Innovation • Compatibility • Success

STANDARDS UNIVERSITY

July 2018 | Volume 9, Issue 2 | The Standard Response

IN THIS ISSUE

The Standard Response: Disaster Recovery

ABOUT THE IEEE STANDARDS EDUCATION E-ZINE

Technical standards are formal documents that establish uniform engineering or technical criteria, methods, processes and practices developed through an accredited consensus process. The purpose of this publication is to help raise awareness of standards, show the importance of standards, present real-world applications of standards, and demonstrate the role you can play in the standards development process. Knowledge of standards and standards activities can help facilitate your professional engineering practice and improve technological developments to meet the needs and improve the lives of future generations.

Serving the community of students, educators, practitioners, developers and standards users, we are building a community of standards education for the benefit of humanity.

Join us as we explore the dynamic world of standards!

CONTENTS

Letter from the Editor

When the Disaster Strikes

Natural disasters—tsunamis, earthquakes, hurricanes and tornadoes—have afflicted destruction on human life for centuries. Unfortunately, in addition to having to bear the brunt of Mother Nature's awe-inspiring force, we also have man-made disasters, whether they be intentional acts of terrorism or a lack of diligent maintenance of electricity wires that cause wildfires. No matter the cause of the disaster, we need to be better prepared before, during and after disasters to minimize the loss of life and damage to property. Many advanced technologies provide forewarning before a hurricane, tsunami, or earthquake; during a disaster, we may use our mobile devices to find the fastest escape routes to safety from a wildfire. The aftermath of a disaster is a mammoth challenge unto itself – from emergency services having to reach the affected locations to the clean-up efforts and rebuilding of communities.

As we deploy technology-based infrastructure to assist us in all three phases of a disaster, it is important to recognize the role technical standards play in such infrastructure. Raimundo Rodulfo, Director of Information Technology for the city of Coral Gables, Florida, did just that in preparation for dealing with the hurricanes that often devastate the Florida coast. "Connected Through a Disaster" tells us the role IEEE 802 standards played in "creating a resistant, reliable communications network to safeguard its infrastructure and ensure uptime of critical services." Along the same lines Jeffry Handal describes the role of communication standards well beyond wireless/Wi-Fi (IEEE Std 802.11) and cellular phones in his article "The Standard Response." Jeffry also walks you through several scenarios in which standards are used in disaster recovery, having personally lived through a few disasters in Louisiana and Texas. I admire his view that we should deploy many of our advanced technologies in the underdeveloped areas, which in many cases—at least from technology access standpoint—resemble post-disaster areas, in order to learn and prepare ourselves for disaster recovery efforts everywhere.

A complimentary proposal is put forward by a team of researchers at the National Institute of Standards and Technology (NIST), who imagine the possibility of simulating a disaster to improve preparedness. They simulated partial disasters through a controlled detonation of an apartment building, stadium, shopping mall, and a convention center. You can begin by reading my commentary and follow along with NIST's seven detailed reports. Thanks to Chris Holloway at NIST for sharing these reports with us.

Communication infrastructure is often destroyed during a disaster such as a hurricane or an earthquake, making it difficult to coordinate the responses and deployment of resources. There is a solution to this problem and it is the development of rapidly deployable and interoperable communication systems. Prof. Kamesh Namuduri describes the details in "Emergency Communication: The Need of the Hour: A Case for Standards in Rapidly Deployable Communication Systems for Public Safety."

Now, if you think technology standards are playing a big role in disaster recovery efforts, let's look at those who work on community service projects, especially in remote and impoverished areas, to prepare for faster recovery. They are the real heroes. Prof. Nick Kirsch, Chair, Engineering Projects in Community Service (EPICS) describes some of the recent projects in his article "EPICS in IEEE teaches and inspires students through community service." I applaud these university students and their mentors for bringing electricity and communication systems to remote areas, not just for everyday convenience, but being prepared in the event of an impending disaster or recovery efforts after a disaster. Why not follow suit and create your own EPICS project using funds from Prof. Kirsch?

As much as we recognize the deployment of technology and the underlying standards in dealing with disasters, there are a number of challenges faced by the first responders and other volunteers that can be addressed through smarter use of the technology. Therein lies the opportunity to recognize use of existing standards, or to develop a few that may be missing, to enable the emerging, disjointed technologies to fit in and develop new infrastructure.

Many of us focus on use of technology to deal with natural disasters, but the threat of man-made disasters are looming large. We have seen several cyberattacks in recent times, each one more severe in its ability to affect and disrupt lives of millions of people. Can we deploy some standards to prevent such attacks? Read the futuristic article "The World in 2050: Safety by Design" by San Jose State University student Tiana Ashley Khong. For this essay, she won the ANSI paper contest last year.

Think about it … before the next disaster strikes and you say in despair 'wish there was a standard!'

Yatin Trivedi, Editor-in-Chief, is a member of the IEEE Standards Association Board of Governors (BoG) and Standards Education Committee (SEC), and serves as vice-chair for Design Automation Standards Committee (DASC) under Computer Society. Yatin served as the Standards Board representative to IEEE Education Activities Board (EAB) from 2012 until 2017. He also serves as the Chairman on the Board of Directors of the IEEE-ISTO.

Yatin currently serves as Associate Vice President for semiconductor design services at Aricent Inc. Prior to his current assignment, Yatin served as Director of Strategic Marketing at Synopsys where he was responsible for corporate-wide technical standards strategy. In 1992, Yatin co-founded Seva Technologies as one of the early Design Services companies in Silicon Valley. He co-authored the first book on Verilog HDL in 1990 and was the Editor of IEEE Std 1364-1995™ and IEEE Std 1364-2001™. He also started, managed and taught courses in VLSI Design Engineering curriculum at UC Santa Cruz extension (1990-2001). Yatin started his career at AMD and also worked at Sun Microsystems.

Yatin received his B.E. (Hons) EEE from BITS, Pilani and M.S. Computer Engineering from Case Western Reserve University. He is a Senior Member of the IEEE and a member of IEEE-HKN Honor Society.

The Standard Response: Disaster Recovery

by Jeffry J. Handal, IEEE volunteer

What do VRRP1, FEMA ICS-4002, and IEEE 379-2014 have in common? They are all standards designed to mitigate some kind of emergency/failover situation. Technology plays a key role in our lives whether it means becoming more efficient at our jobs, allowing us to communicate with family members across the world, or simply using it for entertainment. Have you ever stopped to think of all that is involved in making this work? For instance, where does the electricity come from? How is it generated? How does it make it to my device? Without this single element, all the great software in the world on your expensive device would not work. This really comes into perspective once you have been in a disaster/emergency situation.

Now, let's consider the emergency situation occurs, then what? Do standards have a role to play? Naturally, the answer is a resounding yes! In the last century, as we have learned to depend more on technology, standards have been introduced to help us sustain the lifestyle we have become accustomed to. A classic story that shows the importance of standards during emergency responses is the great Baltimore Fire of 1904.4 The level of response to put out the fire was great by the adjoining cities (i.e., sending their firefighters and firefighting equipment). Unfortunately, there was one problem: none of the out of town equipment would work with Baltimore hydrants. From that experience, the first early national standards started to appear to make sure all hydrants had the same type of standard connection for hose couplings.

The Baltimore fire is just an example of how the needs for standards have been born. When we speak of natural disaster preparedness, we are really narrowing ourselves to only a small segment of emergency responses. By forcing ourselves to think in the broader terms of business continuity, it allows you to grasp situations you would normally not consider that are very elemental and disruptive (e.g., a substation equipment failure; a burst water pipe; an electromagnetic pulse (EMP)). These are all man-made situations that take us down the same road of an emergency response. By forcing ourselves to think of these events and coming up with standards (technological or procedural) it will allow us to mitigate these occurrences. In other arenas, engineers have tried to foresee and prevent similar situations. For example, in the event of radio system aircraft failure, the procedure to land safely and communicate between tower and the pilots of the aircraft is through color-coded flashing lights that have been standardized to mean something specific across the world.

