Cybersecurity and Privacy in an Interconnected, Intelligent Efficiency World

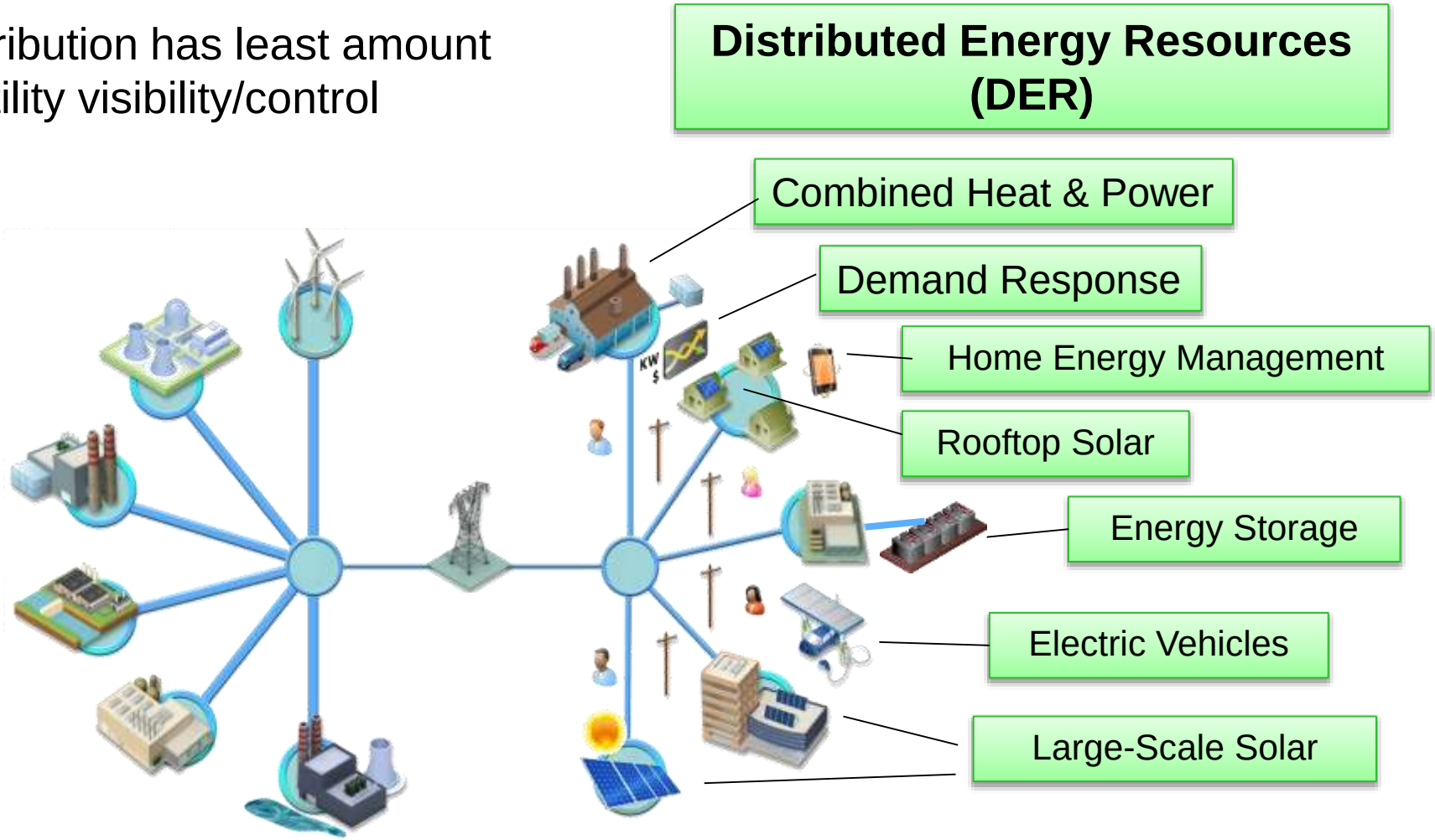
September 15, 2015

Galen Rasche
Sr. Program Manager

grasche@epri.com

The Landscape

- Most new generation connecting at grid “edge”
- The “edge” is the distribution system
- Distribution has least amount of utility visibility/control



Trends Impacting Security

- Increased number of Internet connected systems and devices
- Increased capability of equipment in the field
- Connections with more business players
- Attacks from economic criminals, nation states, and terrorist organizations

EPRI Smart Thermostat Project Analytics Project

Smart Thermostat Project Analytics

"Traditional"

- Premise-level data
- Seasonal/Annual
- Controlled Pilots

"Data-driven"

- Thermostat-level & other data
- Real-time (or more so)
- Applications: RT M&V, others…

