

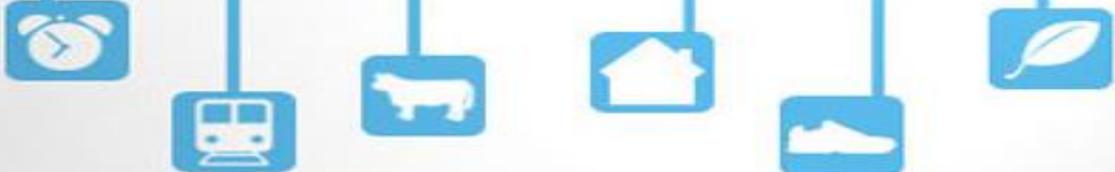
Internet of Things & Security of Business

Karen McDowell, Ph.D., GCIH
University of Virginia – April 2015
Commonwealth of Virginia Security

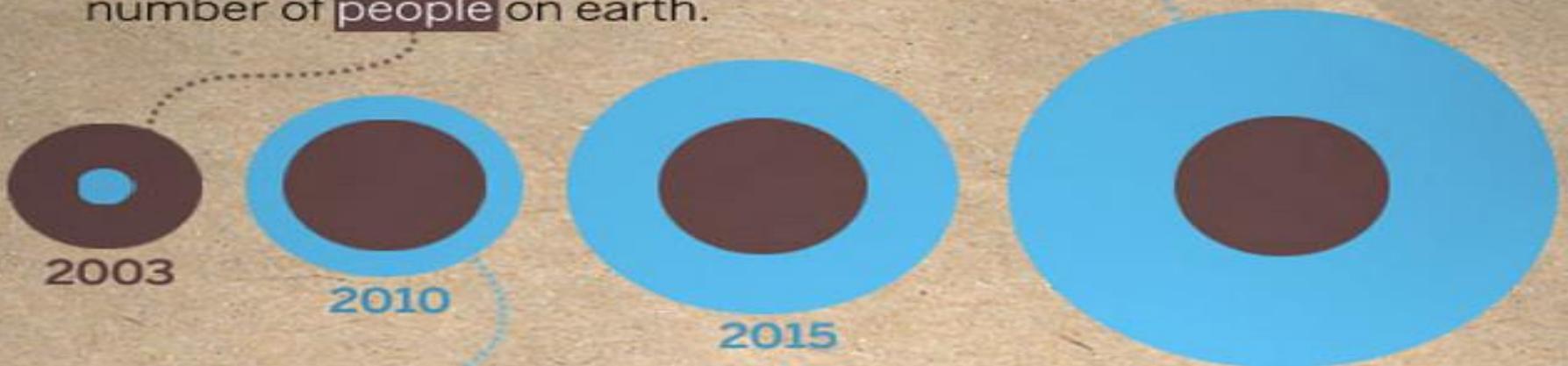


By 2020 Annual Sales of \$9 Trillion

The INTERNET *of* THINGS



During 2008, the number of **things** connected to the Internet exceeded the number of **people** on earth.



By 2020 there will be **50 billion**.

Smart, Connected Devices

People-to-People (P2P)

People-to-Machine (P2M)

Machine-to-Machine (M2M)