Having lived through Hurricane Katrina, or more recently Harvey, and experienced the emergency response to such large-scale natural disasters, it really put standards into perspective as to how vital their role is. In comparing both storms, Harvey's response by government agencies and HAM radio operators has been very streamlined and coordinated. Much can be attributed to lessons learned from Katrina and the development of a "standard" approach to the response. Having a set of known standards as a basis ensured the timely, coordinated, and effortless response to properly setup functioning telecommunication systems. Communication systems were key to improving and savings lives.

It is uncanny to think of the similarities and parallels between living through an emergency situation and living in a third world country. For example, how do you provide disease diagnosis when no lab equipment is available? If you can develop a standard, portable lab that can aid in such a task, you just helped solve a very important riddle. For those researchers out there, instead of waiting for the disaster to happen, third world countries provide a perfect test bed. The added benefit is that you are improving human lives as well—a rarely thought of byproduct of creating and using standards.

Standards also bridge the gap between technology and different sectors of society. A great example of standards fostering a sense of community is the Santa Clara County emergency response system in California: Civil Air Patrol (CAP) with their "eyes" from the air; the local HAM radios operators with their "ears" over the radios waves; and the county government agencies ensuring the safety of everyone. The underlying glue for this to happen are the standards that allow HAM operators to talk to each other; the semiconductor business that allowed the creation of components in the airplane and radio systems; and the "standard" steps in place between government agencies and society groups to respond to situations (e.g., earthquakes). Another example of technological standards helping others in time of need is NetHope5 –telecommunication professionals come together to put the standards (e.g., IEEE 802) they know and love to good use.

As we have briefly reviewed, standards show up in all shapes and sizes. Whether it is on the technology front in the way we make things, or the procedures we follow to communicate and coordinate tasks between humans, they play a key role to ensuring our survival in mitigating the gravity of a situation. Students, researchers, and hobbyists, next time you are working on a project, remember to include standards in your ventures. They will help make your project more robust and meaningful. If a standard is not available in your line of work, help drive and create one. Who knows, your standard may help save a life one day. And remember, standards are key in ensuring human survival.

References

1. Virtual Router Redundancy Protocol (VRRP) – https://tools.ietf.org/html/rfc3768

2. FEMA Incident Command System (ICS) Classes – http://training.fema.gov/emiweb/is/icsresource/trainingmaterials.htm

3. 379-2014 – IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

4. Baltimore Fire of 1904 – https://en.wikipedia.org/wiki/Great_Baltimore_Fire

5. http://www.nethope.org/

Jeffry Handal

Seeking to serve the community, Jeffry Handal became a volunteer of the Institute of Electrical and Electronic Engineers (IEEE) in 2006. In his inception, he became the Student Liaison between the IEEE Student Branch and IEEE Professional Section and the PACE (Professional Activities Committee for Engineers) Coordinator, as part of IEEE-USA, for the Baton Rouge area. In 2007, he accepted the prestigious role of GOLD (Graduates of the Last Decade) Coordinator for the IEEE Region 5 and the GOLD International Committee Liaison. For 2010, he worked closely with children K through 12 as part of the Precollege Education Committee hoping to influence future minds. Additionally, took the challenging role of Region 5's representative to the Employment and Career Services Committee. Here, he worked with both unemployed and employed IEEE members to help them further their careers by designing IEEE member services. In 2012, Jeffry discovered there was a whole different side of IEEE that offered different levels of technical and non-technical engagement. It lead him to propose the creation of a new experimental role for Region 5 called the Standards Coordinator. It is designed to bridge the gap between the MGA and EAB side of IEEE and the Standards Association. For his hard work, in 2013, the EAB and SA recognized his efforts and invited Jeffry to become an official member of the Standards Education Committee. In said role, he is enthusiastically working to promote engagement in standards at different levels of IEEE.

The Need of the Hour: A Case for Standards in Rapidly Deployable Communication Systems for Public Safety

by Kamesh Namuduri

Abstract
From one earthquake to another, from one hurricane to another, and from one terrorist attack to another, the world has seen again and again, the destruction of communication infrastructure caused by natural and man-made disasters and their impact on human lives. In each and every situation, the story repeated itself – communication systems and networks get choked, bringing emergency services to a complete halt. The solution to this problem is the development of rapidly deployable and interoperable communication systems. Despite the efforts from the federal government, academic, and telecommunication industry, the progress has been rather slow. This article makes a case for the need for standards in rapidly deployable communication systems and the engineered ecosystem around them with capabilities to augment first-responder activities during disaster relief operations. The grand vision is availability of a portable and interoperable communication system, the size of a backpack that fits in a fire engine at every fire department in every town in near future. The system should be readily and rapidly deployable in minutes to establish communications to the citizens and first responders. This article describes what has been done so far and what needs to be done to make this vision a reality!

Despite the efforts from the federal government, academic, and telecommunication industry, the progress has been rather slow.

1. Introduction

Emergency situations arise without notice. It could be a plane crash, an earthquake, or a tornado which can cause significant destruction in minutes. It doesn't matter how much we are prepared and planned to deal with them, we may still not be ready when they occur. Power and communications infrastructure, the two most important resources needed for human survival are the first things that get destroyed during these major disasters. As recent as 2017, in Puerto Rico, we witnessed the impact of hurricane Maria on the communication infrastructure and how it brought down the entire cellular network to its heels. It is time to quickly build portable and interoperable communication systems that can be carried in a firetruck and can be deployed on the ground, on roof-tops, or in the air, to facilitate disaster-relief operations. How far are we in achieving this goal? What are the barriers and how can we circumvent them? Let us take a stock!

2. FirstNet and the Birth of Nationwide Public Safety Broadband Network

As of today, first responders still rely on thousands of separate, incompatible, and often proprietary radio networks to communicate with each other during emergencies [1]. Lack of interoperable radio networks leads to bottlenecks for information sharing among the first responders. If first responders are not connected on one network, it becomes hard, and at times impossible, for emergency responders from different jurisdictions or agencies to communicate and work together to save lives [1].

The First Responder Network Authority (FirstNet), an independent division within the U.S. Department of Commerce, was established to build the first nationwide public safety broadband network (NPSBN) to provide first responders with the ability to communicate across jurisdictions and agencies. FirstNet signed a partnership with AT&T to build NPSBN based on industry standards, nationwide spectrum, and device interoperability. On March 17th, 2018, AT&T announced the launch of the dedicated, robust, highly available and redundant distributed core infrastructure. NPSBN separates public safety traffic from commercial traffic and supports functions like Quality of Service (QoS), priority and preemption. It will also support future mission-critical services to be offered by FirstNet, like mission critical push-to-talk and location based services [1].

