TETRA TECH

Clouds and Things…

Implications of the Cloud and Internet-of-Things for SCADA/ICS

January 8, 2018

American Water Works Association
Florida Section

Agenda for this presentation

- Overview of the Cloud, Fog & Internet-of-Things
- IoT device capabilities
- IoT communications capabilities
- Implications for SCADA/ICS
- Planning for the Cloud, Fog & Internet-of-Things
- Q&A

I promise…

- This is *not* a sales presentation

Overview of the Cloud, the Fog and Things

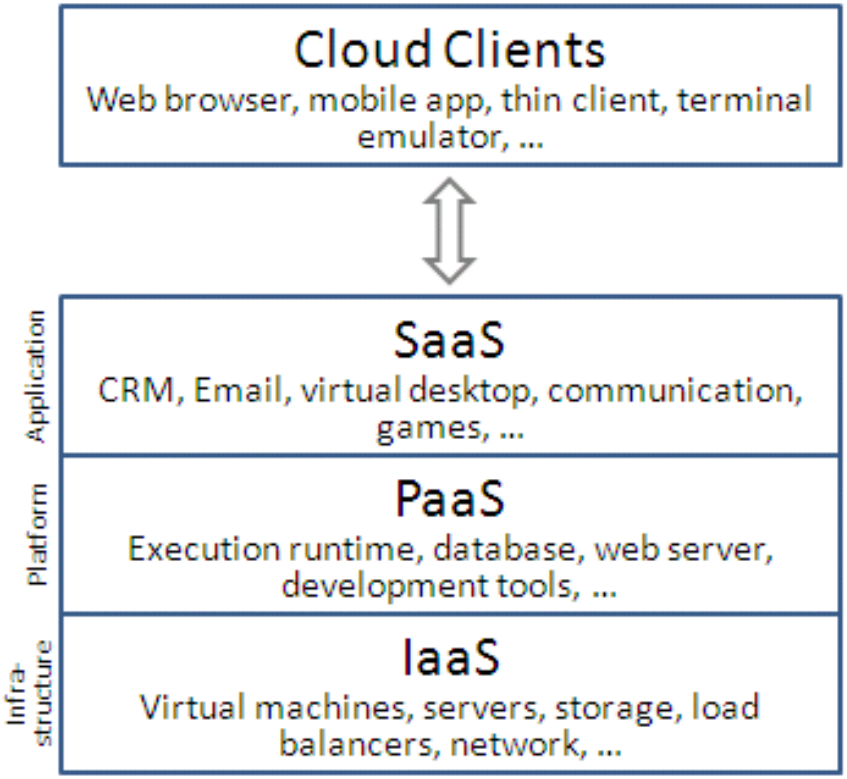
A brief introduction to Internet-connected computing

Cloud Computing

- **Characteristics:**
  - Based on virtualization
  - Servers and other network infrastructure hosted on the Internet to store, manage and process data – "Somebody else's computer"
  - Avoids up-front costs for data center build-out
  - Device and location independence – access from anything, anywhere
  - 3rd party hardware, software *and maintenance*
  - Scalable, flexible, (potentially) robust
  - Pay-as-you-go pricing – like a utility – rather than billed up-front – variable versus capital expense
  - You get what you pay for – Nothing comes for free

Cloud Computing

- **Variations:**
  - Private, public or hybrid models
  - Infrastructure as a Service (IaaS)
    - Virtual Private Network
    - Virtual data center
  - Platform as a Service (PaaS)
    - Application hosting
  - Software as a Service (SaaS)
  - Anything as a Service (Xaas)
    - Storage
    - Security
    - Mobile



Cloud Computing

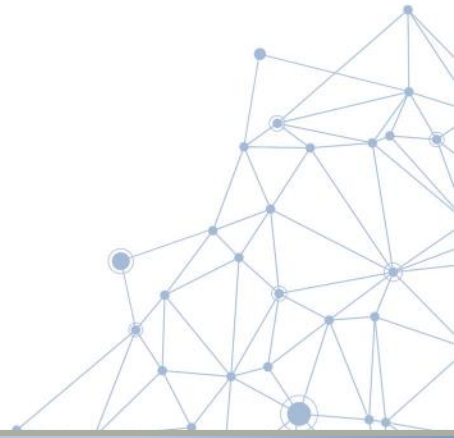
- **The evolution of Cloud Computing:**
  - Virtual Machines – Server-level virtualization
    - Hardware is abstracted
    - Network infrastructure is abstracted
  - Containers – Application virtualization
    - Operating system is abstracted
  - Serverless computing – Process virtualization
    - Application is abstracted

Fog Computing

- **Characteristics:**
  - Processing focused at edge of network near the source – “closer to the ground” – rather than in the cloud
  - Data processed locally in smart devices, reducing communications
  - Addresses the need of edge computing in Internet of Things and Industrial Internet of Things (IoT/IIoT)
  - Data hubs, routers or gateways

