GE Grid Solutions

Cyber Security

John D. McDonald, P.E.

Smart Grid Business Development Leader – North America
Global Smart Grid Strategy Group

IEEE Life Fellow
IEEE PES Substations Committee Chair (2000-2001)
IEEE PES President (2006-2007)
IEEE Division VII Director (2008-2009)
IEEE-SA Board of Governors (2010-2011)
IEEE Smart Grid Steering Committee
CIGRE USNC VP, Technical Activities

IEEE PES Green Mountain Chapter
June 8, 2017

imagination at work

Cyber Security Introduction

Failure Mode and Effects Analysis of Security

1. Function: Describe the function to be analyzed to secure against a specific cyber incident.
2. Failure Mode: Understanding the threat
3. Failure Causes: Understanding the types of attacks
4. Identify Failure Effects and Criticality: How serious are the consequences
5. Understand Solutions: What are the current methods of securing against the attack?
6. Match solution to analysis: Establish a Security system to match the analysis

Understanding the Threat

- *Protecting against -*
  - *The Hacker*
  - *The Vandal*
  - *The Terrorist*
  - *The Disgruntled Employee*
  - *The Competitor*
  - *The Customer*
  - *The Security System*

Types of attack -

- *Eavesdropping*
- *Traffic Analysis*
- *Replaying*
- *Spoofing*
- *Cracking*
- *Social Engineering*
- *Denial of Service*
- *Destruction*
- *Reconfigure*
- *Malware*

Understanding Consequences and Risks

- Analysis of Areas of Attack:
- Control – Take control of switches (meters or substations)
- Information – Interrupt or corrupt data flow
- Configuration – Change configuration to open door for future action
- Safety – Compromise safety of people or things

Protect – Detect - Respond

- Need to properly implement . . .
  - Boarder/Network Security
  - Intrusion Detection System (Passive)
  - Intrusion Prevention System (Active)
  - Configuration & Firmware Management
  - Data Security (Static & Dynamic)
  - Event Management & Logging
  - Authentication & Role Based Access Control
  - Patch Management System

Factors of Authentication

1. **What You Know** – Passwords are widely used to identify a User, but only verify that somebody knows the password.
2. **What You Have** – Digital certificates in the User's computer add more security than a password, and smart cards verify that Users have a physical token in their possession, but either can be stolen.
3. **What You Are** – Biometrics such as fingerprints and iris recognition are more difficult but not impossible to forge.
4. **What You Do** – Dynamic biometrics such as hand writing a signature and voice recognition are the most secure; however, replay attacks can fool the system.

Summary

NERC and Corporate Security Requirements
Functions to Protect
Understanding the threat
Understanding the types of attacks
How likely and serious are the consequences
Security methods
Deploy a matching solution

Case Study: Hacking a GE Industrial Ethernet Switch

Reputation Effects from Media and Tech Conferences

Security (Hacking) Demo

ML800 Managed Switch

- A hard-coded session key can allow a user to access administrative interface without authentication.
- This demo will show the benefit of the patch / firmware update. We will:
  - Perform Man-in-the-Middle attack
  - Use the hard-coded session key to gain administrative access
  - Repeat process on patched ML800

imagination at work

Vulnerability Messages

GE
Grid Solutions

Hard-coded Credentials Vulnerability
ML800/1200/1600/2400
ML810/3000/3100

Product Bulletin

Date: May 31, 2016 CVE : CVE-2016-2310

GE Publication Number: GET-20042

Overview

A vulnerability has been identified in the GE MultiLink ML800 managed switch that could result in unauthorized access. GE's Grid Solutions business unit has validated the vulnerability through testing and confirmed that the issue affecting the ML8
ML1600, ML2400,

