Connected Lighting

Kevin Powell, Emerging Technologies Program Director

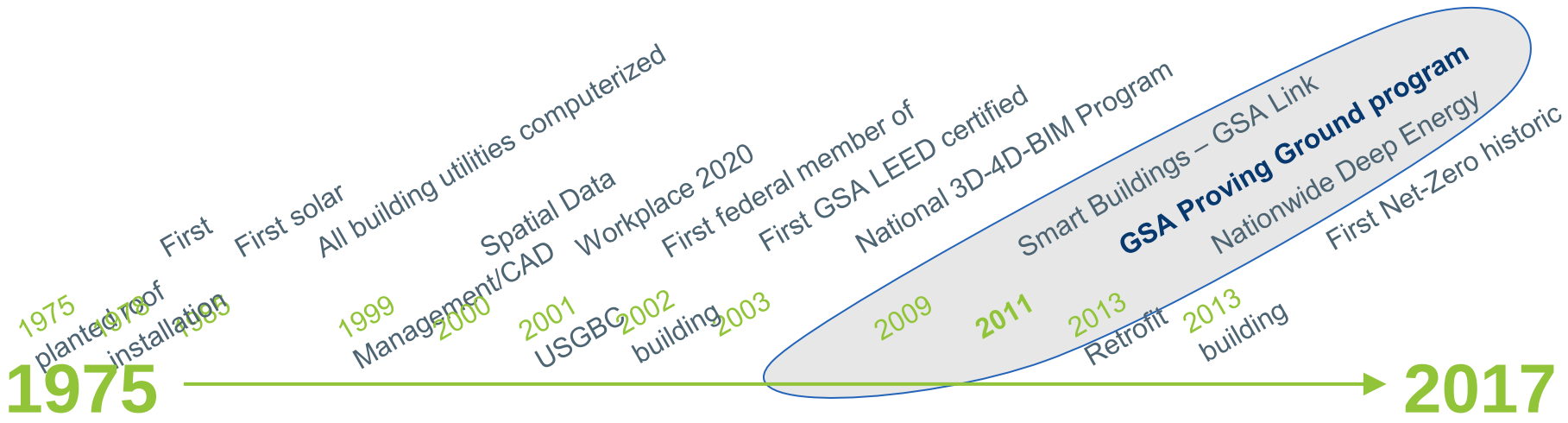
U.S. General Services Administration | 8 June 2017

GSA

Agenda

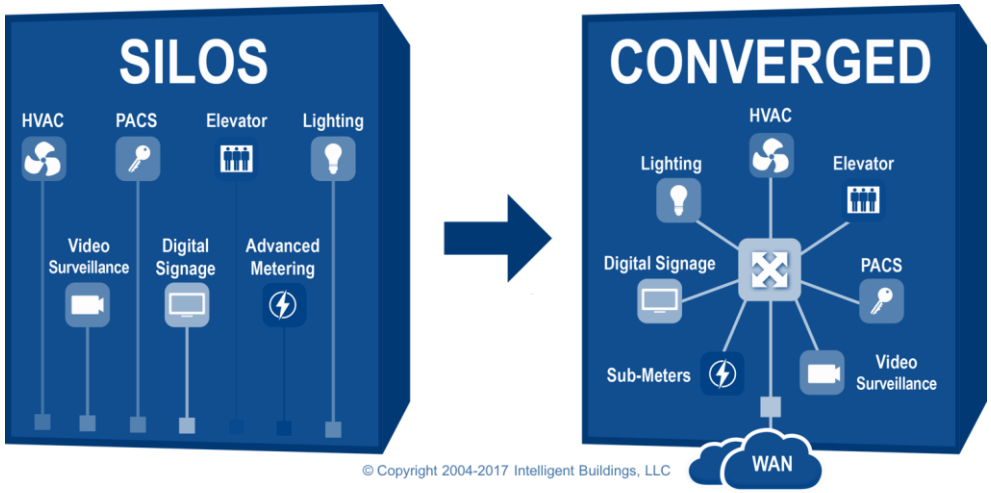
- GSA Leadership in Connected Technologies
- Smart Connected Buildings
- Securing Connected Buildings
- Recommendation for Technology Developers & Building Owners

