Challenges with the Use of *Power Over the Ethernet* for Fire Alarm

SUPDET 2018; Raleigh, NC

12 September 2018 | Casey Grant, Executive Director | FPRF
Agenda: PoE Summit Update

1) Baseline Concepts

2) A Few Words on PoE Fundamentals

3) Spotlight on PoE Activities: An Update

4) PoE and the World of Fire Alarm

5) Visions for Tomorrow
1) Baseline Concepts

--- Cyber Physical Systems ---

• PoE: Power Over the Ethernet
• IoT: Internet of Things (Internet of Everything)
• Cyber Physical Systems: Massive integration of wireless networks, advanced sensors, 3D simulations, and cloud services enabling new generations of Smart Systems
• World of Cyber Physical Systems composed of three basic areas:

1) Gathering of Data (Communication)
2) Processing of Data (Computation)
3) Use of Data (Targeted Decision Making)
1) Baseline Concepts
--- Our Changing World ---

The world is changing, with the convergence of the “electrical world” and the “electronics world”…

Crowds at Papal Elections in 2005 & 2013
(Courtesy of NBC News)
1) Baseline Concepts

--- Data is the New Oil ---

“Data is the new oil. It’s valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc. to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value.”

- **Clive Humby**, UK Mathematician & architect of Tesco’s Clubcard, 2006
1) Baseline Concepts
--- Data is the New Oil ---

IoT is enabling the flow of data
1) Baseline Concepts

--- Data Analytics is Key! ---

Data is the New Oil
1) Baseline Concepts
--- Our Changing World ---

### Comparing the Top Ten Public Corporations 2011, 2016 and 2017

<table>
<thead>
<tr>
<th>Rank</th>
<th>2011 (as of 31/Dec)</th>
<th>2016 (as of 30/Mar)</th>
<th>2017 (as of 31/Dec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Exxon Mobil - $417B</td>
<td>Apple Inc - $597B</td>
<td>Apple Inc - $869B</td>
</tr>
<tr>
<td>2</td>
<td>PetroChina - $326B</td>
<td>Alphabet - $515B</td>
<td>Alphabet - $727B</td>
</tr>
<tr>
<td>3</td>
<td>Apple Inc. - $321B</td>
<td>Microsoft - $434B</td>
<td>Microsoft - $660B</td>
</tr>
<tr>
<td>4</td>
<td>ICBC - $251B</td>
<td>Amazon Inc. - $356B</td>
<td>Amazon Inc. - $563B</td>
</tr>
<tr>
<td>5</td>
<td>Petrobras - $247B</td>
<td>Berkshire Hathaway - $350B</td>
<td>Facebook - $513B</td>
</tr>
<tr>
<td>6</td>
<td>BHP Billiton - $247B</td>
<td>Exxon Mobil - $347B</td>
<td>Tencent - $493B</td>
</tr>
<tr>
<td>7</td>
<td>China Construction Bank - $232B</td>
<td>Facebook - $326B</td>
<td>Berkshire Hathaway - $489B</td>
</tr>
<tr>
<td>8</td>
<td>Royal Dutch Shell - $226B</td>
<td>Johnson &amp; Johnson - $301B</td>
<td>Alibaba Group - $441B</td>
</tr>
<tr>
<td>9</td>
<td>Chevron Corporation - $226B</td>
<td>General Electric - $296B</td>
<td>Johnson &amp; Johnson - $375B</td>
</tr>
<tr>
<td>10</td>
<td>Microsoft - $213B</td>
<td>Wells Fargo - $246B</td>
<td>JPMorgan - $371B</td>
</tr>
</tbody>
</table>

*Note1: Publicly traded companies having the greatest market capitalization.*

*Note2: This list is based on the Financial Times Global 500 rankings.*
In the face of emerging technologies with great promise, is the present “Safety Infrastructure”. It is well-established with a deep history, built on painful lessons of the past.
1) Baseline Concepts
--- Cyber Physical Systems and “Smart Cities” ---