This product bulle
bulletin has been r

Background

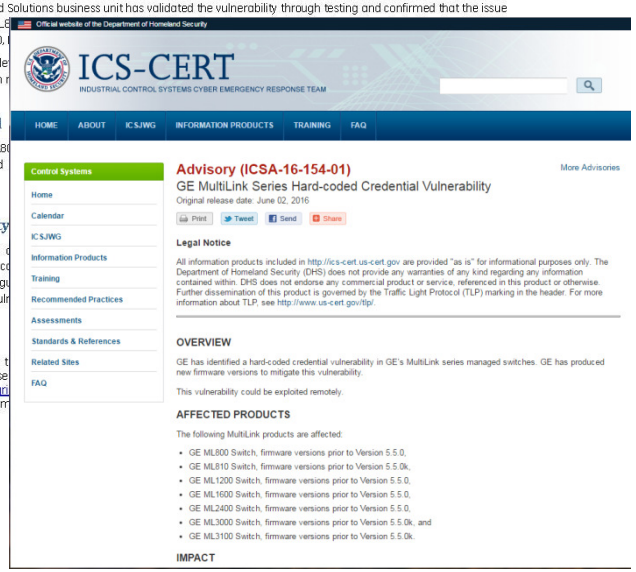
The MultiLink ML8
applications and
environments.

Vulnerability

GE has received
bypass the web c
the device configu
interface. The vul

Mitigation

GE recommends t
vulnerability. Use
https://www.geari
the contact inform



GE Digital Energy

RSA Private Key & DoS Vulnerabilty
ML800/1200/1600/2400
ML810/3000/3100

Product Bulletin

Date: January 6, 2015 **Classification:** General ICS-CERT Advisory: ICSA-15-013-04
Updated: September 8, 2015
GE Publication Number: GET-20024A

Overview

Three vulnerabilities were identified in the GE MultiLink ML800 managed switch that could result in unauthorized access or denial of service. GE Digital Energy has validated these vulnerabilities through testing and confirmed that the issues affecting the ML800 also affect the MultiLink series of managed Ethernet switches including the ML1200, ML1600, ML2400, ML810, ML3000, and ML3100. These vulnerabilities have been publicly disclosed.

This product bull
vulnerabilities, ar
have been resol
bulletin to inform

Background

The MultiLink ML
applications and
environments.

Researcher Eire
coordinated his
Emergency Resp
these vulnerabili
ML800, ML1200,

Additionally, Mr.
cross-site scripti
ML810, ML3000 &

Vulnerability

The three confir
firmware, 2) the
interrupted (DoS
into response pa

Vulnerability Response – ML800 Series

CVSS = 10.0

Product

Energy Connections - ML800

Hardened managed Ethernet switch
Provides high-speed networking w/ management functions for industrial protocols & applications. Used in industrial facilities & substations.

Vulnerability report

Date received: 1-13-2016
Researcher: Jason Larsen (IOActive)
Business unit: EC - Grid Solutions
PSL: Ron Wiederhold

Vulnerability: Hard-coded credential that could be used to bypass the web configuration access controls; could allow a user to gain administrative access to the device configuration resulting in exposure and control of all configuration options available.

1/13 – Receive
- ✓ Report ack. & sent to biz

1/29
- ✓ Vuln replicated

2/22 – Assess
- ✓ Vuln fix

4/12
- ✓ QA testing comp.
- ✓ DRAFT advisory/review
- ✓ ICS-CERT coord.

5/31 – Resolve
- → Release date
- → Fix & comms released

6/14 – Closeout
- → Monitoring – customer inquiries

Remediation

Overview

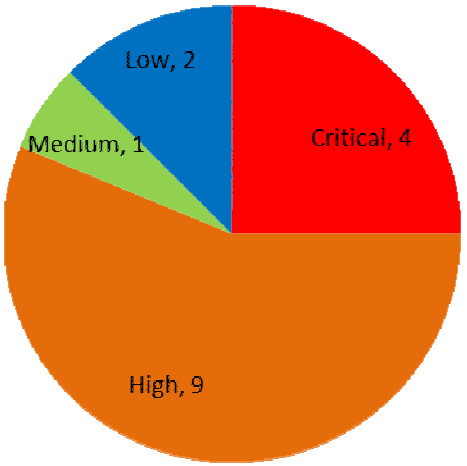
- ✓ GE publication number: GET - 20042
- ✓ CVE: 2016-2310 has been assigned
- ✓ Legal & comms review of GE & ICS-CERT advisories
- ✓ Holding statement prepared

Mitigation

- **Upgrade device firmware:** GE recommends users to upgrade the device firmware to version 5.5.0 https://www.gegridsolutions.com/app/ViewFiles.aspx?prod=ml800&type=7

