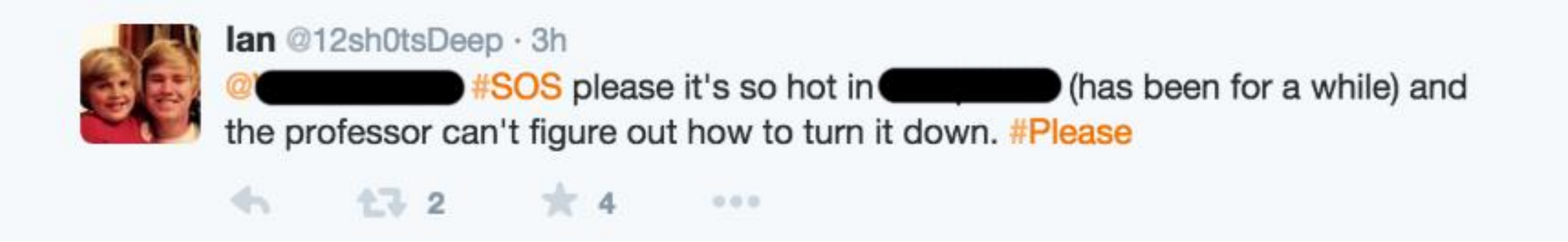
Information Technology in Operations & Maintenance

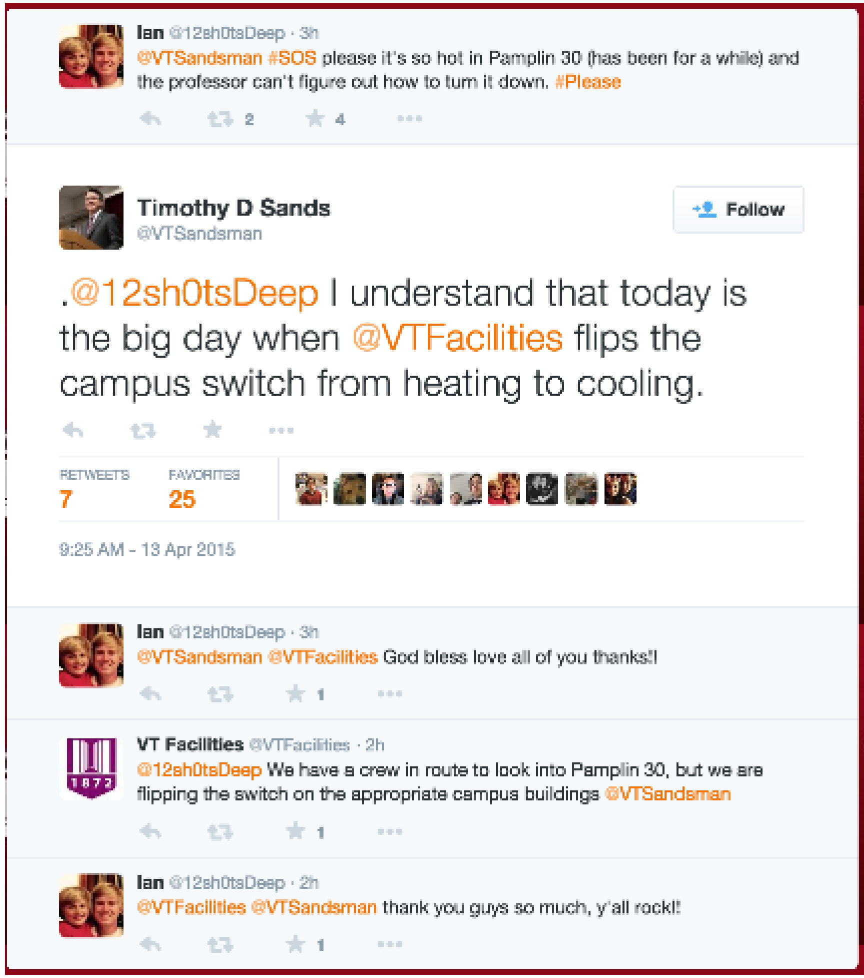
Chris Smeds
Director of Technology & Innovation
U.Va. Facilities Management
smeds@virginia.edu

What would you do?



Ian @12sh0tsDeep · 3h

@[redacted] #SOS please it's so hot in [redacted] (has been for a while) and the professor can't figure out how to turn it down. #Please



Ian @12sh0tsDeep · 3h
@VTSandsman #SOS please it's so hot in Pamplin 30 (has been for a while) and the professor can't figure out how to turn it down. #Please

Timothy D Sands
@VTSandsman

.@12sh0tsDeep I understand that today is the big day when @VTFacilities flips the campus switch from heating to cooling.

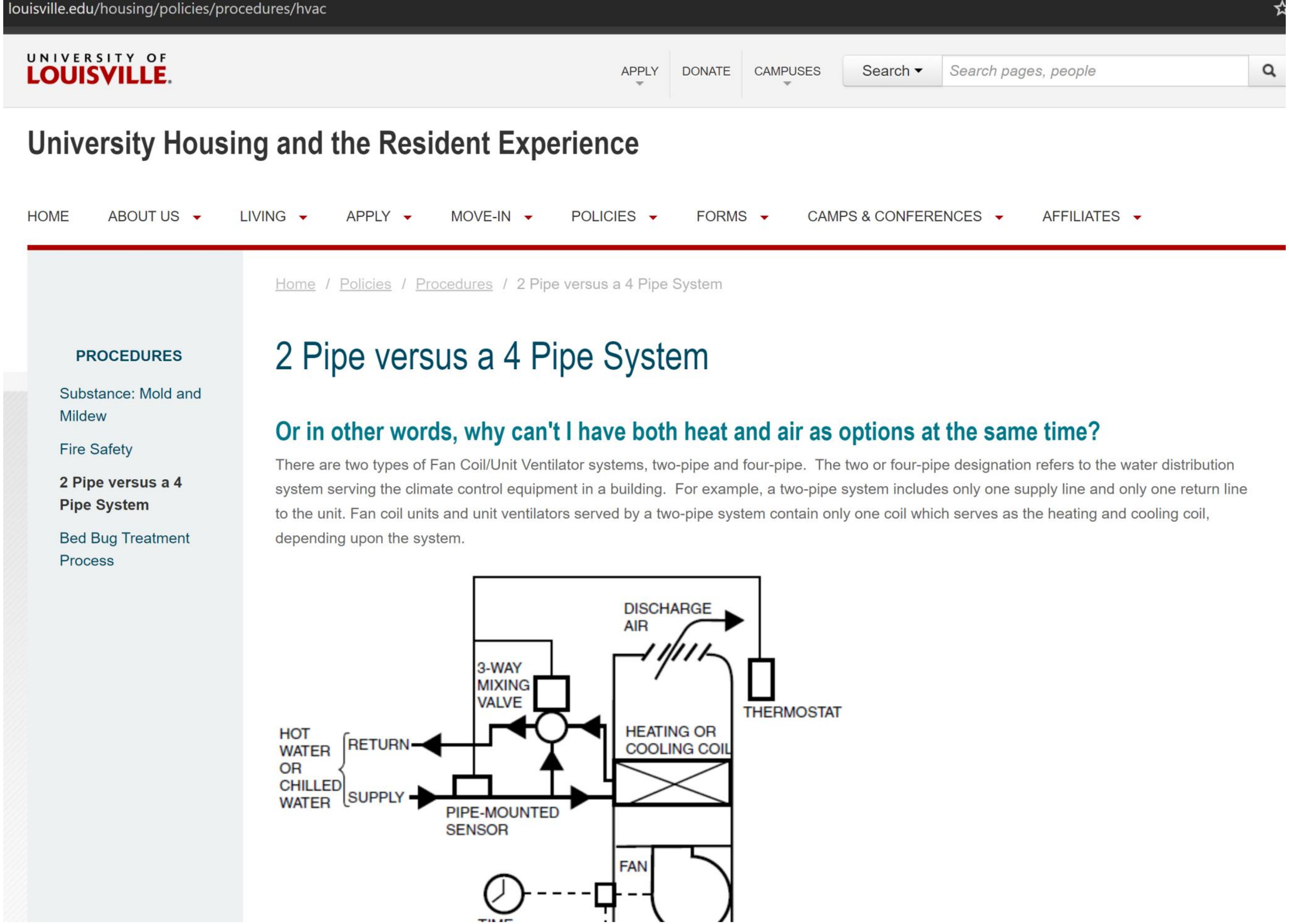
RETWEETS 7
FAVORITES 25

9:25 AM - 13 Apr 2015

Ian @12sh0tsDeep · 3h
@VTSandsman @VTFacilities God bless love all of you thanks!!

VT Facilities @VTFacilities · 2h
@12sh0tsDeep We have a crew in route to look into Pamplin 30, but we are flipping the switch on the appropriate campus buildings @VTSandsman

Ian @12sh0tsDeep · 2h
@VTFacilities @VTSandsman thank you guys so much, y'all rock!!



louisville.edu/housing/policies/procedures/hvac

UNIVERSITY OF LOUISVILLE.

APPLY DONATE CAMPUSES Search ▾ Search pages, people

University Housing and the Resident Experience

HOME ABOUT US ▾ LIVING ▾ APPLY ▾ MOVE-IN ▾ POLICIES ▾ FORMS ▾ CAMPS & CONFERENCES ▾ AFFILIATES ▾

Home / Policies / Procedures / 2 Pipe versus a 4 Pipe System

PROCEDURES

- Substance: Mold and Mildew
- Fire Safety
- **2 Pipe versus a 4 Pipe System**
- Bed Bug Treatment Process

2 Pipe versus a 4 Pipe System

Or in other words, why can't I have both heat and air as options at the same time?

There are two types of Fan Coil/Unit Ventilator systems, two-pipe and four-pipe. The two or four-pipe designation refers to the water distribution system serving the climate control equipment in a building. For example, a two-pipe system includes only one supply line and only one return line to the unit. Fan coil units and unit ventilators served by a two-pipe system contain only one coil which serves as the heating and cooling coil, depending upon the system.

Credit(s) earned on completion of this course will be reported to American Institute of Architects (AIA) Continuing Education Session (CES) for AIA members.

Certificates of Completion for both AIA members and non-AIA members are available upon request.

This course is registered with AIA CES for continuing professional education. As such, it does not include content that may be deemed or construed to be an approval or endorsement by the AIA of any material of construction or any method or manner of handling, using, distributing, or dealing in any material or product.

Questions to specific materials, methods or services will be addressed at the conclusion of this presentation.

AIA Approved Continuing Education

Course Description

This session provides an overview of the information technology (IT) systems used in Operations & Maintenances organizations in a higher education facilities management setting. The session includes discussions of information technology, operational technology and cybersecurity.