**Smart Cities Initiative**

**Worth Watching: Organizations & Activities of Interest**

**Global Cities Team Challenge**

**Smart Cities Council**
1) Baseline Concepts
--- The Established Safety Infrastructure ---

**Key Observation:** Be vigilant for sudden significant game changers and new players.

**WORTH WATCHING:** ORGANIZATIONS & ACTIVITIES OF INTEREST

**SMART CITIES COUNCIL, & ISO 37120**

---

**Baseline Concepts**

--- The Established Safety Infrastructure ---

--- Standardization ---

---**ISO 37120**---

Sustainable development of communities
Indicators for city services and quality of life
Agenda: PoE Summit Update

1) Baseline Concepts

2) A Few Words on PoE Fundamentals

3) Spotlight on PoE Activities: An Update

4) PoE and the World of Fire Alarm

5) Visions for Tomorrow
2) A Few Words of PoE Fundamentals

--- A HUGE Issue ---

A HUGE Issue, with sweeping implications

- PoE: The transmission of electrical power & data (i.e., communications) over the same pathways
- PoE, and IoT and other emerging technologies are a reality
- Everybody and every organization has a role
- Paths forward are not simple
- We are on a collective journey
- The safety infrastructure needs to evolve
2) A Few Words of PoE Fundamentals
--- What Exists Today? ---

Voice and Video IP Phones
WiFi Access Points a/b/g/n
Network Security Cameras – Enclosures – Heaters – Pan and Tilt
Building / Access Control – Gas and Fire Alarms – Digital Signs
Digital and School Clocks – SIP IP Paging – Door locks - Gateways
2) A Few Words of PoE Fundamentals
--- What Exists Today? ---

*SMART ELECTRIC POWER SUPPLY*

An activity detector for your home...

**Ubiquiti PoE Lighting**

**Life Door**

**Sense Electrical Monitoring**

**Whisker Labs**
2) A Few Words of PoE Fundamentals

--- Power Over the Ethernet ---

- Need to support/evolve emerging technologies
- But… we need to:
  - Maintain the present safety infrastructure focus, i.e., safety concerns
  - Respect performance attributes for fire alarm communication

In the face of emerging technologies with great promise, is the present “Safety Infrastructure”. It is well-established with a deep history, built on painful lessons of the past.
Agenda: PoE Summit Update

1) Baseline Concepts
2) A Few Words on PoE Fundamentals
3) Spotlight on PoE Activities: An Update
4) PoE and the World of Fire Alarm
5) Visions for Tomorrow
3) Spotlight on PoE Activities: An Update

--- Power Over the Ethernet ---

- Within NFPA:
  - Initial Focus: NEC®, NFPA 72®, NFPA 730/731
  - Installation documents, e.g., NEC®, NFPA 3/4, NFPA 72®, NFPA 79, NFPA 730/731, & more...
  - Occupancy documents, e.g., NFPA 75, NFPA 76, NFPA 99, NFPA 101, & more...
  - Process documents, e.g., NFPA 85, NFPA 86, & more...
  - Other NFPA Documents?

- Beyond NFPA with other organizations...
3) Spotlight on PoE Activities: An Update
--- Research Roadmap for Smart Fire Fighting ---

Project Report available on the NIST and Foundation websites

\[\text{e.g., www.nfpa.org/SmartFireFighting}\]
3) Spotlight on PoE Activities: An Update

--- Smart Home Summit ---

Smart Home Summit
20-21 October 2015; Palo Alto, California
3) Spotlight on PoE Activities: An Update
--- Durham Workshop ---

• Durham Workshop
  • University of New Hampshire
  • October 2017; Durham NH
  • Goal: facilitate a research planning effort for the consideration of concepts involving Power over the Ethernet (PoE), to identify and prioritizes knowledge gaps and recommend next steps and action items in support of the applicable codes and standards.
3) Spotlight on PoE Activities: An Update

--- Durham Workshop ---

• Summary Observations (Oct 2017)
  1. Regulatory Coordination
  2. Key Technical Issues
  3. Research and Data
  4. Training, Education and Awareness

---

3.2. Intelligent Coordinated Power: Clarify, summarize, categorize, and address all applicable technical data for intelligent coordinated power (ICP) to assure safety and effective implementation.

