Lyn Gomes,
CCP, CLCATT, LEED-AP

Senior Commissioning/
MEP Coordinator,
DPR Construction

Real-world Problems Really do Exist

Building control systems – increasingly connected & increasingly vulnerable to attack

Background: History Rhymes

Jul 27, 2017, 05:00pm EDT

Forbes

Criminals Hacked A Fish Tank To Steal Data From A Casino

Lee Mathews Senior Contributor

Cybersecurity

Observing, pondering, and writing ab

ANDY GREENBERG SECURITY 09.12.2019 11:55 AM

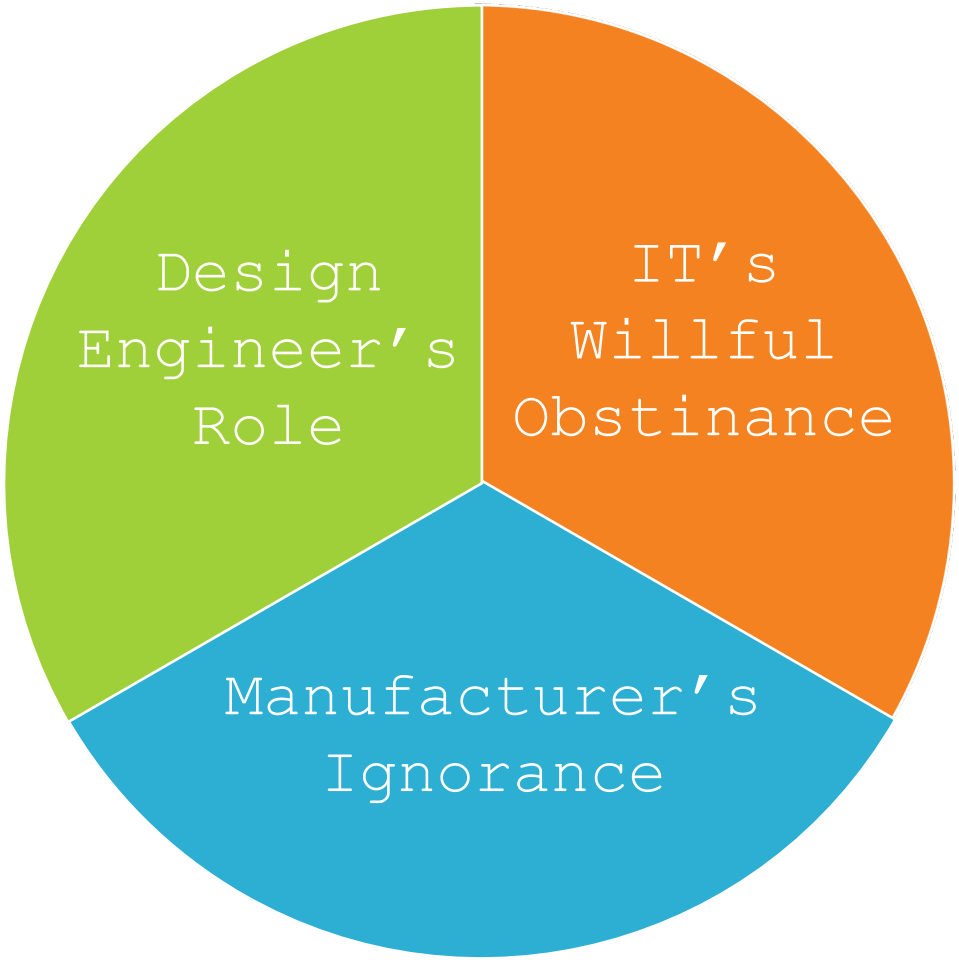
WIRED

New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction

A fresh look at the 2016 blackout in Ukraine suggests that the cyberattack behind it was intended to cause far more damage.