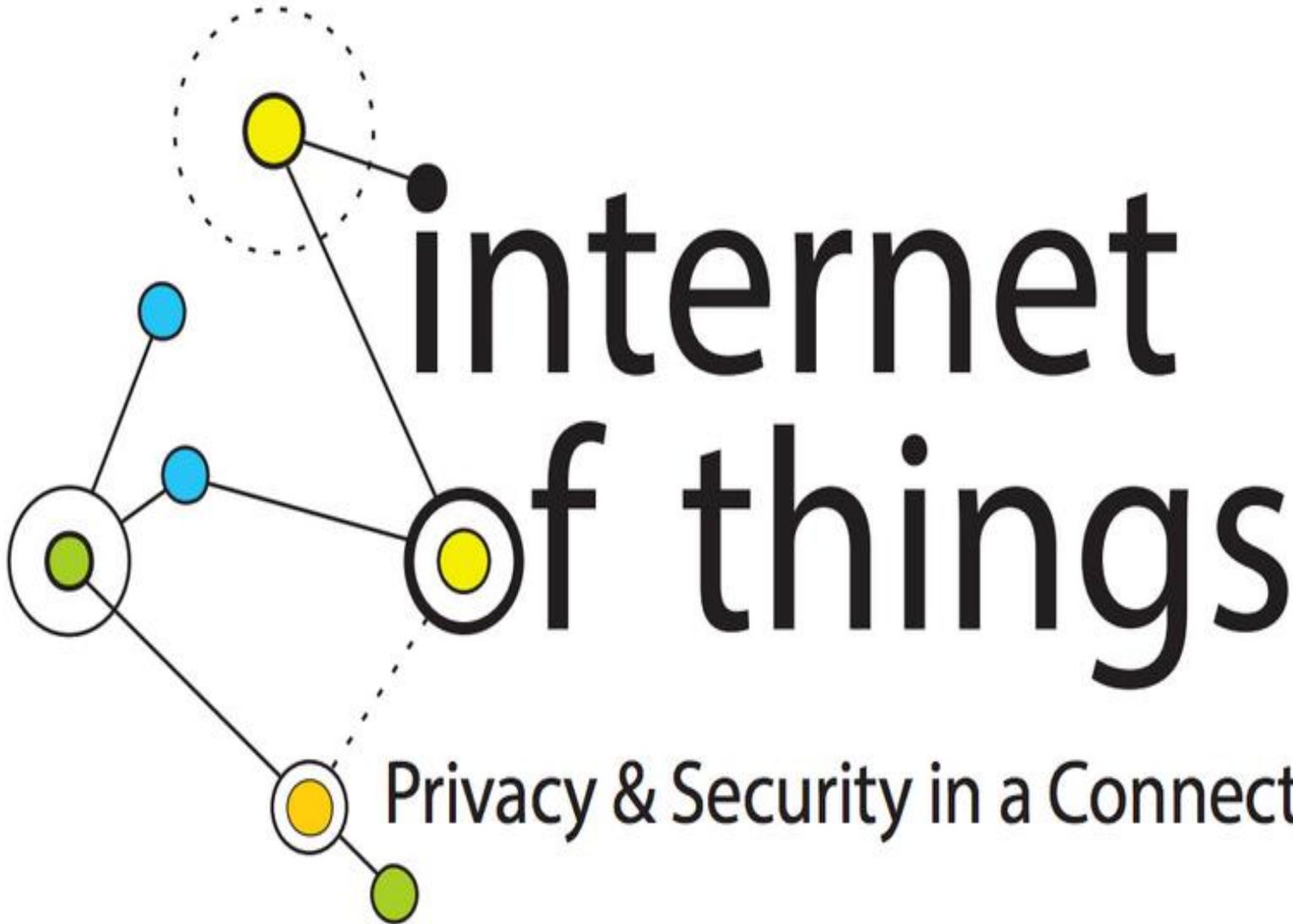
Security and Privacy,
Big Data Storage

POS Devices

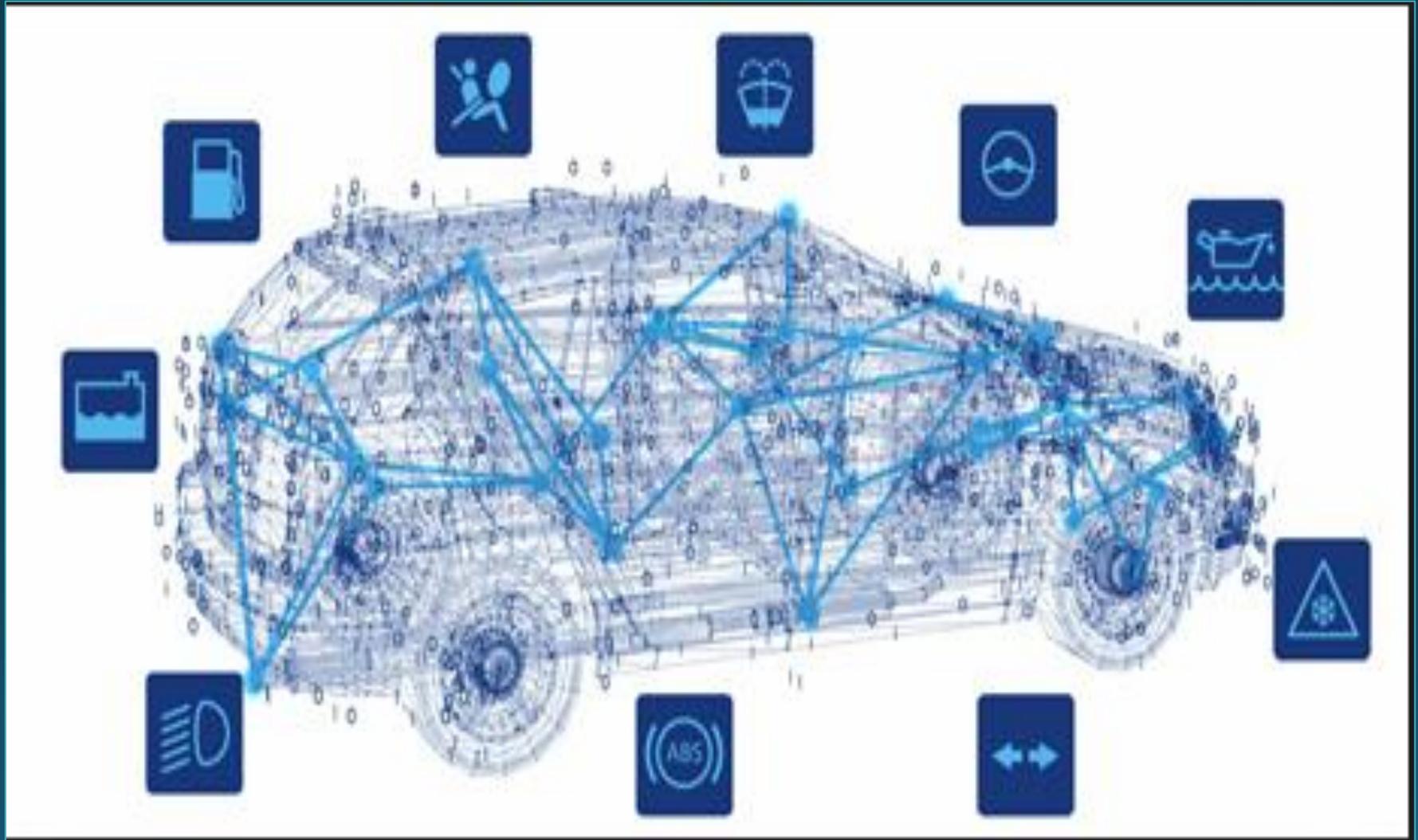


Default Password is 1234

FTC Report 2015



Internet-Enabled Cars



nest

COOL SET TO

11.5

STARTS IN 0:58

25



Monitoring – Doorbots



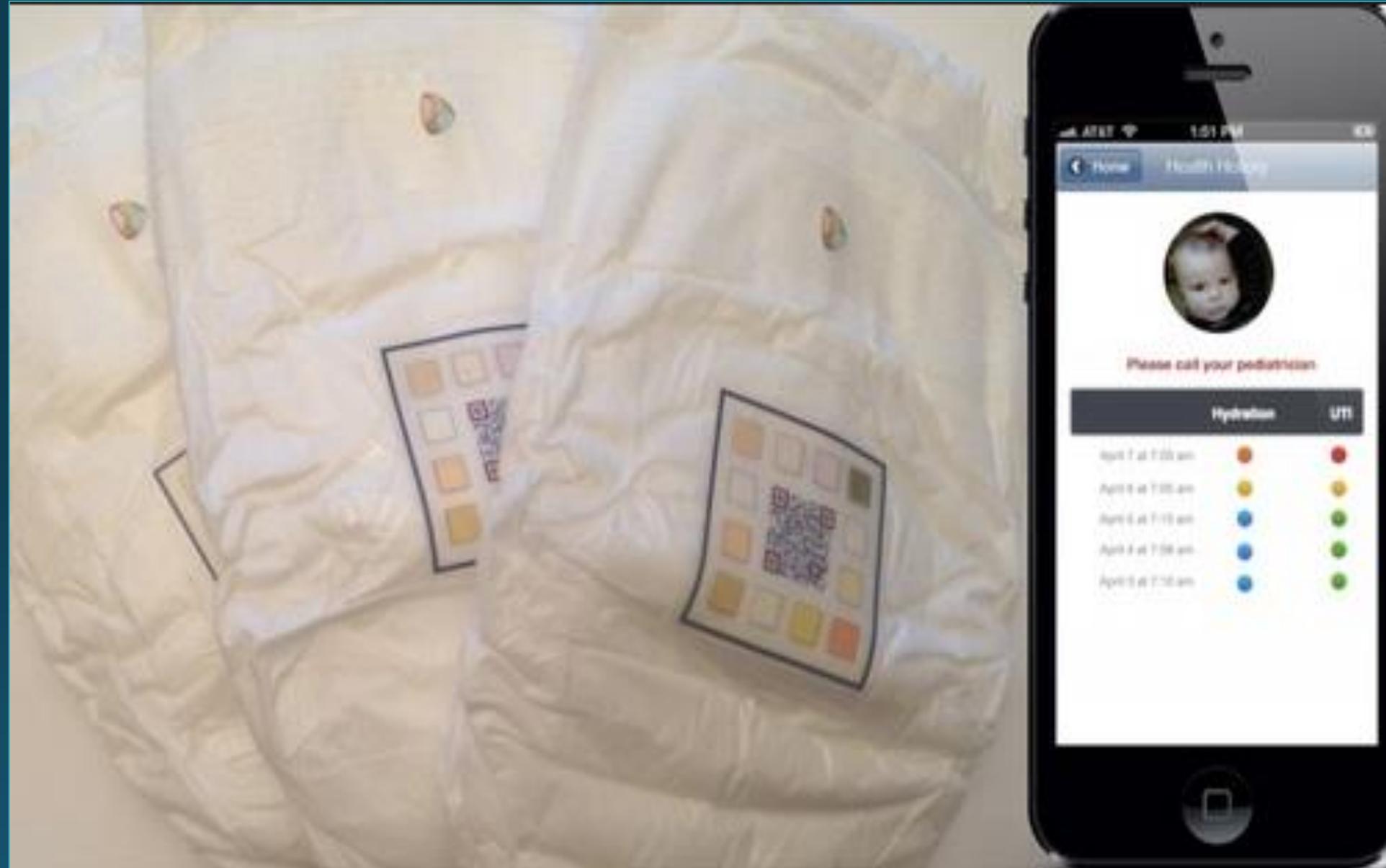
Control



Entertain Your Pets



Smart Diapers for Adults



IOT Mother





Smart Phone as Hub, Linchpin

IOT-connected Home as Office Portal





No Small Complication

Why Firmware Is So Vulnerable to Hacking. Never designed to be secure, now no incentive to fix it



Home Routers: Change Defaults



Google for Hackers

Shodan

Exploits

Scanhub

Maps

Blog

Membership

Register

Login



Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR

FREE SIGN UP

<http://www.shodanhq.com/>

Popular Search Queries: Router w/ Default Info - Routers that give their default username/ password as admin/1234 in their banner.