AIA
Continuing
Education
Provider

Learning Objectives

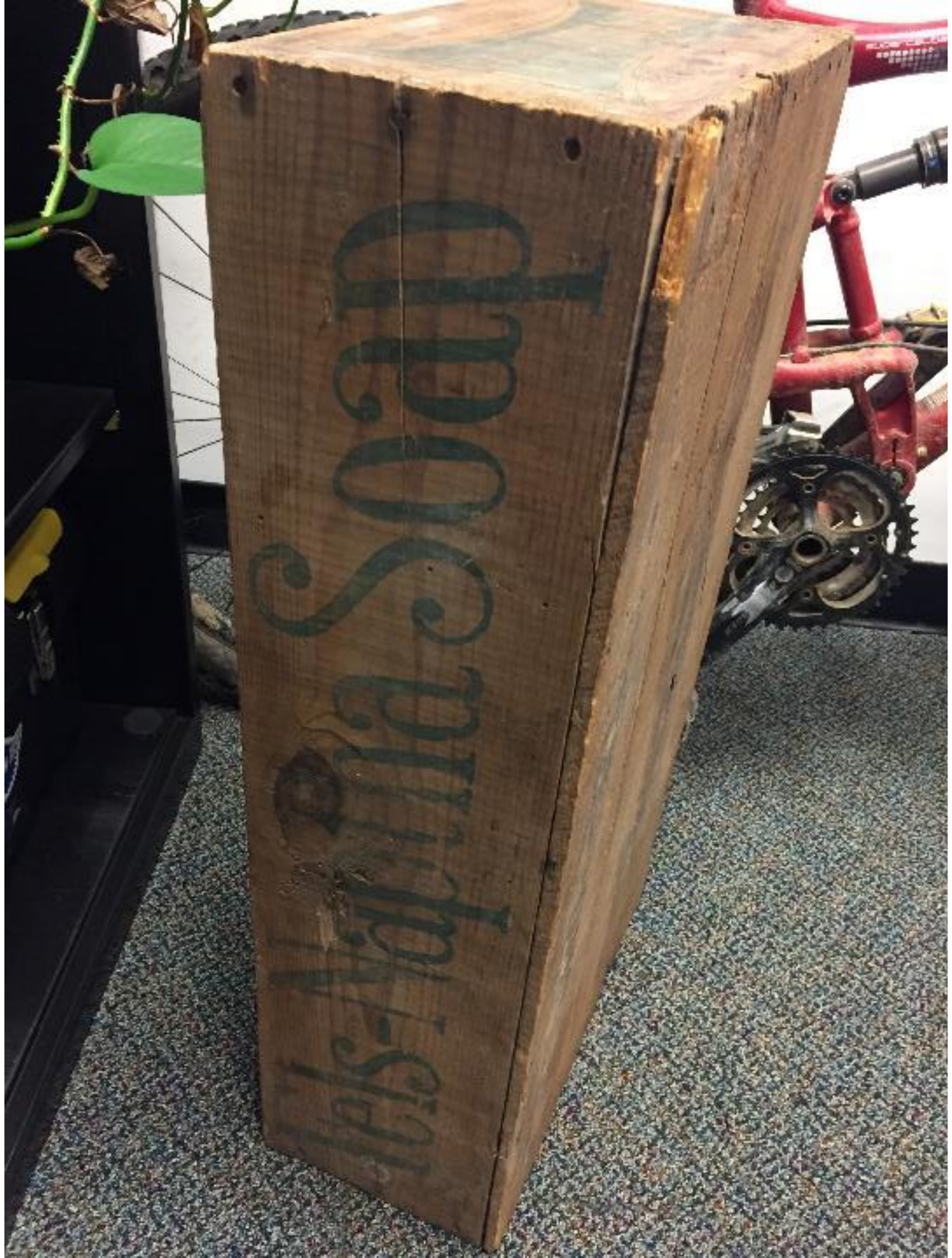
- Overview of IT in an FM Organization
- Discuss Information Technology (IT) Systems used in O&M
- Discuss Operational Technology (OT) Systems used in O&M

AIA Approved Continuing Education

Demystifying Technology

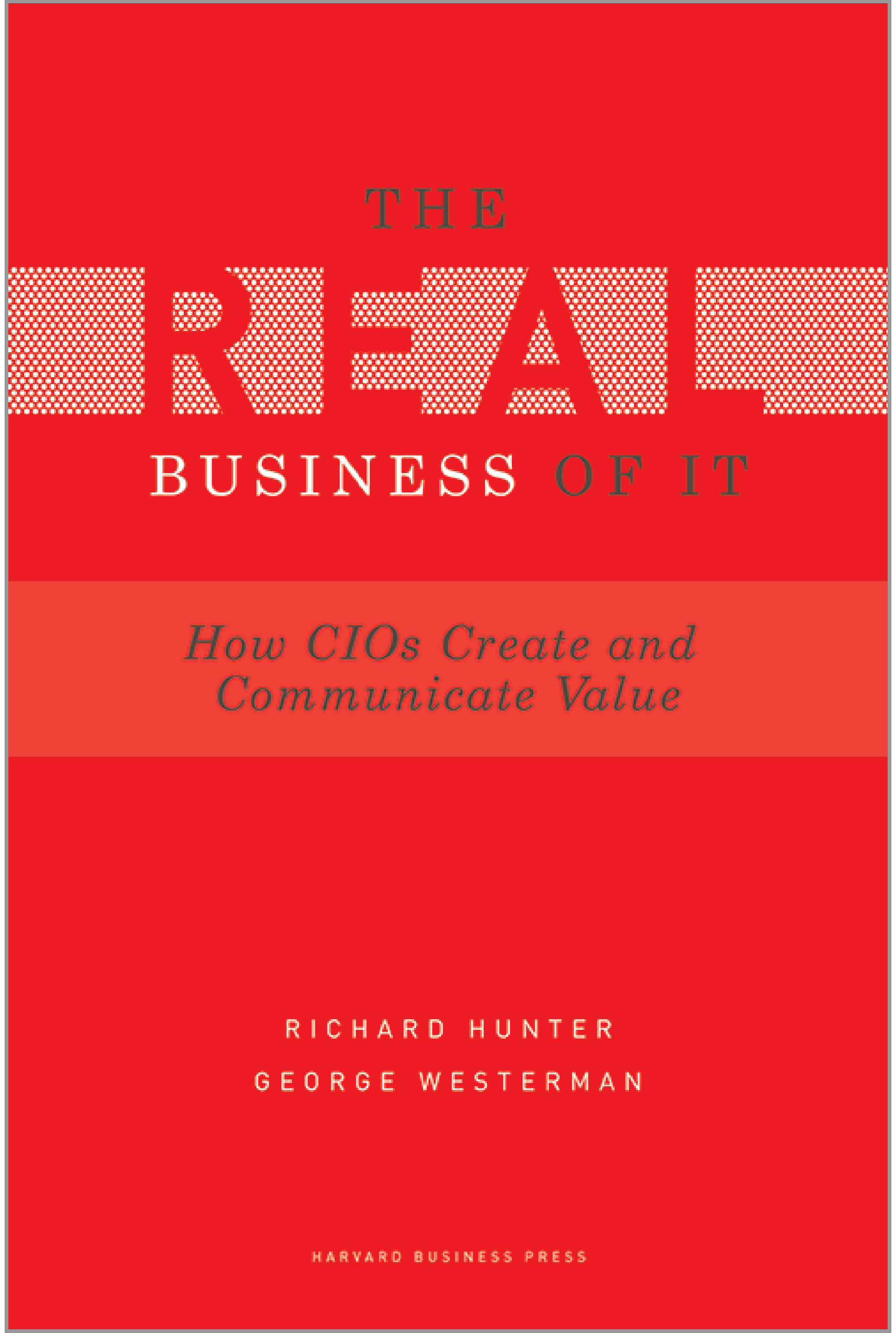
“Today’s cutting edge technology is tomorrow’s broken legacy system.”

Now it's closed and everything's save inside it.
So you're sure I won't loose any of the text?



“Technology by itself is not the point.”

- Tim Cook



THE REAL BUSINESS OF IT

How CIOs Create and Communicate Value

RICHARD HUNTER

GEORGE WESTERMAN

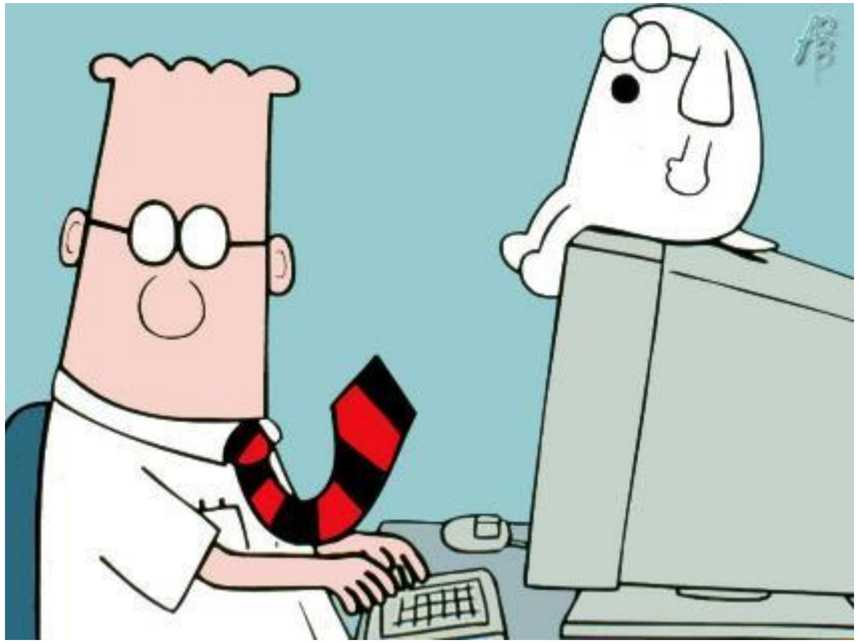
HARVARD BUSINESS PRESS

The roles of IT in FM

- Utility
- Innovation
- Building Automation Systems (a.k.a. Operational Technology)
- Cybersecurity & Compliance

Information Technology

It’s not just for nerds…



- Tools
- Information
- Process

and…

- People

Tools

If all you have is a hammer, everything looks like a nail.

- Things that help us do our job or get things done
  - Email, word processor, spreadsheet, cell phone, GPS
- Easy to see why we use them:
  - They make us more effective
  - Save time & money
  - Allow us to do things we otherwise couldn't do
- But, there are challenges:
  - We have to make them easy to use
  - Making sure you have the right tool for the job | which is faster: pencil or iPad?
  - Cost vs. benefit – how do you measure?
  - "Access to technology" issue
    - How do you get tech to people (or vice versa)?
    - Lost productivity – is he a plumber or a data entry clerk?

Information

Just the facts, ma’am

- Data! Facts! Knowledge!

- Why collect information?
  - Sometimes, you just have to
  - Measure success
  - Helps you improve process…
  - Helps you tell your story

- Different information matters to different people

  What information does a mechanic need?

  What information does a frontline supervisor need?

  What information does a superintendent need?

  What information does an executive need?