Insights and Complexity of the New Data Paradigm

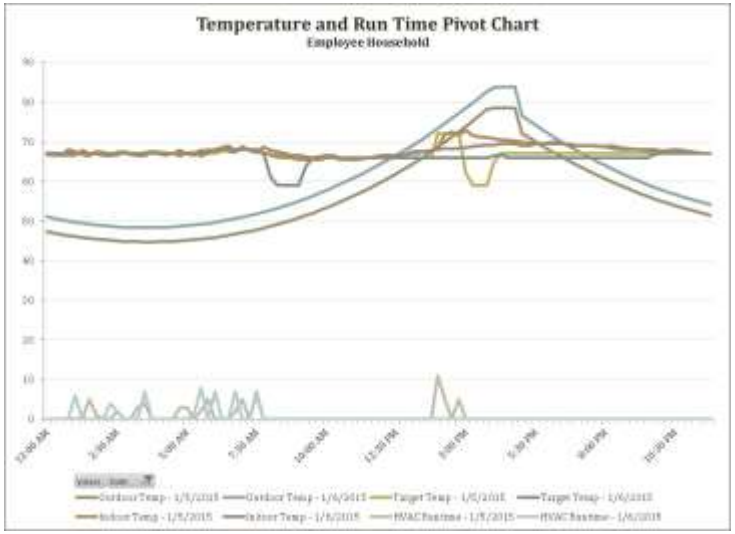
- Single AMI data stream to multiple asynchronous data streams
- Leverage data from different sources to better understand customer behavior and grid uses
- Data privacy and confidentiality should be a primary concern
- Development of new tools and analytical treatments

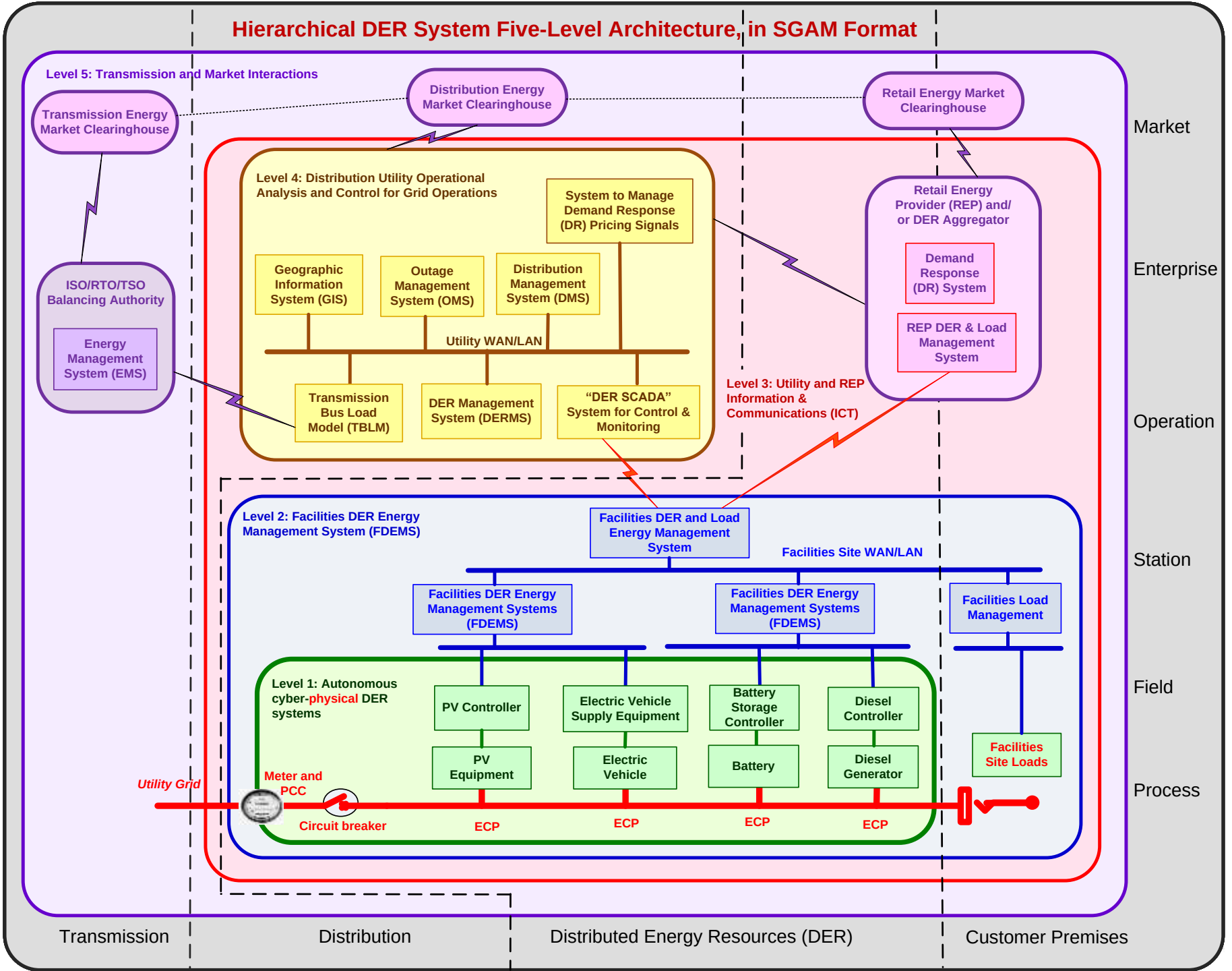
Time stamp to be synced		AMI Data	Device 1 data		Weather data	Device 2 data			Survey data
User ID	Time	Meter Read (kWh)	Indoor Temp	Set point	Out door temp	Cool Run time (min)	Fan On time	Over-ride	Expected DR set point
1234	4/5/2015 5:00 PM	13456.2	72.3	76	94	0	15	No	78
1234	4/5/2015 5:15 PM	13458.4	72.4	76	95	0	15	No	78
1234	4/5/2015 5:30 PM	13460.2	72.4	76	94	5	5	No	78