Boon to Cities and Citizens



Urban Infrastructure



Cows on the IOT



IOT of Slimy Things



Diagnosis: Insecure



Hacking The Car Wash



Critical Infrastructure



SCADA Systems



Hacking Traffic Systems is Easy



Rented Aircraft Engines



Rolls Royce

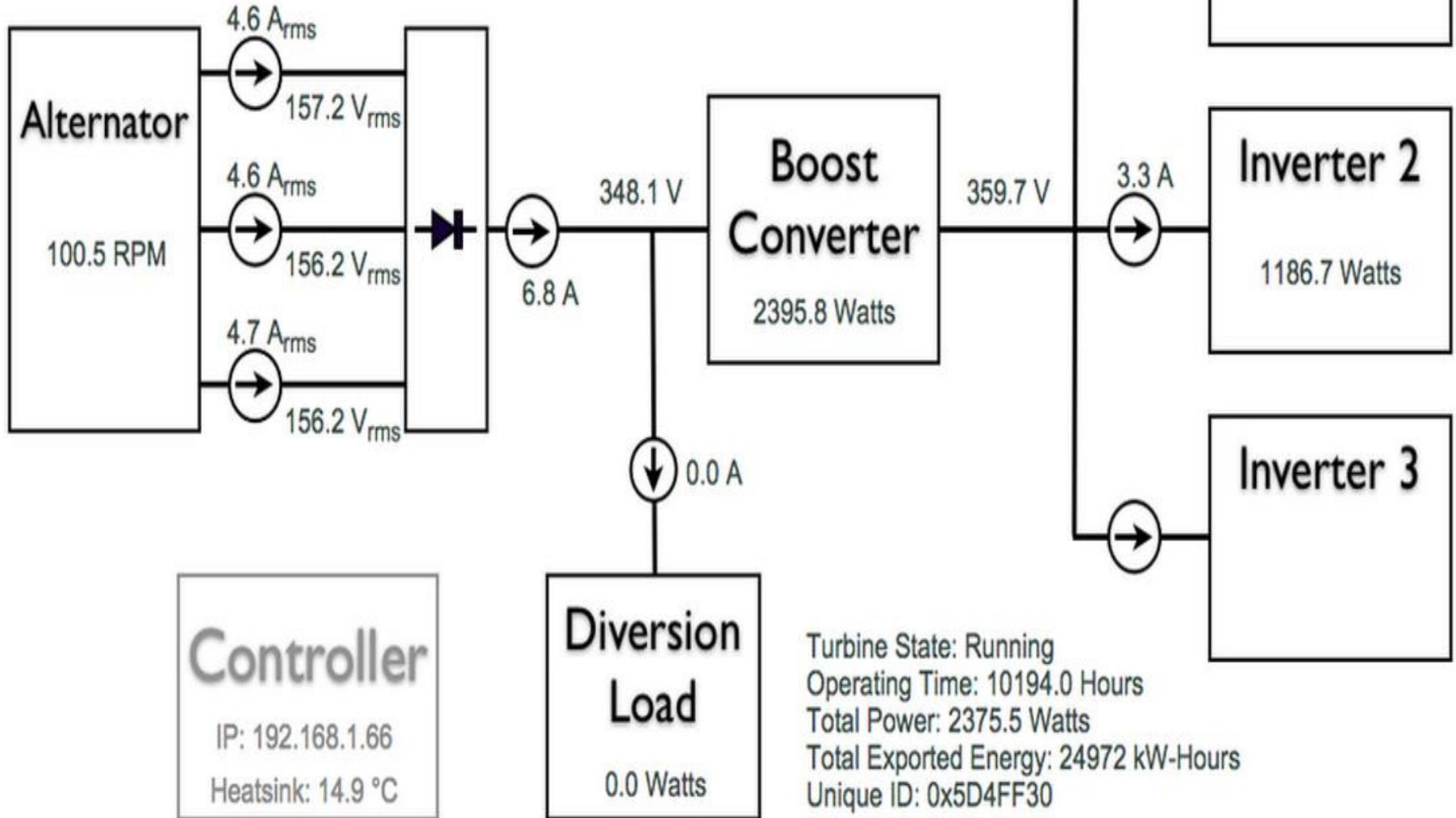
Wind Turbines





Turbine System

Wind Direction: 207.3 °



Why SCADA Security is Fragile

- Cultural, political and technical divisions
- Expense to upgrade, train, equip
- Legacy systems rife with older vulnerabilities
- Routine patching logistically complex
- Rigid compliance mandates
- Air gap myth

Systemic Lack of Security Consciousness

- 70% of IOT Devices contain security vulnerabilities
- Expensive to build security in, cuts profit
- More sensors mean less privacy, everything we do now leaves digital trace
- Lack of layered security in embedded systems create single points of failure, brittle defense