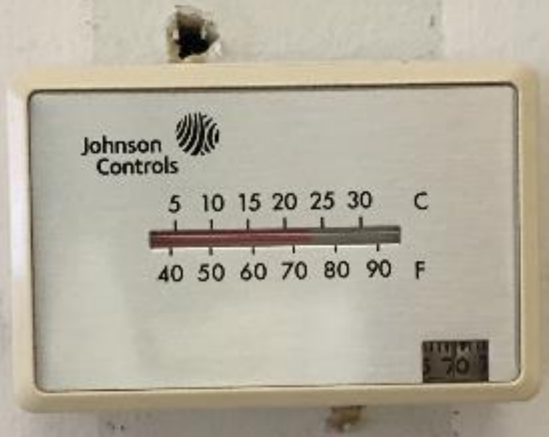
  What information does a customer need?

- Reporting vs. Analytics vs. Business Intelligence (BI)

Process

That's how we roll

- Simply defined: the way we do things
  - Some are good … some are, well, bad!
- Why is process important?
  - We want to do the right things the right way
  - Because we don't want to do bad things more effectively!!!


Johnson Controls
5 10 15 20 25 30 C
40 50 60 70 80 90 F
5 70

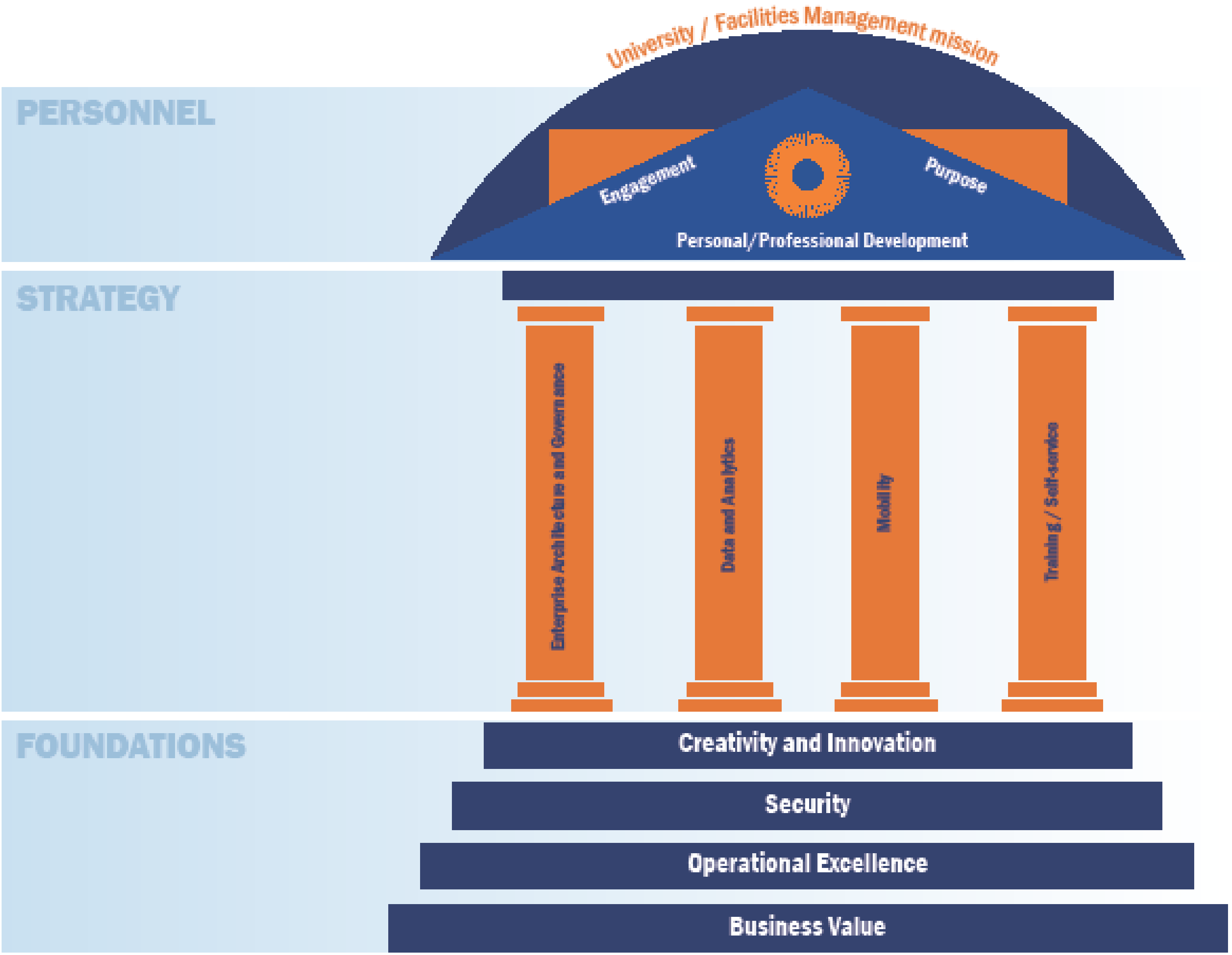
People

Mother knows best

- People love change... or do they?
  - Do people really resist change?
- Change management & unintended consequences
- User experience (UX)
  - Ease of use
  - Efficiency
  - Aesthetic
- **TRAINING!!!**

Putting it all together…

The ideal IT solution: bake **information** (collection) into your **process** – use technology (**tools**) as needed and *REMEMBER* the **PEOPLE**!



University / Facilities Management mission

PERSONNEL

Engagement

Purpose

Personal/Professional Development

STRATEGY

Enterprise Architecture and Governance

Data and Analytics

Mobility

Training / Self-service

FOUNDATIONS

Creativity and Innovation

Security

Operational Excellence

Business Value

Sourcing IT

- Organization of IT in higher education FM
  - In FM department
  - From Central IT
  - Contractor (out-sourced)

Other issues IT thinks about re: Sourcing IT

- Commercial Off the Shelf (COTS) Packages vs. In-house development

- Hosting vs. on premise systems

- Enterprise Resource Planning (ERP) System vs. Best-of-Breed

- System Integration

Information Technology (IT)

Types of IT Systems Found in O&M Organizations

Core IT Systems

- Desktop & mobile devices
- Email / Calendaring / Collaboration Tools
- Word Processing / Spreadsheets / Presentations
- Document Management

+

Line of Business Systems

- Maintenance Management Systems
- Construction/Project Management Systems
- Space Management Systems
- Energy & Utility Systems
- Finance / Procurement / HR

Evolution of Maintenance Management Systems

- Computerized Maintenance Management System (CMMS)
  - Maintenance management
- Enterprise Asset Management System (EAM)
  - Asset management

Evolution of Maintenance Management Systems

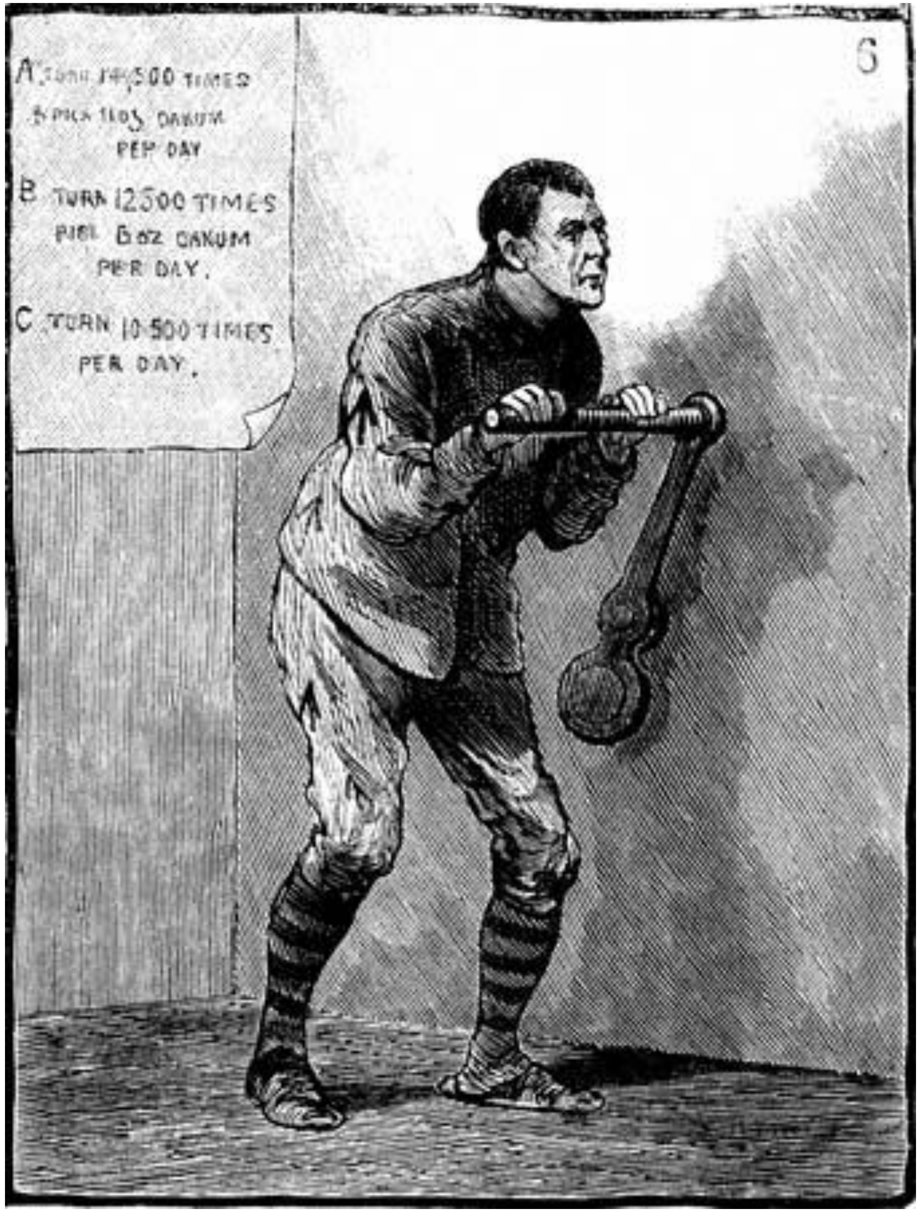
- Computer-Aided Facility Management System (CAFM) aka Facility Management System (FMS)
  - Space management, alphanumerical and graphical
  - Facility management
  - Reactive Maintenance management

- Integrated Workplace Management System (IWMS)
  - Real Estate and Lease management
  - Facilities and Space management
  - Maintenance management
  - Project management
  - Environmental sustainability

What does a Maintenance Management System do?

