Building an IoT Platform for Hazardous Locations

Manuscript to accompany ADIPEC 2018 Presentation,
“Enabling the Best by Preparing for the Worst:
Lessons from Disaster Response for Industrial IoT in Oil and Gas"

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

www.aegex.com

Toward an IoT Platform for Hazardous Locations: Lessons from Disaster Response for Industrial IoT in Oil and Gas

I. 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, certain industries are precluded from taking this significant path forward. Specifically, in some of the world's largest and most critical industries such as oil & gas, chemical, pharmaceutical, energy, utilities, food processing, public safety, defense and others, regulatory restrictions for highly combustible atmospheres restrict the use of commercial electronic devices.

In industries with combustible locations, on average, 15% of the total global workforce does not have regular access to modern mobility and field force information. In order to bring these industries to an IoT revolution, mobile devices, networks and sensors must be 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 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 positively impact oil and gas operations.

By contrast, an effective and modern IoT platform operating in a hazardous location would vastly improve the productivity, 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 positively impact the largest industries in the world, such as oil and gas operations.

However, the challenges of creating an appropriate design for the platform, prototyping it, securing the proper certifications, and conducting 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.

II. 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 prototype testing in large scale volatile location such as a chemical plant or refinery is not a viable option. Lastly, the cost of designing, developing and certifying an intrinsically safe device can be USD$250,000 or more. And, to cover the broad needs of so many industries, thousands of variations are required for pervasive data capture, all of which can amount to hundreds of millions of dollars in capital investment.

Therefore, a practical goal is to establish a method that accelerates development, testing, validation and verification of new technologies that break the trend of relying on decades-old design, communications and security, in order to drive innovation that positively impacts productivity, efficiency and safety in the global economy's largest industries.

III. Hypothesis

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

IV. Pre-Testing Assumptions and Design Criteria

Given the complexities of operating in diverse volatile environments, certain requirements need to be addressed for an "IoT for Hazardous Locations." These Assumptions are defined as follows:

1. To address the Problem and avoid highly bespoke solutions, tests must achieve economies of scale, and, therefore, meet needs across a wide range of industries and their operating environments. Test scenarios should emulate conditions found across operating environments in these markets:
    - Oil and Natural Gas - Offshore/Onshore, Midstream, Downstream
    - Chemicals
    - Pharmaceuticals
    - Public Safety
    - Defense
    - Plastics and Rubber Products
    - Textile Mills and Product Mills
    - CPG, Dry food/goods production
    - CPG, Distilleries
    - Printing and related products
    - Paint and industrial coatings
    - Utilities
    - Aerospace
2. A "single-design" sensor solution is required to ensure homogenized testing and certification processes and enable unique, highly localized configurations.
3. A broad range of operating climates must be tested, accounting for:
    - Intrinsically Safe standards in accordance with ATEX/IECEx Zone 1 or Zone 0, UL 913 5th and/or 8th Edition Class 1 Division 1/Zone 1 and select country specific standards
    - High and low humidity
    - salt air, salt spray
    - IP67 or greater device ruggedness requirement
    - - 40°C to + 60°C operating range
    - Extended-life battery (2+ years) requirements
    - Low-cost replacement of sensors (no calibration)
    - Equipment that is highly resistant to corrosion and chemical degradation
4. Variable communication protocol options must exist.
5. Use and/or installation of equipment must be possible in the presence of volatile conditions.
6. The ability to integrate third-party legacy sensors and solutions must exist.

V. Test Platform Components

To test the Hypothesis, the test platform should include the following major components:

1. **Mobility to Connect Personnel:** Digital transformation of businesses began 40 years ago with the introduction of the desktop personal computer. As other industries moved through LAN's, WLAN's, and cloud computing, hazardous environments remained relegated to fixed HMI terminals developed decades ago. The first step in trials should be to deploy Intrinsically Safe tablets to all test participants to capture and distribute data to personnel operating in a hazardous location ("HazLoc"). Volatile gas leaks can occur without warning, and in a disaster scenario, they can create a large-scale catastrophe.

Figure 1 - aegex10 Intrinsically Safe Tablet

   The test plan, therefore, should include mobile devices that comply with the following criteria:

   - Certified intrinsically safe and comply with all criteria defined in Section IV. The only product to achieve this requirement is aegex10™ Intrinsically Safe Tablet for field force deployment in any environment at any time.