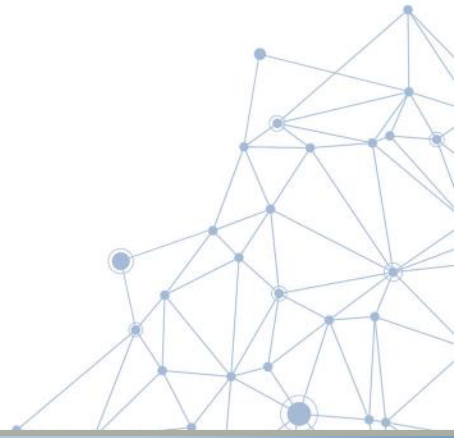
Fog Computing

- **Variations:**
  - Edge computing
  - Mobile edge computing
  - Compute, storage and networking between end devices and cloud computing
  - May be used for security and compliance reasons
  - Smart *everything:*
    - Grid
    - City
    - Buildings
    - Vehicle networks – Cars, roads, ships
    - Software-Defined Networks



Internet of Things (Everything)

- **Characteristics:**
  - Allows monitoring and control of anything that can be measured nearly anywhere
  - Leverages computing advances
    - CPU costs approaching zero
    - Bandwidth costs approaching zero
    - Low-power enables battery and solar options
  - Enables new types of things, new types of sensors
  - Big data is based on little data – “things”



Internet of Things (Everything)

- **Variations:**
  - Industrial Internet of Things (IIoT)/Industrial Internet
    - Machine learning
    - Big data
    - Machine-to-Machine (M2M) communications
  - Intranet of Things
    - Accessibility limited to private network(s)

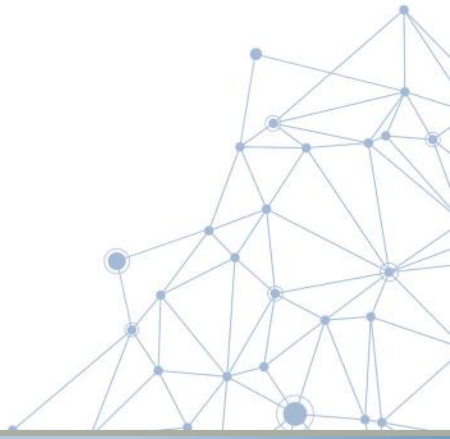
Thinking about things…

If you could monitor anything, anywhere for low initial capital costs, and only usage-based recurring costs, what would you add?

- Flows
- Ph
- Turbidity
- Temperature
- Wind
- Barometric pressure
- Air quality
- Power consumption
- Meter reads and shut-offs
- Offsite cameras
- Physical alarms