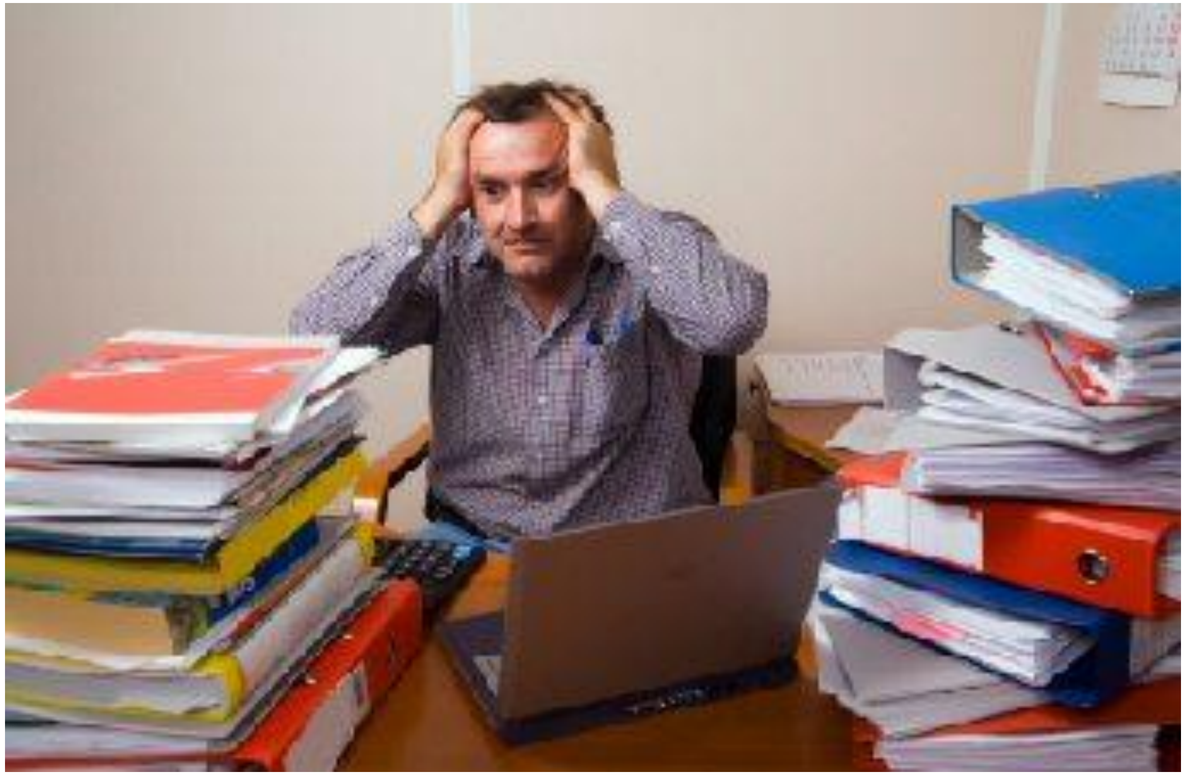
- Assets
- Work Orders
  - Labor
  - Materials
  - Contracted services
- Preventive Maintenance
  - Job plans
  - Frequency
  - Completion status
- Inventory / Shop materials

PM Work Order Generation



Maintenance Management Systems

- Various types of Maintenance Management Systems
  - People-based
  - Paper-based
  - Excel-based
  - CAFM/CMMS/IWMS

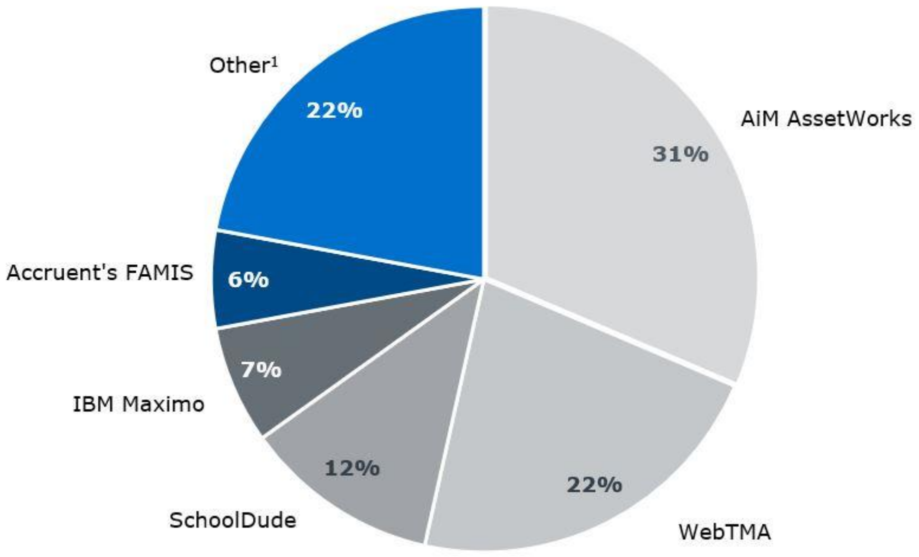


Maintenance Management Systems

Discussion:

- – What are you using?
- – What do you like?
- – What don’t you like?
- – What does it do well?
- – What is it missing?
- – How are you using it?

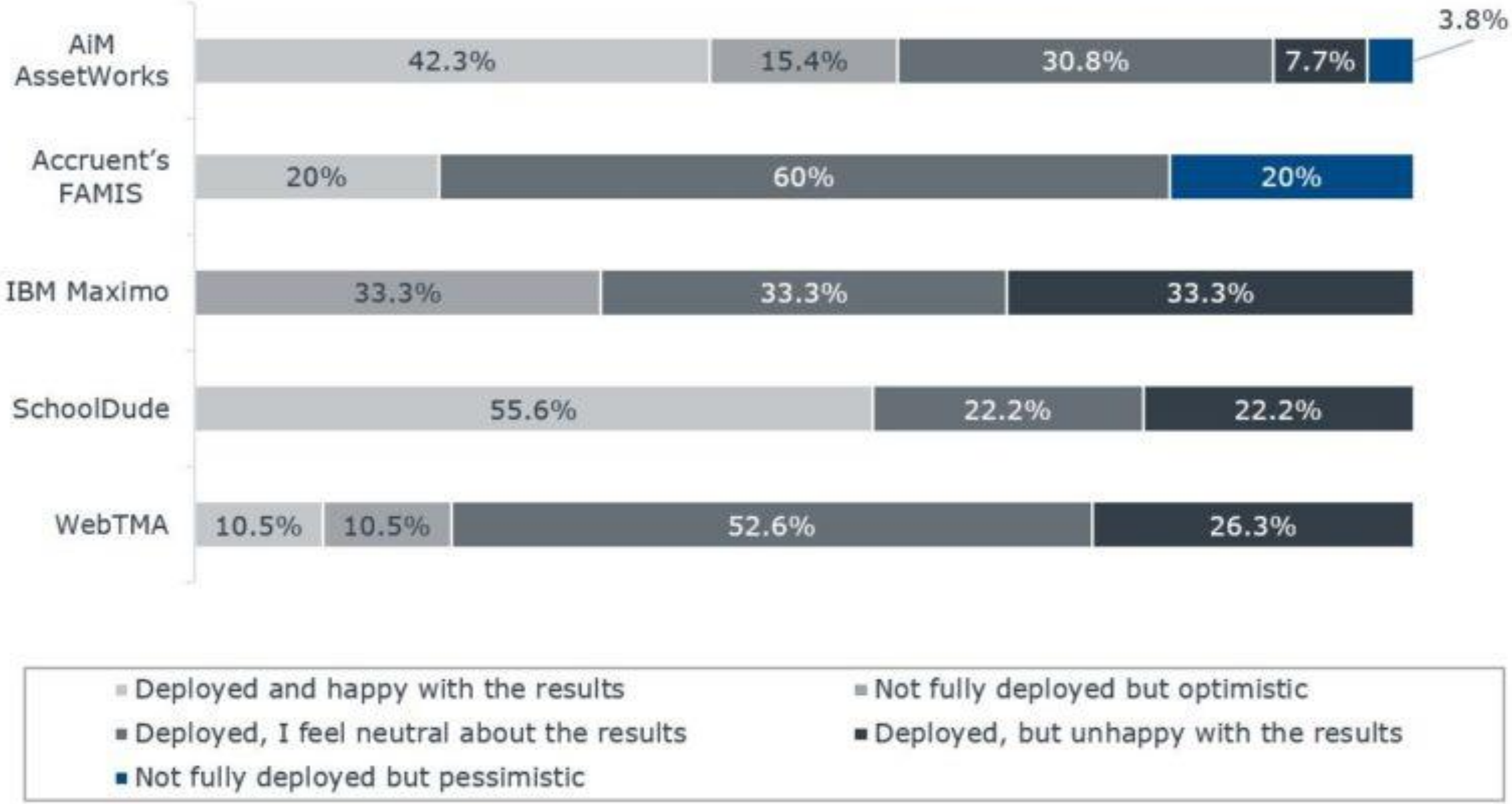
Percentage of institutions using CMMS
n=86



1) The “Other” category includes: Archibus, Home-Grown Systems, IBM TRIRIGA, Peoplesoft, MicroMain, Unifier, NetFacilities, Centerstone, SAP – Plant Maintenance, Plannon, Azzier, Track-It, and schools with multiple systems. Three or fewer institutions reported using each of these platforms.

Satisfaction level by vendor

n=85



Capital Project Management Systems

- Schedule
- Financials
  - Budget
  - Expenses
  - Forecasting
- Resource Allocation
- Project & Portfolio Management

- Discussion:
  - What are you using?
  - What do you like?
  - What don’t you like?
  - What does it do well? What is it missing?
  - How are you using it?

Space Management Systems

- Computer-Aided Design (CAD)
- Geographic Information Systems (GIS)
- Space Management Systems
- Building Information Modeling (BIM)
- Construction Operations Building Information Exchange (COBie)

- Discussion:
  - What are you using?
  - What do you like?
  - What don’t you like?
  - What does it do well? What is it missing?
  - How are you using it?

Energy & Utilities Systems

- Building Automation Systems (BAS) &
  Supervisory Control and Data Acquisition (SCADA)
- Metering
- Monitoring
- Modeling
- Smart buildings
- Dashboards

- Discussion:
  - What are you using?
  - What do you like?
  - What don’t you like?
  - What does it do well? What is it missing?
  - How are you using it?

Other Systems

- Finance
- Human Resources
- Procurement
- Inventory
- Document Management
- Collaboration (e.g. SharePoint)
- Web sites

- Discussion:
  - What are you using?
  - What do you like?
  - What don’t you like?
  - What does it do well? What is it missing?
  - How are you using it?

Operational Technology (OT)

OT Bluff the Listener – Which news story is FAKE?

LIVE
BREAKING NEWS
POLISH TEEN HACKS CITY'S TRAMS
14:13
14-YEAR-OLD USED HOMEMADE TRANSMITTER TO TRIP RAIL SWITCHES | DOZEN INJUR

Casino Hacked Through Fish Tank

FDA Confirms Cardiac Devices Can Be Hacked

Hacker Shuts Down Apartments' Heating System

OT Bluff the Listener – Which news story is FAKE?

LIVE
BREA NEWS
PO SH T N KS S TRAMS
14:13
14-YEAR-OLD USED HOMEMADE TRANSMITTER TO TRIP RAIL SWITCHES | DOZEN INJUR
NEWS SHUTTERSTOCK

Casino Hacked Through Fish Tank

FDA Confirms Cardiac Devices Can Be Hacked

Hacker Shuts Down Apartments’ Heating System

ALL 4 are REAL!!!

OT: What's connected? Which sectors are affected?