3. Rapidly Deployable Communication Systems

FirstNet addressed the central problem of interoperability of disparate radio networks through a common core network. However, there are several other significant barriers to enabling effective emergency communications, and for bridging the gaps in communication infrastructure caused by disasters. Imagine a scenario in which you are pinned down under a concrete slab due to an earthquake and your cell phone is not getting any signal because the nearest cell tower is destroyed due to the same earthquake. In this situation, you are doomed unless someone finds you under the rubble. The solution to this problem is a rapidly deployable communication systems that can provide the connectivity to your cell phone before the battery dies. A portable LTE node (or a 5G cell), for example, can be airlifted to the location to substitute for the dysfunctional cell tower and bridge the gap created by the disaster [9]. Such an aerial deployment of portable LTE node is illustrated in Fig. 1. (top of next page)

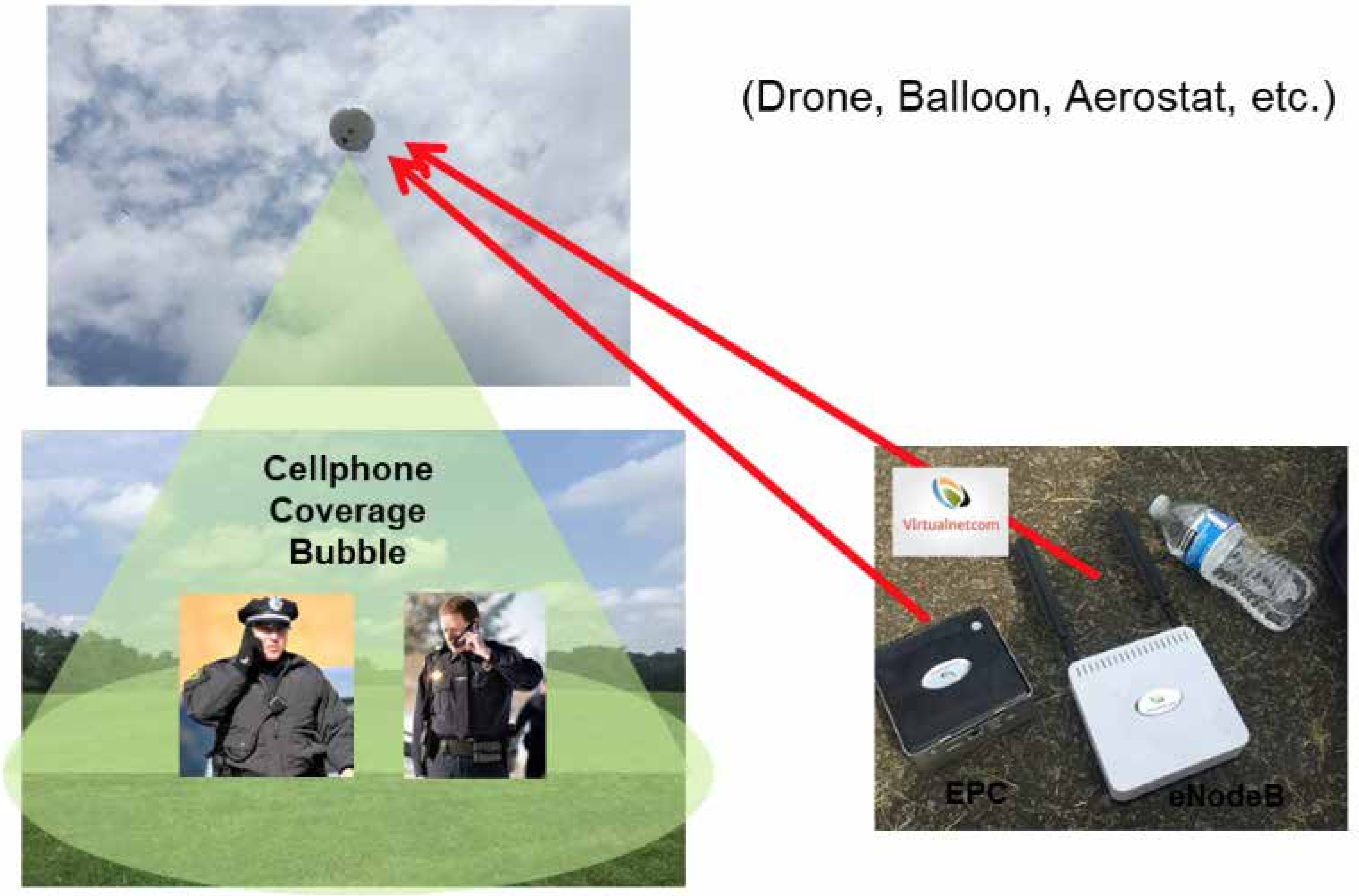


Fig.1: Illustration of a Rapidly Deployable Communication Systems (Image Courtesy: Mutualink Inc. and Virtual Network Communications, Inc.)

An LTE node includes eNodeB and Evolved Packed Core (EPC) shown on the right. Such a system can provide cellular coverage for an area determined by the transmit power of the LTE node and altitude of the deployment. A portable LTE node with a virtualized EPC from Virtual Network Communications Inc., implemented on a System-on-Chip is shown on the right. Such an LTE node with its smallest form factor weighs about three to four pounds, making it easier to airlift in many ways – using a balloon, small Unmanned Aircraft System (sUAS) or an aerostat.

Rapidly deployable communication systems would have been of great use immediately after hurricane Maria in Puerto Rico. At present, however, only prototypes of such deployable systems are available at universities (for example, [5, 6, 7, 10]) and Federal Laboratories such as National Institutes of Standards and Technology (NIST). Although, AT&T deployed what it calls "Cells on Wings" in Puerto Rico several weeks after hurricane Maria, it is a one-time effort. There is an immediate need for developing fundamental engineering processes, standards and best practices to be able to deploy rapidly deployable systems immediately after a disaster. Such a standardization process has recently been initiated by the National Public Safety Telecommunications Council (NPSTC).

4. Building an Ecosystem for Emergency Preparedness

NPSTC's Deployable Systems Working Group (DSWG) developed use cases and the desired operational capabilities of deployable systems [4]. A set of metrics—such as quality of communications, time to deploy, duration of operation in the air, interoperability with existing terrestrial cellular networks, among others—are under development.

In addition to aerial communications, the ecosystem for emergency preparedness includes a component for information acquisition and sharing through Internet of Things (IoT) and a decision-support system based on public safety analytics.

Information Acquisition and Sharing through Internet of Things:

Typically, information sharing is achieved through collaboration and situational assessment strategies. The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate's vision of Next Generation First Responder [2], includes the development of Internet of Things (IoT) that will help assess an emergency situation accurately. There is a need to identify the types of sensors that are necessary for situational assessment during disaster-relief and efficient strategies for data acquisition and information sharing between the first responders and decision-makers. The need for real-time information sharing among the participants engaged in emergency response is as important as the need for communications. These participants include first responders, volunteers and support staff, decision makers and news media [8, 9]. Information sharing enhances situational awareness capabilities of the first responders, and resource allocation capabilities of decision makers. Decision makers, such as the incident commander, should be able to view the situation as it evolves and call for resources when and where they are most needed. DHS S&T