Lessons Learned

- Develop a good rapport with the Researcher(s)
- Researcher's findings are often "Low Hanging Fruit"
- Security assessment, afterwards revealed additional security vulnerabilities
- We spent a lot of time and effort – working with researchers, PSIRT, ICS-CERT, etc. - that could have been avoided



Product - Secure Development Lifecycle (SDL)

Design & Architecture	Development	Test	Manufacture	Incident Management
Design Security into the Products •Security Requirements •Identify roles & malicious roles •Develop use and abuse cases •Identify security features •Threat Modeling	Build Security into the Product •Training for Developers •Use Secure Coding Practice (e.g. OWASP) •Build with Static Code Analysis Tool	Test for Security & Resiliency •Dynamic security testing (Fuzzing); i.e., Achilles Communication Certification (ACC) •Security Assessments or Penetration Testing	Securely Manufacture the Product •Follow stringent manufacturing practices (build as designed) •Develop and provide secure deployment practices document	Manage externally identified issues •Validate report •Develop Remediation Plan •Provide Updates, Patches, etc. •Communicate to product owners

imagination at work

Case Study:
Ukraine Power Outage

Ukraine Power Outage - Summary

What	Unscheduled power outages due to cyber-attack against Distribution Systems
When	December 23, 2015, lasting 1 – 6 hours Initial cyber-attack (phishing email) occurred in March 2015
Consequence	3 regional Oblenergos (utilities) 225,000 end-consumers Remote control lost for months
Who did it	No positive Identification . . .
Why	Unknown – many believe it is due to geopolitics in the region
How	See next slide ☺