EVERY sector is affected

and

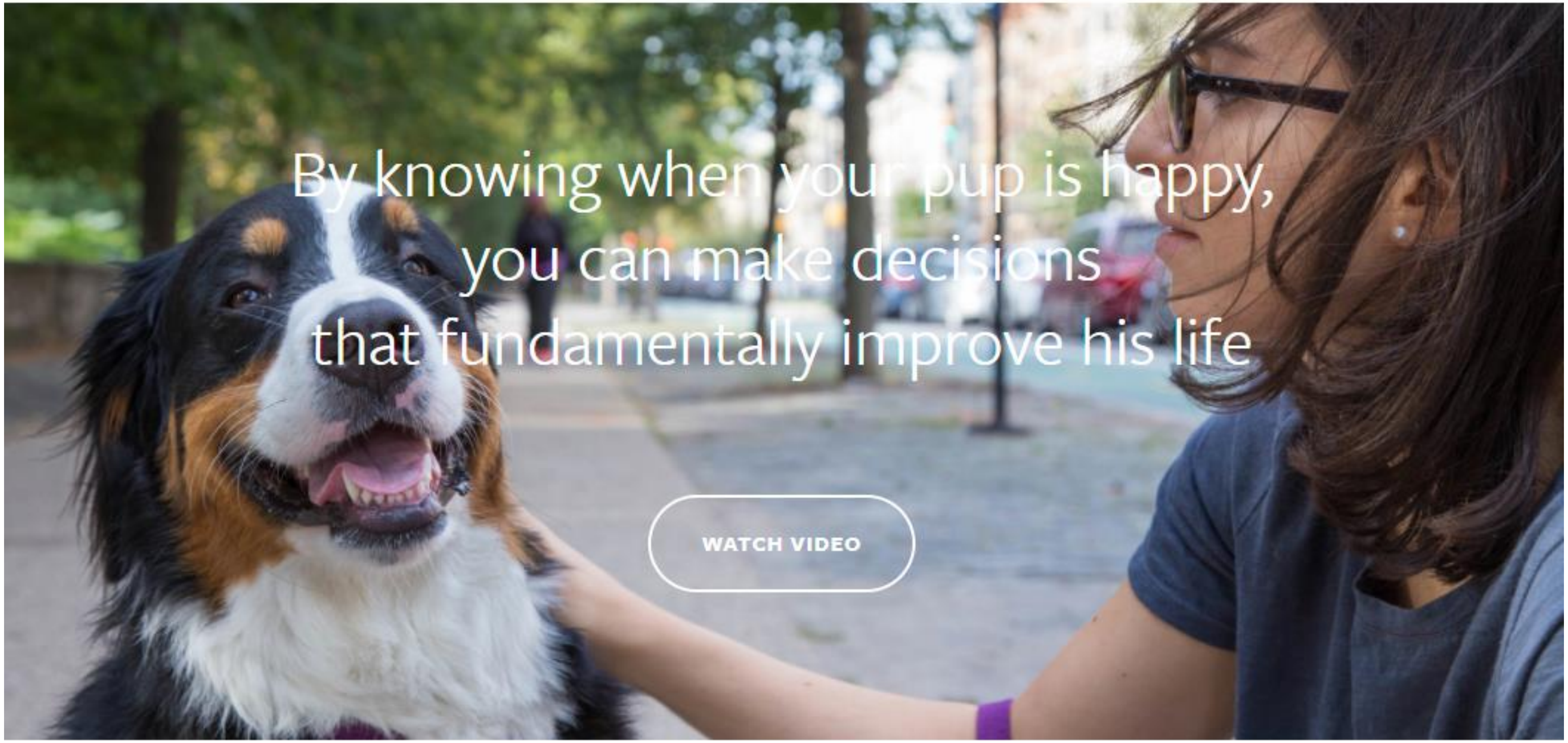
EVERYTHING[*] is connected!

[*] *If it's not currently connected it's probably just a matter of time before it is…*

Internet-connected toilet?

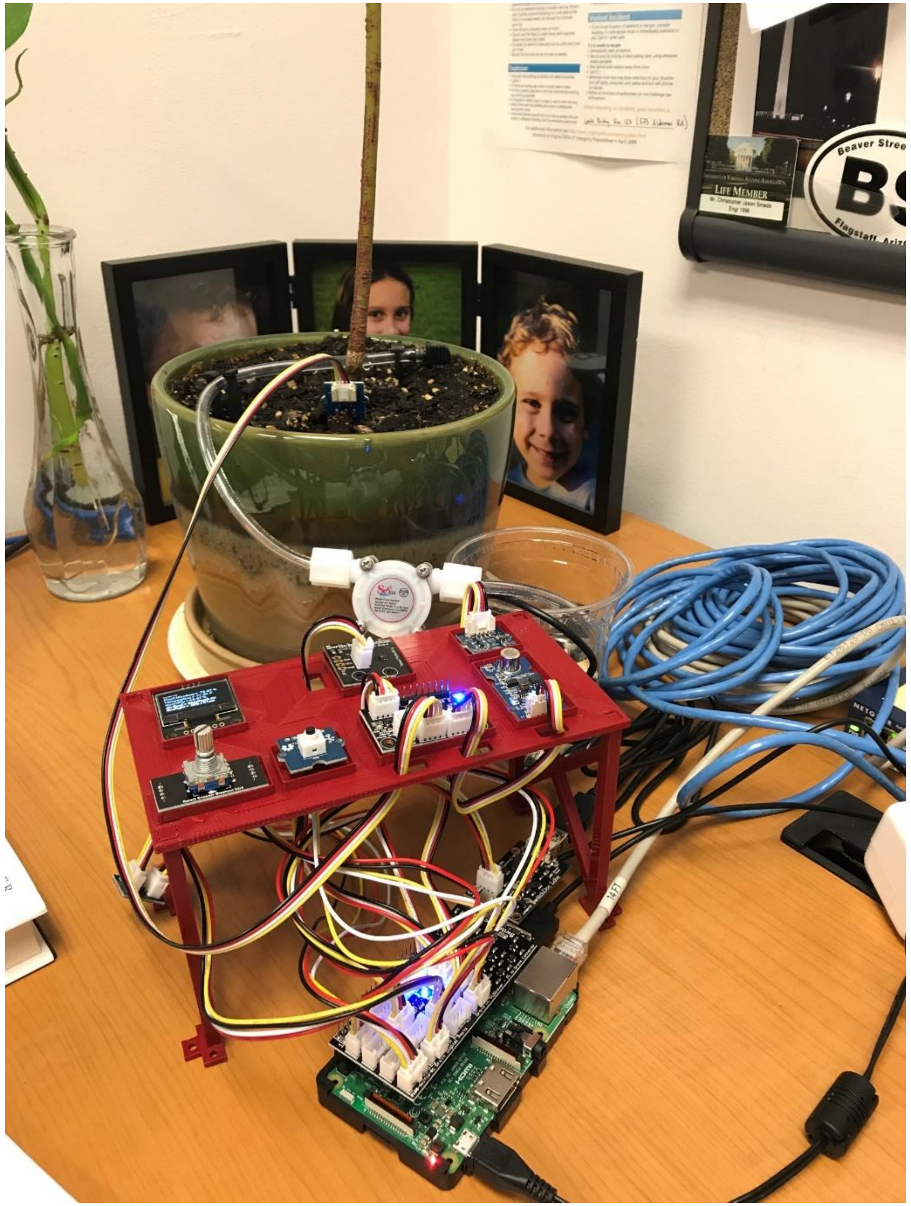
Internet-connected dog?

TailTalk is a smart connected device, worn around the tail, that captures the tail movement and translates it to the emotions our dogs convey.



By knowing when your pup is happy,
you can make decisions
that fundamentally improve his life

Internet-connected houseplant?



WORX

UVA as a case study: OT is everywhere

- Heating, Ventilation & Air Conditioning (HVAC)
- Fire monitoring & suppression
- Elevators
- Lighting systems
- Door & access control
- Electrical metering & switching
- Generators & Uninterruptible Power Systems
- Water & steam distribution systems
- Photovoltaic systems (solar)
- Displays & kiosks
- Key & lockboxes
- Laboratory freezers
- Security cameras
- Research equipment
- Point of sale (POS)
- Pneumatic tube system(s)
- Health System Technology (Clinical engineering)
- Mechanical systems (air compressors, motors pumps, etc...)
- ...

Operational Technology: Making sense of the nomenclature

- Internet of Things (IoT)
- Industrial Control System (ICS)
  - Supervisory Control and Data Acquisition (SCADA)
- Operational Technology (OT)
- Critical infrastructure

  U.S. Dept of Homeland Security: Critical infrastructure consists of the assets, systems, and networks – whether physical or virtual – so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. This is further defined by Presidential Policy Directive 21 (PPD-21)

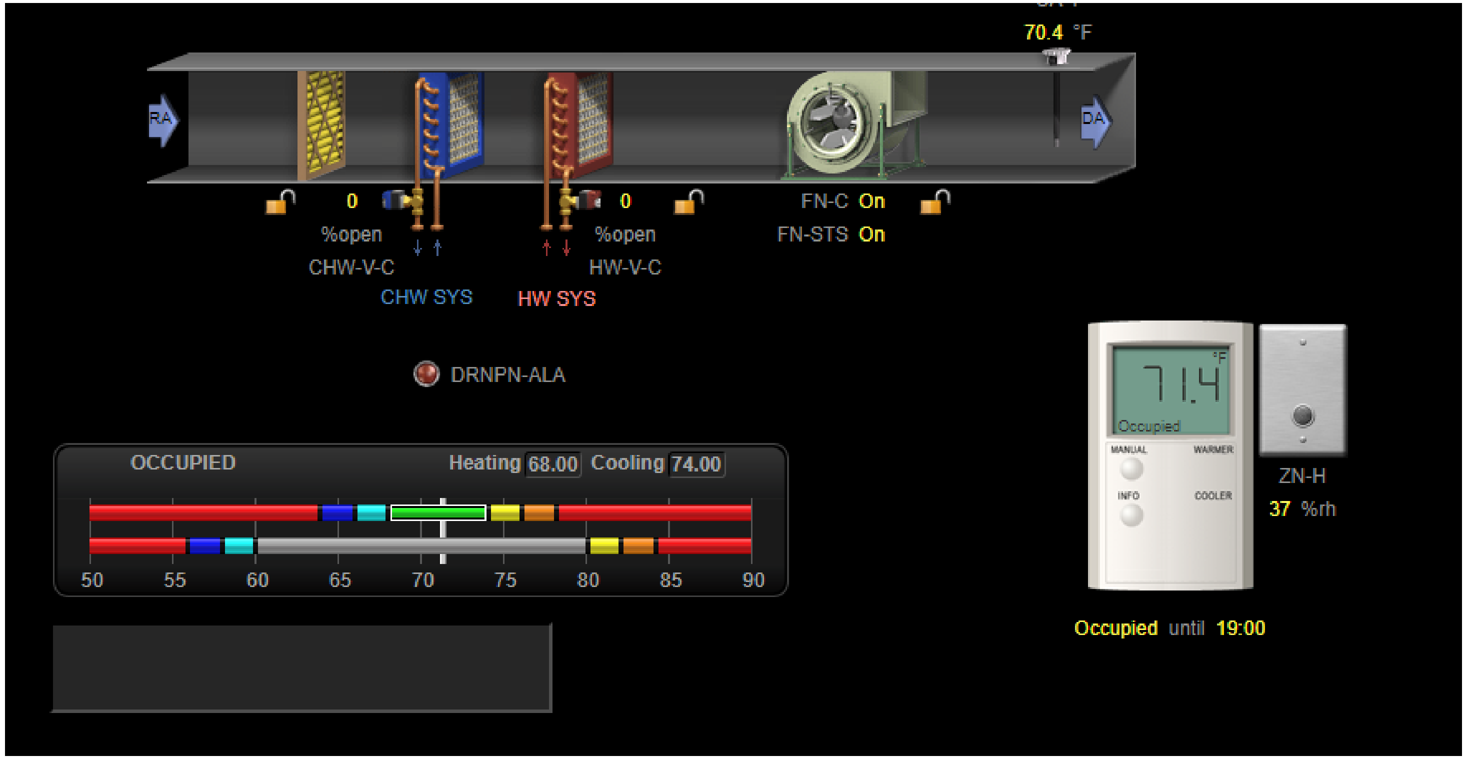
2

UVA Case Study:

Building Automation Systems (BAS)

UVA Case Study: Building Automation Systems (BAS)

- What is BAS and what are we controlling?