   IMPORTANT NOTE ON DEVICES EXCLUDED:

   - Commercial mobile devices that are not designed as intrinsically safe, meaning their safety is based on after-market cases, *do not meet* the criteria since, (a) there is only one (1) point of failure for safety protection that relies solely on the integrity of a third-party-provided external case and; (b) commercial products not designed as intrinsically safe typically have stored capacitance of energy of five (5) to ten (10) times the energy required to ignite hydrogen.
   - Portable gas detectors that alert users to cease the use of non-certified products *do not meet* the criteria since, (a) there is only one (1) point of failure as a form of safety protection when relying solely on the performance of the gas sensor, and (b) in a disaster scenario, relying on users to save their work and shut down mobile devices in the presence of a volatile gas creates new risk factors.

2. **Configurable Sensors:** Sensors of various types that monitor ambient and anomaly conditions are highly specific to a given use case. In a disaster scenario or unique operating condition, sensing devices must be field-configurable to meet local condition requirements.

   In hazardous locations, IoT sensors are to be utilized to monitor the presence of toxic or volatile gases, ambient environmental conditions, and equipment operating condition. All variants must be highly customizable for a diversity of environments and monitoring objectives, while configured in a volatile location.

Just as with the Periodic Table, individual sensing devices should be able to be combined with any other sensors to create custom configurations and highly contextualized analytics. Figure 2 demonstrates typical configuration options of hazardous area sensors.

Endpoint							Battery
Oxygen O2	Hexane C6H14	Butane C4H10			Enviro Light	Enviro Temp	Wi-Fi
Carbon Dioxide C02	Hydrogen H2	Gas LPG	Proximity	Laser (Pipe Alignment)	Enviro Barometer	Enviro Humidity	4G NB-LTE
Carbon Monoxide CO	Ammonia NH3	Ethanol C2H6O	Smoke	Laser (Gas Detection)	Wind direction	GPS/ Shock	Bluetooth
Methane CH4	Ozone 03	Phosphine H3P	Dust	Pipe Pressure	Wind Speed	Light Intensity	Li-Fi
Nitrogen Dioxide NO2	Hydrogen Sulfide H2S	Wild Card	Radiation	Fire/Flash	Rain Gauge	Sound Intensity	NFC
Sulphur Dioxide SO2	Hydrocarbons	Vibration 1M	Vibration 3M	Pipe Sonar	DC Power Input	AC Power Input	LoRa

Figure 2 - Table of Sensor Configuration Options

3. **<u>Meta-Scale Operations:</u>** Hazardous operating environments tend to exist in very large-scale locations where micro-climates can form and may alter air-flow, which can impact chemical plume dispersal, corrosion or even sensor calibration. Integrating data management and machine learning into these large and complex operations is considered "Meta-Scale IoT." Meta-Scale HazLoc areas such as refineries, chemical or pharmaceutical plants, and urban/Smart City environments are typically not available to test the stated Hypothesis because they are either currently in operation, or they contain volatile atmospheres that are too potentially dangerous in which to test.

   For the following test case, we selected a test facility designed for disaster training at The Guardian Centers (Figure 1) near Atlanta, Georgia, in the United States, where we could closely emulate true operating environments. The facility covers 3 square kilometers with more than 100 buildings, a 1-kilometer tunnel, fuel storage and pumping facilities, and a power sub-station, all constructed to legally allow the release of volatile and toxic gases for first responder and disaster scenario training.

Figure 3 - Meta-Scale Test Location

4. **<u>Communications</u>:** IoT solutions must accommodate a diversity of locations, from very remote, to complex and dense environments, such as refineries. Mobile devices must support a variety of wireless standards, from near-field to wide area, and be configurable to operate in low-power and adverse morphologies. To ensure

pervasive communications, all devices must support one or more of the following air interface standards:

- 4G LTE (over 20 bands of support)
- 4G NB-LTE / Cat M LTE (over 20 bands of support)
- Wi-Fi
- Bluetooth
- NFC
- LoRa
- Satellite communications / Remote back-haul
- Li-Fi (these include commercial solutions, private networks and Li-Fi[1]).

5. **Interoperability:** Field service devices such as tablets, remote monitoring and sensing devices, application integration and communications standards must integrate across legacy systems while achieving the test criteria and assumptions defined in this test.

   To achieve this, the IoT sensors must support physical or wireless connectivity to legacy equipment, which, in the following experiment, was achieved by use of a "Wild Card" sensor node and, further, drones, robots, wearables and other devices all worked from common API's to achieve information interoperability on a common cloud. Microsoft Azure with AI provided by IBM Watson were selected.