Ukraine Power Outage - Summary

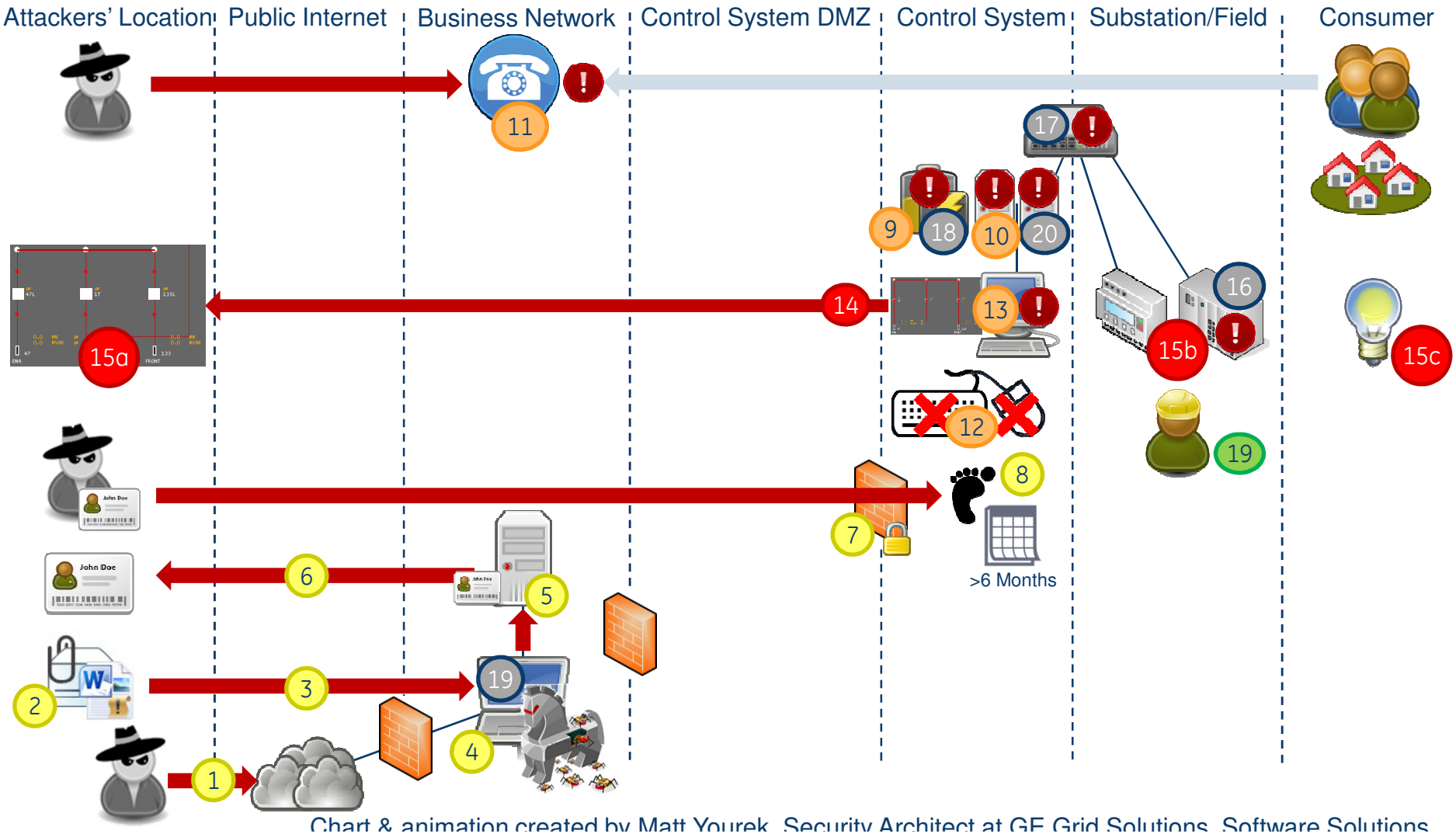