FN-C On

FN-STS On

OCCUPIED Heating 68.00 Cooling 74.00

ZN-H 37 %rh

Occupied until 19:00

UVA Case Study: Building Automation Systems (BAS)

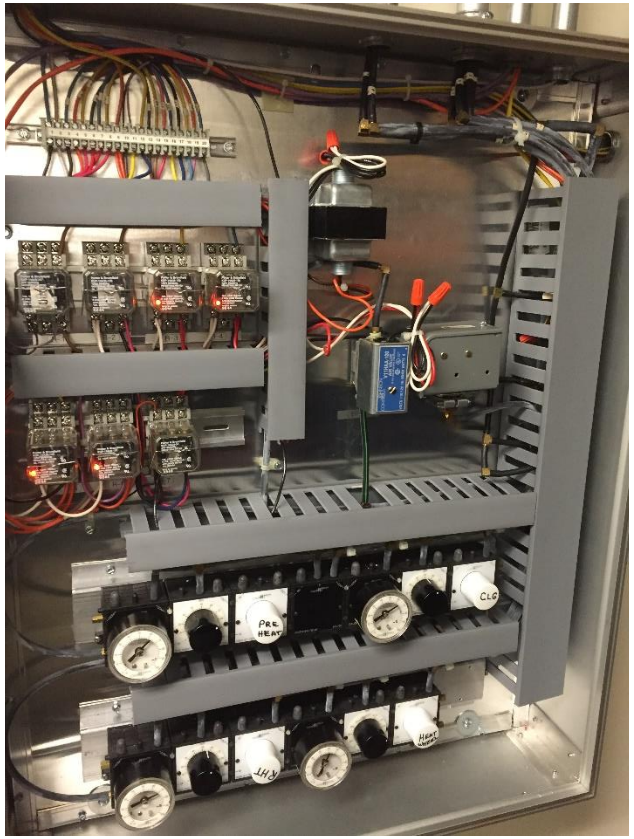
- Started with local manual controls – e.g. switches, valves, etc.

  physically located at the equipment being controlled

GENERAL DUTY SAFETY SWITCH
INTERRUPTOR DE SEGURIDAD DE SERVICIO GENERAL
60 A
240 Vac / V~
SQUARE D
DANGER / PELIGRO
HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH
PELIGRO DE DESCARGA ELÉCTRICA, EXPLOSIÓN O DESTELLO POR ARQUEO
ON
I
O
OFF

UVA Case Study: Building Automation Systems (BAS)

- Moved to pneumatic (compressed air) controls still local to the equipment being controlled

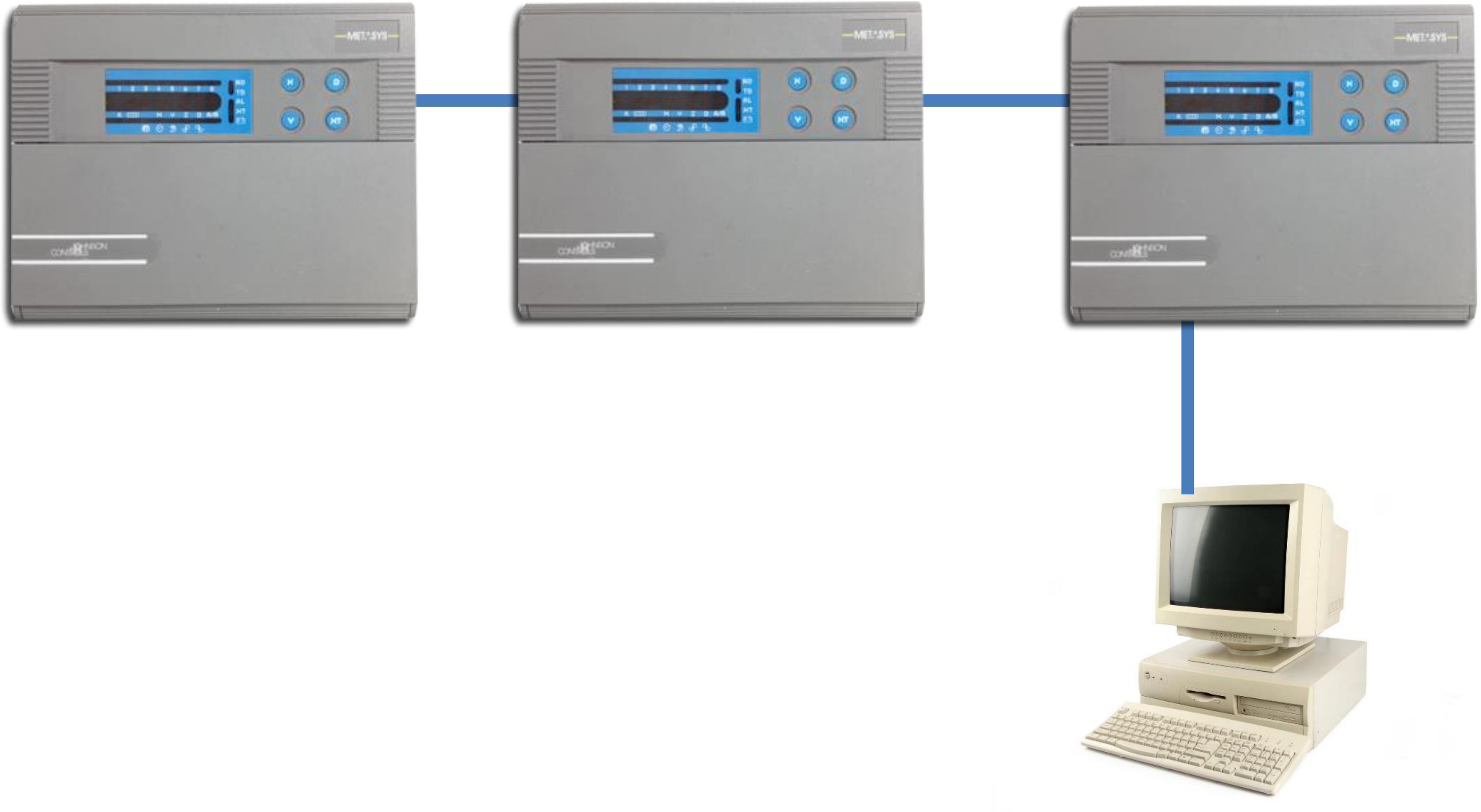


UVA Case Study: Building Automation Systems (BAS)

- Centralized pneumatic/electronic control rooms

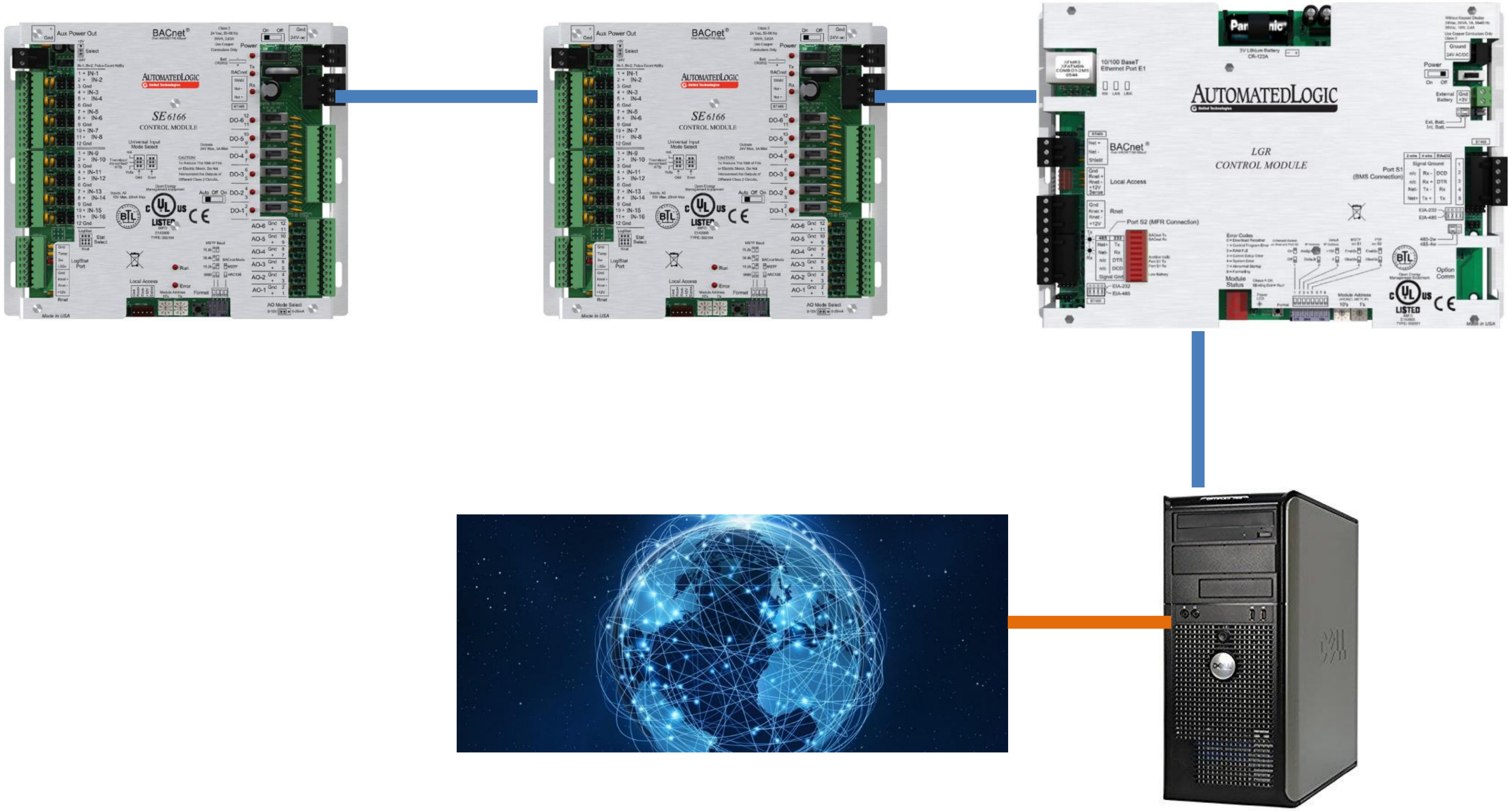
UVA Case Study: Building Automation Systems (BAS)