6. **System Architectures[2]:** 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:

   - Thing-Centric Architecture - machines/things are "smart" on their own and store their own data; only communicate with the Internet for coordination;
   - Gateway-Centric Architecture - gateway houses application logic, stores data and communicates with the 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 the 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

[1] Li-Fi provided by pureLi-Fi of Edinburgh, Scotland

[2] 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.

7. **Security:** All data managed must be protected with the highest possible security protocols for critical operations, required by US Military and US Department of Homeland Security, and compliant with International Transfer Arms Restrictions ("ITAR") to be utilized in private sector oil and gas production, chemical manufacturing, and other highly sensitive industrial processes. This typically requires AES 128 or AES 256 Encryption, or other like standards or methods, including but not limited to Blockchain IoT solutions.
8. **Artificial Intelligence & Analytics in a Meta-Scale Project:** Sensor design and system architecture do not impact efficiency and safety in hazardous locations without first making 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. Analytics and AI are necessary to turn big data into information that is usable.

In summary, a Test Platform for 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, interoperability, machine learning, system architecture, and security, all functioning in unpredictable conditions.

VI. The Experiment

In order to test the above hypothesis, Aegex Technologies, developer of intrinsically safe tablets and IoT sensors, collaborated 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. These staged scenarios represented a "worst-case scenario" to challenge the technologies in real-world situations to assess their performance against the test criteria.

Applying a worst-case catastrophe scenario approach ensures that when personnel, assets and communities are at risk, ease of deployment, interoperability and performance would exceed "normal" operating conditions.

Case Study: Operation Convergent Response (OCR) 2017

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

In June 2017, Verizon, Nokia and Aegex hosted a live demonstration of technologies for first responders, the U.S. Department of Homeland Security, the U.S. Department of Defense and representatives from Oil and Gas, Chemical, Coatings, Aerospace and Insurance/Risk Management industries: Operation Convergent Response (#OCR2017). To test the Hypothesis utilizing disaster scenarios at meta-scale, the following crisis situations were created:

Test Scenario #1: Neighborhood Flood

37 million liters of water flooded six city blocks at 2 meters deep

Test Scenario #2: Chemical Plant Explosion

Realistic chemical plant explosion and 3-story building collapse

Test Scenario #3: Subway Terrorist Attack

Terrorist attack/explosion in 0.5 km subway tunnel

Notes on Infrastructure for the Tests Conducted

To test various system architectures, Aegex IoT sensors were connected via LoRa to an Aegex Gateway that backhauled via a portable Wi-Fi supplied by KLAS Telecom, as well as IoT sensors that communicated via Wi-Fi to Verizon Wireless LTE Network. Both networks were also backhauled via satellite communications to test latency and provide back-up redundancy. All sensor data was distributed and presented by the VCORE fourDscape platform in command and control and on Aegex Intrinsically Safe Tablets in the field. All data was hosted in a Microsoft Azure or IBM Watson environment.

A. Test Scenario #1: Neighborhood Flood

1. Scenario Background

A hurricane approaches a city, but complacent residents and business owners fail to take necessary precautionary measures. The hurricane strikes the city, and water rises 2 meters, trapping victims and damaging utility and communications infrastructure. Submersed hazards are in the water, impeding the rescue. Victims (actors) create distractions while demanding rescue, which puts first responders further at risk.

Figure 4 - Scene from Flood Test Scenario #1

2. Test Plan and Objectives

To test the Hypothesis, numerous technologies were assessed that met the Hypothesis Test Criteria. The objective of this test was to create a common disaster scenario, where new technologies could attempt to avert a larger negative impact on a community. This test aimed to identify solutions and technologies that could significantly improve rescue and recovery efforts, while "unplanned complications" were being introduced. This test enabled organizers to test iterative generations of products and solutions during a multi-day scenario to identify how various solutions can impact a crisis scenario and, thereby, speed product development to achieve daily operational improvements.

Objectives:

- Identify and test technologies that would have mitigated the risk of trapped victims prior to the hurricane
- Identify and test technologies that provided a "forward view" of locations for first responders looking for victims or hazards
- Identify and test technologies that would enable a rapidly deployable solution to a damaged communication system
- Identify and test methods of aggregating information to a common operating environment across public and private information silos.

Figure 5 - Drone monitored by aegex10 Tablet managing victim relief

3. Scenario Results

Network connectivity proved to be a critical priority in response and recovery. Loss of communications among members of a mobile response team, plus the inability to communicate with stranded victims and real-time sensing systems, highlighted the need for a rapidly deployable network. Redundancy of radios in devices provided flexibility in this approach, and therefore, many risks could be mitigated.

