Toward an IoT Platform for Hazardous Locations

Examining the Collaboration of Humans and Edge Technologies in Disaster Scenarios for Insight into Industrial IoT for Extreme Operations

By: Thomas P.Ventulett, CEO
Aegex Technologies, LLC

www.aegex.com

Toward an IoT Platform for Hazardous Locations:

Examining the Collaboration of Humans and Edge Technologies in Disaster Scenarios for Insight into Industrial IoT for Extreme Operations

Background

As more and more industrial organizations are adopting Internet of Things (IoT) strategies and beginning their digital transformation to Industry 4.0 or Smart Manufacturing, they face challenges in adopting technologies due to regulatory restrictions for highly combustible atmospheres such as exist in some of the world's largest and most critical industries - oil & gas, chemical, pharmaceutical, energy, utilities, food processing, defense and others.

In such industries with combustible locations, on average, 15% of the personnel do not have access to mobile devices unless they are certified "intrinsically safe," or incapable of causing a spark that could ignite a volatile environment. Electronic devices must be tested and certified in accordance with standards for ATEX/IECEx Zone 1 or UL Class I Division 1. Thus, the human "sensor" in hazardous area operations, who could conceivably detect perceived anomalies or problems in the maintenance, workflow, process or function of these operations, is relegated to recording observations with pencil and paper and then entering data manually into ERP systems hours or days later. Such lack of real-time communication and data management results in inefficiency, increased costs and elevated safety and asset risk, causing potential down-time and even loss of life in extreme cases.

Where mobile devices are the first step in connecting operations, integrating those with IoT sensors, machine learning and artificial intelligence ("AI") as a unified solution can immensely impact the largest industries in the world.

By contrast, an effective and modern IoT platform operating in a hazardous location would vastly improve the efficiency and safety of operations further beyond the impact of enabling workforces with tablets. Where mobile devices are the first step in connecting operations, integrating those with IoT sensors, machine learning and artificial intelligence ("AI") as a unified solution can immensely impact the largest industries in the world.

However, the challenges of creating an appropriate design for the platform, prototyping it, securing the proper certifications, and conducting realistic field trials in actual hazardous locations prohibit iterative processes that are necessary for innovation, leaving the industry stuck with methods and technologies from the past.

The Problem

Product development cycles for intrinsically safe devices can take months if not years, including the duration for necessary certifications. Additionally, field trials are virtually impossible since testing in a volatile location such as a chemical plan or refinery is not a viable option. Lastly, the cost of designing, developing, and certifying an intrinsically safe device can be $250,000 or more. And, to cover the broad needs of so many industries, thousands of variations may be needed for pervasive data capture, all of which can amount to hundreds of millions of dollars in capital investment.

Therefore, given the significant capital investment and inability to conduct iterative field trials, innovation is stifled. Significant advances in technology and the benefits they yield leave the economy's most significant industries isolated from their advantages.

Hypothesis

If trials could be conducted that enabled testing of IoT concepts and equipment in live volatile or disaster scenarios, effective solutions would emerge, and proof-of-concept trials could be completed prior to product commercialization, with significant cost and time savings.

Pre-Testing Assumptions and Design Criteria

Given the complexities of operating in diverse environments, basic requirements need to be addressed for an "IoT for Hazardous Locations":

- "Single-design" device to resolve massive capital investment required for variations
- Broad range of operating climates from -40°C to +60°C
- Flexibility in communications
- Ease and cost of installation (install while in the presence of volatile conditions)
- Ability to support third-party legacy sensors

With these general assumptions, the following additional factors must also be considered:

- Sensors: Sensors of various types - ambient, base-line, wearable – should be easy to rapidly deploy throughout large and complex "meta-scale" facilities where hazardous explosive conditions exist. Sensor architecture should be highly customizable for diversity of environments and situations.
- Communications: From extremely remote locations to complex radio frequency environments such as refineries, communications must be wireless and low power with sufficient bandwidth and broadcast range.
- System Architectures: Options for data aggregation, analytics and distribution must be considered influences in the system architecture. Functional tests require an assessment of the five architectures defined by Gartner Inc. as follows: [1]
    - Thing-Centric Architecture - machines/things are "smart" on their own and store their own data; only communicate with Internet for coordination;

---

1 Build Your Blueprint for the Internet of Things, Based on Five Architecture Styles
Refreshed: 12 May 2016 | **Published:** 24 September 2014 **ID:** G00269736; **Analyst(s):** *Hung LeHong;* © 2014 Gartner, Inc.