- Programmable electronic controls local to building



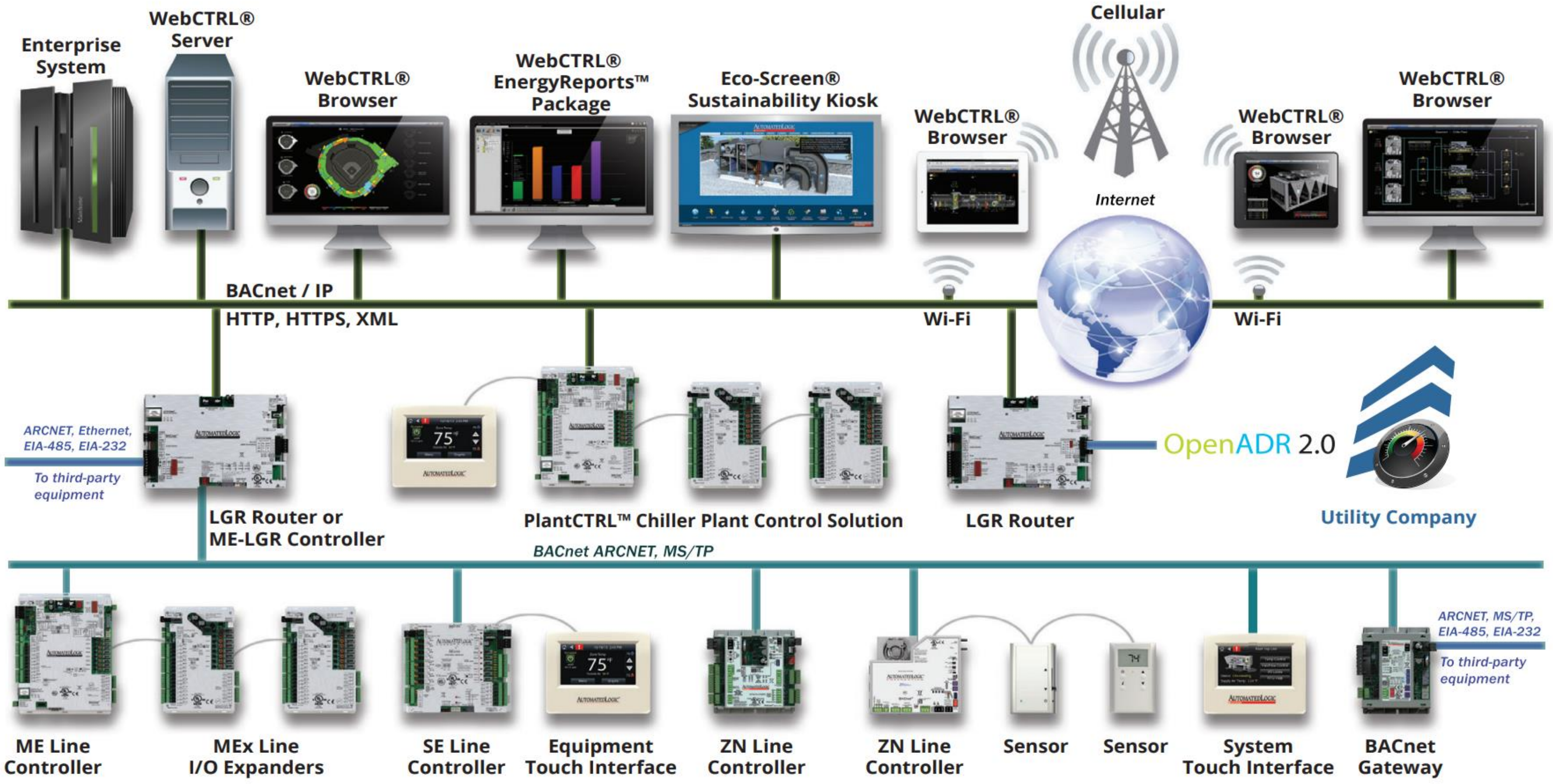
UVA Case Study: Building Automation Systems (BAS)

- Networked direct digital controls (microprocessor based) controls)



UVA Case Study: Building Automation Systems (BAS)

- Modern day (IoT)

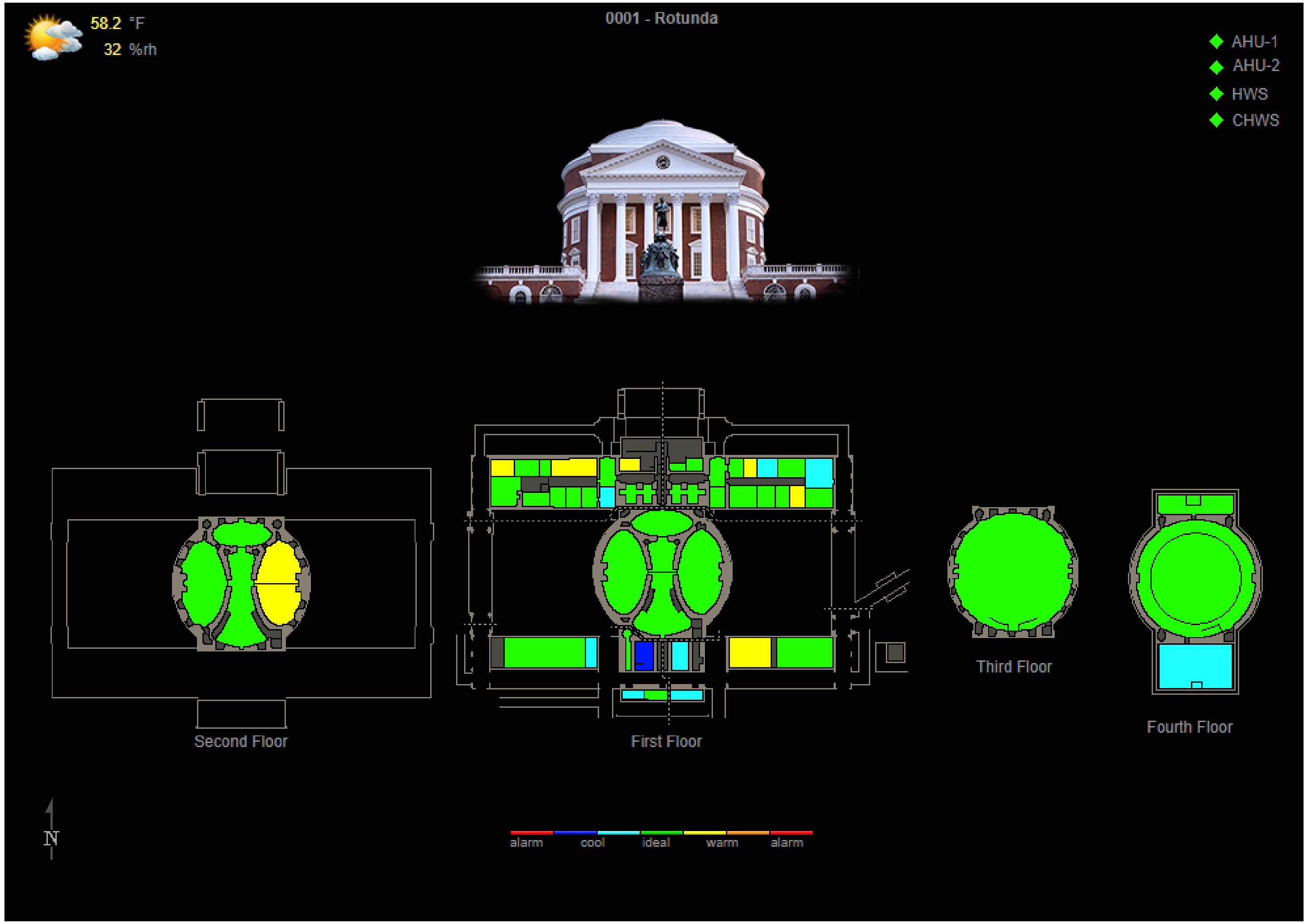


UVA Case Study: Building Automation Systems (BAS)

- 500 Buildings at UVA
- 200 with some type of automation system
- 15,000 distributed controllers
- 95,000 physical sensors/actuators
- Controlling everything from the temperature and air flow in classrooms to the temperature and air flow in the operating rooms.

UVA Case Study: Building Automation Systems (BAS)

- Demonstration of BAS user interface



3

OT Cybersecurity Risks

Three days without power
is very different from
three days without email

IoT cybersecurity risks extend beyond kinetic impacts

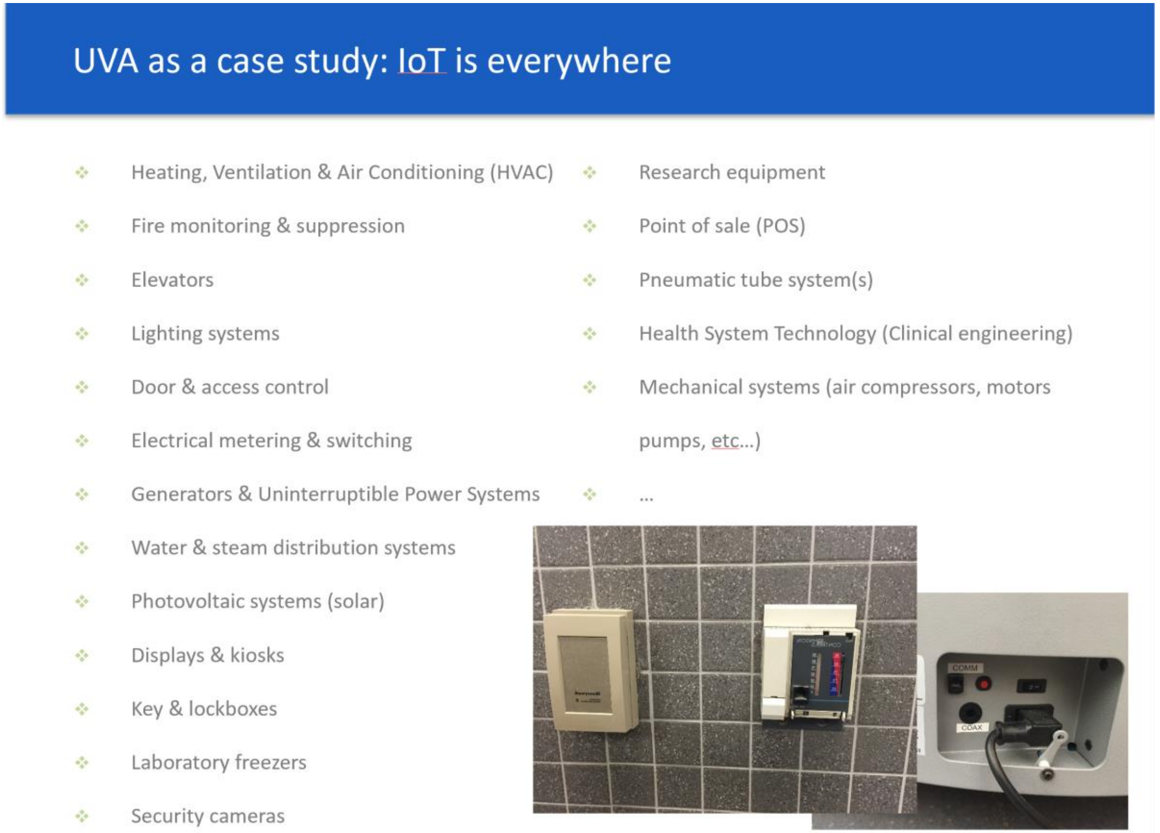
- Vector for intruders (DDoS/lateral movement)
- Privacy
- Theft/Sabotage of Intellectual Property
- Compliance
  - Critical infrastructure
  - Regulatory requirements

4

Best practices
OT Cybersecurity

Best practices in OT cybersecurity – the top strategy

Awareness!!