2.4. Data Integrity: Address new requirements for the objective of maintaining data security and integrity (e.g., software, systems, etc.), especially in support of critical systems like COPS, fire alarms, security, etc.

3.5. Power Supplies: Clarify requirements for primary and back-up power supplies, contingent on occupancies, applications, and other factors.

3. Research and Data

3.2. Predictive Data Analytics: Identify and clarify data needs and prospectively collect essential data for use with predictive data analytics. Establish a centralized national data collection to support policy and regulatory reviews.

3.2. Fundamental Baseline: Conduct research in support of validated modeling and establishing theoretical fundamentals for PoE systems.

2.2. Risk Analysis: Outline an approach for conducting a comprehensive risk analysis for each applicable application, to determine the appropriate factors of safety and other key factors. Clarify the factors of safety for existing systems and approaches for purposes of a benchmark.

2.4. Data Integrity: Address new requirements for the objective of maintaining data security and integrity (e.g., software, systems, etc.), especially in support of critical systems like COPS, fire alarms, security, etc.

2.5. Power Supplies: Clarify requirements for primary and back-up power supplies, contingent on occupancies, applications, and other factors.

3.1. Knowledge Gaps: Conduct research projects in support of all knowledge gaps identified by this workshop, including regulatory issues, technical issues, and other issues such as training, education, and awareness.

Training, Education and Awareness

4.2. Education and Outreach: Provide training and education in support of all aspects of PoE, with a special focus on supporting inspections, enforcement, and communibading.

4.2. Format Delivery: Consider the use of a straightforward and relevant checklist and for each of the third party target audience.

4.5. Awareness Outreach: Facilitate outreach addressing the overall vision of enabling technologies like PoE.

Stakeholder Engagement: Promote and facilitate dialogue and networking, and include all impacted stakeholders.

Address the need to include the entire ecosystem of stakeholders (e.g., designers, developers, vendors, installers, inspectors, and users, etc.).
3) Spotlight on PoE Activities: An Update
--- PoE Summit: Next Steps ---

- PoE Summit: Next Steps
  - NFPA C&E
  - June 2018; Las Vegas NV
  - Goal: to leverage information from attendees and from previous meetings to clarify actionable steps to facilitate full consideration of PoE cabling in modern infrastructure while maintaining established levels of safety.

PoE Summit Proceedings at: www.nfpa.org/Foundation
3) Spotlight on PoE Activities: An Update

--- PoE Summit: Next Steps ---

• Summary Observations (Jun 2018)

1. Vision
2. Training, Education and Awareness
3. Regulatory Coordination
4. Research and Data

3.1 Vision Statement: “This effort seeks to manage the safe evolution of PoE, as a reliable and secure technology, in recognition of its ability to effectively and efficiently utilize carrier pathways for the transmission of both electrical power and communications.”

3.2 Applications & Occupancies. Next term and longer, we can expect to see the use of PoE everywhere there is a cable or conductor. Consistent with the IEC norm of Things, anything with a wire to it will have data with it.

3.3 Equipment & Transmission. MIoT of critical equipment is evolving and the deployment decisions need to be reevaluated. For example, more attention will be given to the reliability of data processing and control. Critical activities like CPS (critical operations’ power systems), fire alarm and power security need to further explore and consider worst-case design criteria. Levels of reliability need to be well defined and consistent across all different contexts and standards. Circuit integrity will continue to be important, and additionally, future consideration of transport data integrity is also needed.

3.4 Key Metrics and Baseline Issues. The baseline issues are application dependent, and physical integrity and data integrity are the most critical. Issues such as security considerations, life safety, EMI, cybersecurity, networking priority, and so on need to be considered. The focus of most concern are the key few critical hazards such as the ignition, fuel load, flame spread, products of combustion, etc., (e.g., from the looping of cables). The concerns for electrical hazards (e.g., shock, arc-flash, fume inhalation, etc.) are considered minimal, unless innovative approaches like pulse power are used.