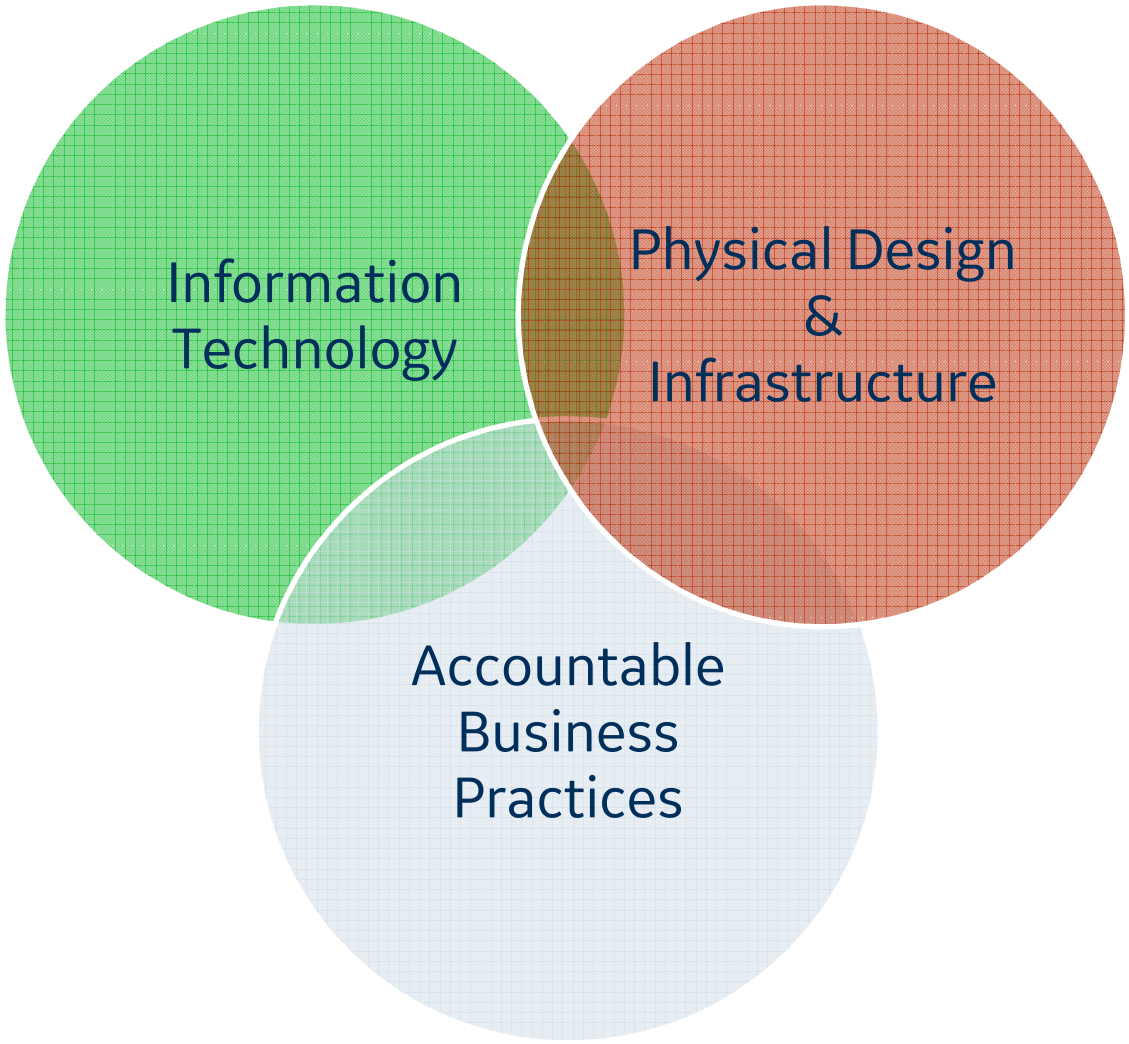