UVA as a case study: IoT is everywhere

- Heating, Ventilation & Air Conditioning (HVAC)
- Fire monitoring & suppression
- Elevators
- Lighting systems
- Door & access control
- Electrical metering & switching
- Generators & Uninterruptible Power Systems
- Water & steam distribution systems
- Photovoltaic systems (solar)
- Displays & kiosks
- Key & lockboxes
- Laboratory freezers
- Security cameras
- Research equipment
- Point of sale (POS)
- Pneumatic tube system(s)
- Health System Technology (Clinical engineering)
- Mechanical systems (air compressors, motors pumps, etc...)
- ...

Best practices in OT cybersecurity – the top technical control

Isolation of assets

- Physical security
  - Don’t overlook – but can be hard in some cases with OT
- Network architecture
  - Separate networks, firewalls, remote access, VPN, DMZ
  - BEWARE of transitive trusts – Target! Stuxnet!
  - Design to prevent lateral movement
  - “Air gaps are just high latency networks”
- Control what is on your network

Best practices in OT cybersecurity – next steps

Basic security hygiene

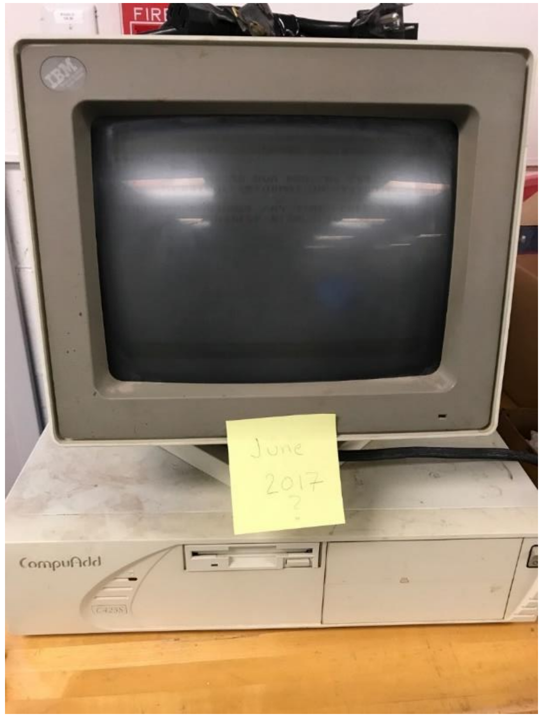
- Patches, upgrades
- Disable unnecessary ports & services
- Device/network scanning & profiling
- Account management
  - Default user names / passwords
  - Password policies
  - Principle of least privilege
- Log & event monitoring
- Anomaly & intrusion detection, e.g. IDS/IPS

Best practices in OT cybersecurity – other practices

- Resiliency / redundancy
  - e.g. redundant systems, failover systems, safety-instrumented systems, “security-instrumented” systems…
- Policies / standards / contractual language
- Education & awareness
- “Analog” Continuity of Operations Planning (COOP)
- Collaboration between IT & OT teams, network, policy, audit, risk management teams…
- Beef up your risk assessment:
  - Penetration testing, third party assessments, Shodan yourself!
  - Think like the enemy!

OT Cybersecurity: There are real world challenges to implementing best practices

- Nature of OT systems
  - Real-time / focus on operations
  - Disparity in system lifecycle
  - Proprietary vs. embedded OS
  - Limited ability to patch/upgrade systems
  - Cost / impact of upgrade
- Security blindness: Lack of awareness & faulty assumptions – "This system can't be hacked…"
- Failure to adequately assess, understand & identify risks
- Products rushed to market
- Organizational silos (IT vs OT)



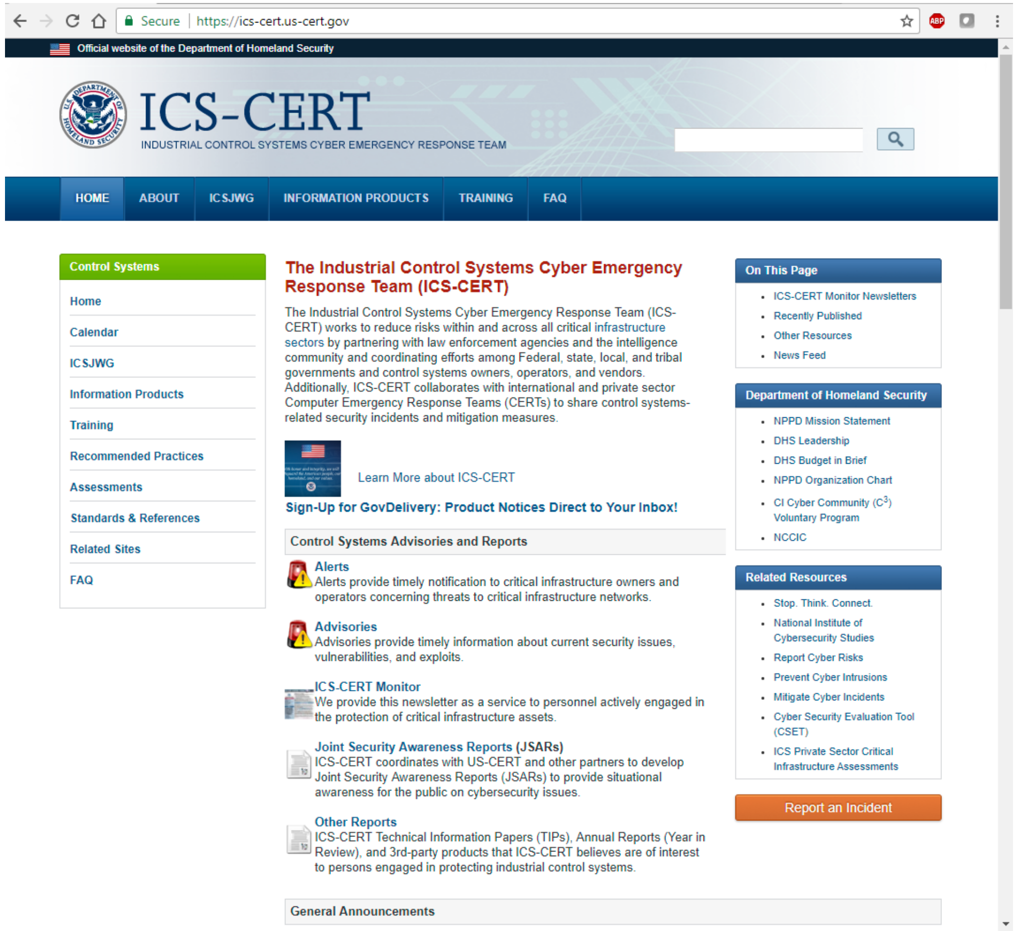
Best practices in OT cybersecurity: Resources

- Standards
  - **NIST 800-82** – Guide to Industrial Control Systems (ICS) Security
  - **NIST 800-53** – Security and Privacy Controls for Federal Information Systems and Organizations
  - **North American Electric Reliability Corporation (NERC)** – Critical Infrastructure Protection Standards
  - **Nuclear Regulatory Commission (NRC)** – Cyber Security Programs for Nuclear Facilities
  - **Committee on National Security Systems Instruction (CNSSI)** – Security Categorization and Control Selection for National Security Systems
  - **Interstate Natural Gas Association of America (INGAA)** – Control Systems Cyber Security Guidelines (Natural Gas Pipeline Industry)

Best practices in OT cybersecurity: Resources

- U.S. Department of Homeland Security – **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) - https://ics-cert.us-cert.gov/**

  - Alerts & Advisories
  - Training
  - Publications
  - References
  - Recommended Practices
  - Community
  - Assessments



Secure | https://ics-cert.us-cert.gov

Official website of the Department of Homeland Security

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Control Systems

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

Learn More about ICS-CERT

Sign-Up for GovDelivery: Product Notices Direct to Your Inbox!

Control Systems Advisories and Reports

Alerts
Alerts provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks.

Advisories
Advisories provide timely information about current security issues, vulnerabilities, and exploits.

ICS-CERT Monitor
We provide this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets.

Joint Security Awareness Reports (JSARs)
ICS-CERT coordinates with US-CERT and other partners to develop Joint Security Awareness Reports (JSARs) to provide situational awareness for the public on cybersecurity issues.

Other Reports
ICS-CERT Technical Information Papers (TIPs), Annual Reports (Year in Review), and 3rd-party products that ICS-CERT believes are of interest to persons engaged in protecting industrial control systems.

General Announcements

On This Page

- ICS-CERT Monitor Newsletters
- Recently Published
- Other Resources
- News Feed

Department of Homeland Security

- NPPD Mission Statement
- DHS Leadership
- DHS Budget in Brief
- NPPD Organization Chart
- CI Cyber Community (C^3) Voluntary Program
- NCCIC

Related Resources

- Stop. Think. Connect.
- National Institute of Cybersecurity Studies
- Report Cyber Risks
- Prevent Cyber Intrusions
- Mitigate Cyber Incidents
- Cyber Security Evaluation Tool (CSET)
- ICS Private Sector Critical Infrastructure Assessments

Additional resources & further reading…

- ICS-CERT – Industrial Control Systems Cyber Emergency Response Team

  https://ics-cert.us-cert.gov/

- NIST 800-82 – Guide to Industrial Control Systems (ICS) Security

  https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

- SANS ICS 410 – ICS/SCADA Security Essentials

  https://www.sans.org/course/ics-scada-cyber-security-essentials

- The End of Cybersecurity, Andy Bochman, HBR

  https://hbr.org/cover-story/2018/05/internet-insecurity

- SCADAhacker.com – https://scadahacker.com

- Darknet Diaries, *https://darknetdiaries.com/ (podcast)*

PRIVACY.FLOWCODE.COM

Thank you!

Questions and/or comments?

UNIVERSITY of VIRGINIA

Chris Smeds

Director of Technology & Innovation

U.Va. Facilities Management

smeds@virginia.edu

This concludes The American Institute of Architects Continuing Education Systems Course

AIA Approved Continuing Education