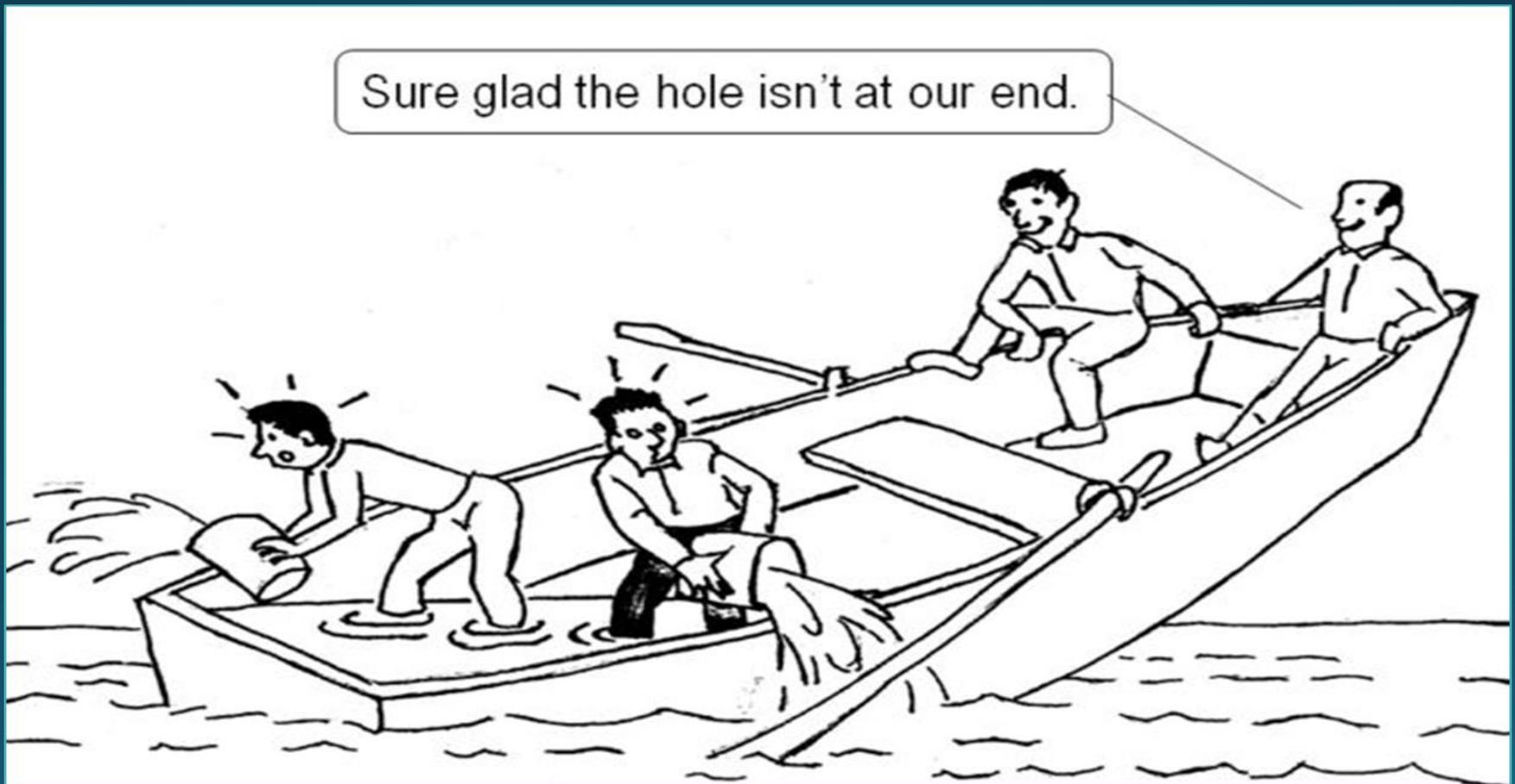
At a Minimum...

1. Business leaders must be security leaders
2. Insist manufacturers and vendors build security into devices
3. We have a shared responsibility
4. Educate users. 90% of all breaches begin with phishing

Internet of Anything



We must, indeed, all hang together or, most assuredly, we shall all hang separately. – Benjamin Franklin



Questions?