Chart & animation created by Matt Yourek, Security Architect at GE Grid Solutions, Software Solutions

Privacy by Design

Privacy by Design: Trilogy of Applications



Source: Ann Cavoukian, Ph.D., Information and Privacy Commissioner, Ontario, Canada
www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Privacy by Design: 7 Foundation Principles

1. **Proactive** not **Reactive**
2. Privacy as the **Default** setting
3. Privacy **Embedded** into Design
4. **Full** Functionality: Positive-Sum, not Zero-Sum
5. End-to-End **Security**: Full Lifecycle Protection
6. Visibility **and** Transparency: Keep it Open
7. Respect for User Privacy: Keep it User-Centric

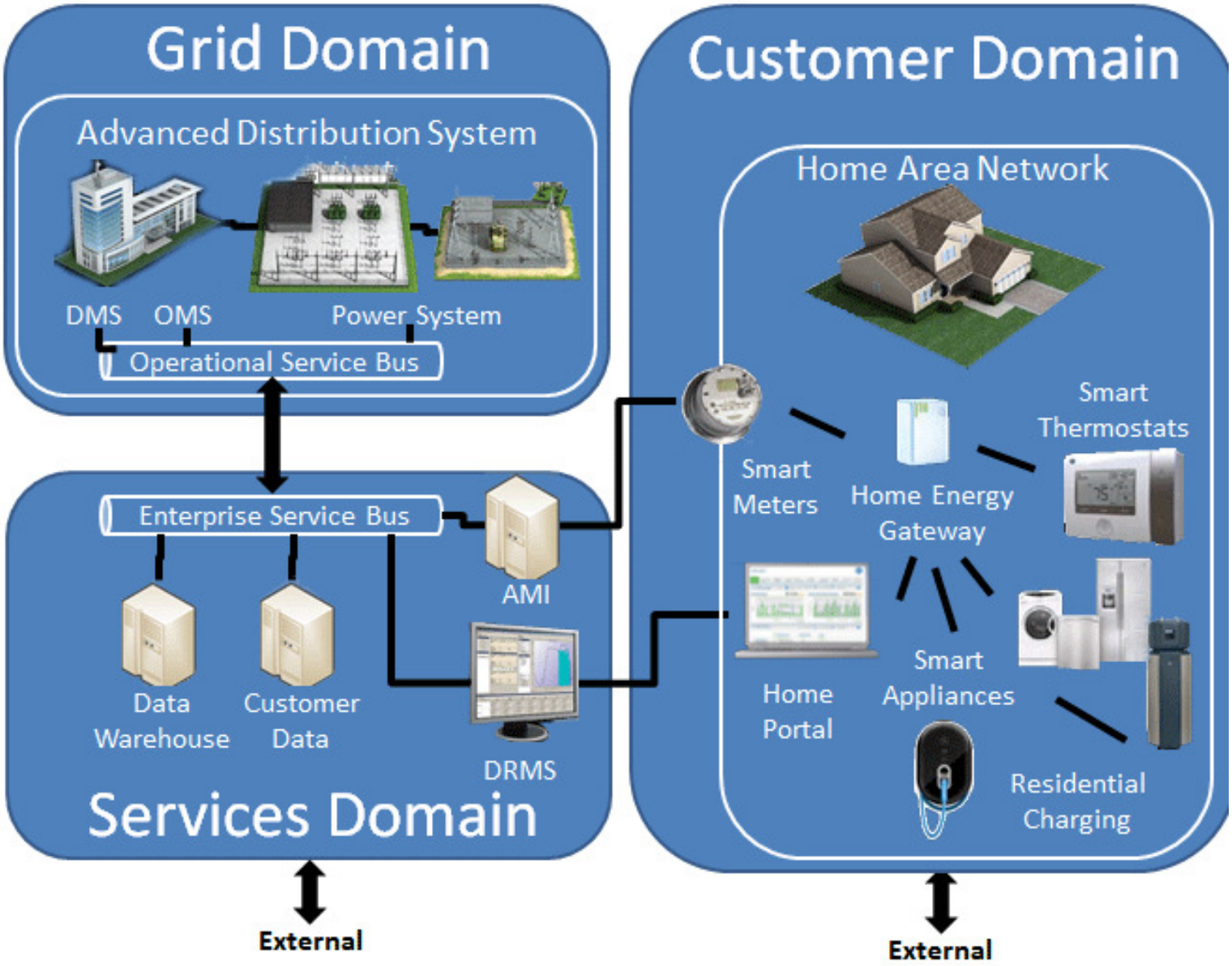
Source: Ann Cavoukian, Ph.D., Information and Privacy Commissioner, Ontario, Canada
www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Personal Information on the Smart Grid