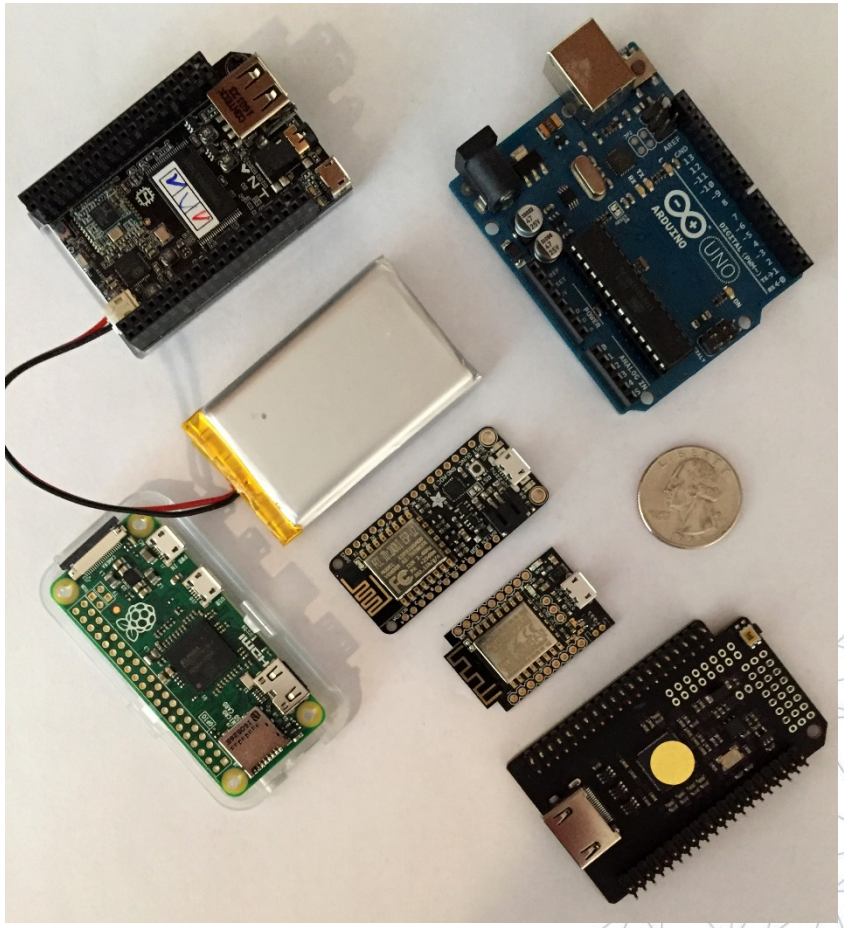
IoT Device Capabilities

Low-cost, low-power, ubiquitous computing



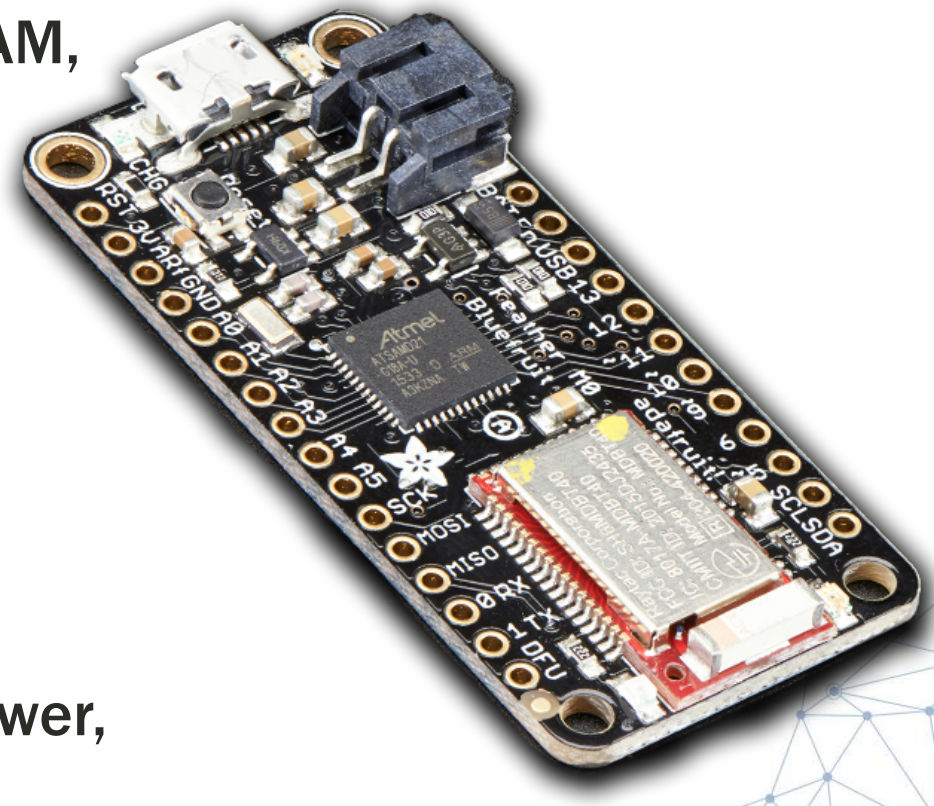
IoT Characteristics

- Anything can be a “thing” with the addition of intelligence and connectivity
- Low-cost hardware is making instrumentation of large numbers of devices economical
- A variety of connectivity options and reach is expanding networks
- Optimization for low power is making battery, solar power and energy harvesting practical



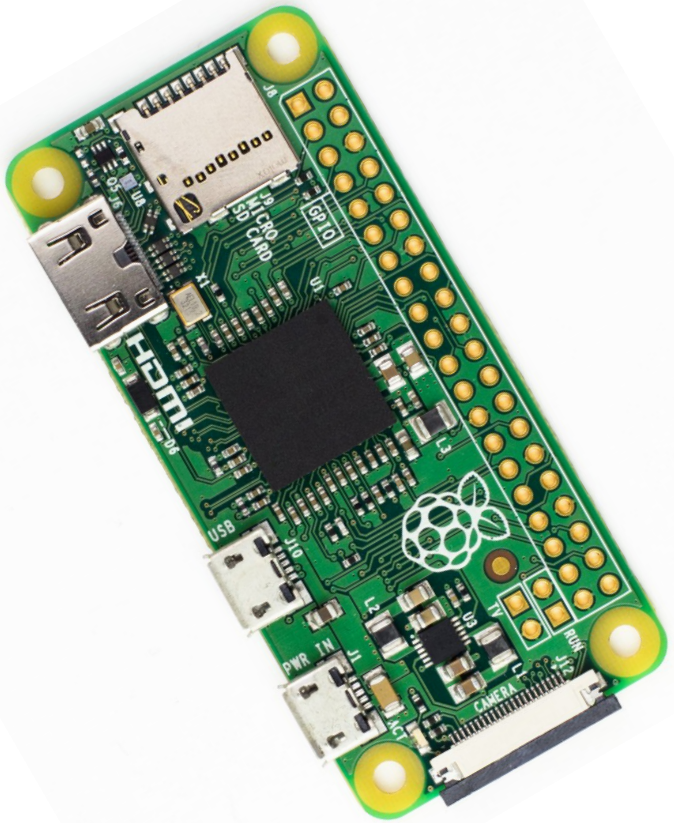
Microcontrollers

- 8-160 MHz CPU, 128 KB RAM, 4 MB Flash
- Connectivity variants:
  - 802.11 b/g/n
  - Bluetooth/BLE
  - LoRa (900 MHz available)
  - Packet radio
- 10 GPIO
- 3-12VDC, <500 mA, low power, sleep modes
- Price: $10.00 - $35.00 retail



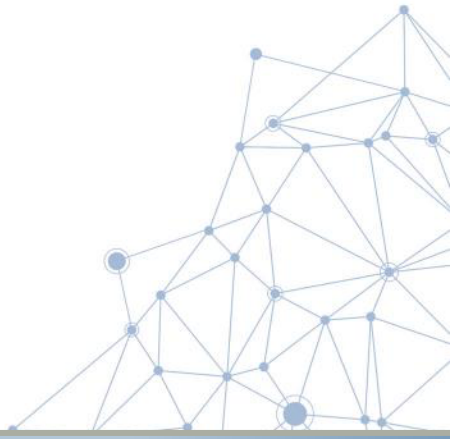
Single Board Computers (SBC)