Battery-powered mobile devices and sensors proved to be critical in maintaining a continual flow of information. Sensors performed as anticipated, shutting down certain power grid components that would have sustained greater damage if electrified and would have created greater hazards for first responders. Further, advance notification through cloud distribution of information enabled a chemical plant operator to begin an early shutdown process, preventing facility operations from heating beyond safe limits and resulting in a fire, as happened following Hurricane Harvey at the Arkema Plant in Texas.[4]

4. Findings and Lessons Learned

The scenario was designed to use the obvious impact of a flood to assess technologies designed for hazardous duty, which do not often co-exist. The stress on infrastructure helped highlight challenges and enabled a fast and iterative process of improvement, where a robust product solution emerged.

Figure 6 - Drone and Elevated Wireless Network

- ✓ First responders had not prepared for the chemical plant element of the rescue. Having the appropriate certified tablets from Aegex ensured their use of maps, overhead view from drones, and sensor feeds, enabling responders to move to areas where un-approved devices would have been prohibited.
- ✓ Deployment of Aegex battery-powered and wireless IoT sensors detected the presence of water and water level, which provided advance alerts to the chemical company operator. LAN and AC powered sensors failed the tests. Had chemicals escaped, the sensors provided redundant advance warning, protecting the first responders in case the situation further deteriorated.
- ✓ Drones delivering a video feed with 30x zoom cameras to IP67 aegex10 tablets could identify the location of possible stranded victims, directing first responders and improving response.
- ✓ A deployed aerostat balloon provided by Nokia lifted a 4G LTE private network over the disaster scene, instantly enabling secure broadband communications.
- ✓ Aggregating all information into Azure enabled numerous parties to collect and securely distribute information in real-time. Assembling all data in Azure enabled intelligent alerts such as intrinsically safe flood sensors equipped with chemical sensors to assist in rescue and recovery.

B. Test Scenario #2: Chemical Plant Explosion

[4] https://www.theatlantic.com/science/archive/2017/08/harvey-flooding-explosion-petrochemicals/538560/

1. Scenario Background

Sensors are deployed at a chemical processing facility with a plan for a full IoT deployment. Data is captured that detects anomalies in pipe and flange vibration and temperature variations. A digital "fingerprint" in the dataset suggests a pending leak but goes un-attended. A tornado is reported in the area, and high winds hit the already-comprised facility. Anomaly alerts show hydrocarbon vapors are detected, and an explosion occurs, collapsing the building, trapping victims and impacting the neighboring community. 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 for first responders. In such a case with dangerous flammable gases present, only intrinsically safe electronics are suitable.

Figure 7 – View of Chemical Plant Explosion Test Scenario underway.

2. Test Plan and Objectives

To test the Hypothesis, numerous technologies were assessed that met the Hypothesis Test Criteria. This test objective was to create a worst-case scenario for failure to monitor and act on AI-derived information in real time. The test attempted to identify certain technologies and solutions that detect a pending disaster and discover how such technologies can be leveraged to aid in rescue and recovery. This test enabled organizers to test iterative generations of products and solutions during a multi-day scenario to identify how various solutions can impact a crisis and, thereby, speed product development to achieve daily operational improvements.

Objectives:

- Identify and test technologies that provide warning of an impending disaster.
- Identify and test technologies that enable first responders to source information, aiding in rescue and recovery, including identification of evacuation zones.
- Identify and test methods of aggregating information to a common operating environment across public and private information silos.

3. Scenario Results

Figure 8 – IoT could have averted the disaster, and used here by First Responders on site, to aid in Search and Rescue

A chemical company's IT department had moved to a full IoT deployment of connected workers and operations, overlaying new intrinsically safe sensing devices rather than relying solely on legacy sensors and manual rounds management. The Operations and Maintenance team elected to continue a "business-as-usual" approach. Workers recorded rounds on paper forms, processed paper hot work permits, and updated systems at the end of shifts. Large areas of fail-points were not monitored by legacy explosion-proof sensors, and rounds could not be digitally validated with real-time location and time stamp of tasks. New intrinsically safe sensors could be configured to monitor broad ranges of inputs and demonstrate the ability to predict a pending leak. With artificial intelligence (AI), the disaster could have been averted, though sensor data was dismissed due to a failure to understand the value of the data captured.

