
2) Standards are great, everyone has one
3) Don’t touch downed power lines

8 References

ISO/IEC27001 - International Organization for Standardization/International Electrotechnical Commission Standard 27001 –Information technology -- Security techniques -- Information security management systems -- Requirements

NIST Special Publication 1108 - NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0∗, January 2010

Second DRAFT NIST IR 7628 Smart Grid Cyber Security Strategy and Requirements

http://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Forms/AllItems.aspx?RootFolder=http%3a%2f%2fosgug%2eucaiug%2eorg%2fUtiliComm%2fShared%20Documents%2fInterium%5fRelease%5f2&FolderCTID=0x012000D61E6400383B0E4DA3A3454503972C5A

9 Bibliography

[1] C. Gentile, S.M. Lopez, and A. Kik, “A Comprehensive Spatial-Temporal Channel Propagation Model for the Ultra-Wideband Spectrum 2-8 GHz,” *IEEE Global Telecommunications Conf.,* pp. 1-6, Dec. 2009.
[2] http://www-x.antd.nist.gov/uwb
[3] W.F. Young, K.A. Remley, J. Ladbury, C.L. Holloway, C. Grosvenor, G. Koepke, D. Camell, S. Floris, W. Numan, A. Garuti, "Measurements to Support Public Safety Communications: Attenuation and Variability of 750 MHz Radio Wave Signals in Four Large Building Structures," *Natl. Inst. Stand. Technol. Note 1552*, Aug. 2009.
[4] D.W. Matolak, K.A. Remley, C. Gentile, C.L. Holloway, Q. Wu, and Q. Zhang, “Ground-Based Urban Channel Characteristics for Two Public Safety Bands,” *Submitted to IEEE Trans. on Antennas and Propagation*, Dec. 2009.
[5] T.S. Rappaport, “Wireless Communications,” *Prentice-Hill, Inc.*, pp. 124-125, 1996.

[8] Bianchi, G., “Performance analysis of the IEEE 802.11 distributed coordination function,” IEEE Journal on Selected Areas in Communications, vol. 18, no. 3, pp. 535–547, 2000.

[9] Zhai, H.Q., Kwon, Y.G., and Fang, Y.G., “Performance analysis of IEEE 802.11 MAC protocols in wireless LANs,” Wireless Communications and Mobile Computing, vol. 4, no. 8, pp. 917–931, 2004.

[10] Daneshgaran, F., Laddomada, M., Mesiti, F., and Mondin, M., “Unsaturated throughput analysis of IEEE 802.11 in presence of non ideal transmission channel and capture effects,” IEEE Transactions on Wireless Communications, vol. 7, no. 4, pp. 1276–1286, April 2008.

[11] Jin, H., Jung, B.C., Hwang, H.Y., and Sung, D.K., “A throughput balancing problem between uplink and downlink in multi-user MIMObased WLAN systems,” in Proc. IEEE WCNC, pp. 17951800, April 2009.

[12] Griffith, D., Souryal, M., Gentile, C., and Golmie, N., “An integrated PHY and MAC layer model for half-duplex IEEE 802.11 networks”, submitted to IEEE Military Communications Conf., April 2010.