GSA Leadership In Innovative Technologies

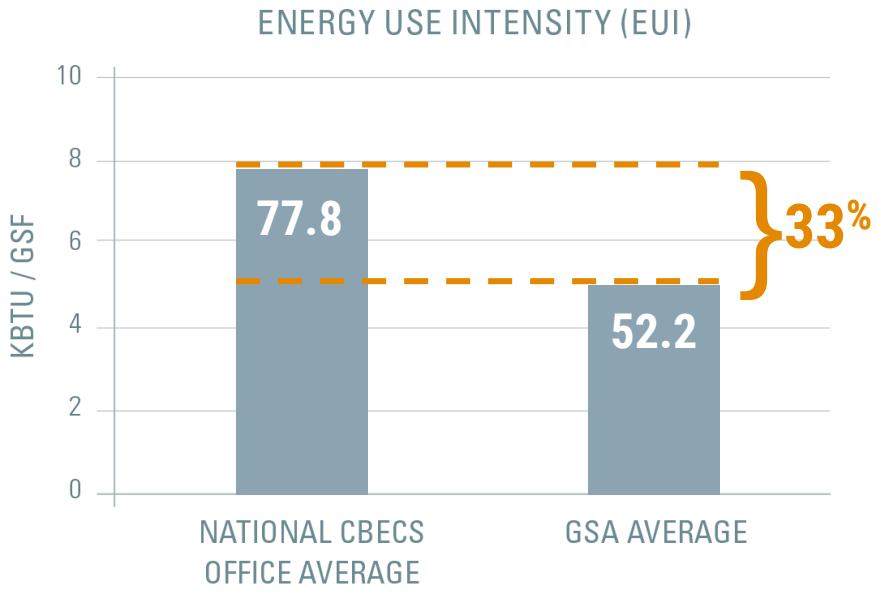


NextGen-Facilities Architecture

- IP and wireless migrating to common communication standards.
- Converged systems enable improved building operations.
- “Digital Ceiling Strategy” a key enabler of converged building architecture



Why Connected Technologies?



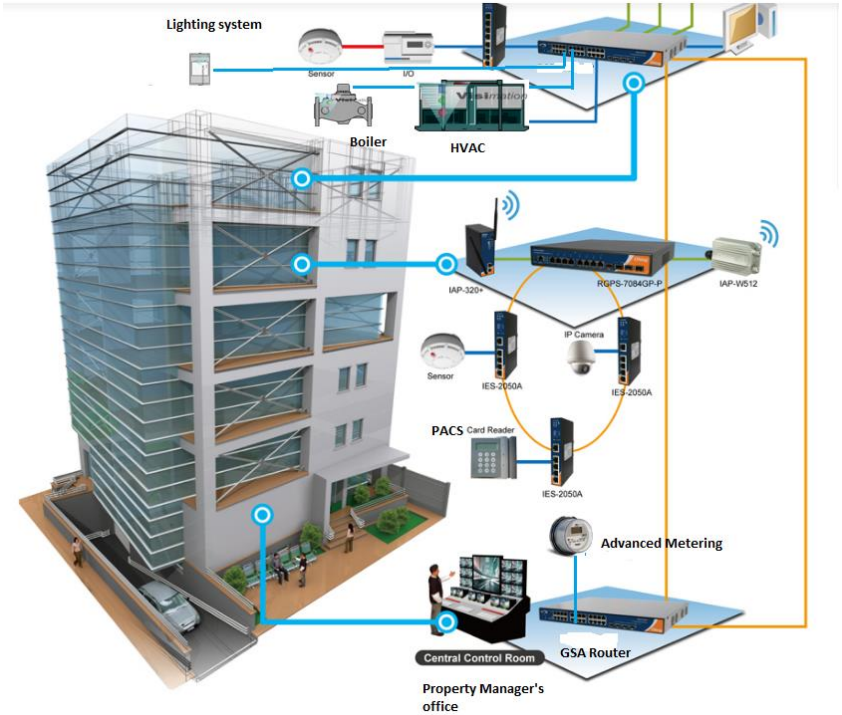
GSA buildings are 33%* more efficient than typical U.S. commercial buildings.

Efficiency partly achieved through connected systems.

*January 2016, GSA Average EUI = 52.2 kBTU/GSF/yr, as reported per legislative mandate; 2012 CBECS, eia.gov

Current State - Ad Hoc

- Building systems utilize IT networks.
- Building operation & maintenance are reliant on technology.
- Security is often an afterthought in solution development.



Advantages and Risks of Connected Technologies

- Integration provides significant cost savings via analytics, fault detection and remote control of systems.
- IT is outside the scope of knowledge of most O&M staff.
- Until recently, there has been a disconnect between IT and facility management.

GSA Security Assessment Process for ICS

- Path Forward:
  - All industrial control systems (ICS) must be scanned and vulnerabilities remediated before they can be integrated onto the GSA network or allowed to communicate wirelessly
- What Must Be Assessed?
  - Any device, appliance, software or hardware of any kind that has control functionality, has the ability to execute commands, process information, and/or communicate via TCP/IP
- Process?
  - There must be a GSA project associated with the device in order to be scanned
  - Same model and version assessed and remediated once

Overall Guidance

Vendors Should

- ❏ “Bake in” cyber security by following NIST 800-53 Rev 4 “Recommended Security Controls for Federal Information Systems and Organizations” and NIST Special Publication (SP) 800-82 Revision 2 “Guide to Industrial Control Systems (ICS) Security”
- ❏ Adhere to NIST FIPS 140-2 Encryption modules and TLS 1.2 or higher encryption
- ❏ Allow sufficient time to submit required information and remediate vulnerabilities identified by GSA IT Security in advance of implementation as part of a project

Challenges

- Industry often builds product with cyber security as an afterthought
- IT security compliance timeline can be at odds with construction critical path
- Vendor may not have resourcing required for responsiveness to IT security process
- Evolving technology and security risks, evolving requirements for IT Security compliance
- Proper contracting to ensure maintenance is included as part of project scope
- Competition creates diverse architecture, at the same time limits ability to standardize
- How to update/upgrade IT enabled components of equipment with long duty cycle

Recommendation for Technology Developers & Building Owners

Opportunity favors the prepared mind

"Sir, the following paradigm shifts occurred while you were out."

For more information: gsa.gov/GPG

Kevin Powell kevin.powell@gsa.gov 510.423.3384