4. Findings and Lessons Learned

The scenario was designed to study how connected workers, combined with low-cost and highly configurable sensors, could augment current business processes and improve operational efficiency and safety. Test partner Verizon selected prototype sensor endpoints and nodes developed by Aegex that were field-fitted for the given use case. The crisis resulting from failure to heed the advance warnings of these digital solutions highlighted the significant impact such technologies could have had. Further, providing Aegex intrinsically safe tablets and sensors to first responders enhanced search and rescue ("SAR") efforts and empowered users to access information on the scene, protecting SAR teams from secondary explosions and accelerating response.

Figure 9 - First Generation Aegex Intrinsically Safe Configurable IoT Sensors

- ✓ A single or dual gas sensor in an explosion-proof housing requires significant time and expense to install and integrate into process control systems. Costs can exceed USD$25,000 for a single piece of equipment and installation. Battery-powered and wireless intrinsically safe sensors that can capture up to 36 simultaneous and independent inputs enable far greater insights and artificial intelligence.
- ✓ Moving personnel to digital rounds management demonstrated a 30% reduction in duplication of effort and lost productivity, driving greater "time on tools."

- ✓ By monitoring users' locations, either with GPS in the aegex10 Intrinsically Safe Tablets or by using the embedded NFC reader as a method to track actions on rounds, all tasks could be verified in real time. Time spent on tasks such as loop checks on OSI PI Vision could be reduced by 66%.
- ✓ Drones delivering a video feed with 30x zoom cameras to aegex10 Intrinsically Safe Tablets provided an overhead view of the scene, spotting possible threats of a further collapse. Additionally, thermal imaging enabled a real-time mapping of the scene to ensure fire crews could focus their response.

Figure 10 - Command and Control from an aegex10 Tablet on site

- ✓ The resulting sensor data was visualized on VCORE Solutions' fourDscape software. fourDscape is a scalable IoT solution comprised of sensor integration, best-in-class visualization and secure SDP communication technology, adaptable to provide security, surveillance and asset optimization solutions in various industry sectors. The post-collapse data was fed to fourDscape for visualization and comparison with pre-disaster data to detect anomalies. The sensor readings and anomaly scores were displayed on the fourDscape 3D dashboard, which were viewed by participants and first responders on Aegex's intrinsically safe tablets.
- ✓ Aggregating all information into Azure enabled numerous parties to collect and securely distribute information in real time. A unique combination of Aegex sensors positioned along a section of pipes and flanges and connected to a Verizon LTE network with LoRa redundancy helped define a predictive signature in advance of a leak. Action on this data could have averted the disaster. The equipment and analytics costs for this capability comprised one-third of the cost of installing a typical single gas detector used in the industry today. The base configuration of AI included some of the following data points on a single device:

Aegex LoRa - Wi-Fi Gateway

  - Vibration
  - Light flash
  - Temperature, Humidity, Air pressure,
  - Carbon dioxide
  - Oxygen
  - Hydrogen sulfide
  - Others

C. Test Scenario #3: Subway Terrorist Attack

1. Scenario Background

A subway system is the location of a terrorist attack. Several large detonations occur, destroying rail cars in a 0.5 km tunnel. Rescue efforts are hindered by blocked access and lack of information about the evolving situation. Confined space exposure to toxic chemicals for victims and rescue personnel is a critical concern, as is the risk of a secondary detonation.

Figure 11 - Subway Tunnel Explosion Test with overturned rail car in the tunnel

2. Test Plan and Objectives

To test the Hypothesis, numerous technologies were assessed that met the Hypothesis Test Criteria. The objective of this test was to create an extreme and challenging scenario that addressed monitoring confined space exposure to toxic or volatile chemicals. The test attempted to identify solutions and technologies that significantly improve rescue and recovery efforts while addressing how such technologies can be deployed during normal operations to mitigate the risk of a crisis. This test enabled organizers to test iterative generations of products and solutions during a multi-day scenario to identify how various solutions can impact a crisis scenario and, thereby, speed product development to achieve daily operational improvements.

Objectives:

- Identify and test technologies that enable low-cost and configurable confined-space monitoring
- Identify and test technologies that enable operations and maintenance crews to manage typical rounds with auditable results, lowering an overall risk profile of critical infrastructure
- Identify and test technologies that would enable a rapidly deployable solution to an enclosed or confined space as may be found inside large industrial facilities or other urban environments
- Identify and test methods of aggregating information to a common operating environment across public and private information silos.

3. Scenario Results

Issues arose immediately with respect to access control and unauthorized access.

Figure 12 - Subway Tunnel Test Scenario following Terrorist Attack

Locations such as subways are open to the public with some access control vial turnstiles. Once on the platform, perpetrators' access along rail lines could have been detected with motion detectors that ignore alerts caused by trains by using contextual data captured by sound or vibration sensors. Early detection of an unauthorized individual gaining access to tunnels could have averted the situation. The breech in access security raised concerns with respect to access management at other obvious strategic targets in an urban environment.