- Price: $5.00
- 1 GHz ARM CPU
- 512MB RAM
- 40 pin GPIO
- USB
- 5v, 700-2500 mA



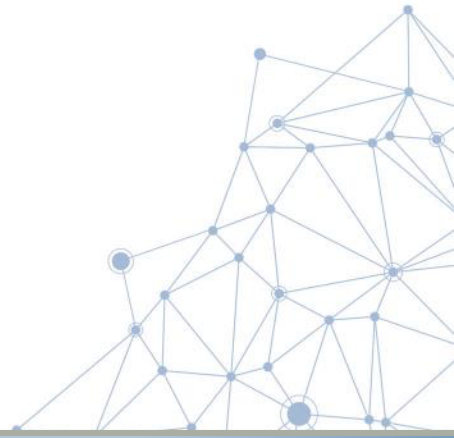
IoT Communications

Long and short range options



IoT Communications

- **Support industrial protocols and/or TCP/IP**
- **Optimized for low-speed, unreliable links**
- **Machine-to-machine – M2M**
- **Publish-subscribe model**
- **Quality-of-Service**
  - Best-effort, fire-and-forget
  - At least once
  - Only once



IoT Communications

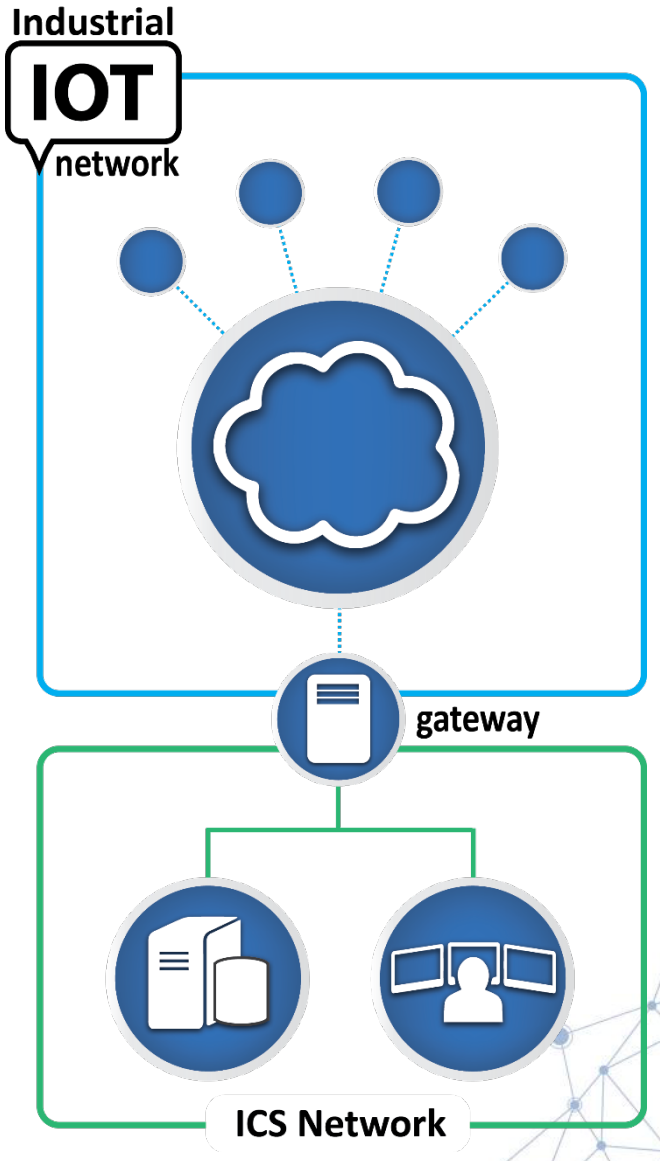
- **Communications are not limited to any particular media or mode:**
  - Wired and fiber Ethernet – Multi-gigabit speeds, hundreds of meters
  - 802.11 WiFi networks – Gigabit speeds, hundreds of meters, line-of-sight
  - Cellular data – Up to 100's of megabit speeds, nation-wide
  - Zigbee, HART, 802.15.4, Bluetooth Low-Entergy short-range networks – Kilobit-Megabit speeds, short range, line-of-sight
  - 6LoWPAN, LoRaWAN, licensed and unlicensed wireless spectrum Serial- Megabit speeds, 10s-100s of Km

IoT Deploymet

- **On-plant:**
  - Wired and fiber Ethernet – Suitable for backbones, individual devices
  - 802.11 WiFi networks – Suitable for backbones (backhaul), individual devices
  - Zigbee, HART, 802.15.4, Bluetooth Low-Entergy – Suitable for individual devices
- **Off-plant:**
  - Cellular data – Suitable for devices, gateways
  - 6LoWPAN, LoRaWAN, licensed and unlicensed wireless spectrum Serial- Megabit speeds, 10s-100s of Km
- **Gateways can tie together different networks**

