Power Over the Ethernet (PoE) Summit: Next Steps

FINAL PROCEEDINGS BY:

Casey Grant, P.E. & Victoria Hutchison
Fire Protection Research Foundation
1 Batterymarch Park, Quincy, MA

Held: 10 June 2018, 2018 NFPA Conference & Expo, Mandalay Bay Conference Center (South Pacific F), Las Vegas, NV

September 2018
Executive Summary

These are the proceedings of the “Power Over the Ethernet (PoE) Summit: Next Steps”, a.k.a., PoE Summit. The event was held on 10 June 2018 in Las Vegas, Nevada. At its most basic level, PoE involves the mixing of power and communications over the same transmission means (e.g., cabling).

This topic is of direct interest to multiple organizations, committees and individuals. This includes those responsible for the administration of model codes and standards that are impacted and/or affected by this topic (e.g., NFPA 70, National Electrical Code®, NFPA 72 Fire Alarm, NFPA 79 Industrial Machinery, NFPA 99 Healthcare, NFPA 730/731 Premises Security, and NFPA 1221 Emergency Services Communication Systems).

The goal of this Summit is 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. In support of this goal, the workshop had the following objectives:

1) Vision Statement: Establish clear direction based on collective vision of where we expect to be in the future.
2) Training, Education and Awareness: Continue to elevate overall awareness and common understanding, with focus toward training and education.
3) Regulatory Coordination: Identify a proposed structure for NFPA-internal and NFPA-external regulatory coordination. Specifically, consider methods to coordinate PoE cabling requirements within NFPA and outside NFPA; establishing NFPA coordinating group objectives (defining PoE, terminology, coordinating between docs); clarifying jurisdictional scope of SDOs, product safety evaluation, certification & others; identifying impacted stakeholders (e.g., role of stakeholders, etc.).
4) Research and Data: Determine if other support/coordinating groups or projects necessary (FPRF projects, simulation team, etc.), and clarify data needs and perceived obstacles.

This Summit is an important step for addressing this issue, but it is only one step in the overall journey to address Power over the Ethernet. The world is changing rapidly, and the devices and technologies that support it, such as PoE, are here to stay. Historically, the safety infrastructure has made great headway in establishing a fire and electrically safe world, and it is paramount that the regulatory community rises to address the new emerging challenges that we are now regularly witnessing.
Acknowledgements

This Summit has been generously supported by the following sponsors: Cisco, Johnson Controls, and Fluke Networks.

Additional support has been provided through the NFPA Research Fund, through the National Fire Protection Association.

This workshop summary report has been prepared by Casey Grant and Victoria Hutchison, at the Fire Protection Research Foundation. The information contained herein is based on the input of multiple professionals and subject-matter-experts. While considerable effort has been taken to accurately document this input, the final interpretation of the information contained herein resides with the report authors. The content, opinions and conclusions contained in this report are solely those of the authors and do not necessarily represent the views of the Fire Protection Research Foundation, NFPA, Technical Panel or Sponsors. The Fire Protection Research Foundation makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

About the Fire Protection Research Foundation

The Fire Protection Research Foundation plans, manages, and communicates research on a broad range of fire safety issues in collaboration with scientists and laboratories around the world. The Foundation is an affiliate of NFPA.

About the National Fire Protection Association (NFPA)

Founded in 1896, NFPA is a global, nonprofit organization devoted to eliminating death, injury, property and economic loss due to fire, electrical and related hazards. The association delivers information and knowledge through more than 300 consensus codes and standards, research, training, education, outreach and advocacy; and by partnering with others who share an interest in furthering the NFPA mission. All NFPA codes and standards can be viewed online for free. NFPA’s membership totals more than 55,000 individuals around the world.

Keywords: Power over the Ethernet (PoE), Ethernet, IEEE, cable, NEC®, NFPA 70, NFPA 72, NFPA 79, NFPA 99, NFPA 730, NFPA 731, NFPA 1221

Report #: FPRF2018-09
Project Panel (Summit Steering Committee)

Amy Cronin, Strategic Code Solutions LLC (RI)

Mark Earley, NFPA (MA)

Ernie Gallo, Alliance for Telecommunications Industry Solutions (NJ)

Joel Goergen, Cisco (CA)

Mike Johnston, National Electrical Contractors Association (MD)

Chad Jones, Cisco (CA)

Dick Roux, NFPA (MA)

George Zimmerman, CME Consulting (CA)
This page intentionally blank
Table of Contents

Executive Summary ............................................................................................................................. ii
Acknowledgements ............................................................................................................................ iii
Project Panel (Summit Steering Committee) ....................................................................................... iv
Table of Contents ................................................................................................................................ vi
List of Tables ...................................................................................................................................... vii
List of Figures ..................................................................................................................................... vii

1) Introduction, Agenda and Attendees ........................................................................................... 1
2) Summit Overview and Background .............................................................................................. 5
3) Summit Panel Discussions .......................................................................................................... 13
4) Break-Out Group Discussions ..................................................................................................... 15
5) Summary Observations .............................................................................................................. 25

Annex B: Power Over the Ethernet – A New Frontier ....................................................................... 41
List of Tables

Table 1: PoE Summit Agenda ........................................................................................................................ 2
Table 2: Summit Attendees........................................................................................................................... 3
Table 3: Break Out Group Questions (1 of 4) .............................................................................................. 15
Table 4: Break Out Group Questions (2 of 4) .............................................................................................. 15
Table 5: Break Out Group Questions (3 of 4) .............................................................................................. 16
Table 6: Break Out Group Questions (4 of 4) .............................................................................................. 16
Table 7: Consolidated Break Out Group Responses ................................................................................... 17
Table 8: Summary Observations from the PoE Summit ............................................................................. 25

List of Figures

Figure 1: Session T64, Power over the Ethernet – A New Frontier .............................................................. 4
Figure 2: PoE Universe of Activity ................................................................................................................. 5
Figure 3: Key Findings from October 2017 “Workshop Proceedings: Power Over the Ethernet” ............ 6
Figure 4: Summit Presentation While In Plenary Session (Page 1 of 6)....................................................... 7
Figure 5: Summit Presentation While In Plenary Session (Page 2 of 6)....................................................... 8
Figure 6: Summit Presentation While In Plenary Session (Page 3 of 6)....................................................... 9
Figure 7: Summit Presentation While In Plenary Session (Page 4 of 6).......................................................10
Figure 8: Summit Presentation While In Plenary Session (Page 5 of 6).......................................................11
Figure 9: Summit Presentation While In Plenary Session (Page 6 of 6).......................................................12
Figure 10: Example of Break Out Group Activities......................................................................................17
Figure 11: Annex A – PoE Fire Alarm Impact (Page 1 of 12) .................................................................... 29
Figure 12: Annex A – PoE Fire Alarm Impact (Page 2 of 12) ................................................................... 30
Figure 13: Annex A – PoE Fire Alarm Impact (Page 3 of 12) ................................................................... 31
Figure 14: Annex A – PoE Fire Alarm Impact (Page 4 of 12) ................................................................... 32
Figure 15: Annex A – PoE Fire Alarm Impact (Page 5 of 12) ................................................................... 33
Figure 16: Annex A – PoE Fire Alarm Impact (Page 6 of 12) ................................................................... 34
Figure 17: Annex A – PoE Fire Alarm Impact (Page 7 of 12) ................................................................... 35
Figure 18: Annex A – PoE Fire Alarm Impact (Page 8 of 12) ................................................................... 36
Figure 19: Annex A – PoE Fire Alarm Impact (Page 9 of 12) ................................................................... 37
Figure 20: Annex A – PoE Fire Alarm Impact (Page 10 of 12) ................................................................. 38
Figure 21: Annex A – PoE Fire Alarm Impact (Page 11 of 12) ................................................................. 39
Figure 22: Annex A – PoE Fire Alarm Impact (Page 12 of 12) ................................................................. 40
Figure 23: Annex B – Session T64 Presentations (Page 1 of 6) ................................................................. 41
Figure 24: Annex B – Session T64 Presentations (Page 2 of 6) ................................................................. 42
Figure 25: Annex B – Session T64 Presentations (Page 3 of 6) ................................................................. 43
Figure 26: Annex B – Session T64 Presentations (Page 4 of 6) ................................................................. 44
Figure 27: Annex B – Session T64 Presentations (Page 5 of 6) ................................................................. 45
Figure 28: Annex B – Session T64 Presentations (Page 6 of 6) ................................................................. 46
Power over Ethernet (PoE) and the Internet of Things (IoT) are sweeping concepts with widespread implications for codes and standards and associated organizations. The proliferation of PoE is expanding as a result of the similar expansion of IoT, i.e., with an increasingly wide spectrum of connected devices. Some are now referring to IoT as the Internet of (every) Thing, since some are now envisioning a world with virtually everything interconnected and communicating back and forth.

At its most basic level, PoE involves the mixing of power and communications over the same transmission means (e.g., cabling). As these concepts proceed and are implemented, the clearly established levels of safety that has already evolved in the built infrastructure should be maintained, if not even enhanced. This includes addressing electrical hazards such as arcing, shock, and surge, and fire protection hazards such as ignition propensity, fuel load, flame spread, and products of combustion.

While these concepts evolve and are embraced, we need to balance safety with optimum performance of important new emerging technologies. This considers key attributes (e.g., availability, durability, maintainability, operability, reliability, stability, interoperability, compatibility, etc.), which in some cases directly affect safety.

Using information from previous meetings, this Summit is intended to clarify specific and actionable next steps. In addition, the PoE Summit is intended to raise awareness and promote direction for the professional technical community focused on the safe implementation of these new concepts. Establishing relationships is an important part of this effort, and this is a positive outcome of this Summit.

The goal of this Summit is to leverage information gathered at this Summit and previous meetings to clarify actionable steps to facilitate full consideration of PoE cabling in modern infrastructure while maintaining established levels of safety.

In support of this goal, the workshop had the following objectives:
1) Vision Statement: Establish clear direction based on collective vision of where we expect to be in the future.
2) Training, Education and Awareness: Continue to elevate overall awareness and common understanding, with focus toward training and education.
3) Regulatory Coordination: Identify a proposed structure for NFPA-internal and NFPA-external regulatory coordination. Specifically, consider methods to coordinate PoE cabling requirements within NFPA and outside NFPA; establishing NFPA coordinating group objectives (defining PoE, terminology, coordinating between docs); clarifying jurisdictional scope of SDOs, product safety evaluation, certification & others; identifying impacted stakeholders (e.g., role of stakeholders, etc.).
4) Research and Data: Determine if other support/coordinating groups or projects necessary (FPRF projects, simulation team, etc.), and clarify data needs and perceived obstacles.

This Summit is of high interest to facility managers, designers and engineers, information technology managers, codes and standards writers, PoE/IoT subject matter experts, and others dedicated to a safe infrastructure. This workshop was attended by individuals and organizational representatives interested in PoE and IoT.
Workshop attendees include those interested in the interoperability between codes, and those impacted by these emerging technologies in the codes and standards. This is not only involving NFPA documents but also those of other organizations. Examples of NFPA codes and standards directly and indirectly impacted by PoE concepts include the following:

**Installation Documents**
- NFPA 3, Standard for Commissioning of Fire Protection and Life Safety Systems
- NFPA 70®, National Electrical Code® (NEC®)
- NFPA 72®, National Fire Alarm and Signaling Code®
- NFPA 79, Electrical Standard for Industrial Machinery
- NFPA 730, Guide for Premises Security
- NFPA 731, Standard for the Installation of Electronic Premises Security Systems

**Occupancy Documents**
- NFPA 75, Standard for the Fire Protection of Information Technology Equipment
- NFPA 76, Standard for the Fire Protection of Telecommunications Facilities
- NFPA 99, Health Care Facilities Code

**Process Documents**
- NFPA 85, Boiler and Combustion Systems Hazards Code
- NFPA 86, Standard for Ovens and Furnaces

The agenda for the PoE Summit is illustrated in Table 1: PoE Summit Agenda.