- What constitutes “personal information” on the Smart Grid is the subject of much discussion;
- • Personal information is defined by the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), as ***“recorded information about an identifiable individual;”***
- • Once it becomes apparent that a Smart Grid technology, system or project will involve the collection of personal information, either directly or through some form of data linkage, privacy considerations immediately apply;
- • Digitization - Digital smart meter data, like all digital data, is vulnerable to accessing, copying, matching, merging and widespread dissemination.

Source: Ann Cavoukian, Ph.D., Information and Privacy Commissioner, Ontario, Canada
www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

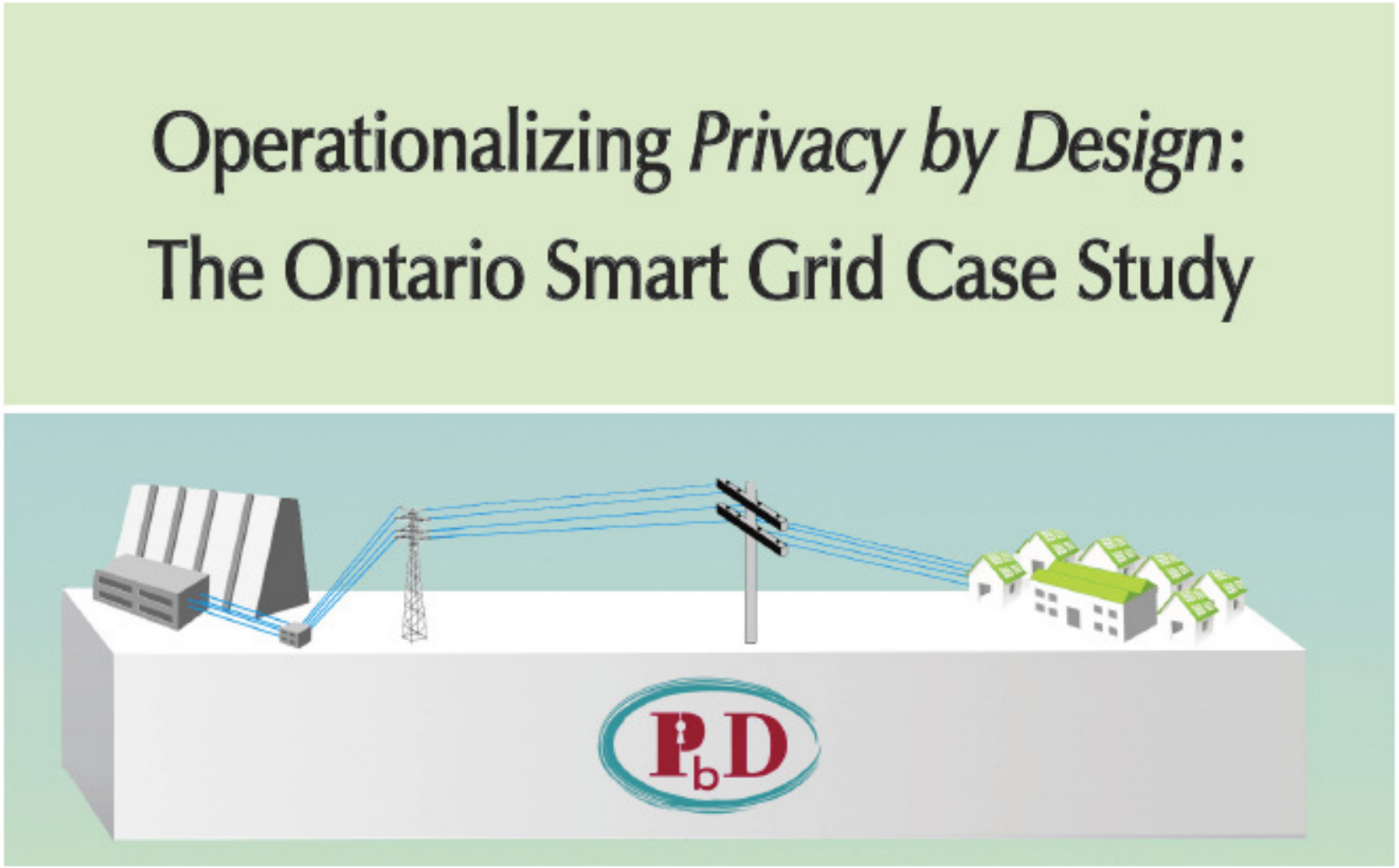
Personal Information on the Smart Grid



Best Practices

1. Proactively embed privacy in designs and governance framework
2. Ensure that privacy is the default – no action required to ensure privacy
3. Privacy a core functionality in the design and architecture
4. Avoid any unnecessary trade-offs to achieve privacy objectives
5. Build in privacy end-to-end, throughout the entire data life cycle
6. Systems must be visible and transparent to consumers
7. Respect consumer privacy