- Gateway-Centric Architecture - gateway houses application logic, stores data and communicates with Internet for things that are connected to it; things do not have to be as smart;
- Smartphone-Centric Architecture - a mobile device houses application logic, stores data and communicates with Internet for things that are connected to it; things do not have to be as smart;
- Cloud-Centric Architecture - cloud acts as connection hub, performs analytics and stores data; things do not have to be as smart;
- Enterprise-Centric Architecture - things are behind firewall and located together; little need for external Internet

- Security: All data managed must be protected with the highest possible security protocols for critical operations, such as oil and gas production, chemical manufacturing, and other highly sensitive industrial processes.

A new style of IoT platform built especially for hazardous area operations would need to include various and affordable types of sensors to cover vast spaces, real-time communications, cloud computing, machine learning, rights management, security, big data storage, analytics and user-friendly visualization, all functioning in highly explosive conditions.

By deploying new IoT technologies that allow people to use technology inside Zone 1/Division 1 hazardous areas, humans can actively interact with machines in real time to dramatically improve productivity, safety and the bottom line in hazardous operations.

Meta-Scale Test Platform

Taking into consideration the design criteria stated above makes modeling a "meta-scale" IoT solution for extremely large and complex hazardous location environments difficult at best. HazLoc areas such as refineries, chemical or pharmaceutical plants, and urban environments are all meta-scale locations that can cover multiple square kilometers and, therefore, require a unique approach not previously proven.


Figure 1 - Guardian Centers Main Campus

To emulate true operating environments, Aegex selected a test facility designed for disaster preparedness and training at The Guardian Centers [Figure 1] south of Atlanta in the USA. The facility covers 3 square kilometers with more than 100 buildings, 1-kilometer tunnel, fuel storage and pumping facilities, and a power sub-station, all established to legally allow the release of volatile and toxic gases for testing and training.

The Experiment

In order to test the above hypothesis, Aegex Technologies, developer of intrinsically safe tablets and IoT sensors, joined forces with Verizon Enterprise Solutions and Nokia to conduct a 3-day test and conference during which various new technologies would be demonstrated in staged disaster scenarios at The Guardian Centers emergency response training facility.

Case Study: Operation Convergent Response (OCR) 2017

In June 2017, Verizon, Nokia and Aegex co-hosted the single largest live demonstration of technologies for first responders, the U.S. Department of Homeland Security, and the U.S. Department of Defense: Operation Convergent Response (#OCR2017). IoT sensors, real-time encrypted data streaming, wearables, tablets, drones and robotics communicating over LoRa, Wi-Fi, Bluetooth, LTE and SatComm were tested during a series of five catastrophic live disaster scenarios.

Hands-on research was conducted by Aegex Technologies, Verizon, Nokia and multiple technology partners that tested various edge technologies with first responders in realistic disaster scenarios during the event. OCR2017 provided a unique opportunity to test IoT under extreme conditions, such as a staged chemical plant explosion, subway incident, neighborhood flood, cybersecurity attack, tornado disaster and hostage rescue. The results gave insight into the need for continued collaboration on IoT capabilities that can better manage not only emergency response, but everyday operations in hazardous industries. To learn more visit: http://aegex.com/ocr-2017/

Use Case #1 – Hazardous Area Secure Computing and Sensing

- Setting
    - Accidents, natural disasters, or terrorist attacks
- Goals and Objectives
    - Test live video from tablets in operational hazardous conditions with AES 256 encryption without latency or consumption of power to preserve battery life over multiple wireless systems.
    - Connect end-to-end devices (tablets to tablets or tablets to control rooms)
    - Improve efficiencies, safety, collaboration, and situational awareness