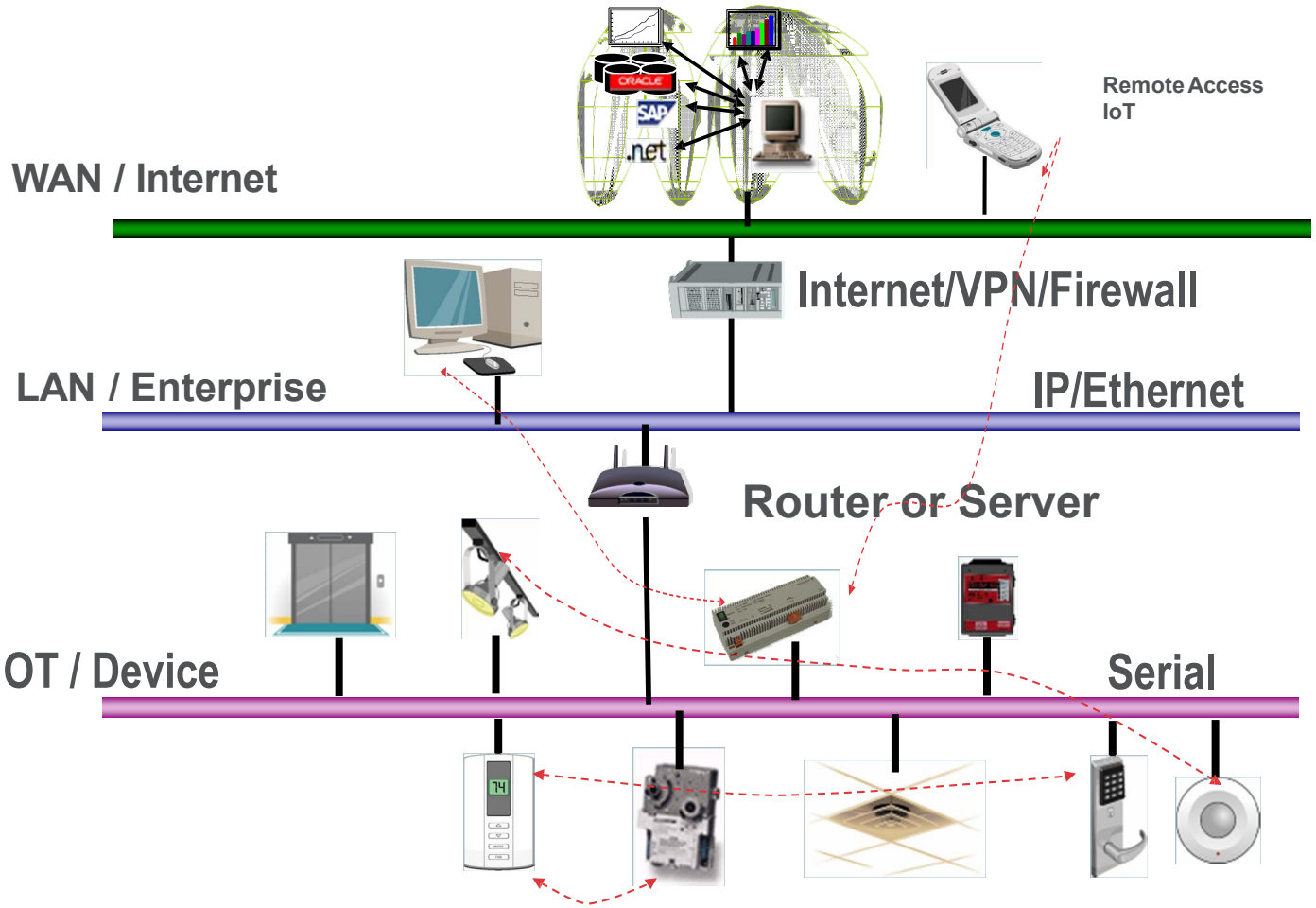
State of the Industry

for Network Architecture



Key Concepts & System Architecture

- Acronyms
  - ICS: Industrial Control Systems
  - OT: Operational Technology
  - CISA: Cybersecurity and Infrastructure Security Agency
- Control systems
  - Network based
  - Specialized software
- Team-based solutions
- Facilities Engineers roles are changing