Additionally, the costs to infrastructure of monitoring tunnels would be prohibitive with common current technologies. New, highly configurable sensors that are easy to install and do not require an installed power and communication backbone provided in this test a pervasive view of operations prior to and following the disaster scenario. An ad-hoc Wi-Fi, LTE and Li-Fi network enabled a connected response, ensuring first responders had real-time access to evolving conditions, including confined-space atmospheric conditions.

4. Findings and Lessons Learned

The scenario was designed to use the unique benefit of the Guardian Centers' 0.5km tunnel with real subway cars to model confined-space testing at a realistic scale. Industrial facilities and public infrastructure are obvious terrorist targets, and the implications can be catastrophic. The scenario yielded interesting lessons learned in after-action reviews, which primarily addressed the need for further study technologies for prevention.

- ✓ Due to the presence of volatile gases in the tunnel, standard issue tablet computers would not be allowed to support personnel in accessing maps, schematics and other valuable information while in the tunnel. Providing aegex10 Intrinsically Safe Tablets enabled personnel to remain connected and speed response.

Figure 13 - HazMat teams escorting victims and high-bandwidth communications supported by pureLiFi

- ✓ Aegex IoT Sensors can be wall-mounted or ground-mounted in and around hazardous locations, making deployment of Aegex IoT battery-powered and wireless sensors throughout the tunnel fast and easy. The sensors provided critical information about the presence of hazardous gases and identified significant uses cases in prevention. Motion/proximity sensors that easily mount to the intrinsically safe

Aegex IoT solution can provide powerful insights about authorized access. Motion detectors combined with sound or vibration, as well as numerous other sensors on a single endpoint, generates powerful contextual data not possible with current methods.

- ✓ Aggregating all information into Azure enabled numerous parties to collect and securely distribute information in real-time. Assembling all data in Azure enabled intelligent alerts such as unauthorized access that assisted in rescue and recovery.

VII. Addressing the Hypothesis - Findings

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

We developed three large-scale tests at a location that mirrors meta-scale industrial challenges. Lab testing alone could not have mimicked the extreme challenges faced in real disaster scenarios. Numerous solutions, in fact, emerged in a matter of days that could have taken years in product design, lab testing, certifications and commercialization. Solutions that emerged from testing the Hypothesis during Operation Convergent Response 2017 include:

- ✓ Intrinsically safe tablets from Aegex provided a go-anywhere-at-any-time mobility solution that meets not only rugged performance requirements but, more importantly, is certified for any hazardous or non-hazardous environment. A key lesson learned across all tests is the dangerous assumption that an area is not explosive until it is too late. Aegex solves this by designing and building the lightest, thinnest and easy-to-carry Windows 10 tablet designed and certified to meet global standards for industrial safety.
- ✓ The power of an IoT/Industry 4.0 deployment will alter industries in countless ways. A single-use sensor does not significantly generate contextual data. (Note: an air temperature sensor vs. surface temperature offset by a light sensor generates contextual information, not false positives). Enabling personnel to assemble sensor arrays of up to 32 different sensing nodes in one device generates a different view of complex environments than is often expected. The Aegex IoT Sensors system enabled site diagnostics not previously available to industry or public safety.
- ✓ IoT Sensors must be extremely low-cost and quick/easy to install.
- ✓ IoT Sensors, tablets and other devices must support multiple radios for communications redundancy.
- ✓ Devices may be deployed to a broad range of operating environments, thereby requiring uniform certifications appropriate for all settings.

- ✓ The Windows 10 operating system provided the foundation for secure uniformity across all device platforms.
- ✓ Drones with live video feed to mobile devices provided a new perspective and powerful situational awareness in operational and crisis scenarios.
- ✓ Real-time, cloud-based data may impact response time and paint a broader picture of emergency/critical situations for more impactful learning.
- ✓ Digital tools can bring silos of information together to link teams in concerted efforts for emergency response.
- ✓ 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 hours.

VIII. Conclusion

Some disasters cannot be prevented. But many can, or at least the impact can be minimized with better data and better communications. Monitoring conditions surrounding critical assets and operations can help organizations be prepared if problems arise. With current and accurate information, emergency response can be more coordinated, efficient and safe.