Figure 2 - aegex10 Intrinsically Safe Windows Tablet

- Challenges
    - Any location where there is the potential for hazardous combustible atmosphere **requires** highly specialized, purpose built electronic equipment to meet UL Class 1 | Division 1 (C1D1) or ATEX/IECEx Zone 1 certifications
    - How to secure, collect and share sensitive data, including operations, maintenance, workflow, personal health and other mission-critical data

Solution #1

Several encryption methods were tested, and a final solution proved to meet all test criteria. Integrating FHOOSH software enabled devices to communicate end-to-end, securing data in transit and at rest without latency or power drain. See Figure 3. In one trial, the aegex10 tablet streamed continual video over wi-fi for 6 hours 59 minutes without FHOOSH and 6 hours 57 with FHOOSH.

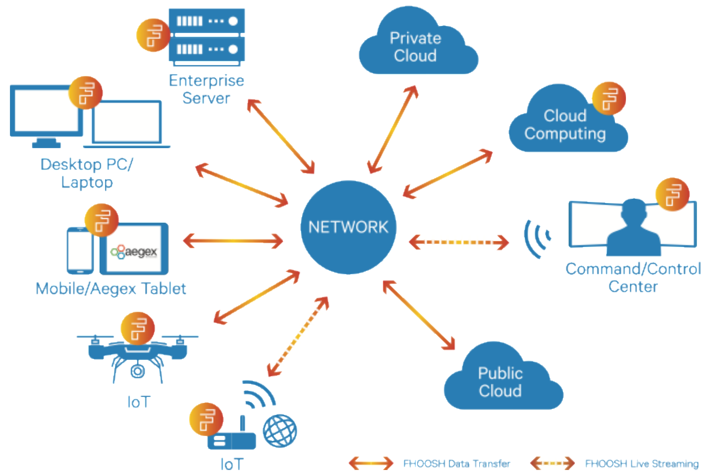

Figure 3 - Aegex + Fhoosh Architecture

Use Case #2 - Chemical Leak Detection

- Setting
  - Chemical plant explosion and building collapse as seen in Figure 4
- Goals and Objectives
  - Test sensors, networks and AI systems for integrity and reliability
  - Identify leading indicators within data collected to avert disaster
  - Improve situational awareness following a disaster to improve safety and effectiveness of response.
- Challenges
  - Although the vast area tested was not designated as a hazardous area, following the release of volatile gases including methane, broader areas became explosive and, therefore, tablets and sensors had to be intrinsically safe to not be a source of ignition.
  - Power for sensors did not exist, so long-life battery-based solution was required.
  - Wi-Fi and LTE systems were impaired due to the disaster, and redundancy of alternate communications was necessary.

Figure 4 - Chemical Plant Explosion and Collapse

To test various system architectures, sensors were connected via LoRa to an Aegex Gateway that backhauled via Wi-Fi, as well as sensors that communicated via LTE to Verizon. Data from these sensors was collected by SensorInsight's Integrate, a middleware platform that can be hosted in a Microsoft Azure or IBM Watson environment.

Figure 5 - Aegex LoRa - Wi-Fi Gateway

The data was fed to Simularity's Artificial Intelligence (AI) for anomaly detection. The sensor readings and anomaly scores were displayed on SensorInsight's application dashboard and viewed by first responders on Aegex's intrinsically safe tablets.

This complete end-to-end solution would enable industrial facility owners to spot and deal with small leaks before they become big problems, avoiding costly and dangerous situations.

Testing the Solution

For the chemical plant scenario at OCR2017, real-time anomaly alerts about the leak could have been noticed by building management when it first happened, before deadly amounts of the chemicals built up and led to the collapse of the building. However, in this exercise, we also demonstrated the use of this complete end-to-end hazardous area solution for managing disasters that were *not* prevented.