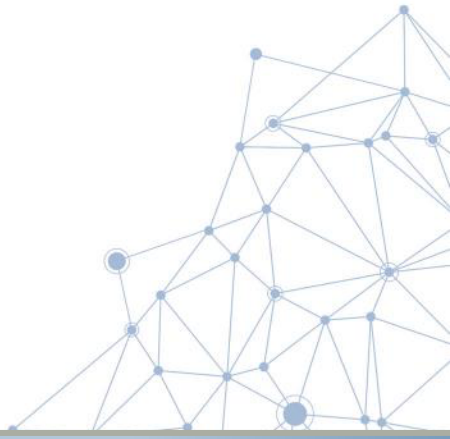
Communications Gateways

- Groups of things may communicate with intermediate brokers and/or gateways across different media and networks
- Gateways can provide more robust capabilities
- Brokers simplify communications
  - Publish
  - Subscribe, unsubscribe
  - Quality of Service
    - At most once
    - At least once
    - Exactly once



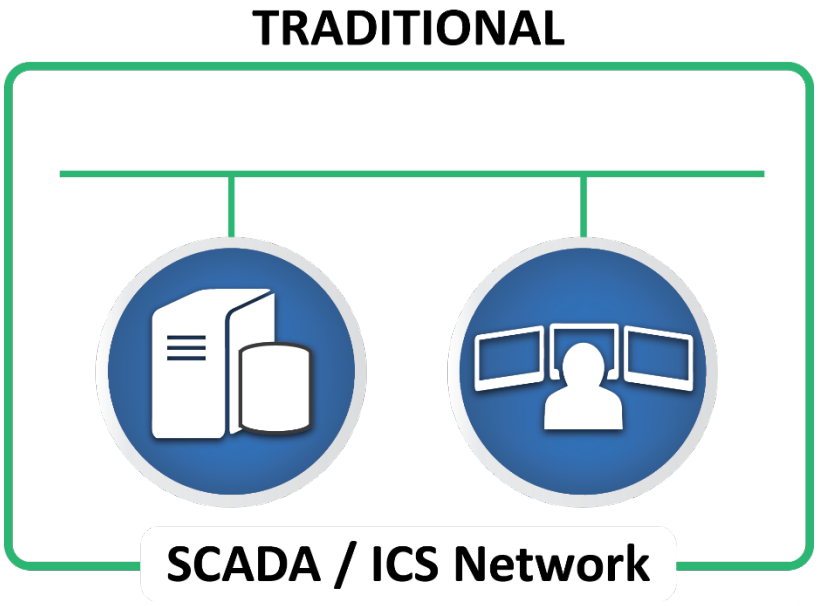
Implications for SCADA/ICS

The expanding network perimeter



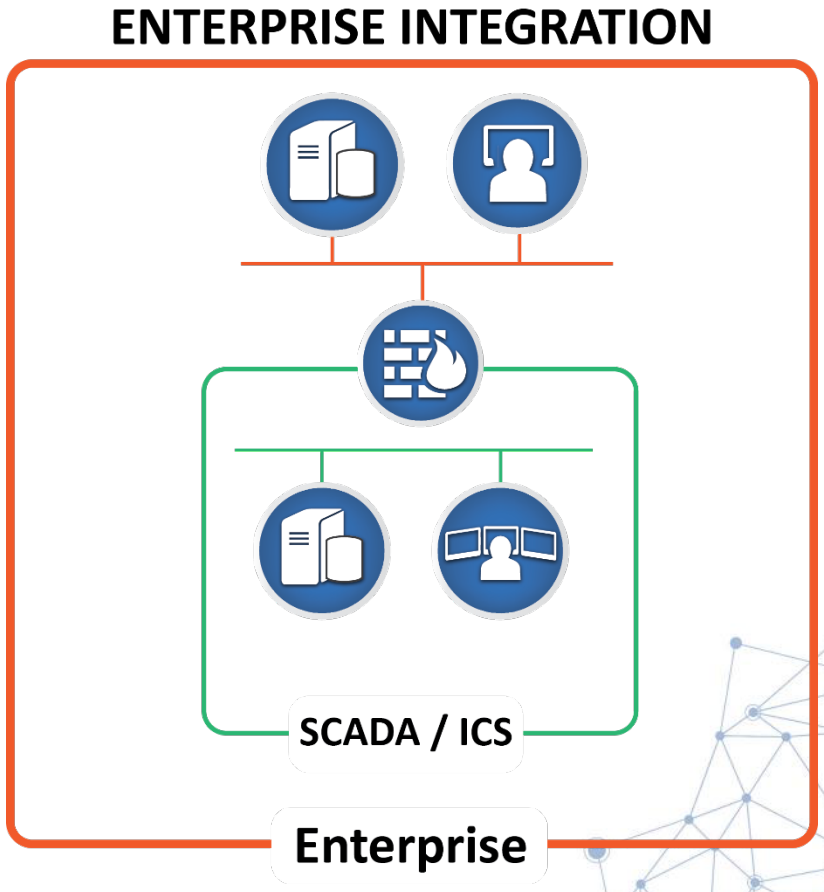
Traditional SCADA/ICS Networking

- Isolated systems
- Connectivity limited to system networks



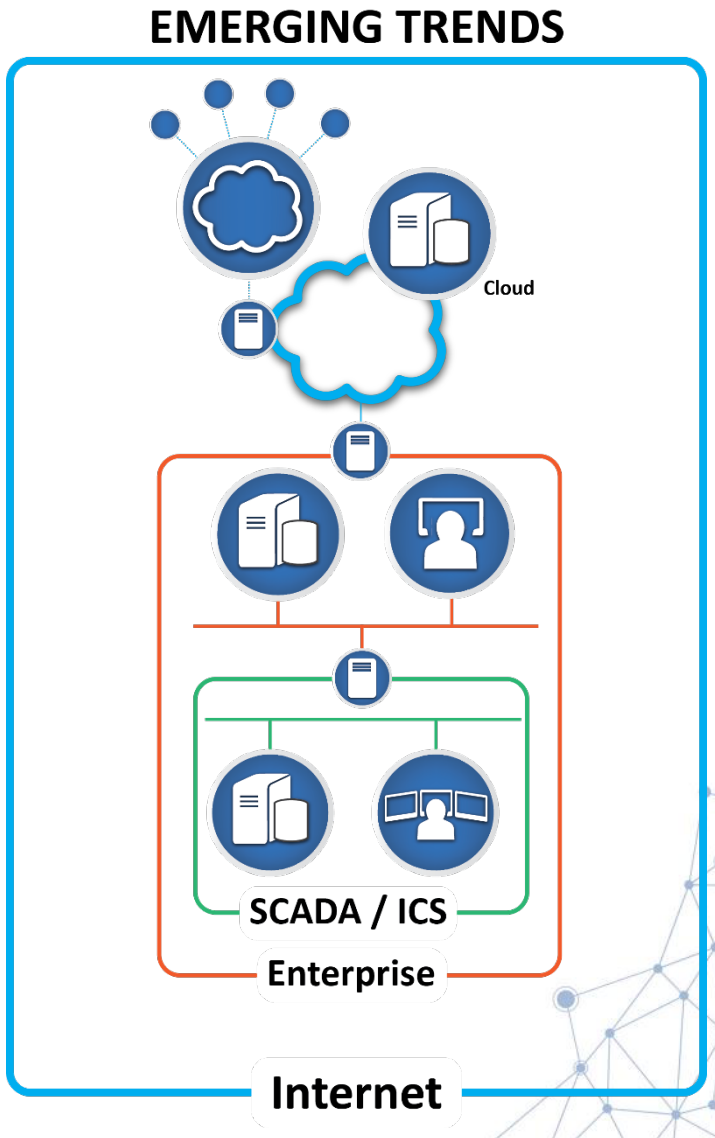
Current Enterprise Integration Trend

- Limited connectivity between SCADA/ICS and Enterprise applications and data over Enterprise networks
- Data shared via public historian, “dashboards” are common
- SCADA/ICS assets isolated behind dedicated firewall
- Little or no SCADA/ICS Internet connectivity