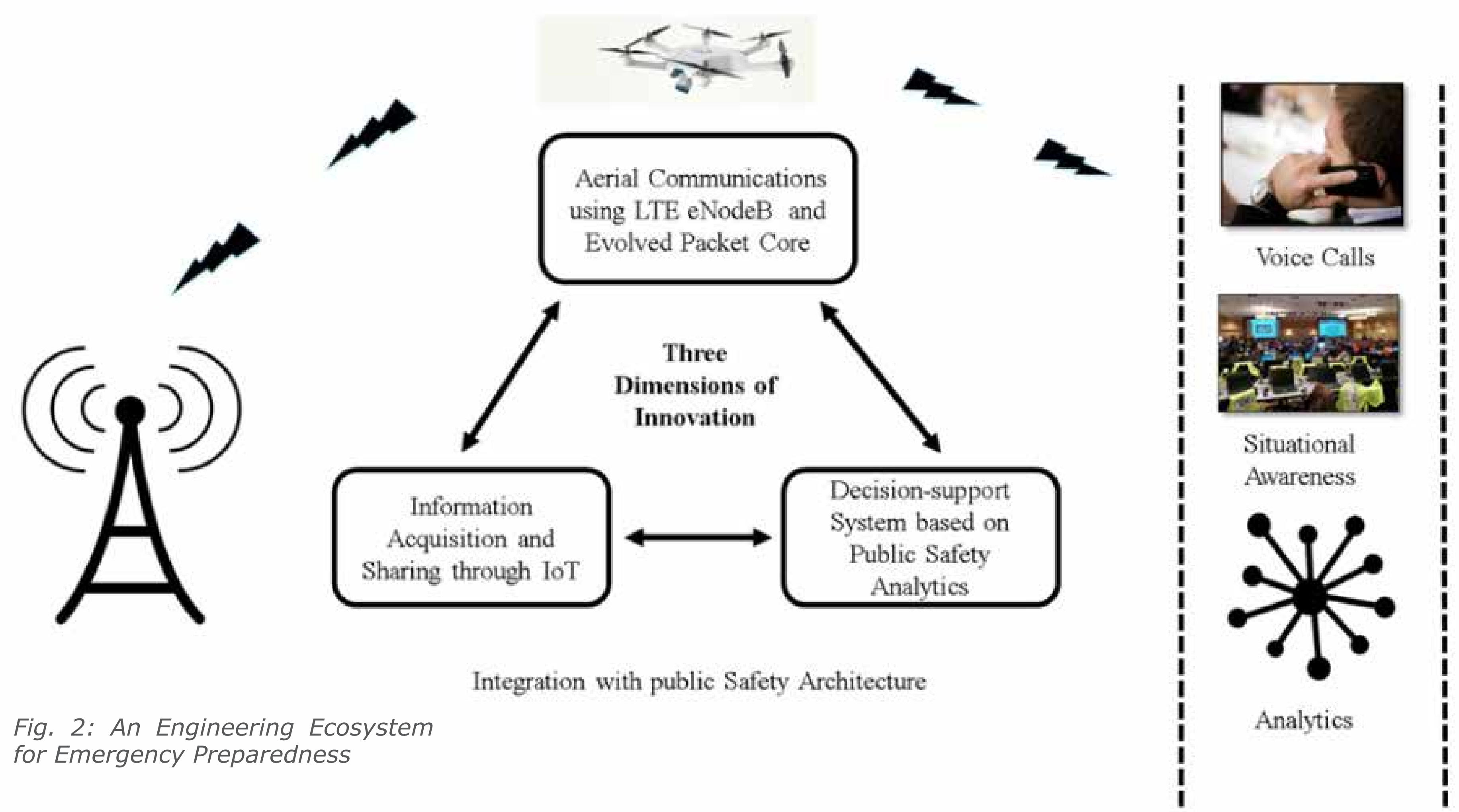

Aerial Communications using LTE eNodeB and Evolved Packet Core
Three Dimensions of Innovation
Information Acquisition and Sharing through IoT
Decision-support System based on Public Safety Analytics
Integration with public Safety Architecture
Voice Calls
Situational Awareness
Analytics

Fig. 2: An Engineering Ecosystem for Emergency Preparedness

launched the Incident Management Information Sharing (IMIS) pilot to harness the capabilities of IoT to improve first responders' situational awareness during emergencies [2].

Decision-support System based on Public Safety Analytics:
The focus in this dimension is the real-time analysis of data including voice, images and video collected from different sources—and most notably, the aerial platform. NIST identified public safety analytics as an important capability and created an R&D roadmap [3]. Data Analytics will result in actionable information for decision makers during emergencies and disaster recovery operations. Data collected by means of remote sensing systems, environmental sensors, and wearable devices integrated into first responders' personal protective equipment, may be overwhelming to process and analyze in real-time [8]. However, if successfully processed to the level of information, such data will allow the incident commander to generate actions with greater efficiency, to allocate resources and assets with greater precision, and to manage relief operations with greater efficacy.

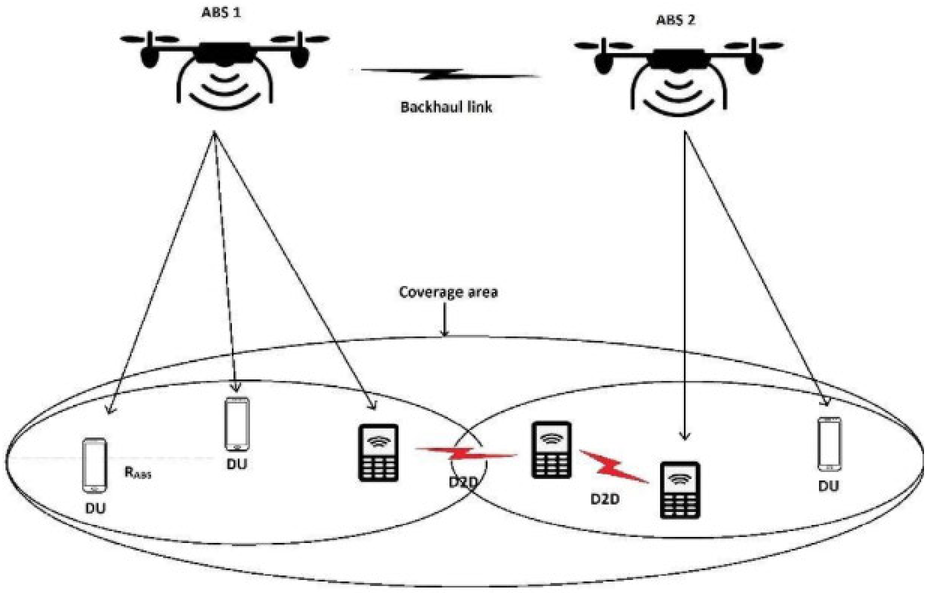


Fig. 3: Networking of two communication systems requires a microwave backhaul link (ABS: Aerial base Station, DU: Downlink User, D2D: Device-to-Device link, RABS: Radius of ABS)

5. Scaling and Integration with Nationwide Public Safety Broadband Network
Size and power constraints limit the coverage area for a deployable communication system placed on an aerial platform. The solution for expanding the coverage area is by networking several small systems together. This requires a backhaul solution such as a microwave or in-band communication links among the deployable systems. A microwave link between two deployable communication systems requires a line-of-sight between them, which is difficult to maintain when the aerial platforms are not stationary. There is a need to investigate this topic further and develop solutions for connecting communication systems deployed through aerial platforms including drones, balloons, and aerostats. Alternative strategies include running a fiber-optic wire from the aerial node to the ground.

Integration with the nationwide public safety broadband network is another important challenge. A deployable system provides coverage to an isolated bubble unless it is connected to the terrestrial network through wired or wireless communication links. Fig. 4 shows a possible deployment where the aerial node placed on a tethered aerial platform is connected to the terrestrial network through a satellite service.

Summary: Rapidly deployable communication systems are the need of the hour during disaster-relief operations. Standards for deployment, scaling, and integrating with terrestrial networks are required to speed up the development process. Further studies include 5G based deployable system design and integration, air-to-air, and air-to-ground channel modeling with 5G systems.