Figure 14 - Aegex Technologies Next Generation IoT Solution

When building an Internet of Things for Hazardous Locations, organizations must consider the special conditions that govern machine learning in highly volatile industrial operations, as well as disaster response activities. The IoT for Hazardous Locations must include specific components that are purpose-built for hazardous environments in order to capture and utilize big data coming out of these operations, and then use that information to prevent emergencies from becoming catastrophes.

The tests conducted for this research yielded valuable information, which has enabled products to be brought to market with proven capabilities. It has also identified areas where continued study and learning should take place. Lastly, it has strongly influenced the design of the Aegex IoT Platform for Hazardous Locations, which includes IoT Sensors that evolved from the prototype product seen in Figure 9 into the commercial version shown in Figure 14.

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 and the way teams respond to emergencies, thus improving efficiency, productivity and safety.

Hands-on research was conducted by Aegex Technologies, Verizon, Nokia and multiple technology partners that tested various technologies with first responders in realistic

disaster scenarios during the event. OCR2017 provided a unique opportunity to test IoT under extreme conditions.

To build on the impact of the research conducted, a second gathering of former and new participants will construct a new series of tests in November 2018 during Operation Convergent Response 2018 (#OCR2018). Scenarios will include a staged earthquake-induced refinery collapse, active shooter crisis, subway biological terror attack, hurricane and subsequent flood, highway pile-up, helicopter crash, and nuclear detonation. The results will give 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: https://aegex.com/company/ocr-2018 or https://ocr2018.vztechnologies.com/

APPENDIX A

IoT PLATFORM COMPONENTS

Field trials were conducted based on a typical IoT infrastructure stack[5]. Key components included data capture devices, wireless infrastructure, cloud computing, AI and actionable delivery to users. Figure 15 summarizes each of these components, and they are further defined below.

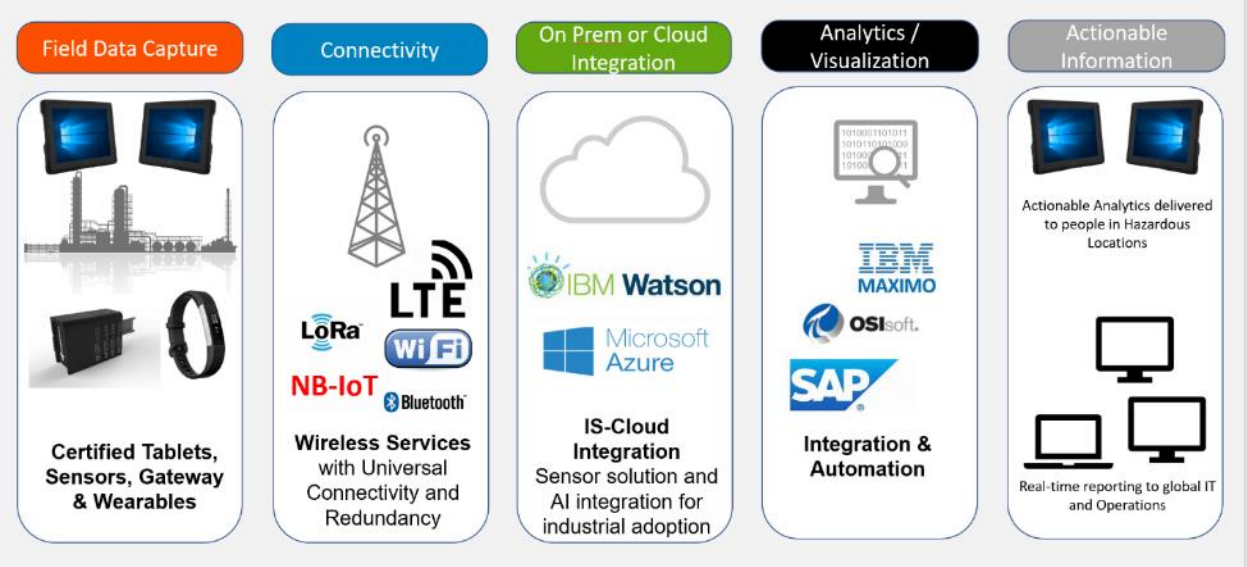

Figure 15 Aegex Technologies IoT Platform Architecture

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 (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 devices 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.

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

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

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

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 array of sensors in Figure 16, 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 16 - 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.

First responders were able to monitor the levels of noxious gases present via fourDscape on Aegex tablets and locate the sources of the leaks. They were then able to shut down operations and conduct rescue efforts quickly and safely.

Aegex IoT sensors also alerted responders and participants to vibrations indicating the approach of violent aftershocks from the earthquake, allowing them to preare seconds or minutes beforehand to avoid serious injury.

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.[6] 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[7].