Emerging Trends

- SCADA/ICS assets located outside the firewall
- Communication over Enterprise, 3rd party networks and Internet
- Perimeter between networks is blurring
- Wireless replacing wires
- SCADA/ICS Internet access is now *required*



Planning for the Cloud and Things

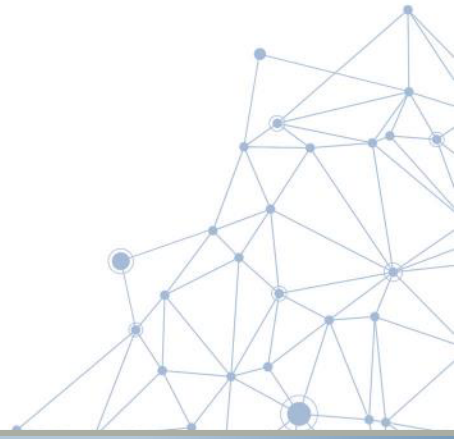
Considerations for successful planning and deployment

Cloud Computing Considerations

- **Data ownership**
  - Somebody else owns the hardware
  - Somebody else *might* own the data
- **You get what you pay for… and rarely anything else**
  - Security
  - Redundancy
  - Uptime
  - Bandwidth
  - CPU
  - Storage
- **Migrating to another provider may be difficult… or impossible**

Cloud Computing Considerations (cont'd)

- Your cloud solution is only as robust as your connection to it
- Your cloud solution is only as secure as your network
- Contingency planning, backup and recovery are extra-cost options
- Consider compliance requirements!