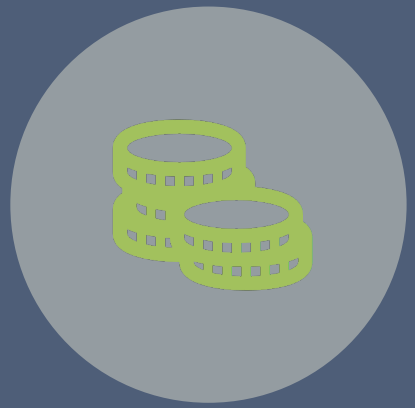


Picture: Ron Bernstein, RBCG Consulting – used with permission

Example 1: Lighting Control System

CISA VULNERABILITY IDENTIFIED

MANUFACTURER “OBSOLETES” PRODUCT LINE



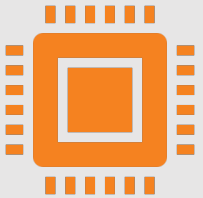
CAPITAL LEVEL EXPENDITURE

Example 2: A Core HVAC Component

Internet accessible control valve	Conversations with manufacturer make it clear that:	Security fails of this device could:
No authentication No encryption	No understanding between encryption and authentication Device security not considered as part of their scope-of-work (as do many EORs)	Present vulnerabilities to OT and IT/Enterprise networks Lose temperature control for building Cause physical damage to equipment (freezing of coils/water leaks after a thaw) Brick devices (re-write firmware)