<table>
<thead>
<tr>
<th>TIME</th>
<th>Sunday, June 10, 2018</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00 – 11:15 am</td>
<td>Call to Order, and Meeting Preliminaries</td>
<td>Workshop Objectives &amp; Deliverables</td>
<td>Casey Grant</td>
</tr>
<tr>
<td>11:15 – 11:30 pm</td>
<td>Key Findings from Previous Meetings (e.g., Durham &amp; ESRAC)</td>
<td></td>
<td>Casey Grant</td>
</tr>
<tr>
<td>11:30 – 12:30 pm</td>
<td>Panel Discussion: Addressing the Vision of PoE</td>
<td>(Panelists: Ernie Gallo, Mark Hilbert, Chad Jones, Alan Manche, Denise Pappas, George Zimmerman)</td>
<td>Panel Members</td>
</tr>
<tr>
<td>12:30 – 1:00 pm</td>
<td>Networking Deli Lunch</td>
<td></td>
<td>All Attendees</td>
</tr>
<tr>
<td>1:00 – 1:45 pm</td>
<td>Panel Discussion: Coordination across Codes and SDOs – Barriers &amp; Opportunities</td>
<td>(Panelists: Shane Clary, Mike Johnston, John Kovaclk, Wayne Moore)</td>
<td>Panel Members</td>
</tr>
<tr>
<td>1:45 – 2:30 pm</td>
<td>Panel Discussion: Next Steps &amp; Future Actionable Items</td>
<td>(Panelists: Donny Cook, Joel Goergen, Randy Ivans, Tom Parrish)</td>
<td>Panel Members</td>
</tr>
<tr>
<td>2:30 – 2:45 pm</td>
<td>Break-Out Group Assignments and Break</td>
<td></td>
<td>All Attendees</td>
</tr>
<tr>
<td>2:45 – 3:45 pm</td>
<td>Break-Out Groups Complete Questionnaire</td>
<td></td>
<td>All Attendees</td>
</tr>
<tr>
<td>3:45 – 4:45 pm</td>
<td>Break-Out Group Reports</td>
<td></td>
<td>All Attendees</td>
</tr>
<tr>
<td>4:45 – 5:00 pm</td>
<td>Workshop Closing Remarks and Adjournment</td>
<td></td>
<td>Casey Grant</td>
</tr>
</tbody>
</table>

The PoE Summit had a diverse group of attendees, representing a range of backgrounds and technical areas. Table 2 provides a summary of PoE Summit attendees. Each attendee was assigned to one of four breakout groups, to facilitate focused discussion on the certain key issues. These were randomly assigned an identifying color of Yellow, Green, Blue and Red. The attendees included individuals that are members of a wide range of applicable NFPA Technical Committees, and other individuals that are subject matter experts on PoE related topics.
Additional components have been added to these proceedings as annex material, since they are directly related to the overall concept and relate to the Summit focus. This includes Annex A: The Impact of PoE and Emerging Technologies on the Fire Alarm Industry; and Annex B: Power Over the Ethernet – A New Frontier.

Annex A of these Proceedings is a separate but related summary generated to clarify and assess the impact of PoE for the fire alarm community and specifically how it relates to NFPA 72 type applications. This includes a TOWS (threats, opportunities, weaknesses and strengths) analysis to assess the impact of emerging technologies on NFPA 72. This section describes the outcome of this effort and proposed actionable strategies. This materials has been generated based on a request from the Research Foundation’s Fire Alarm Research Planning Council, and is intended to provide key background information on this topic as it relates to and impacts NFPA 72®, National Fire Alarm and Signaling Code®.

Annex B of these Proceedings is a brief summary of an additional speaker and panel session held after the PoE Summit, later in the week at the NFPA C&E in Las Vegas on Tuesday 12/June/2018. This was titled Session T64, Power Over the Ethernet - A New Frontier, and involved a panel discussion with presentations and a plenary discussion with the audience. This supplementary effort provided an expanded discussion on PoE concepts, and additional outreach to a wider network of interested parties, since it was recognized that there were some attendees that were unable to attend the PoE Summit on 10 June 2018 due to conflicts. This also promoted important extended outreach and relationship building on this issue. Figure 1 provides an illustration from this supplemental session.

--- Table 2: Summit Attendees ---

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Organization</th>
<th>Breakout Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>George</td>
<td>Amar</td>
<td>Novot Service Company, Inc.</td>
<td>Green</td>
</tr>
<tr>
<td>Suzanne</td>
<td>Alfano</td>
<td>NEMA</td>
<td>Blue</td>
</tr>
<tr>
<td>Fred</td>
<td>Altrock</td>
<td>Somnet</td>
<td>Blue</td>
</tr>
<tr>
<td>Vincenzo</td>
<td>Boccardi</td>
<td>NEMA</td>
<td>Blue</td>
</tr>
<tr>
<td>Brian</td>
<td>Boughman</td>
<td>Generac</td>
<td>Yellow</td>
</tr>
<tr>
<td>C.</td>
<td>Boyle</td>
<td>Academy of Fire Sprinkler Technology</td>
<td>Yellow</td>
</tr>
<tr>
<td>George</td>
<td>Boyle</td>
<td>Raw Protect Inc</td>
<td>Yellow</td>
</tr>
<tr>
<td>Theodore</td>
<td>Bruschi</td>
<td>Fluor Networks</td>
<td>Yellow</td>
</tr>
<tr>
<td>Chris</td>
<td>Bullock</td>
<td>Cisco Systems</td>
<td>Green</td>
</tr>
<tr>
<td>Warren</td>
<td>Burns</td>
<td>Telgan Engineering &amp; Consulting</td>
<td>Green</td>
</tr>
<tr>
<td>Dave</td>
<td>Busick</td>
<td>National Association of Home Builders</td>
<td>Yellow</td>
</tr>
<tr>
<td>Paul</td>
<td>Carpenter</td>
<td>Integrity Institute of Technology</td>
<td>Green</td>
</tr>
<tr>
<td>Theresa</td>
<td>Chambers</td>
<td>Vector Security</td>
<td>Green</td>
</tr>
<tr>
<td>Shane</td>
<td>Chery</td>
<td>Bay Alarm Company</td>
<td>Green</td>
</tr>
<tr>
<td>Tony</td>
<td>Colman</td>
<td>Electrical Training ALLIANCE</td>
<td>Blue</td>
</tr>
<tr>
<td>Dr.</td>
<td>Coon</td>
<td>Herky County Development Services</td>
<td>Blue</td>
</tr>
<tr>
<td>Amy</td>
<td>Cremin</td>
<td>Strategic Codo Solutions</td>
<td>Blue</td>
</tr>
<tr>
<td>Fred</td>
<td>Dixon</td>
<td>Charmacs Canada</td>
<td>Blue</td>
</tr>
<tr>
<td>Jim</td>
<td>Durrant</td>
<td>BSM/9B</td>
<td>Yellow</td>
</tr>
<tr>
<td>Mark</td>
<td>Earley</td>
<td>NFPA</td>
<td>Green - Silver</td>
</tr>
<tr>
<td>Ben</td>
<td>Easton</td>
<td>NFPA</td>
<td>Blue</td>
</tr>
<tr>
<td>Tommy</td>
<td>Farr</td>
<td>UFC for Southern Nevada</td>
<td>Blue</td>
</tr>
<tr>
<td>Dan</td>
<td>Fiegenen</td>
<td>Siemens</td>
<td>Blue</td>
</tr>
<tr>
<td>Nick</td>
<td>Foster</td>
<td>ES &amp; RCCD, TLT</td>
<td>Blue</td>
</tr>
<tr>
<td>Cliff</td>
<td>Goffen</td>
<td>Ontario Power</td>
<td>Green - Lead</td>
</tr>
<tr>
<td>Joel</td>
<td>Goringo</td>
<td>Cisco</td>
<td>Blue</td>
</tr>
<tr>
<td>Cassy</td>
<td>Grant</td>
<td>PFR</td>
<td>Green</td>
</tr>
<tr>
<td>Michael</td>
<td>Hamrock</td>
<td>Fire Alarm</td>
<td>Yellow</td>
</tr>
<tr>
<td>James</td>
<td>Hatlin</td>
<td>City of Irving</td>
<td>Yellow</td>
</tr>
<tr>
<td>Mitchell</td>
<td>Heffley</td>
<td>CMG</td>
<td>Yellow</td>
</tr>
<tr>
<td>Michael</td>
<td>Hillen</td>
<td>EJ Electric</td>
<td>Yellow</td>
</tr>
<tr>
<td>Mark</td>
<td>Hiltner</td>
<td>V.I.T.H.E. Electrical Inspection &amp; Training</td>
<td>Blue</td>
</tr>
<tr>
<td>Mark</td>
<td>Horton</td>
<td>CadillacNorth Inc</td>
<td>Green</td>
</tr>
<tr>
<td>Christian</td>
<td>Hurd</td>
<td>Carroll Bloom</td>
<td>Green</td>
</tr>
<tr>
<td>Victoria</td>
<td>Hutchinson</td>
<td>TFE</td>
<td>Blue - Silver</td>
</tr>
<tr>
<td>Randy</td>
<td>Hunter</td>
<td>UL, LLC</td>
<td>Blue</td>
</tr>
<tr>
<td>Bill</td>
<td>Johnston</td>
<td>NEMA</td>
<td>Green</td>
</tr>
<tr>
<td>Robert</td>
<td>Jones</td>
<td>EG Texas Golf Coast</td>
<td>Green</td>
</tr>
<tr>
<td>Chad</td>
<td>Jones</td>
<td>Cisco</td>
<td>Yellow</td>
</tr>
<tr>
<td>David</td>
<td>Jones</td>
<td>NFPA</td>
<td>Green</td>
</tr>
<tr>
<td>Dan</td>
<td>Mullen</td>
<td>The Rowland Companies</td>
<td>Green</td>
</tr>
<tr>
<td>John</td>
<td>Kovacs</td>
<td>DE, LLC</td>
<td>Yellow</td>
</tr>
<tr>
<td>Peter</td>
<td>Lantinen</td>
<td>Dept. of Veterans Affairs</td>
<td>Blue</td>
</tr>
<tr>
<td>Freda</td>
<td>Lawhorn</td>
<td>AMI (Aztec Corp)</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Organization</th>
<th>Breakout Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keith</td>
<td>Lefland</td>
<td>DAII</td>
<td>Blue</td>
</tr>
<tr>
<td>Alan</td>
<td>Kraniche</td>
<td>Schneider Electric</td>
<td>Green</td>
</tr>
<tr>
<td>Maria</td>
<td>Kirk</td>
<td>Semnet</td>
<td>Yellow</td>
</tr>
<tr>
<td>James</td>
<td>Knowles</td>
<td>Space Age Electronics, Inc.</td>
<td>Green</td>
</tr>
<tr>
<td>Joel</td>
<td>Moody</td>
<td>Electrical Safety Authority</td>
<td>Blue</td>
</tr>
<tr>
<td>Thomas</td>
<td>Moore</td>
<td>Chair CFP &amp; NFPA 70</td>
<td>Yellow</td>
</tr>
<tr>
<td>Wayne</td>
<td>Moore</td>
<td>Jessem Hughes</td>
<td>Blue - Gold</td>
</tr>
<tr>
<td>Jamie</td>
<td>Mundy</td>
<td>Fire Alarm Institute</td>
<td>NCL</td>
</tr>
<tr>
<td>Paul</td>
<td>Mullen</td>
<td>Johnson Controls</td>
<td>Green</td>
</tr>
<tr>
<td>Tom</td>
<td>Norton</td>
<td>Nordion Service Co., Inc.</td>
<td>Yellow</td>
</tr>
<tr>
<td>Tony</td>
<td>O'Brien</td>
<td>Cisco</td>
<td>Red - Silver</td>
</tr>
<tr>
<td>Alan</td>
<td>Pakula</td>
<td>UL, LLC</td>
<td>Blue</td>
</tr>
<tr>
<td>Ted</td>
<td>Oglesea</td>
<td>Electrical Safety Authority</td>
<td>Yellow</td>
</tr>
<tr>
<td>Lisa</td>
<td>Orzuman</td>
<td>E85</td>
<td>Yellow</td>
</tr>
<tr>
<td>Michael</td>
<td>Parfitt</td>
<td>Telcor Inc</td>
<td>Green</td>
</tr>
<tr>
<td>Donald</td>
<td>Popkin</td>
<td>Valcom</td>
<td>Yellow - Lead</td>
</tr>
<tr>
<td>Tami</td>
<td>Parnell</td>
<td>Telgan</td>
<td>Yellow</td>
</tr>
<tr>
<td>Steve</td>
<td>Parfitt</td>
<td>Kidde Fire &amp; Safety</td>
<td>Blue</td>
</tr>
<tr>
<td>Chris</td>
<td>Parfitt</td>
<td>Interlink</td>
<td>Blue</td>
</tr>
<tr>
<td>Jason</td>
<td>Parfitt</td>
<td>Interlink</td>
<td>Yellow</td>
</tr>
<tr>
<td>Steve</td>
<td>Parfitt</td>
<td>Interlink</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