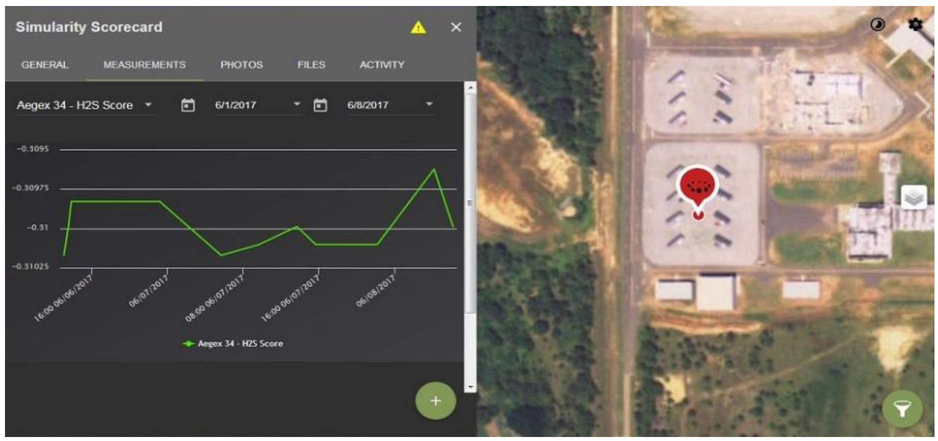

Figure 6 - SensorInsight's dashboard shows the anomalous readings for hydrogen sulfide and

In this case, a hydrogen sulfide leak was detected. When this happens, the space should be ventilated. If the gas cannot be removed, first responders need to use appropriate respiratory protection and any other necessary personal protective equipment (PPE), rescue equipment and communication equipment. Atmospheres containing high concentrations (greater than 100 ppm) are considered immediately dangerous to life and health (IDLH), and a self-contained breathing apparatus (SCBA) is required. In such a case, with dangerous flammable gases, only intrinsically safe electronics, which are incapable of producing enough heat or energy to cause a spark, should be used.

As the disaster unfolded, first responders were able to monitor the levels of chemical hazard using the Aegex tablets. This helped them properly prepare for and locate the source of the toxic leak.

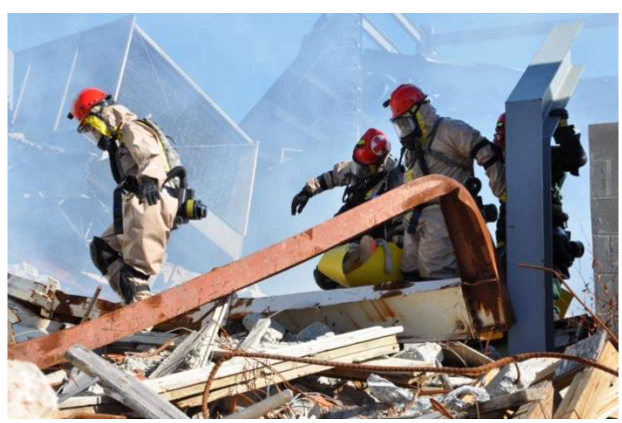

Figure 7 - First Responders Training During OCR Field Testing

Lessons Learned

- ✓ Sensors must be extremely low-cost and quick/easy to install.
- ✓ Sensors may be deployed to a broad range of operating environments, thereby requiring uniform certifications but the ability for field customization for pervasive system learning.
- ✓ Some of the unlicensed spectrum solutions suffer significant bandwidth limitations. They can be suitable in some but not all circumstances.
- ✓ Cloud vs. Edge AI may adversely impact response time but paints a broader picture and more impactful learning.
- ✓ Whether monitoring a gas leak, predicting a component fail, or modeling an urban disaster, a clear and simple strategy can enable efficiency and safety within days.

Conclusion

An Internet of Things for Hazardous Locations must consider the special conditions that govern machine learning in highly volatile industrial operations. It must also include specific components that are purpose-built for hazardous environments in order to capture and utilize big data coming out of these operations.

By connecting people, machines and processes to the cloud in the world's most explosive hazardous locations, Aegex Technologies' IoT Platform can help transform the way hazardous industries operate, thus improving productivity and safety.