Planning Cloud Computing

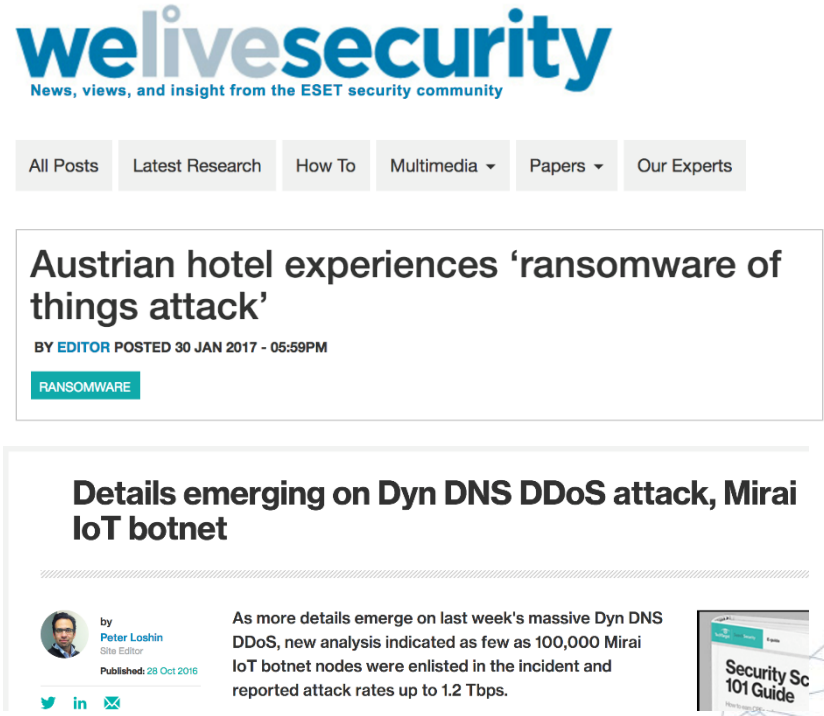
- **Strategic considerations:**
  - Include pricing for redundancy and recovery options
  - Don’t confuse data *retention* with backup
  - Consider data ownership and compliance requirements
  - Look for interoperable services, avoid lock-in
  - Not everything has to be located on the Internet. Look for the right mix of “on-prem” versus “off-prem”.

Planning Cloud Computing

- **Operational considerations:**
  - Consider support requirements (24X7 v NBD)
  - Ensure the interface between SCADA/ICS and the outside world is secure
  - Ensure internal networks and Internet links are as robust as your cloud solution
  - Test *and modify* backup and recovery plans
  - Leverage cloud access flexibility

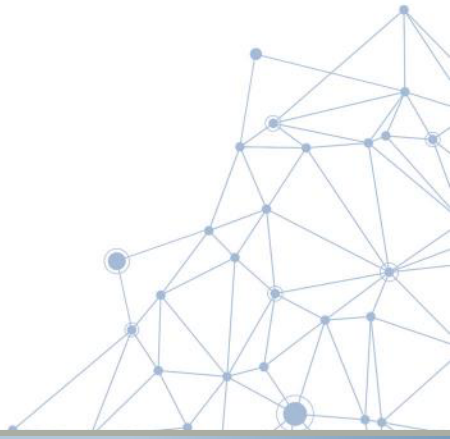
IoT Considerations

- "Attack surface" (possible points of attack) grow with number of devices
- One device can potentially attack many
- Potential Denial-of-Service (DoS) attacks now include power consumption for battery and solar-powered devices
- Many security solutions are proprietary and not interoperable
- Shared credentials are a threat (device loss or theft)
- Large numbers of devices linked by low bandwidth communications are difficult to maintain



Planning IoT Networks

- **Strategic considerations:**
  - Don’t let initial pricing become the primary driver behind design decisions
  - Assume networks will grow - dramatically
  - Prepare for IPv6 as the number of devices begins to grow



Planning IoT Networks

- **Operational considerations:**
  - IPv6 devices can be isolated with a IPv6-IPv4 gateway or router
  - IIoT can be used both on-plant and externally. Structure networks accordingly.
  - Consider incorporating wireless technologies (cellular, ZigBee, wireless HART, LoRa, BLE)

Planning IoT Cybersecurity

- **Strategic considerations:**
  - Plan for security up front, rather than attempt to address it after deployment
  - Look for emerging cybersecurity standards and interoperable products, avoid lock-in
  - Incorporate plans for updating large numbers of remote devices

Planning IoT Cybersecurity

- **Operational considerations:**
  - Don’t allow one device to attack many
  - Secure communications over shared networks
    - VPN
    - TLS
  - Isolate simple devices behind gateways with full security capabilities
  - Require mutual authentication between devices
  - Avoid shared credentials to reduce threat of loss or theft
  - Include tamper detection

Current Cybersecurity Guidance

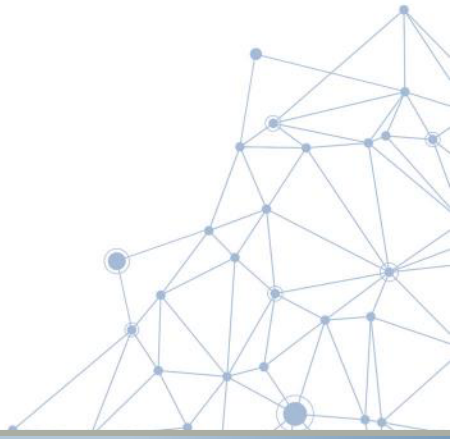
- IoT security in similar state to Internet in the 1990s
- Current* cybersecurity guidance for SCADA/ICS does not address IoT and Cloud/Fog computing
- Good IoT security is based on good network security

* January 2018

Thinking ahead…

- Cloud/Fog computing and IoT present compelling cases for expanding the network beyond traditional perimeters
- Even if you don't expect to adopt Cloud, Fog or IoT wholesale, be prepared for some need to connect remote assets to your control system – securely
- 10 years ago, would you have anticipated connecting SCADA/ICS networks to the Enterprise?
- IoT security is at roughly the same level of sophistication as the Internet was 20 years ago
- Lessons previously learned can be applied to these new challenges

Questions?