Figure 1 provides an illustration from this supplemental session.
2) Summit Overview and Background

To support the Summit Breakout Groups to address specific details of the PoE topic, general information was first provided to clarify key issues and support a common mindset for all the attendees. This was accomplished through a single background presentation along with a set of three Panel discussions.

The background presentation included preliminary background information and the Summit agenda. Most of this was presented in the beginning of the Summit, but then the remaining agenda-oriented slides were used throughout the remainder of the meeting. The information was presented by Casey Grant, serving in the role as Summit emcee.

The background presentation included the following: (1) A few words on fundamentals; (2) The ultimate objective; (3) PoE in the NFPA context; and (4) Where do we go next? This provided a perspective looking within the NFPA family of codes and standards, and also looking to the exterior with other codes and standards developers.

One key concept was to succinctly describe the universe of PoE, recognizing that this is a challenging task since it is such a sweeping issue. Figure 2: PoE Universe of Activity, attempts to summarize the key concepts and involved organizations in a single illustration. A primary theme is to balance advancing technology with the established safety infrastructure. The present “Safety Infrastructure” needs to coordinate with emerging technologies that show great promise, and do so without repeating past disaster. Today’s “Safety Infrastructure” has a well-established deep history built on painful lessons of the past. The intent is preserve or enhance today’s “Safety Infrastructure”.

![Figure 2: PoE Universe of Activity](image)

**PoE**  
**Power Over Ethernet**

**US Electrical SDOs**
- ATIS
- BICSI
- IEEE
- IES
- NECA
- NEMA
- NFPA
- TIA
- UL

(Note: also IEC, ITU, and Ethernet Alliance)
The PoE Summit is focused on building upon earlier similar work. In particular, it intends to continue promoting the outcomes of an earlier similar workshop titled: “Workshop Proceedings: Power Over the Ethernet”. This was held in October 2017 in Durham, NH and attempted to provide preliminary guidance on research planning for the PoE issue. The outcome of the October 2017 PoE Workshop was distributed with the PoE Summit meeting agenda, and is summarized in Figure 3: Key Findings from October 2017 “Workshop Proceedings: Power Over the Ethernet”.

<table>
<thead>
<tr>
<th>SUMMARY OBSERVATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Regulatory Coordination</td>
</tr>
<tr>
<td>1.1. Terminology: Define and promote a universal understanding of key terminology (e.g., PoE, Power, Communication, Wire, Cable, Intelligent Coordinated Power, etc.).</td>
</tr>
<tr>
<td>1.2. Goals and Objectives: Declare clear goals and objectives for all transmission applications (e.g., minimize fire and electrical hazards, maintain data integrity, etc.).</td>
</tr>
<tr>
<td>1.3. Occupancies and Applications: Clarify and define occupancy requirements for applications involving PoE concepts, and categorize applications based on their criticality (e.g., COPS Critical Operations Power System, fire alarm, security, etc.).</td>
</tr>
<tr>
<td>1.4. Key Attributes: Establish the performance parameters that all devices, components and associated systems need in terms of key attributes (e.g., availability, durability, maintainability, operability, reliability, stability, interoperability, compatibility, etc.).</td>
</tr>
<tr>
<td>1.5. Enforcement: Indicate essential details for inspection and re-inspection, in the form of relevant and useable checklist information.</td>
</tr>
<tr>
<td>1.6. Products: Facilitate the focus on “listed” products through standards that provide assurance of the products functioning as expected for their intended purpose and in support of scalable installations.</td>
</tr>
<tr>
<td>1.7. Document Coordination: Generate a clear and simplified overview of the entire regulatory landscape relating to this topic. Establish an advisory council (or equivalent) to coordinate technical requirements between the codes and standards of all involved organizations.</td>
</tr>
<tr>
<td>2. Key Technical Issues</td>
</tr>
<tr>
<td>2.1. Power versus Communication: Define, categorize and clarify requirements for the multiple options of transmitting power and communications, over one or multiple conductors (e.g., power only, communication only, communication/data/power in some combination, etc.), in coordination with defined occupancy and applications, as well as existing versus new installations.</td>
</tr>
<tr>
<td>2.2. Intelligent Coordinated Power: Clarify, summarize, categorize, and address all applicable technical details for Intelligent Coordinated Power (ICP) to assure safe and effective implementation.</td>
</tr>
<tr>
<td>2.3. 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 baseline.</td>
</tr>
<tr>
<td>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 alarm, security, etc.</td>
</tr>
<tr>
<td>2.5. Power Supplies: Clarify requirements for primary and back-up power supplies, contingent on occupancies, applications and other factors.</td>
</tr>
<tr>
<td>3. Research and Data</td>
</tr>
<tr>
<td>3.1. Predictive Data Analytics: Identify and clarify data needs and prospectively collect essential data for use with predictive data analytics.</td>
</tr>
<tr>
<td>3.2. Fundamental Baseline: Conduct research in support of validated modeling and establishing theoretical fundamentals for PoE systems.</td>
</tr>
<tr>
<td>3.3. 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.</td>
</tr>
<tr>
<td>4. Training, Education and Awareness</td>
</tr>
<tr>
<td>4.1. Training and Education: Implement training and education in support of all aspects of PoE, with a special focus on supporting inspection, enforcement and commissioning.</td>
</tr>
<tr>
<td>4.2. Format Delivery: Consider the use of a straight-forward yet relevant checklists and/or punch lists to facilitate third party support and enforcement.</td>
</tr>
<tr>
<td>4.3. Awareness Outreach: Facilitate outreach addressing the overall virtues of emerging technologies like PoE.</td>
</tr>
<tr>
<td>4.4. Stakeholder Engagement: Promote and facilitate dialogue and networking, and involve all impacted stakeholders. Address the needs of the entire ecosystem of stakeholders (e.g., designers, developers, vendors, installers, inspectors, end-users, etc.).</td>
</tr>
</tbody>
</table>

Figure 3: Key Findings from October 2017 “Workshop Proceedings: Power Over the Ethernet”

This overall presentation is summarized at the end of this section as Figures 4 through 9, Workshop Presentation While in Plenary Session. This supplemented information that was also handed out to all attendees, such as the Summit agenda, attendee list, and the summary observations from the October 2017 PoE Workshop. All of this was meant to support and subsequent Panel discussions and the Breakout Group discussions.
“POWER OVER THE ETHERNET”
SUMMIT: NEXT STEPS

Location: Mandalay Bay Conference Center, South Pacific Pavilion, Las Vegas, NV
Workshop Date/Time: Sunday, June 10, 2016, 11 am – 5 pm

“POWER OVER THE ETHERNET” SUMMIT: NEXT STEPS
WELCOME AND INTRODUCTORY REMARKS
Location: Mandalay Bay Conference Center, South Pacific Pavilion, Las Vegas, NV
Workshop Date/Time: Sunday, June 10, 2016, 11 am – 5 pm

“POWER OVER THE ETHERNET” SUMMIT: NEXT STEPS
AGENDA

1) A Few Words on Fundamentals
2) The Ultimate Objectives
3) PoE in the NFPA Context
4) Where do we go next?

Power Over the Ethernet

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

Power Over the Ethernet

Who are we (at this Summit)?
- The NEC Crowd
- The Fire Alarm Crowd
- The Other NFPA Crowd
- The Newcomers

Figure 4: Summit Presentation While In Plenary Session (Page 1 of 6)
**Future Direction: Power Over the Ethernet**
- Important for anyone addressing PoE, IoT, interoperability between codes, impact by these emerging technologies in the codes and standards, within NFPA and beyond
  - Within NFPA:
    - Installation documents, e.g., NEC® IEC® NFPA 202 NFPA 70 NFPA 70A NFPA 70B NFPA 1240.017
    - Other documents, e.g., NFPA 70 NFPA 70A NFPA 1240.017
  - Process documents, e.g., NFPA 70 NFPA 70A NFPA 1240.017
- Beyond NFPA with other organizations
  - Example: ICC® Registered Communications Distributor Installation (RCDI)

**Power Over the Ethernet**

The world is changing, with the convergence of the electrical world and the 'electronics world'.

**Introduction and Background**

1. A Few Words on Fundamentals
2. The Ultimate Objectives
3. PoE in the NFPA Context
4. Where do we go next?
Figure 6: Summit Presentation While In Plenary Session (Page 3 of 6)
Figure 7: Summit Presentation While In Plenary Session (Page 4 of 6)
Figure 8: Summit Presentation While In Plenary Session (Page 5 of 6)
Figure 9: Summit Presentation While In Plenary Session (Page 6 of 6)
3) Summit Panel Discussions

A set of three separate Panel discussions were provided, in addition to the Summit Overview Presentation, to facilitate plenary discussion and to promote a common mindset among the collective Summit participants. The approach with the Panel discussions was meant to maximize the number of speakers in the limited time frame on the Summit, and to engage audience participation in the open discussion that followed the brief presentations by each Panelist.

The topic of the first Panel discussion was “Addressing the Vision of PoE”. This recognizes that the professional community is lacking a unified common vision of what needs to be done on this topic and how best to accomplish it. The Panelists participating in this discussion included: Ernie Gallo, Mark Hilbert, Chad Jones, Alan Manche, Denise Pappas, and George Zimmerman. This discussion highlighted the coming together of different technical worlds; the need for clear scopes of activity; and clarification of common terminology.

The second Panel discussion focused on the “Coordination across Codes and SDOs” (Standards Developing Organizations). Participants in this Panel discussion included: Shane Clary, Mike Johnston, John Kovacik, and Wayne Moore. This discussion clarified that some organizations are ahead of others (e.g., IEC via Smart Cities); timeliness of different SDO processes is noteworthy; there is a need for higher level correlation (i.e., inter-organizational); and the challenges of higher level coordination are significant.

The final Panel discussion addressed “Next Steps & Future Actionable Items”. The participants were: Donny Cook, Joel Goergen, Randy Ivans, Tom Parrish. Highlighted discussion items included: need to address definitions as a starting place; a lot of PoE is already installed and needs to be addressed; transmission integrity and power are two separate issues and are application specific; and data security is a major concern and no longer secondary.
4) Break-Out Group Discussions

A key part of the PoE Summit was the separation of all attendees into four Break-Out Groups to further address key issues. The group questions were organized prior to the Summit to facilitate certain important issues.