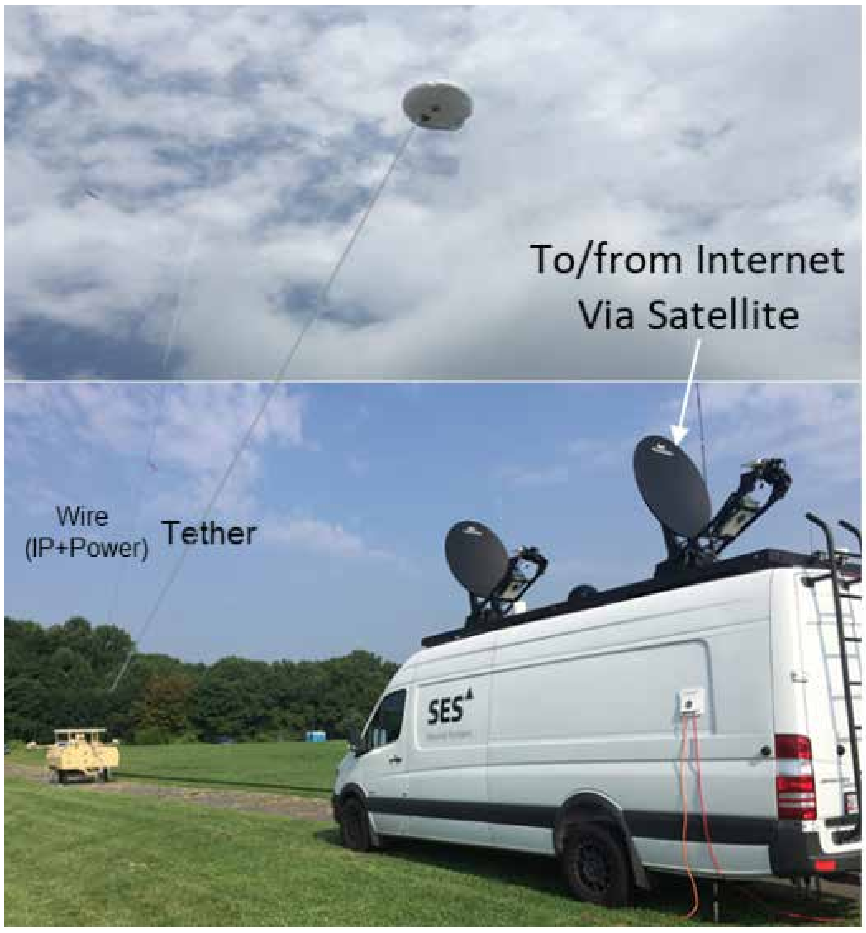


Fig. 4: A aerial node connected to the terrestrial broadband network through a tethered backhaul and satellite service. (Image Courtesy: Mutualink Inc.)

Acknowledgements: This article is based on the research work carried out under a National Science Foundation grant titled "NSF 1622978: Networked Aerial Base Stations for Enabling Emergency Communications during Disaster Recovery".

References

1. Firstnet (2012), www.firstnet.gov, accessed on May 22, 2018.

2. DHS (2015), S&T Pilot Aimed at Improving First Responder Situational Awareness, Department of Homeland Security, https://www.dhs.gov/science-and-technology/frg-iot-pilot, 2015, accessed on May 22, 2018.

3. NIST (2016), Ryan Felts, Marc Leh, and Tracy McElvaney, Public Safety Analytics R&D Roadmap, NIST Technical Note 1917, April 2016.

4. NPSTC (2016), http://www.npstc.org/, accessed on May 22, 2018.

5. Wypych, T., Angelo, R., & Kuester, F. (2012), AirGSM: An unmanned, flying GSM cellular base station for flexible field communications. In Aerospace Conference, pp. 1-9, 2012.

6. Weinert, A., Erickson, P., Reis, H., Breimyer, P., Hackett, T., Samperi, M., and Bilen, S. (2013).

7. Enabling communications in disadvantage environments: An airborne remote communication (ARC) platform. In International Conference on Technologies for Homeland Security (HST), pp. 797-803, 2013.

8. Botterell, A., (2006). The Common Alerting Protocol: an open standard for alerting, warning and notification. In: Proceedings of the 3rd International ISCRAM Conference, 497–503, 2006.

9. Homeland Security (2006), Communications Interoperability Performance Measurement Guide, 2011.

10. K. Namuduri (2017), "Flying cell towers to the rescue," in IEEE Spectrum, vol. 54, no. 9, pp. 38-43, September 2017.

Kamesh Namuduri is a Professor of Electrical Engineering at the University of North Texas. He received his B.S. degree in Electronics and Communication Engineering from Osmania University, India, in 1984, M.S. degree in Computer Science from University of Hyderabad in 1986, and Ph.D. degree in Computer Science and Engineering from University of South Florida in 1992. Over the past eight years, his research is focused on aerial networking and communications. He co-organized a series of workshops on "Airborne Networking and Communications" in conjunction with AIAA, AUVSI, and ACM Conferences. He is serving as the chair for the IEEE Standards Working Group (IEEE 1920.1: Aerial Communications and Networking Standards). He is a co-editor for the book titled "Unmanned Aerial Vehicle Networks" published by the Cambridge University Press in 2017. He published over one hundred research articles. He is leading the Smart and Connected Community project on "Deployable Communication Systems" in collaboration with the government, public, and private organizations. This living laboratory project was demonstrated thrice during the Global City Teams Challenge hosted jointly by the National Institute of Standards and Technology and US Ignite in 2015, 2016, and 2017. He contributed to the development of research agenda, requirements and blueprints highly deployable communications systems led by the National Institute of Standards and Technology and National Public Safety Telecommunications Council.

Disaster Recovery
Can We Be Prepared by Simulation?

by Yatin Trivedi

We often hear that government and non-government agencies conducting disaster relief work are unprepared for the scale of the task at hand. They are overwhelmed on many fronts ranging from how to start locating the survivors to getting food and medicine to them. Despite having access to advanced and expensive technologies, the disaster scene poses many challenges to first responders. For example, many of us are aware of the incompatibility of communication equipment and channels among the fire, police and other agencies during 9/11 attack. We frequently ask ourselves how we be better prepared for the use of technologies during disaster recovery. Similar to understanding the potential failure modes of any large-scale system, we would like an opportunity to conduct a simulated study in a controlled environment of what actually happens when the disaster strikes. Of course, this is a tall order because we cannot construct a large-scale disaster area and destroy it.

This is where one has to think outside the box and look for an unconventional approach. When the aging Veterans Stadium in Philadelphia was going to be demolished to make room for the new construction, the National Institute of Standards and Technology (NIST) team reached out to the authorities. This was a perfect case to simulate the disaster at a stadium. We can imagine full capacity audience (approximately 25,000) at a football game when the disaster strikes. Through controlled demolition stages we can study how several sections may collapse, what happens to the access routes, public announcement system, wireless access points, etc.

The NIST team specifically chose to study propagation and detection of radio signals before, during and after the implosion. Radio signals are the fundamental technology of the modern communication systems, along with the underlying standards such as the IEEE 802.11 family for wireless communication. They conducted experiments for radio-mapping, attenuation and debris-radiator. They anticipate the data collected through such studies will help develop better communication systems and technologies, including enhanced standards and safety practices, for disaster recovery efforts.

Having defined the scope of their study and how to setup and conduct such study, they set out to work with the demolition crew before, during and after the simulated disaster. Once they realized the benefit of a simulated disaster environment, they proactively sought out different types of building structures—an apartment building, an office building, a shopping mall, a warehouse, a hotel, and a convention center. Each of these simulated disaster environment studies were documented thoroughly, the results were analyzed and reports were published.

These reports are publicly available and can be accessed through the following links:

Propagation Measurements Before, During, and After the Collapse of Three Large Public Buildings

Radiowave Propagation in Urban Environments with Application to Public-Safety Communications

Radio-Wave Propagation Into Large Building Structures—Part 2: Characterization of Multipath

Radio-Wave Propagation Into Large Building Structures—Part 1: CW Signal Attenuation and Variability

Radiowave Propagation in Urban Environments with Application to Public-Safety Communications

Propagation and Detection of Radio Signals Before, During, and After the Implosion of a Large Sports Stadium (Veterans' Stadium in Philadelphia)

Propagation and Detection of Radio Signals Before, During, and After the Implosion of a 13-Story Apartment Building

Propagation and Detection of Radio Signals Before, During, and After the Implosion of a Large Convention Center

I encourage you to read these detailed study reports and build further studies so we all can learn from them and be better prepared to deal with disasters, whether natural or man-made.