APPENDIX A

IoT PLATFORM COMPONENTS

Field trials were conducted based on a typical IoT infrastructure stack[2]. Key components included data capture devices, wireless infrastructure, cloud computing, AI and actionable delivery to users. Figure 2 summarizes each of these components, and they are further defined in Figure 9 below:

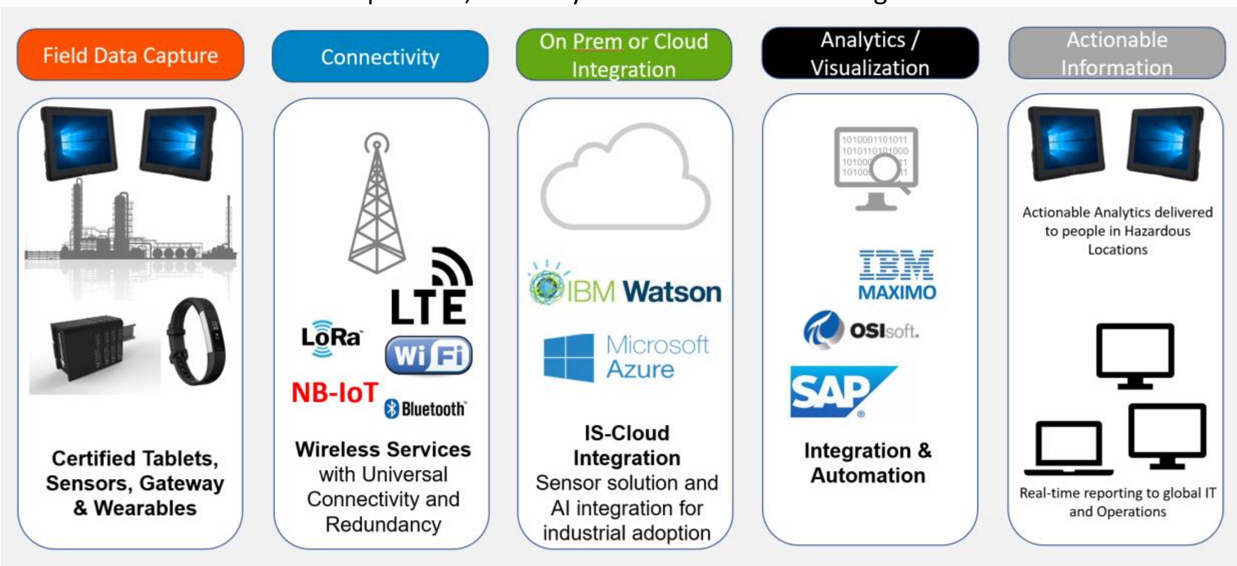

Figure 8 – Industrial IoT System Architecture

1. *Field Data Capture devices*
   a. *Aegex10 Intrinsically Safe Tablet*

The first step in connecting everything in a hazardous environment is to connect people to the cloud. To do this, Aegex developed the aegex10™ Intrinsically Safe Tablet, a Windows 10 tablet that can be used in the most explosive (UL Class I, II, III Division 1 and ATEX/IECEx Zone 1) industrial environments in oil and gas, chemical and other industries' hazardous locations. With the fundamental requirement of connecting people for any eventuality, mobile should be certified for the worst conditions, because at the time of a disaster, information is critical. It is not the time to leave a device behind.

> With the fundamental requirement of connecting people for any eventuality, mobile should to be certified for the worst conditions, because in the time of a disaster information is critical. It is not the time to leave a device behind.

Additionally, the tablet connects Bluetooth data-capture sensors, biometric wearables and other peripherals that have been designed safe for use in hazardous locations utilizing Aegex patented intellectual property. These peripherals connected to the aegex10™ also mimic a gateway architecture by enabling low-power devices to backhaul data via multiple radios.

   b. *Intrinsically Safe IoT Sensor*

[2] The system architecture for testing has been addressed in a previous paper published by Aegex Technologies and can be found here.