Following the last Panel discussion, all attendees separated into four different groups to discuss the key issues that needed to be addressed. The questions are summarized in Table 3-6: Break-Out Group Questions. These questions were distinctly separated into four sections: (1) Vision; (2) Training, Education and Awareness; (3) Regulatory Coordination; and (4) Research and Data.

Table 3: Break Out Group Questions (1 of 4)

1. **VISION (20 minutes in group discussions)**
   1.1. **Vision Statement**: Provide comments and/or edits to the following vision statement: “This effort seeks to manage the evolution of PoE as an emerging technology, in recognition of its ability to effectively and efficiently utilize common pathways for the transmission of both electrical power and communications.”
   1.2. **Applications & Occupancies**
      1.2.1. Where are we going to see the use of PoE, near-term?
      1.2.2. Where are we going to see the use of PoE, long term?
      1.2.3. What end-use equipment is going to utilize PoE, near-term?
      1.2.4. What end-use equipment is going to utilize PoE, long term?
   1.3. **Equipment & Transmission**
      1.3.1. How will mission critical equipment be impacted?
      1.3.2. How should critical activities like COPS, fire alarm and premises security be handled?
      1.3.3. What types of cables are in use for PoE?
      1.3.4. What cables are going to be needed?
      1.3.5. Are circuit integrity cables going to be needed?
   1.4. **Key Hazards and Baseline Issues**
      1.4.1. Identify, define and prioritize the critical baseline issues, such as: (i) levels of integrity (e.g., COPS, fire alarm, security, egress, lighting, etc.); (ii) interruption and surge hazards (for equipment); factors of safety; and other topical issues.
      1.4.2. Identify and prioritize with rank) the key electrical hazards (e.g., shock, arc-flash, surge, interruption, etc.) and key fire related hazards (fire ignition, fuel load, flame spread, products of combustion, etc.).
   1.5. **Terminology**: What key terms need standardized universal definitions (e.g., PoE, wire, cable, managed loading, etc.)?
   1.6. **Other Issues**: Are there any other issues not addressed elsewhere? For PoE safety, are there any declarative statements on this topic that are important and should be stated?

Table 4: Break Out Group Questions (2 of 4)

2. **TRAINING, EDUCATION and AWARENESS (10 minutes in group discussions)**
   2.1. **Training and Education**: Which organizations should implement training and education in support of PoE, with a special focus on supporting inspection, enforcement and commissioning?
   2.2. **Format Delivery**: What are the key elements that should be included in straight-forward yet relevant checklists and/or punch lists to facilitate third party support and enforcement?
2.3. **Awareness Outreach**: Provide examples to outreach efforts that address the overall characteristics of PoE.

2.4. **Stakeholder Engagement**: Identify the target stakeholders whose further engagement should be promoted and facilitated. Consider the entire ecosystem of stakeholders (e.g., designers, developers, vendors, installers, inspectors, end-users, etc.).

2.5. **Other Issues?** Are there any other issues not addressed elsewhere? For PoE safety, are there any declarative statements on this topic that are important and should be stated?

---

**Table 5: Break Out Group Questions (3 of 4)**

<table>
<thead>
<tr>
<th>3. REGULATORY COORDINATION (15 minutes in group discussions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1. <strong>Organizations:</strong></td>
</tr>
<tr>
<td>3.1.1. Identify the key standardization organizations whose further engagement should be promoted and facilitated for PoE.</td>
</tr>
<tr>
<td>3.1.2. Are there any realistic existing venues for United Nations type organization for PoE?</td>
</tr>
<tr>
<td>3.1.3. Who could (or should) be the host of a United Nations type organization for PoE?</td>
</tr>
<tr>
<td>3.1.4. In general, can this issue be characterized as the electrical industry versus the electronics industry? Why or why not?</td>
</tr>
<tr>
<td>3.2. <strong>Key Issues:</strong></td>
</tr>
<tr>
<td>3.2.1. Clarify the governance a United Nations type organization for PoE (e.g., who would appoint, etc.)?</td>
</tr>
<tr>
<td>3.2.2. What is or will be the role of the federal government with regulatory issues (e.g., how will we deal with changes to FCC and phone lines)?</td>
</tr>
<tr>
<td>3.2.3. What are the barriers for a United Nations type organization for PoE?</td>
</tr>
<tr>
<td>3.2.4. What key issues should be addressed first, that are ideal for joint regulatory coordination?</td>
</tr>
<tr>
<td>3.2.5. Identify and prioritize key product issues and concerns (e.g., certification, aftermarket, counterfeit, etc.)</td>
</tr>
<tr>
<td>3.3. <strong>Other Issues?</strong> Are there any other issues not addressed elsewhere? For PoE safety, are there any declarative statements on this topic that are important and should be stated?</td>
</tr>
</tbody>
</table>

---

**Table 6: Break Out Group Questions (4 of 4)**

<table>
<thead>
<tr>
<th>4. RESEARCH and DATA (15 minutes in group discussions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1. <strong>Data &amp; Data Analytics.</strong></td>
</tr>
<tr>
<td>4.1.1. Identify and prioritize key data &amp; data analytic needed to impact policy and related activities.</td>
</tr>
<tr>
<td>4.1.2. Identify and describe the barriers and obstacles for addressing data in support of safety concerns, including non-technical (e.g., legal, privacy, labor, security, etc.)</td>
</tr>
<tr>
<td>4.2. <strong>Managed Loading (aka, dynamic loading or smart loading).</strong></td>
</tr>
<tr>
<td>4.2.1. What are the primary obstacles for the safe use of managed loading?</td>
</tr>
<tr>
<td>4.2.2. Clarify the necessary safeguards (e.g., integrity/protection/etc.).</td>
</tr>
<tr>
<td>4.3. <strong>System Reliability:</strong></td>
</tr>
<tr>
<td>4.3.1. Clarify the reliability of interconnection/integration and various communication methods for reliable and secure operation</td>
</tr>
<tr>
<td>4.3.2. Describe how supervision and battery back-up will be handled?</td>
</tr>
<tr>
<td>4.3.3. For cyber security, how will we assure security of data sent over PoE and networks?</td>
</tr>
<tr>
<td>4.4. <strong>Factors of Safety.</strong></td>
</tr>
<tr>
<td>4.4.1. What are the key elements and characteristics that require factors of safety?</td>
</tr>
<tr>
<td>4.4.2. Clarify what is presently used (if known), and what is needed.</td>
</tr>
<tr>
<td>4.5. <strong>Scalability of Applications.</strong> What are the barriers for the safe use of plug-and-play approaches that can substantially increase the needs of the supporting infrastructure (e.g., power supplies, etc.)?</td>
</tr>
<tr>
<td>4.6. <strong>Other Issues?</strong> Are there any other issues not addressed elsewhere? For PoE safety, are there any declarative statements on this topic that are important and should be stated?</td>
</tr>
</tbody>
</table>
The break-out groups were evenly balanced with a diverse mix of attendees. They were given a neutral identifier in no order of priority as follows: Yellow Group; Green Group; Blue Group; and Red Group. They collectively reported back during the plenary session as summarized in Table 7: Consolidated Break-Out Group Responses. This summarizes the raw output from each of the four break-out groups (with editing for clarity and consistency). It’s noted that not all groups responded to each question.

Each break-out group used a corner of the plenary session meeting room to separately and independently address each of the questions. Figure 10 provides illustrations of the Break Out Group activities. Each group had an appointed lead facilitator, a recorder and a timekeeper.

At the conclusion of the break-out group sessions each group facilitator presented their groups findings. This was followed be a general discussion of issues by all workshop participants. The open discussion revealed multiple consistencies between the four groups, and these are captured in the Summary Observations of these Proceedings.

### Table 7: Consolidated Break Out Group Responses

<table>
<thead>
<tr>
<th>1. VISION</th>
</tr>
</thead>
</table>

#### 1.1 Vision Statement: Provide comments and/or edits to the following vision statement: “This effort seeks to manage the evolution of PoE as an emerging technology, in recognition of its ability to effectively and efficiently utilize common pathways for the transmission of both electrical power and communications.”

- **YELLOW:** Reliability; Safety; Security.
- **GREEN:** Add reliably to the vision statement; Functional protection vs. physical protection; Add safety/safely.
- **BLUE:** Everything its used for; fire alarm systems, cameras, sensors; POE is about infrastructure wiring
- **RED:** Something about safety; “the safety aspects of”.... The evolution of PoE; Don’t need to say ‘emerging’ it doesn’t add anything; Do we say PoE or “power and communications”, Ethernet is limiting. “Transmission of power of communications cables”; Transmission of electrical energy, safety, and communications data integrity, e.g., at the end of a statement.

#### 1.2 Applications & Occupancies.

1.2.1 Where are we going to see the use of PoE, near-term?

- **YELLOW:** Anything with a cable is where we will see the use of PoE.
- **GREEN:** Lighting; Cameras; Point of sale terminals; IP phones; Fire alarm; Security alarm.
- **BLUE:** In building systems; Class 2 Power Source; Depends on signaling and protocols; Server Networks.
1.2.2 Where are we going to see the use of PoE, long term?

- **YELLOW:** IOT; IIOT; Communication; Egress; Safety; Security; Schools; Airports; Industrial hard safety requirements is where we will not see it; Physical security; Data integrity; We will need standards in industry.
- **GREEN:** Appliances (larger); 5G deployment; In the house; LiFI; Health care; Manufacturing; Smart cities; Enhanced occupany detection.
- **BLUE:** Powering all smoke detectors; code doesn’t say you can do it right now; Emergency Lighting applications; Development of Innovation and Technology Panel to address this.
- **RED:** Anything with a wire to it, will have data as well; Replace the way we use electricity right now, instead of power receptacles, ‘Ethernet’ ports.

1.2.3 What end-use equipment is going to utilize PoE, near-term?

- **YELLOW:** Everything.
- **GREEN:** All display equipment; All low power equipment.
- **BLUE:** LED lighting; LED Strobes; Energy Storage (Router, switch, Battery management commissioning, network security, ISP).

1.2.4 What end-use equipment is going to utilize PoE, long term?

- **YELLOW:** Everything.
- **BLUE:** Routers; IP Switches.

### Equipment & Transmission

1.3.1 How will mission critical equipment be impacted?

- **YELLOW:** This is the way for the future; The application will be how the system will be used; Critical systems will drive PoE (not PoE driving Critical Systems); If not installed in accordance with standards, it will not work.
- **GREEN:** Reliability issues; We don’t fully know.
- **BLUE:** Integrity; COPS equipment.
- **RED:** But to a financial services company, the computer is ‘mission critical’ fire alarm is a different class of mission critical; Data communications integrity becomes important, the infrastructure has to be substantial (protected); Different levels of reliability? Will it be the same or different? Life Safety, etc. Based on life safety and property damage; Dividing ‘mission critical’ into those that affect ‘property’ and those that affect ‘life safety’; Until we know what ‘mission critical is’ we can’t be sure. The code handles this for generators.

1.3.2 How should critical activities like COPS, fire alarm and premises security be handled?

- **YELLOW:** Although codes and standards harmonize with one another, we need codes and standards need to reference one another; Current standards reflect current operations.
- **GREEN:** Segregated/dedicated systems; Need for product certification; Unified secondary power; Power priority scheme for power and data.
- **RED:** They should be well defined; They have Class N(?); COPS is handled (now) okay, maybe add in ‘worst case conditions’; Why not just incorporate what we do now into the PoE thing (same reliability etc.); We have existing regulations in there that give us a guide already. Need to make sure that it works at temperature (operation survivability) to include. 72 has to be survivable for voice alarm systems. It’s also based on risk factors; Multiple levels of reliability: they need to be well defined and consistent across all different standards; Separate network for mission critical systems (or perhaps network priority)

1.3.3 What types of cables are in use for PoE?

- **YELLOW:** CTIA 568.C; IEC 11801.
- **GREEN:** Cat 3, 5, 6, 7 etc. LAN cables; What about terminations?
- **BLUE:** CAT 5E – 6A.
1.3.4 What cables are going to be needed?