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

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

Special Acknowledgements and Contributions:

Research conducted for this paper required the support and effort of many people and organizations. These and many other tests have demonstrated that the power of the right technologies can significantly and positively impact lives and communities. Special thanks to **Verizon Enterprise Solutions**, **Nokia, Guardian Centers** and the hundreds of participants that challenged our thinking and ideas to ensure the very best solutions are available to our customers, partners and communities.

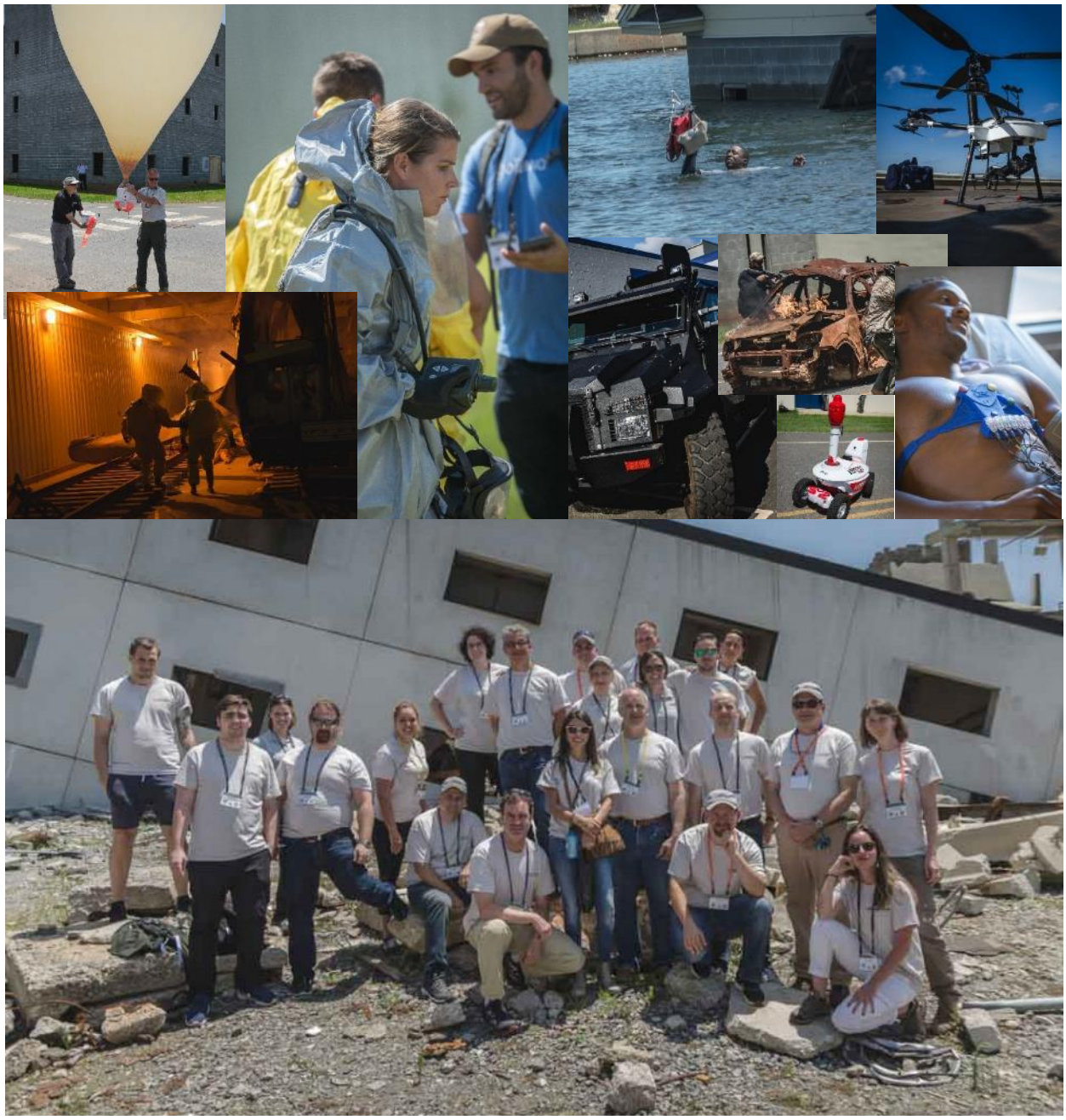

Figure 17 – TOP: Images of just a few of the people that put themselves at risk for the sake of assessing technologies that will impact industries and communities. BOTTOM: the Aegex Technologies Team managing tests at #OCR2017.