3.5 Terminology. Universal recognition of key terms are needed through standardized definitions (e.g., PoE, classifications of PoE, arcs, radical, cabling, managed leading, pulse power, data integrity, etc.).

3.6 Other Issues. Other issues that higher-level organization is needed among the involved stakeholders (standards developing organizations); long-term maintenance and reliability over time is needed; and data security is essential.

2. TRAINING, EDUCATION AND organizes.

2.1 Training and Education. Organizations should implement training and education in support of PoE, with a special focus on supporting inspection, enforcement and compliancing, including but not limited to: AECA AEC, NESC, NFPA, and IEC standards (including NFPA 70, NEC, and the Engineering NEC-A (Non-Combustible) NEMA (for manufacturers); NFPA 101 (Health Code certification); NFPA 104; NFPA 90A. In the future, NFPA’s role may include coordinating the numerous groups.

3.2 Smart Devices. Certain key steps should be included in a forward-looking yet intelligent checklist; and/or a checklist list to facilitate third-party support and enforcement, such as listing and labeling of products; and manufacturer’s instructions. There should be a Standardized Enforcement Document? Group or may act as a checklist as an ‘Electrical Inspector’s Guide’ and a detailed document. This should consider when necessary: policy list for compliance; apps classroom training articles on PoE; for nonexperts; and so on.

3.3 Awareness Outreach. A PoE Handbook is needed to provide a baseline hierarchy. Affiliated groups that will be impacted includes, like BOMA, also need outreach. Consider frameworks that can be circulated and shared, in partnership arrangements. Include IT (information technology) expertise among the other subject experts in the development of materials.

3.4 Stakeholder Engagement. The targeted stakeholders for further engagement should consider the entire ecosystem of stakeholders (e.g., designers, developers, vendors, installers, operators, end-users, etc.), and include at least the following: AEC (AEC) Building Owners (smart buildings) Equipment Manufacturers (NEMA, IEC) Labor Unions (NSIC, IBECA, IBEA, IBE, ITC) Professionals.

3.5 Other Issues. Other issues include specific branding (e.g., PoE Terminology; Data Assistance Teams; and development of a publication approaches.

3.1 Organizations. Key stakeholders are important to engagement and other groups, whose further engagement should be promoted and facilitated for PoE include: ASIS, BICSI, IEC, ICC, IAS, ISF, ISO, NFPA, NEMA, IEC, UL and others. Given that a United Nations-type organization has what can be a challenge, though some groups like ISO and IEC are already driving this issue. In general, as electrical industry and the electronics industry are symbiotically working together on PoE.

3.2 Key Issues. Governance of a United Nations-type organization for PoE will be a challenge (e.g., elected officials). This is better a bottom-up activity rather than a top-down approach (e.g., federal government). The large scale scope of PoE makes this a particular challenge. The least first issues that need to be addressed are a mission statement, a value statement, and a board of directors. Other critical key issues include, as examples, after-market certification; counterfeits; lack of awareness; lack of installation standards; post installation commissioning; reliability; plug devices; safety; and security.

References and Data

4.1 Data & Data Analytics. Key data & data sources are needed: includes policy and regulatory activities, include for example, PoE, the Incidents; and power supply failures. The access and collection of data on a wide scale is seen as a high-level challenge.

4.2 Measured Loading Data, Equipment Testing or Smart Testing. A primary challenge for the safe use of managed lighting is that it is complex system and requires technical expertise. This will require data from equipment manufacturers to properly sequence alarm times for prioritized critical and non-critical equipment.

4.3 System Reliability. The reliability of interconnected/integrated and various communication methods is essential for reliable and secure operation. Issues of “interoperability” ability to function on a common platform with similar equipment and “compatibility” ability to connect with similar equipment) are important. Other security is important, including systems (such as a traditional fire alarm system or other automatic).