• **YELLOW**: Depends on the application.
• **GREEN**: To be developed; Ampacity and data rates; 2-hr fire rated cables; Segregated cables by function: Data, Phone, Life safety, By owner; Cable identification.
• **BLUE**: Whatever is required for the application.
• **RED**: The two-wire cable discussed during a panel.

1.3.5 Are circuit integrity cables going to be needed?

• **YELLOW**: PoE circuits need to be protected for the application; Yes, but we will need to redefine circuit integrity (definition broadened).
• **GREEN**: In some cases depending on code; May depend on redundancy.
• **BLUE**: In some applications; Life safety and fire alarm; Communications.
• **RED**: Yes (survivability rating, 2 hour fire rating); If it’s an application that needs data, the test may need to be changed. (may need additional integrity tests, data, etc.).

1.4 Key Hazards and Baseline Issues

1.4.1 Identify, define and prioritize the critical baseline issues, such as: (i) levels of integrity (e.g., COPS, fire alarm, security, egress, lighting, etc.); (ii) interruption and surge hazards (for equipment); factors of safety; and other topical issues.

• **YELLOW**: Application dependent; Applications will drive it; Industrial Process Safety; Physical integrity and data integrity are the most critical.
• **GREEN**: Redefine property protection (physical data); Limit of power and build to it; Reliability on critical systems; Surge; Obsolescence/life cycle; EMI interference.
• **BLUE**: Wireless can be hacked very easily – security issues; Same as other electrical equipment; Nothing different; Surge hazards.
• **RED**: Data Integrity; Cyber Security; Algorithm-based decision making (making sure the data is correct to make the decision); Data integrity, autonomous functions (fan control, based on the data); Integrity of speed of data (if you start overloading you’ll throttle back) (network priority).

1.4.2 Identify and prioritize with rank) the key electrical hazards (e.g., shock, arc-flash, surge, interruption, etc.) and key fire related hazards (fire ignition, fuel load, flame spread, products of combustion, etc.).

• **YELLOW**: Bundling of the cables is the most concern (Ambient heat); This is why 725.144 of the NEC (2017 ed.) exists; Degradation of data; Termination of circuits; Degradation of insulation.
• **GREEN**: Shock-5; Arc flash-6; Surge-4; Fire ignition -1; Fuel load-2; Flame spread-3; Overload-1b; Bundling-1a.
• **BLUE**: Less electrical hazards with PoE but depends on the level; 1. Surge Protection and interruption on all shared equipment; 2. Fire ignition, fuel load, flame spread, and products of combustion would be the same as standard cables today; Arc Flash – non issue; Shock – non issue.
• **RED**: POE as exists today: limited shock/arc flash, surges are small, interruption is the most relevant. Right now 70E says anything over 50v is a shock hazard, so that would be a potential, it’s 52, but still needs to be addressed; Surge protectors (to protect equipment) (the safety features of the equipment) (lightning as well); Arc flash and shock, less so, UNLESS we’re also talking about pulse power, in which case shock/arc flash is an issue.

1.5 Terminology

What key terms need standardized universal definitions (e.g., PoE, wire, cable, managed loading, etc.)?

• **YELLOW**: Definition of POE: Power over balance twisted pairs IEEE 802.3; Definition: Distinction between cable and cabling (cable is wire and cabling is collection of wires).
• **GREEN**: PoE; Different classification structure; Not class 1, 2, 3 circuits; System (dc) what is POE.
• **BLUE:** Power over Ethernet more effectively as it pertains to electrical standards, Subset of power over communications cable/circuit; Data Integrity; Manage Loading (future); Smart Power and smart cable; Pulse Power; Manage Power and Loading.

• **RED:** PoE; Pulse Power; Data integrity; Classifications (classes of PoE, we already have circuit classifications). Class 1 PoE vs Class 1 Circuit (disambiguation); Already in Code: Minimum current voltage (every circuit has current voltage) but we don’t consider power. What is the ‘threshold’ for what counts as power. Power limited circuits; Loading on Bundles; What is ‘critical’? (could be overall NFPA needs coordination); Nominal vs. Rated.

1.6 Other Issues? Are there any other issues not addressed elsewhere? For PoE safety, are there any declarative statements on this topic that are important and should be stated?

• **YELLOW:** We need to communicate with other organizations who have already done this; PoE application will happen faster than the standards to control it; TIAs or some method to update codes/standards.

• **GREEN:** Long-term maintenance and reliability over time; Software and firmware updates; Security; Data corruption; PoE control of higher voltage circuits; Does it require physical protection.

• **BLUE:** Security of the data; Overloaded Cable.

• **RED:** Temperature (as in ambient or operating) because it goes to the data integrity, which drops at a much lower temperature than it becomes a fire/safety hazard.

### 2. TRAINING, EDUCATION and AWARENESS

2.1 Training and Education: Which organizations should implement training and education in support of PoE, with a special focus on supporting inspection, enforcement and commissioning?

• **YELLOW:** RCDD → NICET; IAEI (International Association of Electrical Inspectors); AIA; Manufacturers; NRTL Labs.

• **GREEN:** NFPA; IBEW; IEEE; NEMA; NECA; IAEI; ICC; NFPA can take the lead in training in safety and code compliance.

• **BLUE:** NECA -> contractors; ETA; IAEI -> inspectors; IEEE -> engineers; BICSI -> installers of communication; NFPA -> AHJ’s, others; ACE.

• **RED:** NECA; (All of them); BIDSI, NFPA, IAEI, NJACT, IEC; NFPA’s role may be in coordinating. There are sometimes too many voices trying to educate.

2.2 Format Delivery: What are the key elements that should be included in straight-forward yet relevant checklists and/or punch lists to facilitate third party support and enforcement?

• **YELLOW:** There is an existing litmus test”; Listing and labeling of product; Manufacturers instructions; Technology industry has provided; NRTL; We don’t like checklists; Third Party Verification vs inspection are two different things.

• **GREEN:** Online; Web meetings; Punch list for compliance; App; Classroom; Articles; PoE for non-experts.

• **BLUE:** Online Delivery; Lunch and learn.

• **RED:** Standardized Enforcement Document (maybe or maybe not checklist); Electrical Inspector’s Guide (maybe this for ‘PoE’); SIMPLE checklists; Commissioning: Requirements from ICC for energy efficiency, but states nix those. If they’re required to commission, that will limit non-qualified individuals installing systems; End to End Testing: covered by 3 and 4. Each one subsystem has to acceptance test first; Commissioning Needed. (maybe just for mission critical).

2.3 Awareness Outreach: Provide examples to outreach efforts that address the overall characteristics of PoE.

• **YELLOW:** Educate this entire industry; Outreach with BOMA to educate them on PoE and the impact of life and safety; Than we can educate FM and inspectors; Legislative → Put in adoptable format.

• **GREEN:** Roadshow: NFPA expo, Relevant tradeshows, Discuss with legislative bodies, You-tube video, Branding.

• **BLUE:** Need a POE Handbook; NFPA and IEEE could help; Next evolution in technology committee – where to raise awareness and training; New Technology Forum; Standards Council Involvement.

• **RED:** Involve the groups from training standpoint (inspectors, contractors, enforcement, standards writers, designers). Manufacturers; Electrical inspectors, and IT (new).
2.4 **Stakeholder Engagement**: Identify the target stakeholders whose further engagement should be promoted and facilitated. Consider the entire ecosystem of stakeholders (e.g., designers, developers, vendors, installers, inspectors, end-users, etc.).

- **YELLOW**: All the above; BOMA; Labor Unions; NECA; NAHB; Codes/Standards organizations: IEBW, IEC, ICC, IEC.
- **GREEN**: Installers; Inspectors; Designers; Facility owners; IEEE; Branding; ESFI.
- **BLUE**: Same as 2.1; Inspectors; End-users/consumers/Owners; IEC.
- **RED**: Beyond already discussed; Electrical Inspectors; *IT Professionals*; Building Developers (smart buildings); Equipment Manufacturers (NEMA) (they will go down this path themselves, the other groups may be more important); The manufacturers should have an existing package. The bigger gap may be ‘start up’ companies that don’t come from a ‘life safety’ world, but will interact with life safety systems; AHJ and what they approve.

2.5 **Other Issues?** Are there any other issues not addressed elsewhere? For PoE safety, are there any declarative statements on this topic that are important and should be stated?

- **GREEN**: None.
- **BLUE**: Should have specific branding (POE Trademark) – too late now; Data Assistance Team; Run Simulations (volunteer) (ex. NEC sump pump ground fault (GFCI); Specify a problem -> solution: we think... simulation: “real world best estimation”; Small scale problems.
- **RED**: N/A.

---

### 3. **REGULATORY COORDINATION**

3.1 **Organizations:**

3.1.1 Identify the key standardization organizations whose further engagement should be promoted and facilitated for PoE.

SDOs:

- **YELLOW**: IBEW; IEC; ICC; IEC; IES.
- **GREEN**: NFPA; NEMA; IEEE; NRTL; UL; IEC; ISO; ATIS; TIA; ITU.
- **BLUE**: NFPA; All Organizations listed in presentation.
- **RED**: NFPA, UL, BICSI (See above); IEEE 802.3; IEEE (but broad); TIA, FCC.

3.1.2 Are there any realistic existing venues for United Nations type organization for PoE?

- **YELLOW**: No; TIA (telecommunications industry association), BICSI (building industry consulting services international), IEEE that are already driving it.
- **GREEN**: IEEE.
- **BLUE**: Us; (in this room) - This group at POE Summit should lead it; Have FPRF lead this “New Technology Forum” frequently.
- **RED**: IEC; Advisory Council on Electrical Safety (Test Labs with OSHA, CPSC, open forum); A clearinghouse that is open for different SDOs, not pay for play, can be seen as a ‘facilitator’; DOD (security angle) Federal Government.

3.1.3 Who could (or should) be the host of a United Nations type organization for PoE?

- **YELLOW**: IEEE, TIA and IEC should host this.
- **GREEN**: IEEE.
- **BLUE**: US at POE summit; Including NFPA/FPRF.
- **RED**: Unsure.

3.1.4 In general, can this issue be characterized as the electrical industry versus the electronics industry? Why or why not?
• **YELLOW:** Not compatible yet but innovation is trying to make it compatible. This goes back to equipment standards vs. installation standards. Electrical would be installations standards and electronic equipment be the equipment standards. These need to be integrated.

• **GREEN:** N/A.

• **BLUE:** BICSI, NFPA.

• **RED:** Those are the same, electronics are a part of the electrical system; *Not viewed as a battle.*

### 3.2 Key Issues:

#### 3.2.1 Clarify the governance a United Nations type organization for PoE (e.g., who would appoint, etc.)?

- **YELLOW:** TIA, BICSI.
- **BLUE:** We should lead it; Like this meeting with a narrower focus (Longer meeting); Elected officers; Should occur quarterly with working groups in between; Outcome: suggested public input (proposals) for various documents to adopt.
- **RED:** Unsure.

#### 3.2.2 What is or will be the role of the federal government with regulatory issues (e.g., how will we deal with changes to FCC and phone lines)?