Bluetooth Vulnerabilities

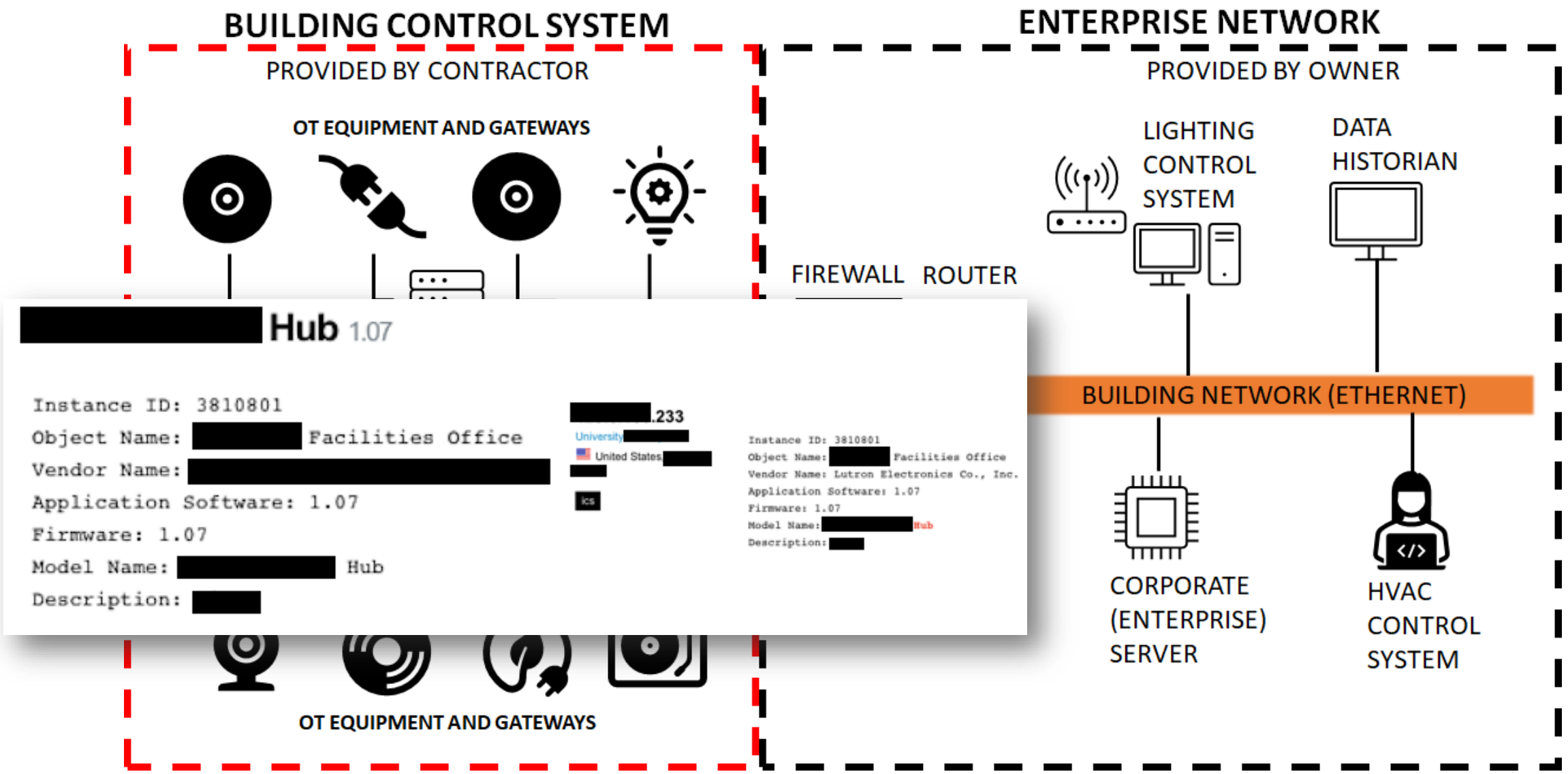
Bluetooth-to-ethernet gateway



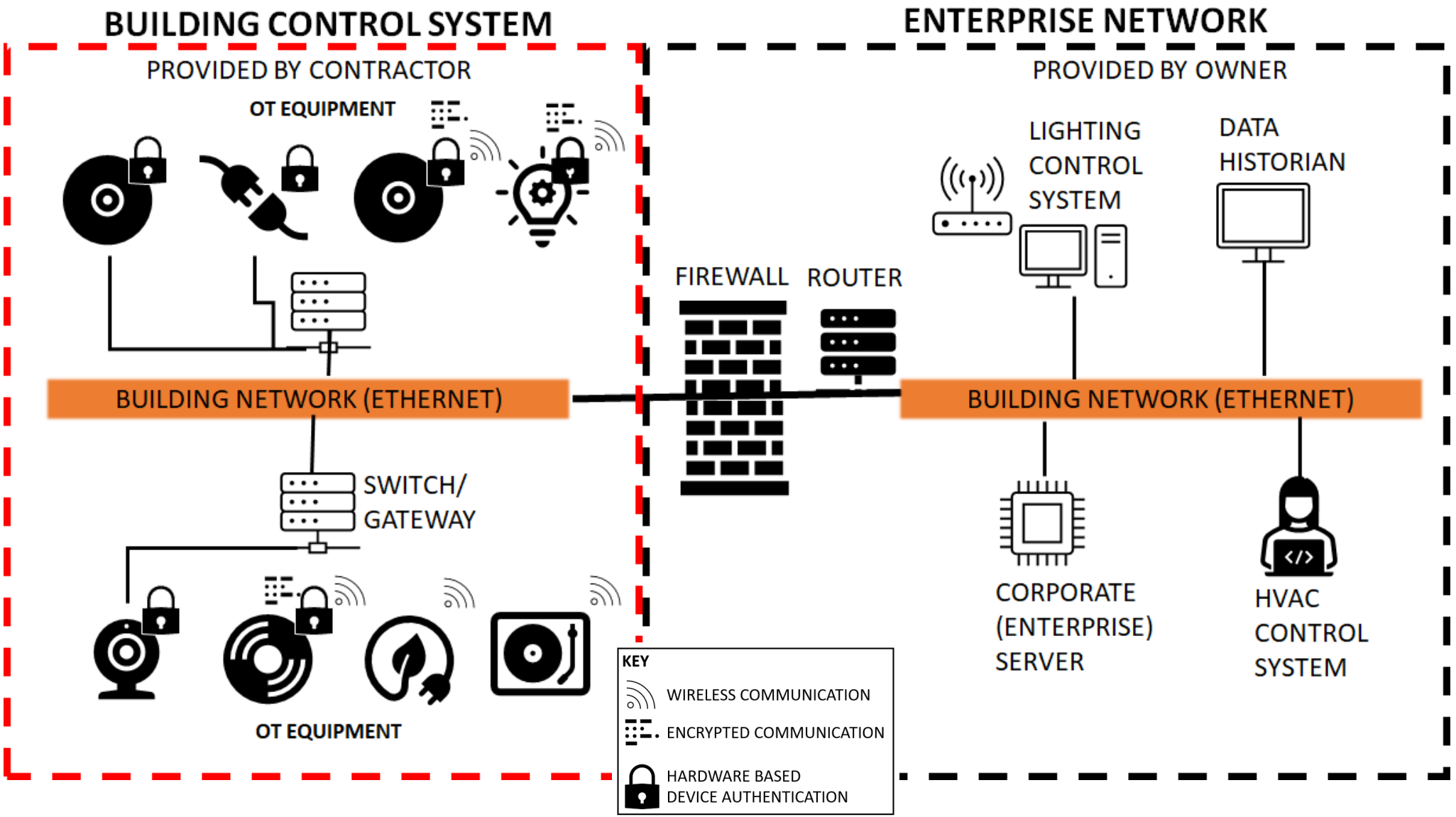
Easy to hack, making it simple to get into the ethernet network