Yatin Trivedi, Editor-in-Chief, is a member of the IEEE Standards Association Board of Governors (BoG) and Standards Education Committee (SEC), and serves as vice-chair for Design Automation Standards Committee (DASC) under Computer Society. Yatin has served as the Standards Board representative to IEEE Education Activities Board (EAB) from 2012 until 2017. He also serves as the Chairman on the Board of Directors of the IEEE-ISTO. Yatin currently serves as Associate Vice President for semiconductor design services at Aricent Inc. Prior to his current assignment, Yatin served as Director of Strategic Marketing at Synopsys where he was responsible for corporate-wide technical standards strategy. In 1992, Yatin co-founded Seva Technologies as one of the early Design Services companies in Silicon Valley. He co-authored the first book on Verilog HDL in 1990 and was the Editor of IEEE Std 1364-1995™ and IEEE Std 1364-2001™. He also started, managed and taught courses in VLSI Design Engineering curriculum at UC Santa Cruz extension (1990-2001). Yatin started his career at AMD and also worked at Sun Microsystems. Yatin received his B.E. (Hons) EEE from BITS, Pilani and M.S. Computer Engineering from Case Western Reserve University. He is a Senior Member of the IEEE and a member of IEEE-HKN Honor Society.

Connected Through a Disaster

by Raimundo Rodulfo

Just as residents of many south Florida towns prepare their homes and families for natural disasters—boarding up windows, stocking up on vital supplies, identifying evacuation centers, etc. —city officials must also take steps to ready for these emergency situations. After being hit hard by hurricanes in 2004 and 2006, city leaders in Coral Gables, Florida, created a resistant, reliable communications network to safeguard its infrastructure and ensure uptime of critical services. With the adoption of IEEE 802 ® standards, the City of Coral Gables developed a system that enables residents to stay connected even when Mother Nature strikes at her hardest.

Raimundo Rodulfo is the director of information technology for Coral Gables. His team works with city leadership to achieve efficiencies, innovation and process improvements through technology solutions, smart city initiatives and projects. When Rodulfo started with the city as an IT analyst in 2004, the network was simpler, more segregated and less burdened with diverse services to support. From every perspective, the needs and expectations of the network have grown more challenging and complex in the years since. Rodulfo's team led the creation of a new, more robust network based on IEEE 802 about 10 years ago.

In September 2017, the new system was put to the test when Hurricane Irma—considered to be the continental United States' most powerful hurricane since Katrina of 2005 delivered tremendous damage to the Northeastern Caribbean and much of Florida. Irma lashed Coral Gables, with numerous downed power lines, trees and traffic lights throughout the city. The system survived the storm and was able to provide digital services and communications to emergency responders and constituents during and after the wrath of Irma.

"Because of the resilience of our infrastructure, we've been able to sustain critical services such as police, fire and 911 emergency systems and communications, even though many of our network sites lost power during Hurricane Irma," said Rodulfo. "We've created a robust design based on IEEE 802 protocols. Through those standards, failover capabilities are built in the design of our network at multiple layers at the fiber optics, metropolitan Ethernet network, satellite systems or point-to-point wireless links."

Poor interagency communication during emergency response and recovery operations can have disastrous consequences for a city and its residents. Coral Gables officials had learned through experience that could not depend solely on a terrestrial communication infrastructure due to the destructive nature of tropical storms and hurricanes. Such events can uproot wireless base stations, disconnect vital communication cables, and flood central offices. The old system offered a limited degree of redundancy and lacked interoperability between public safety agencies.

In order to update the system, Coral Cables looked to industry standards developed by IEEE. The IEEE 802 suite of end-to-end networking standards underpin the internet, "Wi-Fi," the Internet of Things (IoT), Big Data, cloud computing, the smart grid, computer gaming, eHealth, industrial automation and numerous other high-tech applications. IEEE 802 standards undergird the functionality and resiliency of products and services so that cities like Coral Gables can avoid dire communication failures. The new system developed by Rodulfo's team uses a combination of redundancy layers to ensure uptime and availability.

"We learned a lot from hurricanes in 2004 and 2006, and that influenced subsequent designs," Rodulfo said. "For example, we learned that there would be a high probability of losing power completely in different areas. We learned the hard way that not all the service providers would be 100 percent available, so we learned to be more and more diversified."

Despite large-scale hurricane damage, the metropolitan network maintained critical information systems during and after Hurricane Irma. Vital

sites never lost communication with each other or with the responders' eets. The network's performance in such a challenging circumstance not only merited accolades in the IEEE Standards Association 2017 World Standards Day video contest, it also earned Rodulfo and his team recognition for a job well done from the mayor of Coral Gables, Raul Valdes-Fauli.

As soon as the threat of Hurricane Irma passed, Rodulfo, his team and other city officials put heads together to review new lessons learned.

“Every experience is an opportunity for continuous improvement,” he said. “We are continually reviewing and upgrading the network core and working to make it smarter. There is always the challenge of maintaining mission-critical services and cybersecurity and increasing speed and capacity to support new smart city services, and we constantly have to make our network more resilient.”

Rodulfo's department maintains and supports more than 200 home-grown programs and off-the-shelf applications, including specialized products for the enterprise, public safety and community services. Information technology is a key component of the city's emergency management and operation plans. His team is called upon to ensure resilience, security and high-availability technology services and communications during emergency events, as well as during normal operations. Most recently, Coral Gables has implemented a new Crime Intelligence Center, deployed CCTV and license-plate readers and acquired and deployed CrimeView applications. These innovative advancements are helping to prevent and fight crime as well as improve safety and quality of life for residents, businesses and visitors.

As public-safety agencies become more dependent on the sharing of data, images and video during and after emergencies, a robust network is vital for cities like Coral Gables. Because of IEEE 802 protocols, the city is ready to meet the needs of these agencies and its residents, even in the wake of natural disasters like Hurricane Irma. Consensus technical standards such as IEEE 802 help the world stay connected in chaos.

Mr. Rodulfo has been with the City of Coral Gables Information Technology Department since 2004. As the Information Technology Director, he is responsible for strategic planning, oversight and management of city-wide IT operations, infrastructure and initiatives. Prior to joining the City of Coral Gables, he was employed by Bellsouth where he worked for seven years as a Development Engineer for their Communication Network Operations and Control Process Automation systems. Additionally, he worked on joint projects with Lucent, Motorola, and Agilent Technologies, and developed electronic systems for Siemens and NCR. Mr. Rodulfo holds a Master's Degree in Engineering Management from Florida International University (FIU), a Graduate Certificate in Enterprise Systems from FIU, and a Bachelor of Science in Electrical and Electronics Engineering from National Polytechnic University. Mr. Rodulfo is a Licensed Professional Engineer (P.E., Florida and National NCEES Record) and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE). In addition, he is a certified Project Management Professional (PMP) and Six Sigma Black Belt (CSSBB). Mr. Rodulfo has received several awards and recognition throughout his career, including IEEE Senior Member, Bellsouth Employee of the Year, Coral Gables Employee of the Month, Governing Body Member and speaker at CIO Executive Summits, and panelist at the FIU Cybersecurity Conference.

EPICS in IEEE Teaches and Inspires Through Community Service

by Dr. Alessio Meloni

EPICS IN IEEE
Engineering Projects in Community Service

Engineering Projects in Community Service (EPICS) is a program that is making a lasting impact on students and communities around the world. EPICS in IEEE empowers students to work with local service organizations and use their technical knowledge to help a community in need. The program fosters technological innovation while benefiting humanity. It not only helps the communities, but also helps students to broaden their skills through engineering-based projects and encourages them to pursue engineering as a career for community improvement. Our program is directly in line with the IEEE motto: Advancing Technology for Humanity.

One EPICS in IEEE project that benefitted both the students and the community, focused on powering an orphanage in Honduras with solar energy. Montaña de Luz is a home to children affected by HIV/AIDS, providing them with refuge, empowerment, and hope. However, this orphanage in rural Honduras had expensive and unreliable electricity, with frequent power outages, disrupting the lives of staff and children. EPICS in IEEE awarded a $10,000 grant to the engineering students at Ohio State University (OSU) to create a new solution for this orphanage. The students implemented a 1250W solar generator, repaired a 400W wind turbine generator, replaced bulbs with high- efficiency LED light bulbs, and taught workshops for children to learn everything from creating small nightlights to solar-powered flashlights. Thanks to EPICS in IEEE and the OSU students, this greatly reduced the orphanage's electricity bill, allowed vital appliances to stay running during a power outage, and even provided them with valuable skills to create power of their own.