- **YELLOW:** Keep it at the local level.
- **GREEN:** Other international standards; Commercial interests.
- **RED:** Unsure; FCC, DOD(?), Service Providers for next-gen DSL are very closely related; GDPR (Privacy); Data protection/Privacy.

#### 3.2.3 What are the barriers for a United Nations type organization for PoE?

- **YELLOW:** Inertia and egos.
- **GREEN:** See 3.2.2 response.
- **BLUE:** Large, wide scope issue.

#### 3.2.4 What key issues should be addressed first, that are ideal for joint regulatory coordination?

- **YELLOW:** Definitions and make them so we can agree on the definitions; Education on enforcement; Scope and Purpose.
- **GREEN:** Difficult to answer.
- **BLUE:** Define Poe and the goal
  - Vision statement
  - Mission statement

#### 3.2.5 Identify and prioritize key product issues and concerns (e.g., certification, aftermarket, counterfeit, etc.)

- **YELLOW:** Breach; Reliability; Safety security.
- **GREEN:** Rogue devices; Lack of installation standards; How to determine if devices are compliant after installation; Lack of awareness.

### 3.3 Other Issues? Are there any other issues not addressed elsewhere? For PoE safety, are there any declarative statements on this topic that are important and should be stated?

### 4. RESEARCH and DATA

#### 4.1 Data & Data Analytics

#### 4.1.1 Identify and prioritize key data & data analytic needed to impact policy and related activities.

- **YELLOW:** PoE fire incidents – None; Power Supply Failures – Only document incidents.
- **RED:** “Washing Machine Example” *what are the boundaries and barriers in terms of access?* The washing machine could be providing data, and it’s also an access point, especially if everything is connected (cybersecurity).
4.1.2 Identify and describe the barriers and obstacles for addressing data in support of safety concerns, including non-technical (e.g., legal, privacy, labor, security, etc.)
   • **YELLOW**: N/A.

4.2 Managed Loading (aka, dynamic loading or smart loading).

4.2.1 What are the primary obstacles for the safe use of managed loading?
   • **YELLOW**: Complex system and requires lots of expertise.
   • **RED**: Data prioritization: how do we scheme things to guarantee alarm times?; Prioritizing critical (and non critical) requirements for deployment.

4.2.2 Clarify the necessary safeguards (e.g., integrity/protection/etc.).
   • **YELLOW**: Design and complexity of the system; Competent design

4.3 System Reliability:

4.3.1 Clarify the reliability of interconnection/integration and various communication methods for reliable and secure operation
   • **YELLOW**: Establish new guidelines for PoE, manufactures will follow; IEC-TC 48 – cover connected hardware globally for data communications.
   • **BLUE**: Only one device can talk at a time; Need reliability standards; Not directly related to power over communication circuit/cable – if no POE power, Ethernet protocol is still a problem.
   • **RED**: AFCI’s: when they came out, there was no requirement to test with other lamps/washing machines, because there was no interoperability/compatibility, so this is an important issue for these standards to look at; *This is important, should there be a compatibility document?? Similar to Backnet and MODBUS.*

4.3.2 Describe how supervision and battery back-up will be handled?
   • **YELLOW**: NFPA 72; UL 924.
   • **BLUE**: Management and Analytics; Use big data to make decisions.

4.3.3 For cyber security, how will we assure security of data sent over PoE and networks?
   • **YELLOW**: UL 2900; ISA 62443.
   • **BLUE**: Can easily hack into fire alarm system; Needs to be addressed.

4.4 Factors of Safety

4.4.1 What are the key elements and characteristics that require factors of safety?
   • **YELLOW**: Covered by NEC with UL Table.

4.4.2 Clarify what is presently used (if known), and what is needed.
   • **YELLOW**: Covered by NEC with UL Table.

4.5 Scalability of Applications. What are the barriers for the safe use of plug-and-play approaches that can substantially increase the needs of the supporting infrastructure (e.g., power supplies, etc.)?
   • **YELLOW**: This is massive; Plug and play will not work in the life safety world and it needs to; If designed and installed with standards, there are no barriers to support the system into the future; Designed for growth.

4.6 Other Issues? Are there any other issues not addressed elsewhere? For PoE safety, are there any declarative statements on this topic that are important and should be stated?
   • **YELLOW**: A lot of work needs to be done; Subject to field verification; Coordination between SDO.
5) Summary Observations

The information gathered at this PoE Summit has been synthesized with previously gathered information to identify actionable next steps to facilitate full consideration of PoE cabling in modern infrastructure, without compromising established levels of safety.

The Summit has supported the continued networking and relationship building and allowed the technical details to be further addressed. A diverse group of stakeholders and representatives of key NFPA codes and standards have participated. The general concepts of PoE and an appreciation for its importance has been established and/or further advanced among key impacted NFPA codes and standards, and the door is open for further efforts to more comprehensively address the issues raised.

In addition to the networking and relationship building inherent to this activity, this Summit also addressed: (1) the future vision of PoE; (2) training, education and awareness; (3) regulatory coordination; and (4) research and data. This was also the primary structure of the Break-Out Groups. The following are the key summary observations from this PoE Summit.

Table 8: Summary Observations from the PoE Summit

<table>
<thead>
<tr>
<th>1. VISION</th>
</tr>
</thead>
</table>

1.1 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 common pathways for the transmission of both electrical power and communications.”

1.2 Applications & Occupancies. Near term and long term, we can expect to see the use of PoE everywhere there is a cable or conductor. Consistent with the Internet of Things, anything with a wire to it will have data as well.

1.3 Equipment & Transmission. Mission critical equipment is evolving and the definition needs to be re-evaluated. For example, more attention will be given to the reliability of data processing and control. Critical activities like COPS (critical operations power systems), fire alarm and premises security need to further evolve and consider worst-case design situations. Levels of reliability need to be well defined and consistent across all different codes and standards. Circuit integrity will continue to be important, and additionally, future consideration of reliable data integrity is also needed.

1.4 Key Hazards and Baseline Issues. The critical baselines issues are application dependent, and physical integrity and data integrity are the most critical. Issues such as surge; obsolescence, life cycle; EMI interference, networking priority, and so on need to be considered. The hazards of most concern are the key fire related hazards such as fire ignition, fuel load, flame spread, products of combustion, etc., (e.g., from the bundling of cables). The concern for electrical hazards (e.g., shock, arc-flash, surge, interruption, etc.) are considered minimal, unless innovative approaches like pulse power are used.

1.5 Terminology. Universally recognized key terms are needed through standardized definitions (e.g., PoE, classifications of PoE, wire, cable, cabling, managed loading, pulse power, data integrity, etc.).

1.6 Other Issues. Other issues include: High-level organization is needed among the involved SDOs (Standards developing organizations); long term maintenance and reliability over time is needed; and data security is essential.
2. TRAINING, EDUCATION and AWARENESS

2.1 Training and Education. Organizations should implement training and education in support of PoE, with a special focus on supporting inspection, enforcement and commissioning, including but not limited to: ACE; AIA; BICSI (for installers of communications); ETA; IAEI (for enforcers); IBEW; ICC; IEC; IEEE (for engineers); NECA (for contractors); NEMA (for manufacturers); NFPA; NICET (with RCDD certification); NJACT; and NRTL Labs. In the future, NFPA’s role may include coordinating the numerous groups.

2.2 Format Delivery. Certain key elements should be included in straight-forward yet relevant checklists and/or punch lists 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” (may or may not as a checklist); an “Electrical Inspector’s Guide”; and commissioning guidance. This should consider web meetings; punch list for compliance; apps; classroom training; articles on PoE for non-experts, and so on.

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

2.4 Stakeholder Engagement. The targeted stakeholders for further engagement should consider the entire ecosystem of stakeholders (e.g., designers, developers, vendors, installers, inspectors, end-users, etc.), and include at least the following: AHJs; BOMA; Building Developers (smart buildings); Equipment Manufacturers (NEMA); ESFI; Labor Unions; NAHB; NECA; IBEW; ICC; IEC; IT Professionals.

2.5 Other Issues. Other issues include: specific branding (e.g., POE Trademark); Data Assistance Teams; and development of simulation approaches.

3. REGULATORY COORDINATION

3.1 Organizations. The key standardization organizations (and similar groups) whose further engagement should be promoted and facilitated for PoE include: ATIS; BICSI; FCC; IBEW; ICC; IEC; IEEE; IES; ISO; ITU; NEMA; NFPA; NRTL; TIA; and UL. An existing venues for a United Nations type organization for PoE will be a challenge, though some groups like IEEE and IEC are already driving this issue. In general, the 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 officers). This is better as a bottom-up activity rather than a top-down approach (e.g., federal government). The large wide scope of PoE makes this a particular challenge. The ideal first issues that need to be addressed are a mission statement, a vision statement, and definitions. Other critical key issues include, as examples: aftermarket; certification; counterfeit; lack of awareness; lack of installation standards; post installation compliance; reliability; rogue devices; safety; and security.

4. RESEARCH and DATA

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.

This Summit is an important step for addressing this issue, but it is only one step in the overall journey to address Power over the Ethernet. The world is changing rapidly, and the devices and technologies that support it, such as PoE and IoT, are here to stay. Historically, the safety infrastructure has made great headway in establishing a fire and electrically safe world, and it is paramount that the regulatory community rises to address the new emerging challenges that we are now regularly witnessing in today’s world.
Annex A: The Impact of PoE and Emerging Technologies on the Fire Alarm Industry

This Annex has been prepared by Victoria Hutchison of the Fire Protection Research Foundation, as a supplement to the PoE Summit proceedings.

The Impact of PoE and Emerging Technologies on the Fire Alarm Industry

DATE: 17 AUGUST 2018

By: Victoria Hutchison, Fire Protection Research Foundation

© 2018 Fire Protection Research Foundation

1 Batterymarch Park, Quincy, MA 02169-7417
Email: foundation@nfpa.org web: nfpa.org/foundation

Figure 11: Annex A – PoE Fire Alarm Impact (Page 1 of 12)
Table of Contents

Table of Contents ........................................................................................................................................... i
List of Tables .................................................................................................................................................. ii
List of Figures .............................................................................................................................................. ii
1. Background ............................................................................................................................................... 1
2. Status of Power-Over-Ethernet .............................................................................................................. 1
3. Regulatory Challenges ............................................................................................................................. 2
4. TOWS Analysis ....................................................................................................................................... 5
5. Conclusion ............................................................................................................................................... 8
6. References ............................................................................................................................................... 9

Figure 12: Annex A – PoE Fire Alarm Impact (Page 2 of 12)
List of Tables

Table 1 TOWS Analysis Approach ................................................................. 7

List of Figures

Figure 1 TOWS (Threats/ Opportunities/ Weaknesses/ Strengths) Relationship .............. 5
Figure 2 TOWS Analysis of NFPA 72 regarding new technologies.................................. 6

Figure 13: Annex A – PoE Fire Alarm Impact (Page 3 of 12)
1. Background

The Internet of Things (IoT) continues to bring people, processes, data and things together in a variety of environments. As our environments become more intelligent, more adaptive and more integrated, Power-over-Ethernet (PoE) is evolving as a common means of not only controlling the communications between the numerous intelligent devices connected to their networks, but also as a means of power. PoE is essentially simplifying building’s electrical power and communication infrastructure.

The 2018 PoE Summit: Next Steps in Las Vegas, NV, had a significant presence by the fire alarm industry. Thus, this analysis will have a particular focus on the impact of PoE and other emerging technologies on NFPA 72. Since the general goal of NFPA 72 National Fire Alarm and Signaling Code is to “change the code in a fashion that makes installed fire alarm systems more operationally reliable, permits the proper use of the most modern technology, and incorporates features to keep the fire alarm systems free of false alarms,” how new technologies and changes to the FCC are impacting fire alarm systems will be analyzed (Moore, 2015).