Simply plugging in a gas sensor or anemometer is not feasible in a hazardous area or large cityscape. Power outlets do not exist in hazardous locations because of the risk of spark in combustible atmospheres; therefore, only devices with the right certifications can be used.

Given the variety of hazardous environments (unlimited numbers of compounds, dusts, particulates, fibers, etc.) that can exist across industries and even within single facilities, flexibility and customer-specific customization is necessary. Therefore, each device deployed must support some array of the sensors identified in Figure 10. Due to the complexity of certifying and manufacturing every eventuality, the devices should be field-modifiable to meet specific onsite requirements.

To achieve a viable IoT Platform for Hazardous Locations, Aegex has applied its patented intellectual property developed for the aegex10™ IS Tablet to the following array of devices, with the ability to mix and match types of specific sensors, types of devices, radio options and power options to create a sufficient base platform to inexpensively deploy all five Gartner IoT Architectures in a remote location or meta-scale complex.

Temperature
Wind direction
Wind Speed
Rain Guage
Gases (Benzene)
Gases (Butane)
Gases (Oxygen)
Gases (CO2)
Gases (CO)
Gases (CH4)
Gases (Ethanol)
Gases (LPG)
Gases (Hexane)
Gases (Smoke)
Gases (H2)
Gases (Ammonia)
Gas (Ozone)
Gas (Hydrogen Sulfide)
Gas (Phosphine)
Light Intensity
Nuclear Radiation
Laser and Trip sensor
Sound Intensity
Liquid pipe Pressure
Fire/Flash
Proximity (very short Distance s
Humidity
Air Pressure
Air Quality (Dust)

Figure 9 - Sensor Options

2. Communications Layer

Just as with every aspect of a complex IoT architecture, there are a multitude of options for the air interface or method of communications to and from remote sensing devices. Testing each standard for signal strength in diverse environments, requirements for bandwidth, power consumption and security proved to be key challenges. In a final assessment, the following radios were tested in various operating environments to determine the most universal viability:

- LoRa
- Wi-Fi
- Bluetooth (Low Energy – BLE)
- LTE
- Cat M LTE
- NB – LTE

Each of the above had advantages and disadvantages, and ultimate system integration, existing infrastructure and speed to market will drive the outcome that businesses will deploy.

3. Cloud Solutions

Capturing information and communicating it to a cloud instance is at the heart of a successful IoT deployment. Consideration of cloud solutions is driven by numerous variables. Providing a software as a service ("SaaS") solution to global enterprises is generally unreasonable. Global enterprises have vast legacy systems that must be considered, and true analytics are successful when all information can be assessed in a holistic fashion. Therefore, sensors should report to global cloud infrastructures where the customer "owns" the data. Enabling devices to report to the primary cloud providers such as Microsoft Azure or IBM Watson meets these criteria.

4. Artificial Intelligence & Analytics in a Meta-Scale Project

Outside of the scope of assessing AI and analytics platforms, it should be noted that sensor design and system architecture does not impact efficiency and safety in hazardous locations without making the information actionable. In a typical offshore oil rig with 30,000 sensors for capturing data, only 1% of that captured data is being turned to actionable information used to make decisions. This same percentage holds true for other industries as well.[3] It is an exercise in futility to capture billions of data points and then fail to turn them into a usable form that would allow field workers to make necessary, if not life-saving, adjustments.

5. Delivery and Actionable Information

The fundamental objective of a meta-scale IoT solution for hazardous locations is to drive productivity, efficiency and safety in operations. Therefore, visualization of information that is distributed to users or, ultimately, things operating autonomously from human intervention are the end goals. Understanding these goals enables organizations to start "at the beginning" by connecting people and things and, ultimately, organizations[4].

---

[3] "The Right Moment for Analytics," by Pallav Jain, Gloria Macias-Lizaso and Guido Frisiani, McKinsey & Company 2016

[4] "Connecting Manufacturing IoT to Complete the Enterprise Data Cycle," by Thomas P. Ventulett, Aegex Technologies 2016