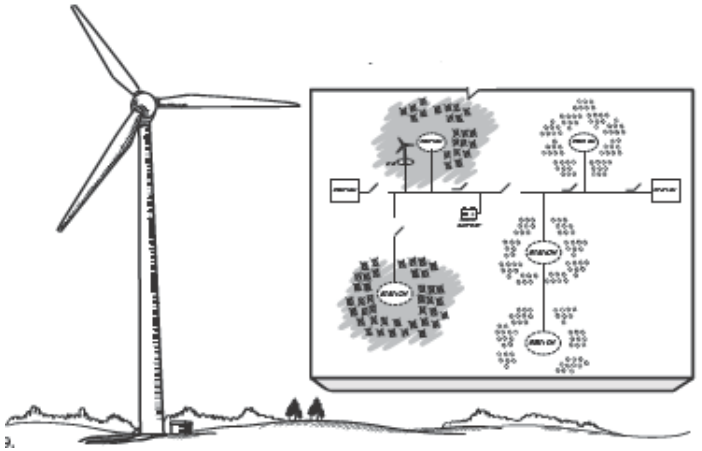
Case Study — Hydro One



Privacy by Design: www.privacybydesign.ca

Hydro One – Advanced Distribution System

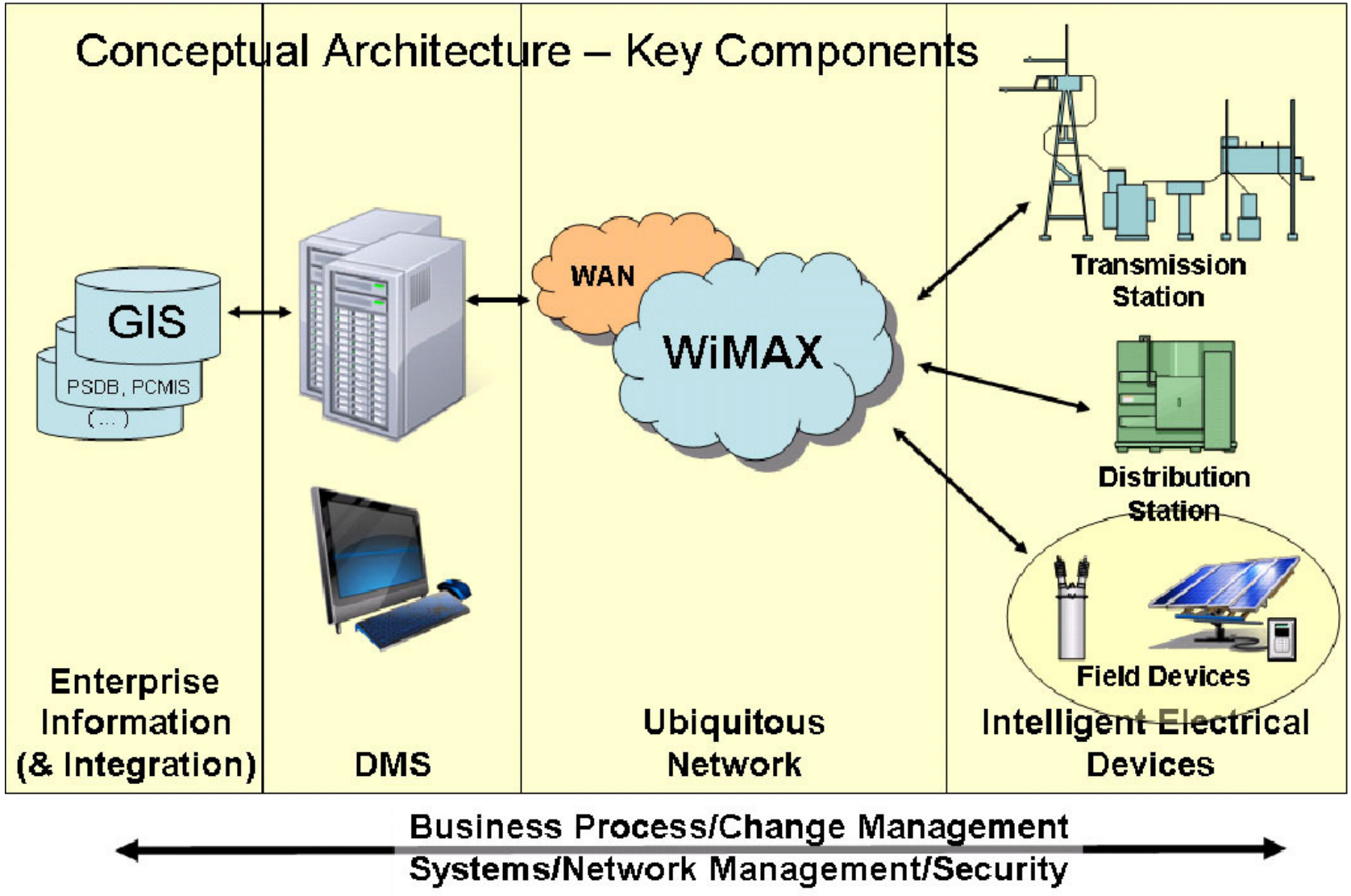
1. Optimize connection of Distributed Generation (DG) on the Distribution Network
2. Improve Distribution Reliability and Operations
3. Optimize Outage Restoration
4. Optimize Network Asset Planning



hydro one

imagination at work

Hydro One – Advanced Distribution System



Hydro One – Advanced Distribution System

Operationalizing Privacy by Design into ADS

1. Separation of Domains
   - Transcription of messages
   - Message management tools
2. Privacy data between the Domains
   - Aggregate data according to location not customer name
   - Critical safety concerns could require tie to customer name
3. Demand Response and Privacy
   - System must be designed with privacy at it's core
   - Manage privacy connecting with external parties such as ISO
4. Load Forecasting
   - Aggregate meter load on various points on feeder
   - Remove customer name – use meter location