Due to the evolution of the Internet of Things (IoT), we can now remotely connect to practically any communication device through Ethernet or other networks. Although incorporating computer-based technology into fire alarm systems is not a new concept for the Fire Alarm Industry, due to concerns of maintaining integrity and reliability, fire alarm signals have previously never been transmitted through an integrated network.

Traditionally, fire alarm systems used a private network with customized copper wiring to connect detection devices to the fire alarm control unit. Private networks were utilized to ensure high integrity, reliability, and security of the transmitted fire alarm signals to prevent other communication signals from interfering with the operational reliability of the fire alarm system (NFPA 72 Supplement 3, 2016).

However, the world is changing. Utilizing copper telephone lines for fire alarm communication is in the past and integrating building and fire and life safety systems through network technologies is the future.

2. Status of Power-Over-Ethernet

We are living in an age of smart systems, connected devices, and cloud-based IoT solutions. As of 2016, there were approximately 11 billion IoT devices connected to the Internet and this is expected to increase to nearly 30 billion devices by 2020 (Nordrum, 2016). These technological advancements are having a transformative impact on virtually every industry, including fire protection and life safety. Interconnecting fire, emergency communications, security, and life safety systems are helping to enhance safety, optimize processes, and reduce costs. As the availability of high-speed internet, development and implementation of powered devices, and the demand for cost-effective, fast, and efficient data communication increases, the demand for PoE is expected to increase accordingly.

"Power over Ethernet is a technology for wired Ethernet local area networks (LANs) that allows the electrical current necessary for the operation of each device to be carried by the data cables rather than by power cords" (Rouse & Schmidt, 2018).
Using Ethernet cabling as a single source of power and communication enables the following (Veracity UK Ltd., 2016):

- **Simplification** in the installation and use of powered devices
- **Flexibility** in device placement
- **Scalability** of access to network connections
- **Reliability** from a universally compatible power source that is backed up by an uninterruptable power supply (UPS)
- **Cost savings** in installation and material costs.

The infrastructure for low powered data (Ethernet) regulated by the NEC and other codes and standards is changing. Whereas previously the cables used were only operating at very low power levels, this same cable infrastructure is now being used to supply power for IP phones, security cameras, lighting, PLC controllers, mass notification, kiosk/annunciation, charging of electronic devices and other applications (Veracity UK Ltd., 2016).

In 2003, the Institute of Electrical and Electronics Engineers (IEEE) developed IEEE 802.3af standard titled, *Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)* – now referred to as Power over Ethernet – which standardizes a system supplying low voltage power to networked devices via the communications line (B&B Electronics, 2018). Since the demand for delivering more power over Ethernet cables and the number of PoE enabled powered devices is increasing exponentially, there is an essential role for PoE as the internet of things continues to grow. As a result, IEEE is developing a new standard: IEEE 802.3bt titled Next Generation PoE to address this continually evolving technology (B&B Electronics, 2018).

In addition to the IEEE, other standard development organizations such as ATIS, BICSI, IES, NECA, NEMA, NFPA, TIA, and UL along with IEC, ITU, and the Ethernet Alliance all address Power over Ethernet – indicating the broad scope of this technology and its widespread implications (Grant et al., 2018). Within NFPA alone, the following documents are impacted by PoE technology: NFPA 70 (NEC®), NFPA 72, NFPA 730/731, NFPA 34, NFPA 79, NFPA 75, NFPA 78, NFPA 99, NFPA 101, NFPA 85, and NFPA 86, among others.

### 3. Regulatory Challenges

Until recently, the fire alarm industry has been very stable, and in general has not had to undergo many major changes. However, advancements in technology are forcing the fire alarm industry to change with it. The industry is now accepting these changes in terms of modifications and additions to the codes and standards, accepting the elimination of old technologies, and acknowledgement of user’s expectations (Wilhelm, 2015). In today’s society, users want to use the latest technology, while having features such as mobility, flexibility, reliability, security, etc. NFPA 72 is now adopting to the present changes and challenges, preparing for additional changes in the future, and is continuing to develop solutions for PoE and other technologies. While change is now taking place within the regulatory landscape with respect to Power over Ethernet, there have been significant challenges to overcome to reach this point. The challenges presented by PoE on the fire alarm industry will be discussed within this section.

Initially, the communications industry had great concerns when Power over Ethernet was introduced as a means of transporting both data and power through the same cable. Adding power to a communications cable presents significant hazards that were not previously an issue.
However, in this technological era of the internet of things, various technologies including PoE and others, are here to stay. Thus, it is of critical importance for regulatory organizations to keep up with current and emerging technologies, address the challenges at hand, and present solutions to stay relevant as various technologies continue to evolve.

Communication methods for fire alarm systems are undergoing a significant transformation. For over forty decades, fire alarm signals were communicated to the fire departments via landline telephones—a technology many thought would never cease to exist. However, the Federal Communications Commission (FCC) has recently announced their intention to discontinue the use of the legacy phone system over the next few years (Feld, 2016). The Plain Old Telephone System (POTS) has been determined to not be sustainable, and for that reason, will soon become an obsolete technology (Wilhelm, 2015). While copper phone lines will not be entirely eliminated immediately, the phone system will transition to a mix of digital platforms where wireless technologies will be incorporated into national communications platforms as the transition from switch networks to broadband is made (Feld, 2016).

Since the legacy phone system has long been the primary means of fire alarm communication, the changes to the FCC presented the NFPA 72 technical committee with significant challenges with respect to how to address the changing infrastructure. Phasing out POTS lines meant that thousands of alarm panels would not be monitored unless new technology was adopted (Wilhelm, 2015). While the fire alarm industry had been aware of other technology options (e.g., Internet Protocol, Managed Facilities Voice Network (MFVN), Global System for Mobile Communications (GMC), etc.) for a significant period of time none of them had been adopted due to their inability to ensure reliability and redundancy that is equivalent or superior to the current system.

The NFPA 72 Committee had similar concerns when considering integrating fire and life safety systems with building networks (i.e., non-fire or non-mass notification systems). There are a variety of issues that could arise from integrating building and fire/life safety systems such as a reduction in reliability, availability, security, etc. With more data being transmitted over the network, there was also significant concern around the receivers potentially experiencing delays in receiving the transmitted signals due to heavy network traffic (NFPA 72 Supplement 3, 2016).

Fire codes have been slow to adopt the approved use of common networks such as Ethernet. One reason for its slow adoption of Ethernet technologies stems from its failure to report a connection to a ground (a fundamental requirement for fire alarm systems) and the associated uncertainty regarding the ability to adequately document, control, and test these network systems (NFPA 72 Supplement 3, 2016).

Further, an informal study determined that Ethernet monitoring undergoes a downtime of approximately 0.75 to 1.5% of the time—typically due to manual upgrades, testing, or maintenance on the network (Moore, 2015). Traditionally, however, if the reliability of the fire alarm system is less than 99.9999%, it is not acceptable. Since network technologies were previously being forced into existing pathway designations, fire alarm systems were unable to adequately meet the existing requirements for Class A, B, C, D, E, or X pathways. This led to a NFPA 72 task group developing the "Class N" pathway designation. For NFPA 72 A.12.3.6 (1), “the Class N pathway designation is added to specifically address the use of modern network infrastructure when used in fire alarm and emergency communication systems" (NFPA 72, 2016).

Since Ethernet wiring often fails to meet the fault-monitoring requirements of traditional fire alarm pathways, the Class N circuit classification requires a redundant pathway that has its "operational capability verified through end to end communication” (NFPA 72. Supplement 3, 2016).
addresses the primary concerns regarding reliability of fire alarm communication via Ethernet networks.

While solutions are being developed, the safety infrastructure is continually being challenged by the rapid influx of new technologies. Although, timely adaptation of safety protocols for these technologies is a challenge, it is much needed. For example, NFPA 72 now addresses network technologies in the 2016 edition, however using Ethernet cables as a means of distributing both power and communication was established in 2003 to support devices such as Wi-Fi access points (B&B Electronics, 2018).

The thorough and robust code development process is a strength in terms of ensuring that the adopted technologies are reliable, secure, and adequately meet the performance criteria specified within NFPA 72. However, technologies are evolving at a pace that far exceeds the code development time frames of three to five years; therefore new technologies are entering the marketplace for significant periods of time before they can be properly addressed by the applicable codes and standards. A significant factor in the delayed adoption of new technologies is the general lack of a comprehensive understanding of new technologies — requiring research efforts, educational seminars, and trainings for the applicable parties.

These technologies are continuing to present immense opportunities in terms of building and life safety system integration and economic benefit. But while new technologies bring great opportunities, they also present threats to the operational reliability and security of the established means of fire alarm communication specified in NFPA 72. To address the present threats and opportunities and develop actionable strategies for NFPA 72 to continue to embrace emerging technologies, a TOWS analysis was conducted in the following section.
4. TOWS Analysis

A TOWS (threats, opportunities, weaknesses and strengths) Analysis was conducted to assess the impact of emerging technologies on NFPA 72. The outcome of this effort is summarized in this section.

This TOWS Analysis primarily focuses on the impact of the perceived opportunities and subsequent threats presented by new technologies, such as Power over Ethernet (PoE), on the fire alarm industry. Further, the strengths and weaknesses of NFPA 72 provide a basis for an opportunity centric perspective. Thus, the path for further analysis and the development of specific recommended strategies is rooted on taking advantage of these opportunities, but upon the backbone of the strengths and weaknesses of NFPA 72, while taking into account and minimizing the threats on reliability, security, and availability of fire alarm communication.

This is illustrated in Figure 1, TOWS Relationship for NFPA 72, and is intended to provide a platform for further discussion to establish actionable and implementable strategic objectives.

![TOWS Analysis Diagram](image)

**Figure 1: TOWS (Threats/Opportunities/Weaknesses/Strengths) Relationship**

When utilizing this TOWS analysis approach, the strengths and weaknesses are generally looking inward, while the opportunities and threats are generally looking outward. The present areas of influence on NFPA 72 at this time predominantly involves the outside environment through emerging technologies and the evolution of the Internet of Things. Thus, this exercise is centered on the opportunities and threats.

All of the strengths and weaknesses of NFPA 72 are identified, along with the opportunities and threats presented by emerging technologies. All the identified elements on this topic are illustrated in Figure 2 below.
Figure 2 TOWS Analysis of NFPA 72 regarding new technologies

Now that the opportunities, threats, strengths and weaknesses have been identified and compiled, this information is now available for analysis for the establishment of strategic plans.

Table 1, TOWS Analysis Approach, provides a useful logic pattern for conducting this analysis. In Table 1, the “Weaknesses-Threats” in Quadrant I address the effort needed to eliminate weaknesses to avoid threats. The “Weaknesses-Opportunities” in Quadrant II focuses on improving weaknesses by taking advantage of opportunities. The “Strengths-Threats” in Quadrant III address the strengths we use to minimize threats presented by emerging technologies and
changes to the FCC. Finally, the “Strengths–Opportunities” in Quadrant IV are focused on using the strengths of NFPA 72 and the Fire Alarm Community to take advantage of opportunities.

Table 1 TOWS Analysis Approach

<table>
<thead>
<tr>
<th>Weaknesses (internal, negative)</th>
<th>Opportunities (external, positive)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quadrant I</strong></td>
<td><strong>Quadrant II</strong></td>
</tr>
<tr>
<td>Weaknesses-Threats Strategies</td>
<td>Weaknesses-Opportunity Strategies</td>
</tr>
<tr>
<td>What actions will minimize the</td>
<td>What actions will minimize the</td>
</tr>
<tr>
<td>weaknesses involving the</td>
<td>weaknesses involving the</td>
</tr>
<tr>
<td>identified threats?</td>
<td>identified opportunities?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strengths (internal, positive)</th>
<th><strong>Quadrant III</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Strength-Threats Strategies</td>
<td>Strength-Opportunity Strategies</td>
</tr>
<tr>
<td>How can we utilize strengths to</td>
<td>What strengths can be used to</td>
</tr>
<tr>
<td>minimize identified threats?</td>
<td>maximize the identified opportunities?</td>
</tr>
</tbody>
</table>

From the TOWS analysis approach identified in Table 1, actionable strategies were identified from the threats, opportunities, strengths, and weaknesses specified in Figure 2. Actionable strategies from this TOWS analysis are outlined below.