4.4 Factors of Safety. The key elements and characteristics that require factors of safety should be consistent with those already established by the codes and standards, such as the NEC, NFPA standards, NFPA 101 (Health Code certification); NFPA 104, NFPA 90A. In the future, NFPA’s role may include coordinating the numerous groups.

4.5 Sustainability of Applications. The safe use of plug-and-play approaches can significantly reduce the need for the supporting infrastructure (e.g., power supplies, etc.), and this is a significant problem. The issues of scalability are important and need to be addressed if levels of safety are not to be sacrificed.

4.6 Other Issues. Other issues include: the need for field verification; and need to address the growing inventory of existing installations.
Agenda: PoE Summit Update

1) Baseline Concepts
2) A Few Words on PoE Fundamentals
3) Spotlight on PoE Activities: An Update
4) PoE and the World of Fire Alarm
5) Visions for Tomorrow
4) PoE and the World of Fire Alarm
--- Impact of Emerging Technology on NFPA 72 ---

- FCC is forcing change for Fire Alarm Communication
  - Phasing out traditional telephone lines and replacing with broadband network technologies.
- Large undertaking for the fire alarm industry
  - Even if other devices were upgraded, the fire alarm system was likely still using the legacy telephone system.
- Must maintain the safety infrastructure (i.e. reliability) of the traditional phone system
4) PoE and the World of Fire Alarm
--- Fire Alarm Integration with Other Networks ---

- **Interconnectivity Concerns**
  - Concerns of fire alarm signal not taking precedence over other signals on the network during an emergency.
  - Network devices may not be as robust as FA equipment.

- **Solutions**
  - Require all FA devices interconnected on the network to be listed for FA use.
  - Involve a network expert when integrating FA with other networks.
4) PoE and the World of Fire Alarm
--- NFPA 72 Solutions to PoE Challenges ---

Reliability and Redundancy

• Class N Circuit
  – Applies to network technologies (i.e. PoE)
  – Addresses reliability and redundancy (by meeting or exceeding the reliability and redundancy of outgoing POTS lines)
    • Systems tested at a higher frequency (every 90 sec instead of 24 hr)
• PoE is not new, but is now seen as reliable enough to be used for fire alarm systems – when properly installed.
Supervision and Battery Back-up

• PoE for Fire Alarm Systems are part of the Class N signal path.
  – Data cables and other accessory equipment are not supervised.
  – Fire alarm panel does not monitor path itself; looking for regular handshake signal returning from the fire alarm device at end of cable.
    • By monitoring the functionality of the communications, the integrity of the line can be determined.
  – FA panel will show trouble if the cable is unplugged or power is lost.
  – All PoE applications used for fire alarm systems are still required to comply with NFPA 72 – including battery back up requirements.
4) PoE and the World of Fire Alarm
--- Challenges Utilizing PoE for Fire Alarm Systems ---

Cyber-security

- Recommended use of firewalls and secure networks
- Still a major gap that needs addressed.
4) PoE and the World of Fire Alarm
--- TOWS Analysis ---

- Identify:
  - Threats
  - Opportunities
  - Weakness
  - Strengths

- Emphasis on threats and opportunities presented by emerging technologies.
4) PoE and the World of Fire Alarm

--- TOWS Analysis ---

**Threats:**
- Changes to regulatory oversight
- Uncertainty
- Rapid turnover of technology

**Opportunities:**
- New technology
- Cost benefit
- Integration
- Connectivity
- Widespread application

**Threats:**
- Changes to Regulatory Oversight: The legacy phone system (via FCC) is being phased out, forcing NFPA 72 to modify Fire Alarm Communication pathways.
- Uncertainty: The potential impact of using Ethernet or other networks on the reliability, security, availability, survivability and durability of fire alarm communication is unknown.