Sample Use Cases for Data from Customer Resources

- Understanding customer preferences
- M&V 2.0 – Real time performance verification for EE & DR
- Optimizing DR potential
- Flexible Load Operations
- Locational load control
- Understand changing load usage
- Analyzing rate structures
- Customer Targeting for EE & DR programs
- Understanding micro-level EE & DR potential

Figure 4: Auxiliary Heat usage is avoided by stepping the setpoint incrementally




Hierarchical DER System Five-Level Architecture, in SGAM Format
Level 5: Transmission and Market Interactions
Transmission Energy Market Clearinghouse
Distribution Energy Market Clearinghouse
Retail Energy Market Clearinghouse
Market
Level 4: Distribution Utility Operational Analysis and Control for Grid Operations
System to Manage Demand Response (DR) Pricing Signals
Geographic Information System (GIS)
Outage Management System (OMS)
Distribution Management System (DMS)
Utility WAN/LAN
Transmission Bus Load Model (TBLM)
DER Management System (DERMS)
"DER SCADA" System for Control & Monitoring
ISO/RTO/TSO Balancing Authority
Energy Management System (EMS)
Retail Energy Provider (REP) and/ or DER Aggregator
Demand Response (DR) System
REP DER & Load Management System
Enterprise
Level 3: Utility and REP Information & Communications (ICT)
Operation
Level 2: Facilities DER Energy Management System (FDEMS)
Facilities DER and Load Energy Management System
Facilities Site WAN/LAN
Facilities DER Energy Management Systems (FDEMS)
Facilities DER Energy Management Systems (FDEMS)
Facilities Load Management
Station
Level 1: Autonomous cyber-physical DER systems
PV Controller
Electric Vehicle Supply Equipment
Battery Storage Controller
Diesel Controller
PV Equipment
Electric Vehicle
Battery
Diesel Generator
Facilities Site Loads
Field
Utility Grid
Meter and PCC
Circuit breaker
ECP
ECP
ECP
ECP
Process
Transmission
Distribution
Distributed Energy Resources (DER)
Customer Premises

Threat Model and Security Challenges

Threat Model

- Adversaries with intent
- Insiders or outsiders, groups or individuals
- Failure in people, processes, and technology, including human error
- Loss of resources, in particular key employees or communications infrastructure
- Accidents
- Natural hazards as they impact cyber security

Threat Agents

- Economic Criminals
- Malicious Criminals
- Recreational Criminals
- Activist Groups
- Terrorists
- Hazards

Recent IoT Vulnerabilities

Jeep Hack: Fiat recalls 1.4 million vehicles for software fix

by Chris Matthews @crobmatthews JULY 24, 2015, 11:41 AM EDT

Fortune

Samsung's smart fridge could be used to steal your Gmail login

by Stacey Higginbotham @gigastacey AUGUST 24, 2015, 1:10 PM EDT

Fortune

#IoTsec Disclosure: 10 New Vulnerabilities for Several Video Baby Monitors

Posted by Tod Beardsley in Information Security on Sep 2, 2015 9:28:04 AM

Moving Forward…

- Address **interconnected systems** – both IT and control systems
  - Cyber security needs to be addressed in all systems, not just critical assets
  - Augment existing protection controls, as applicable
- Continuously **monitor and assess** the security status
- Ensure that devices can be upgraded to patch vulnerabilities
- Acknowledge will be some security breaches
  - Focus on response and recovery
  - *Fail secure*
    - Address both safety and security

Together…Shaping the Future of Electricity