**Weakness-Threats Strategies:** What actions will minimize the weaknesses involving the identified threats?

- Engage manufacturers of the emerging technologies or other tech companies to support research efforts to provide a more thorough understanding of its impact, if any, on reliability, security, availability, etc. of fire alarm systems to enable the adoption of change as new technologies emerge.

**Weaknesses-Opportunity Strategies:** What actions will minimize the weaknesses involving the identified opportunities?

- Be current and stay aware of emerging technologies to promote building and fire safety system integration, connectivity, and cost savings to the end users.

**Strength-Threats Strategies:** How can we utilize strengths to minimize identified threats?

- NFPA 72 has a 120 year history of which they have adapted to changes in the evolution of fire alarm communication technologies. Utilize the committee’s experience with adapting to changes and new technologies to mitigate the present threats.

**Strength-Opportunity Strategies:** What strengths can be used to maximize the identified opportunities?

- The robust and established process of the NFPA 72 technical committee can provide a thorough evaluation of new technologies to ensure reliability.
- Maximize the opportunities presented by the widespread installation of NFPA 72 fire alarm systems for technologies such as PoE.
- Create and dedicate a NFPA 72 task group to continually address emerging technologies, similar to the strategy implemented to develop the Class N pathway to enable the approved use of network technologies for fire alarm systems.

Figure 20: Annex A – PoE Fire Alarm Impact (Page 10 of 12)
5. Conclusion

Emerging technologies are having a significant impact on NFPA Codes and Standards. Power over Ethernet is a prime example of a technology that presents significant challenges to various codes such as NFPA 72, NEC, NFPA 3/4, NFPA 730/731, etc. with respect to reliability, safety, integration, security, etc.

This report summarizes an effort to address current status of emerging technologies such as PoE and building and life safety system integration as well as the research needs and perceived obstacles with respect to using PoE and other network technologies as a pathway for fire alarm communication. The purpose of this effort is to take an assessment of all influencing factors to clarify the current and future direction for the Fire Alarm Industry with respect to emerging technologies such as PoE.

A TOWS Analysis (threats, opportunities, weaknesses and strengths) was conducted to support consideration of the optimum strategic direction as the traditional methods of fire alarm communication are changing. Through this process, all the identified elements were collected, processed, and summarized.

This TOWS Analysis primarily focused on how to minimize the perceived threats that have evolved from various opportunities. The information from this TOWS Analysis is intended for analysis and use to establish implementable strategic plans. Based on a review of all the available information, the actionable strategies from this effort are the following:

**Actionable Strategies for Fire Alarm Industry**

- **Conduct Research on Emerging Technologies.** It is of critical importance to have a solid understanding of emerging technologies, how they work, and how they will influence current approaches. If internal research groups continually address these technologies, technical committees may be able to address these issues on a more frequent basis.

- **Leverage Strengths.** Leverage the strengths of NFPA 72’s history to take advantage of the opportunities to embrace new technologies and minimize the corresponding threats to safety.

- **Embrace Emerging Technologies.** Embrace emerging technologies and the development of reasonable solutions to allow implementation into the marketplace while maintaining reliability, survivability, and security of fire alarm systems. Designate a task group to continually address emerging technologies, their place in the market, and the feasibility of adopting the technology.

- **Focus on All Hazards.** Consider an all-hazards approach to ensure ability to maintain reliability and security of fire alarm communication in support of safety.
6. References


Moore, W. (2015). Tech Trio: Three changes to the new NFPA 72 will have a major impact on the design and installation of fire alarm and mass notification systems. *NFPA Journal*.


This is a summary of an additional session addressing Power over the Ethernet held at the 2018 C&E in Session T64. This was held on Tuesday, 12 June 2018; from 3:30 PM – 5:00 PM. The session involved the following speakers: Mark Earley, Ernie Gallo, Joel Goergen, Casey Grant, Mike Johnston, Chad Jones, and George Zimmerman.

The following describes this panel discussion session. NFPA 70, National Electrical Code, has been the cornerstone of the electrical industry for over 120 years. While the NEC Correlating Committee recognizes that the code has to be reactive to trends in the electrical industry, it also recognizes that, working together with the electrical industry, it can be proactive as well. The goal of the code is safe and sound growth of emerging areas. This panel presentation focused on the advantages of adopting the current edition, pointed to some of the new areas under consideration for the 2020 edition and beyond, and discussed the significant challenges created for owners, designers, installers, and enforcement where the latest edition is not adopted in a timely manner.
Figure 24: Annex B – Session T64 Presentations (Page 2 of 6)
PoE Summit
- Venue: Panel Discussions and Break-out Groups
- Focus: Structured around Summit Objectives
- Intent is to build on previous direction

PoE Summit Proceedings will be posted at: www.nfpa.org/poeresources

---

2018 NFPA Conference & Expo

Power Over Ethernet: A New Frontier... Into the Future
Presented by:
Joel Goergen
Distinguished Engineer
Cisco Systems, Inc.
Putting the Pieces in Place for the Future

---

Defining Class II Smart Power: PoE is Managed Power Control to 90W

- Power Controller
  - Manages the power system and maintain total power budget
  - Detects a valid load before starting
  - Provides short-circuit detection and power limiting
  - Allows the user on/off control
  - Continuously monitors power to loads
  - Automatically removes power when load is removed
  - Provides analytics

- Communications Link
  - Supplies communications between the two points
  - Determines communications and link integrity
  - “For BOTH power and communications
  - “Good” link means the cable and connections are reliable
  - “Not Good” link means NOT reliable to operate
  - Fast enough to react to changing conditions

---

Looking out 6 Years
Power + Communications = Great Marriage

---

Innovation... Makes the World Go Around

Technology Evolution
- Micro Processor
- Power eGaN FET
- Communication Protocol

Drivers
- Cost
- Access
- Reliability
- Convenience
- Safety

Users
- Managed Devices
- Analytics
- Saving Time

Easy to provide back-up Power from one location

---

Figure 25: Annex B – Session T64 Presentations (Page 3 of 6)
Always Safe Current

Direct Annex Technical Seminar
Annex T 7 2019

What is Always Safe Current (ASC)?
- This is the amperage that is low enough to ignore bundle size
- In practice, the only defined ASC is 300mA for 2A AWG
- It is possible to calculate ASC for other conductors using the ratio of resistance

How Do we Calculate ASC?
- Equate the power dissipation in each conductor of different AWG conductors
- Write this power in terms of current and resistance
- Solve for ASC

\[
F_1 = F_2
\]

\[
I_1^2 + R_1 = ASC^2 + R_2
\]

\[
ASC^2 = I_1^2 \frac{R_1}{R_2}
\]

Calculated ASC

<table>
<thead>
<tr>
<th>ASG</th>
<th>CHV/THM</th>
<th>ASC</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>0.0233</td>
<td>0.462</td>
</tr>
<tr>
<td>20</td>
<td>0.0294</td>
<td>0.536</td>
</tr>
<tr>
<td>20</td>
<td>0.0375</td>
<td>0.475</td>
</tr>
<tr>
<td>25</td>
<td>0.0868</td>
<td>0.120</td>
</tr>
<tr>
<td>20</td>
<td>0.0929</td>
<td>0.518</td>
</tr>
<tr>
<td>25</td>
<td>0.0948</td>
<td>0.537</td>
</tr>
<tr>
<td>25</td>
<td>0.1059</td>
<td>0.180</td>
</tr>
</tbody>
</table>

Simplifies Design and Inspection

<table>
<thead>
<tr>
<th>Cable</th>
<th>Length</th>
<th>PCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>117.9</td>
<td>117.9</td>
</tr>
<tr>
<td>29</td>
<td>102.8</td>
<td>102.8</td>
</tr>
<tr>
<td>20</td>
<td>92.4</td>
<td>92.4</td>
</tr>
<tr>
<td>31</td>
<td>81.7</td>
<td>81.7</td>
</tr>
<tr>
<td>22</td>
<td>71.5</td>
<td>71.5</td>
</tr>
<tr>
<td>23</td>
<td>63.6</td>
<td>63.6</td>
</tr>
<tr>
<td>24</td>
<td>56.4</td>
<td>56.4</td>
</tr>
</tbody>
</table>

Simplifies Design and Inspection

<table>
<thead>
<tr>
<th>Cable</th>
<th>Length</th>
<th>PCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>116.9</td>
<td>116.9</td>
</tr>
<tr>
<td>29</td>
<td>102.4</td>
<td>102.4</td>
</tr>
<tr>
<td>20</td>
<td>92.9</td>
<td>92.9</td>
</tr>
<tr>
<td>31</td>
<td>81.5</td>
<td>81.5</td>
</tr>
<tr>
<td>22</td>
<td>71.2</td>
<td>71.2</td>
</tr>
<tr>
<td>23</td>
<td>63.6</td>
<td>63.6</td>
</tr>
<tr>
<td>24</td>
<td>56.4</td>
<td>56.4</td>
</tr>
</tbody>
</table>

Figure 26: Annex B – Session T64 Presentations (Page 4 of 6)
Simple Design and Inspection

<table>
<thead>
<tr>
<th>IEEE Class</th>
<th>Cable Gauge</th>
<th>Bundle Size</th>
<th>Length (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>24</td>
<td>Unlimited</td>
<td>100</td>
</tr>
<tr>
<td>7</td>
<td>23</td>
<td>Unlimited</td>
<td>90</td>
</tr>
<tr>
<td>8</td>
<td>22</td>
<td>Unlimited</td>
<td>80</td>
</tr>
</tbody>
</table>

Length is average bundle length. For Class 5, this can be 100 m; longest as average is 100 m max.

Length Distribution of Installed Base

2018 NFPA Conference & Expo

PoE: The New Frontier: Diversification and dealing with it

Presented by:
George Zimmerman, Ph.D.
President & Principal
CME Consulting, Inc.

What exists today....

Every device you can imagine...

TODAY! – Living the dream....
Power + Communications = Great Marriage
How to tell one from another?

- Consumer choice creates chaos
  - “Democracy is the worst system except for all the others”
- Standards make a difference

This Drives Needs

- Forethought:
  - What will be out – both products and code - there in 6 years is already in development
- Simplicity:
  - Separate out the 90% we don’t have to worry about
- Training:
  - Easily recognize what is safe
- Smart code, allowing innovation:
  - Recognize intelligent safety is in devices, not in the walls
  - Recognize we can’t list everything one can imagine.
  - Focus code on identifying key features for safety, not specific technologies recognizing the features

One way: Ethernet Alliance PoE Logo

Certifying 802.3-based PoE

- Identifies interoperable PSEs, PDs
- Includes power class for PDs & PSEs
- First certifications announced Jan. 2018

Thank You

George Zimmerman,
CME Consulting, Inc.
george@cmephyconsulting.com

2018 NFPA Conference & Expo

CEUs: To receive CEUs for this session, scan your badge at the back of the room before leaving

Evaluation: Complete a session evaluation on the mobile app. (Search app store for ‘NFPA 2018 C&E’)

Handouts: Handouts will be available via the mobile app and at nfpa.org/conference

Recordings: Audio recordings of all sessions will be available free of charge via NFPA Xchange.