Another notable project brought Internet access to the remote community of Abisinia in Nicaragua. With no Internet, children did not have any access to computers in school, putting them at a huge disadvantage to those who had the means to access and share endless information online. In addition, the community's health clinic was overpopulated with patients who doctors believed could have avoided a visit if they had Internet access to educate themselves on the risks of pollution, especially because the streets were covered in trash.

EPICS in IEEE funded a $8,727 grant for this community's need to the IEEE Student Branch at Villanova University in partnership with Ruben Dario High School (New Guinea) and the Nicaraguan nonprofit organization Association for Local Government (APRODEL). Thanks to the opportunity afforded by EPICS in IEEE, this community now has an Internet café located within 100 yards of the school and health clinic, acting as a new hub for the community.

Without the support of the students, local organizations, and those who have donated to EPICS in IEEE, these communities would not have the technology or education they have today. It is those who feel a strong call to action to do the right thing who provide immense resources required for these projects. They are the ones who inspire and enable the next generation of engineers and scientists and greatly improve the quality of life for communities around the world.

It is projects like these which EPICS in IEEE supports to provide students with an opportunity to develop devices and systems to aid communities worldwide. Whether it's providing hot water to a camp in Canada, electricity to communities in Pakistan, or mobility for disabled children in the United States, EPICS in IEEE works to provide financial support to make these projects possible — building stronger students, stronger communities, and a stronger tomorrow.

In today's technology-based world, community service agencies need to utilize technology to help those in need. These communities need the help of those with strong technical backgrounds to best assist them, something that EPICS in IEEE acknowledges and uses to their advantage.

EPICS in IEEE stands out as a nonprofit by not only assisting communities in their local challenges, but also encouraging students to pursue engineering as a career for community improvement. By using engineering as the basis of their community service, they were able to better the community and students in ways other community service agencies could not. EPICS in IEEE is not only transforming lives, but inspiring careers.

References

1. EPICS in IEEE
2. EPICS in IEEE Progress Report 2016
3. EPICS in IEEE Progress Report 2017

Nicholas J. Kirsch is an Associate Professor in the Department of Electrical and Computer Engineering at the University of New Hampshire. He obtained his B.S. degree in Electrical Engineering from the University of Wisconsin – Madison in May 2003. Nicholas received an M.S. degree in Electrical Engineering and Telecommunications in June 2006 and a Ph. D. in Electrical Engineering in June 2009 from Drexel University in Philadelphia, Pennsylvania. In 2001 and 2002, Nicholas worked for W.L. Gore & Associates on fiber optic link modules and long-wavelength lasers. In graduate school, he worked with the Drexel Wireless Systems Laboratory and the Applied Communication and Information Networking group in Camden, NJ. His research interests include Multiple-input multiple-output (MIMO) communications systems, wireless sensor networks, cognitive radio, software defined radios, transparent antennas, and spectrum sensing technologies. This work is supported by the National Science Foundation, University of New Hampshire, and the Institute of Electrical and Electronic Engineers. Nicholas is currently the chair of the Engineering Projects in Community Service in IEEE program, which funds students to solve problems and engage with local non- profit organizations. Nicholas is a member of IEEE, Eta Kappa Nu, and AAAS.

The World in 2050: Safety by Design

by Tiana Ashley Kong

Abstract
This paper compares technological advances in intelligent buildings, autonomous vehicles, and smart roads to their lack of safety service standards for consumers and users. Companies continuously compete with one another to come up with innovative technology but in doing so often put consumers and users at risk. The Internet of Things (IoT) and cloud service platforms make it possible to build intelligent buildings that reduce company costs and environmental impacts, produce autonomous vehicles that reduce consumer costs and risks while making lives efficient, and construct smart roads that reduce risks and increase efficiency. All those amazing technologies can provide enormous benefits for communities, but they fall victim to lack of security. Hackers pose a serious threat to IoT, cloud service platforms, and devices that rely on both services to work, and all it takes is one small alteration in the programs to cause severe damage to societies all over the world. To provide a better understanding of the severity of lack of safety, I created a scenario in the not-so-distant future where hackers caused a global catastrophe. To prevent such a catastrophe to occur again, governments and technology companies from all over the world realized that innovation means nothing without safety and they worked together to establish safety by design service standards with the motto: "safety before innovation," leading to the blissful and progressive era of 2050. This essay will look at the inner workings and benefits of intelligent buildings, autonomous vehicles, and smart roads to allow better understanding of how IoT and cloud service platforms play a vital role in making each one possible. Explanations of their inner workings and benefits are followed by recent examples of how hackers are able to turn what seemed like fool-proof secure technology into a business and consumer nightmare giving light to the desperate need for safety by design service standards.

The World in 2050: Safety by Design

In 2028, the world experienced the collapse of cloud service platforms unlike anything it had ever seen before. A few days before the Christmas holiday, two major cloud service platforms were hacked into and collapsed, resulting in hundreds of thousands of deaths all over the world, emergency responders unable to respond, hospitals shutting down, and businesses being completely out of commission for an entire week. The world we knew came to a screeching halt, and all it took was minor alterations of major cloud service platform programs by vindictive members of society wanting to make a political statement. Even with supposed fool-proof security in place to prevent such a cyber-attack to occur, it didn't prove to be too difficult a task for the hackers to carry out the world's largest cyber terrorist attack it had ever known. After the Internet of Things (IoT) programs were altered, the interconnected sensors and devices connected to the cloud service platforms failed, resulting in the malfunctions of autonomous vehicles worldwide causing over two million road crashes and hundreds of thousands of deaths. Due to the high dependence of autonomous emergency service vehicles since the early 2020's there weren't enough emergency vehicles available for responders to help citizens. Hospitals worldwide had been completely shut down due to their Building Automatic Systems relying on IoT and the cloud service platforms resulting in the death of patients already in the hospitals and preventing hospitals from taking new patients that desperately needed their care. It took collaborating governments and technology companies a few days to gain access to the cloud service programs but by then the damage had been done worldwide. It became clear if we were to continue living in a world that heavily relied on IoT we needed to adopt new service standards, which incorporated safety by design to prevent future failures.

The year is 2050, it's been twenty-two years since the largest cyber terrorist attack occurred and societies are thriving all over the world. For nearly two years after the attack, governments and technology companies from all over the world worked together to develop the safety by design service standards with the motto: "safety before innovation." These standards ensure that companies must incorporate security measures at the very primal stages of innovative technology to ensure the safety of consumers and societies. When a company creates innovative technology, extensive security tests must be conducted and the technology must pass with a 100 percent safety approval rating before it may proceed with development accompanied by security tests at every step of the way. This has completely shifted the way companies do business, slowing down processes and innovation, but it ensures safety for customers and users. Since the new service standards were implemented the sales and development of intelligent buildings, autonomous vehicles, and smart roads increased dramatically. People felt safe once more allowing our cities to become more dependent on IoT thus providing efficient and blissful lifestyles. Even though it took the catastrophe of 2028 to open our eyes to the dire need of stronger safety guidelines, we are now living in a progressive era where government and industry collaboration resulted in improved service standards.

As defined by the Institute of Customer Service, "service standards are important to customers, potential customers, employees, and management for they help define what customers can expect and to remind businesses of the challenges and obligations they face" ("Setting Customer Service Standards," 2015). With the development of IoT came innovative technologies which provided services to the community through various benefits. If innovation continues to outweigh safety then a global disaster, similar to the above scenario, is inevitable, which is why it's crucial for innovators to adopt safety by design service standards. By putting safety before innovation, we are getting the maximum benefits of a world run by IoT; technological advances continue to improve our lives and we feel secure knowing safety is priority. If safety by design service standards are not adopted, then with every step forward we take with a technological advance we take two steps back when the lack of safety is exposed. Let's look at intelligent buildings, autonomous vehicles, and smart roads to understand the importance of adopting the safety by design service standards.