**Opportunities:**
- Emerging Technologies: Embrace new applications of technologies (i.e. Ethernet as means of transmitting both power and communication).
- Cost Benefit: Promote cost savings for users.
- Integration: Enable integration of building and fire and life safety systems.
- Connectivity: Focus on promoting the world of connectivity (e.g. IoT).
- Widespread Application: NFPA 72 is widely implemented in public and private buildings. Opportunity to implement PoE or other technologies into these existing NFPA 72 systems as well as any new facilities as the transition to network systems is made.
4) PoE and the World of Fire Alarm
--- TOWS Analysis ---

**Weaknesses:**
- Ability for timely adaptation
- Technology outpacing safety infrastructure
- Training needed for new technologies

**Strengths:**
- Tradition
- Key Performance Features
- Robust, Established Process
- Developing Solutions
- Widespread Application

---

**WEAKNESSES**
- **Ability for timely adaptation**: The safety infrastructure is stable, but the stability hinders timely adaptation to new technologies.
- **Technology is outpacing the safety infrastructure**: There is a fast-paced movement by Tech Companies and Manufacturers that are continually pushing the use of new technologies. It is critical for relevant codes to keep up with this revolution to ensure safety and stay relevant.

**STRENGTHS**
- **Tradition**: The traditional approach of NFPA 72 is philosophically consistent with Power over Ethernet, which is the transmission of power and communication over the same pathways.
- **Key Performance Features**: NFPA 72 has a long-term history of established reliability, security, survivability, etc. of fire alarm systems.
- **Robust, Established Process**: NFPA 72 involves a robust ANSI accredited review process with over 12 technical committees composed of over 200 volunteer subject matter experts and stakeholder representatives.
- **Developing Solutions**: In the 2016 edition, NFPA 72 created a "Class N" circuit to enable the use of network technologies for Fire Alarm Communication.
- **Widespread Application**: NFPA 72 is widely used for public facilities and many private facilities.
Agenda: PoE Summit Update

1) Baseline Concepts
2) A Few Words on PoE Fundamentals
3) Spotlight on PoE Activities: An Update
4) PoE and the World of Fire Alarm

5) Visions for Tomorrow
5) Visions for Tomorrow
--- Actionable Strategies ---

1) Identify, prioritize and conduct research on emerging technologies to develop strategies to adapt them while maintaining (or enhancing) the safety infrastructure.

2) Leverage the strengths of the Fire Alarm Industry to maximize the opportunities of new technologies and build new relationships.

3) Establish a declaration of fundamental principles via a dedicated task group to address emerging technologies.

4) Focus on all hazards when utilizing network technologies for fire alarm communication.
5) Visions for Tomorrow
--- Research Gaps ---

Examples:

1) Address Cyber-security – how easy is it to hack into a fire alarm network?

2) Establish clear levels of reliability, for the full integration of fire alarm systems with other building systems.

4.1 Data & Data Analytics. Key data & data analytics are needed to impact policy and related activities, include for example: PoE fire incidents; and power supply failures. The access and collection of data on a wide scale is seen as a significant challenge.

4.2 Managed Loading (aka, dynamic loading or smart loading). A primary obstacle for the safe use of managed loading is that it is a complex system and requires lots of expertise. This will require data prioritization to properly sequence alarm times for prioritized critical and non-critical requirements.

4.3 System Reliability. The reliability of interconnection/integration and various communication methods is essential for reliable and secure operation. Issues of "interoperability" (ability to function on a common platform with similar equipment) and "compatibility" (ability to co-exist with similar equipment) are important. Cyber security is important, including existing systems (i.e., a traditional fire alarm system is often vulnerable).

4.4 Factors of Safety. The key elements and characteristics that require factors of safety should be consistent with those already established by the codes and standards, such as the NEC® and UL standards.

4.5 Scalability of Applications. The safe use of plug-and-play approaches can substantially increase the needs of the supporting infrastructure (e.g., power supplies, etc.), and this is a significant problem. The issues of scalability are important and need to be addressed if levels of safety are not to be sacrificed.

4.6 Other Issues. Other issues include: the need for field verification; and need to address the growing inventory of existing applications.