ANY CONNECTED DEVICE IS VULNERABLE

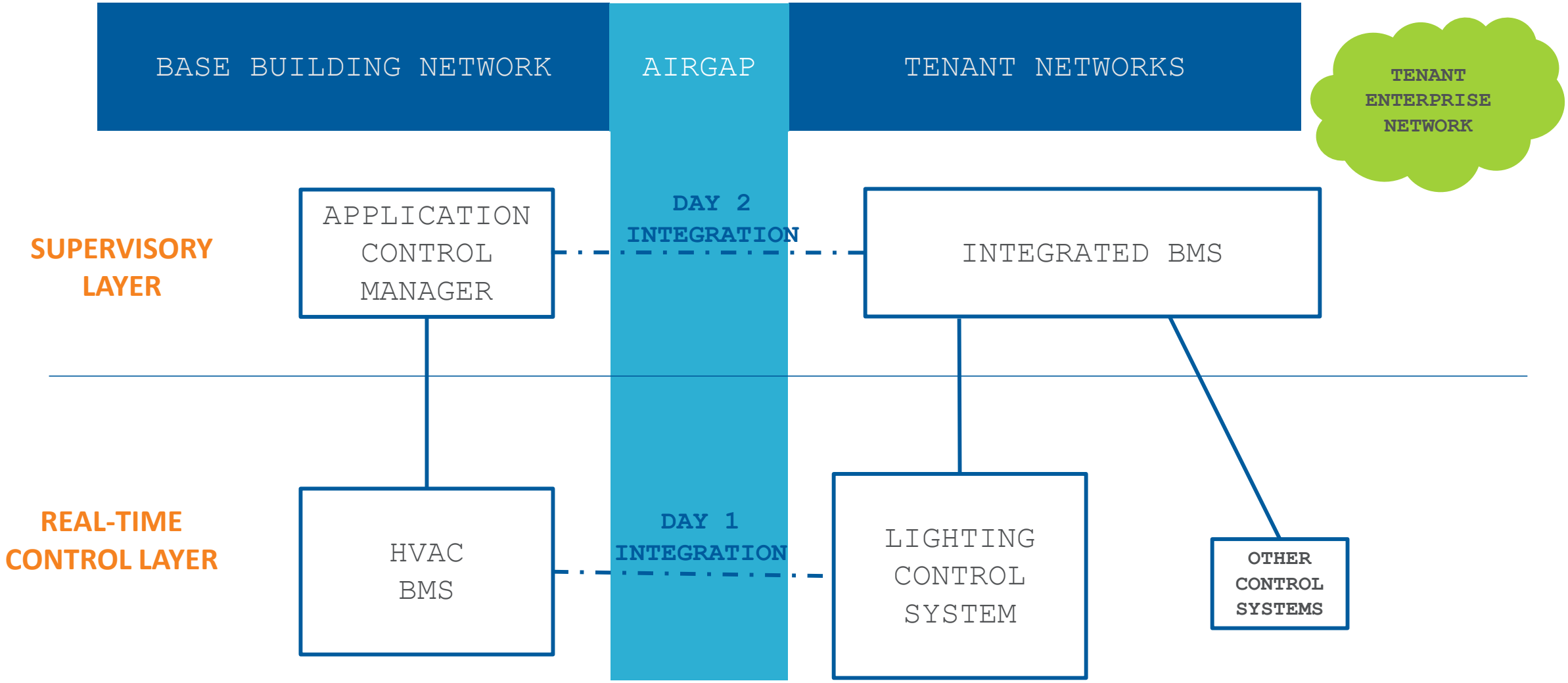
Example 3: LCI Connected to Wi-Fi



Example 4: The Good and the Bad



Example 5: Network Structure Matters



Recommendations

01
- Cyber/physical security always
  - Cyber is never a substitute for physical security

02
- Know what's on your network & install patches

03
- Create an offline recovery kit

01
- Follow NIST's Guide to Industrial Control Systems (ICS) Security (SP 800-82)

02
- Importance of network architecture
  - Tosibox goes INSIDE the firewall
  - Tosibox can't be the outside access point

03
- Allude to overlap in the approach
  - This is good! Shows consensus of robust best practices that are not proprietary

Thank you!

LynG@dpr.com