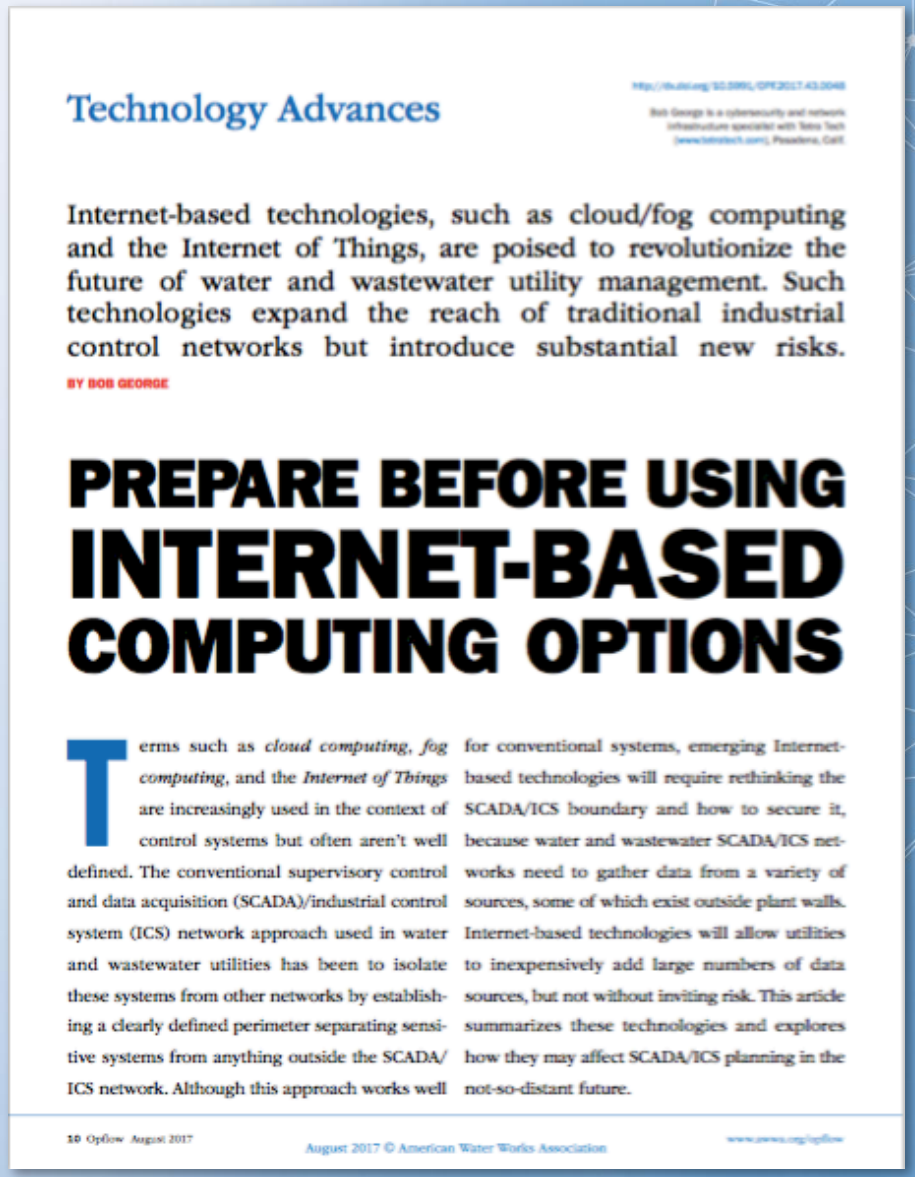
TETRA TECH

Thank You

For more information, please contact:

Bob George, CISSP
bob.george@tetratech.com

The full article is available in the AWWA Opflow Magazine, August 2017 issue



Technology Advances

Internet-based technologies, such as cloud/fog computing and the Internet of Things, are poised to revolutionize the future of water and wastewater utility management. Such technologies expand the reach of traditional industrial control networks but introduce substantial new risks.

BY BOB GEORGE

PREPARE BEFORE USING INTERNET-BASED COMPUTING OPTIONS

Terms such as *cloud computing*, *fog computing*, and the *Internet of Things* are increasingly used in the context of control systems but often aren't well defined. The conventional supervisory control and data acquisition (SCADA)/industrial control system (ICS) network approach used in water and wastewater utilities has been to isolate these systems from other networks by establishing a clearly defined perimeter separating sensitive systems from anything outside the SCADA/ICS network. Although this approach works well for conventional systems, emerging Internet-based technologies will require rethinking the SCADA/ICS boundary and how to secure it, because water and wastewater SCADA/ICS networks need to gather data from a variety of sources, some of which exist outside plant walls. Internet-based technologies will allow utilities to inexpensively add large numbers of data sources, but not without inviting risk. This article summarizes these technologies and explores how they may affect SCADA/ICS planning in the not-so-distant future.

American Water Works Association
FloridaSection