The world is becoming more reliant on IoT and cloud computing with many intelligent buildings being built to service the community by reducing costs, risks, environmental impact, and improving internal environment of the buildings. It's possible to also convert already existing buildings into intelligent buildings, but either way the process requires constant cooperation and collaboration from all the stakeholders involved which include management, operations, suppliers, customers, and especially the information technology (IT) department. When setting up an intelligent building it's important for the stakeholders to consider and prepare for technological and security changes early in the development process to allow for such changes to occur smoothly without much interruption. By combining the Building Automatic System (BAS) with IoT, companies can use the buildings sensors to store data on the cloud using a cloud-based building-analytic system. Once a building's BAS is combined with IoT, data from the sensors is sent to the cloud where it is stored and analyzed and then sent back to a dashboard which is accessed by the stakeholders, helping them make effective and efficient decisions to reduce costs. Since the BAS connects with IoT, the data that is stored and analyzed allows the BAS to take predictive measures by sensing minor issues that could result in a failure, which helps reduce risks. The occupants of the building are still able to control functions of the intelligent building such as lighting, equipment, heating, and air while they are there which allows an ideal and comfortable environment. However once the occupants leave, the BAS sensors will detect the empty space and turn everything down reducing costs as well as the negative impact on the environment (Walden, 2016).

It's easy to brush off the idea of a hacker wanting to gain access into a building's BAS, so they could have control over the building's heating and lights. But what people might not think about is that by gaining access into the building's BAS, a hacker can gain access to confidential information. IBM's security research group conducted an ethical hacking exercise just to see how vulnerable intelligent buildings really are. During this exercise, the group discovered issues in the BAS architecture that allowed them to not only gain access to the BAS but to a central server as well. The security issues that lead to this realization included exposed administration ports on routers and identical passwords for multiple systems. Not only did the group gain access to one BAS but also gained access to multiple buildings across the company. After the exercise the team's lead Paul Ionescu discussed how companies could take action to increase their BAS security and he stated roughly 29 percent were in the process of improving their cyber security (Millman, 2016).

Twenty nine percent is a very miniscule amount considering how many companies heavily rely on IoT services and devices to store their data. Companies investing in intelligence buildings reap benefits which include reduced costs, risks, and environmental impacts, but in doing so it's important to incorporate safety by design service standards. What good are the benefits if a hacker is able to gain access to the BAS resulting in access to confidential information that can harm the company and its consumers? When constructing the BAS, it's important for the IT department to integrate safety through testing the security each step of the way until accomplishing a 100 percent safety rating. In doing so they are ensuring the company's and consumer's data is safe while creating an innovative building to better service the internal and external communities.

Autonomous vehicles, also known as driverless cars, and smart roads are services already being integrated into our lives and much of the technology found in autonomous vehicles can be found in recently manufactured vehicles driven by people. A person operated vehicle that has collision avoidance, drifting warning, and self-parking features is just one small step away from being an autonomous vehicle. Autonomous vehicles use sensors and cameras to communicate with each other in real time to detect objects such as other vehicles, cyclists, pedestrians, stop lights/signs, and other stand still objects to prevent collisions (“When Cars Drive Themselves,” 2017). They can also communicate with each other through collected data that is sent and stored in the cloud using a cloud-based analytic system. This data could include weather conditions, speed limits, and road collisions that were detected by other vehicles (“Smart Roads,” 2016).

To better assist autonomous vehicles, smart roads are being built and just like autonomous vehicles, the roads are embedded with sensors by installing interactive road technology that sends data to a cloud-based analytic system to be stored, analyzed, and transmitted to autonomous vehicles (“Smart Roads,” 2016). The sensors will be able to detect weather conditions, surrounding objects, and work in conjunction with smart traffic signals allowing autonomous vehicles and smart roads to communicate with each other to provide a safe environment for travelers and pedestrians (Igbenoba, 2016). Integrating autonomous vehicles and smart roads provides enormous benefits. Every year over one million people die in road crashes globally (“Annual Global Road Crash Statistics,” 2016) all of which are results of human errors; all it takes is a few seconds of distraction, vehicle malfunctions due to a company purchasing cheap parts, or a consumer neglecting to take their vehicle in for a routine checkup to result in a road crash. Autonomous vehicles will be able to detect if there is a problem with the vehicle and alert the owners and manufacturers and prohibit the use of that vehicle until the problem is dealt with. Along with the safety benefits, autonomous vehicles would create a stress-free environment for consumers. One would be able to talk, text, play games, or even do work on their laptops while on their way to their destination (Igbenoba, 2016). Parents could program the vehicle to drop off the kids at school and come back to take them to work or run errands. It would mean only one vehicle is needed for a whole family thus reducing traffic and costs in fuel and insurance (Kroenke & Boyle 123-125, 2016). But with all these benefits there is still a major concern with safety.

In a recent experiment, reporter Andy Greenberg offered to test drive an autonomous vehicle while two researchers hacked into the car’s systems to see how much of the vehicle they could control. Within no time the researchers had hacked into the computer’s air conditioning, stereo, and even the accelerator. This experiment showed just how powerless a driver could be if their autonomous vehicle was hacked into (Hempfield, 2017). This is where the safety by design service standards would come into effect. Safety would have to be at the heart of developing autonomous vehicles and smart roads. If companies such as Tesla and Ford are planning for a world where every consumer has an autonomous vehicle, then their innovation means nothing without safety enforced service standards. No consumer in their right mind will buy an autonomous vehicle if hackers can easily gain access to the vehicle’s computer systems or gain access into the smart roads computer systems potentially wreaking havoc to the city. In order for consumers to feel comfortable purchasing autonomous vehicles and cities developing smart roads, there must be a large-scale recognition of safety by design service standards requiring 100 percent safety ratings at every stage of development.

As innovation continues to drive technology at impressive rates, safety is constantly being ignored because companies are competing to get the newest technology in the hands of consumers to stay ahead of competitors putting many users and consumers at risk. Safety by design service standards are essential to consumers but overlooked until a disaster occurs prompting necessary actions to be taken to prevent it from happening again. This cannot continue to be the case if we wish to have a world where people and businesses heavily rely on IoT. Intelligent buildings, autonomous vehicles, and smart roads are just some technologies that can only succeed if technology companies adopt safety by design service standards; safety before innovation.

References

- “Annual Global Road Crash Statistics.” Association for Safe International Road Travel. 2016. http://asirt.org/initiatives/informing-road-users/road-safety-facts/Road-crash-statistics. Accessed 10 Mar. 2017.

- Hempfield, Clarence. Why a Cybersecurity Solution for Driverless Cars May Be Found Under the Hood. 18 Feb. 2017. https://techcrunch.com/2017/02/18/why-a-cybersecurity-solution-for-driverless-cars-may-be-found-under-the-hood/. Accessed 1 Mar. 2017.

- Igbenoba, Antonette. Autonomous Vehicles and the Internet of Things. 10 Nov. 2016. https://informationcounts.com/autonomous-vehicles-and-the-internet-of-things/. Accessed 15 Mar. 2017.

- Kroenke, David M., and Randall J. Boyle. Using MIS. 3rd ed., Pearson Education, 2016.

- Millman, Rene. How Vulnerable Are Smart Buildings to Cyber Attacks?. IFSEC Global. 29 Mar. 2016. https://www.ifsecglobal.com/how-vulnerable-are-smart-buildings-to-cyber-hacks/. Accessed 11 Mar. 2017.

- “Setting Customer Service Standards.” The Institute of Customer Service. 8 Jun. 2015. https://www.instituteofcustomerservice.com/research-insight/guidance-notes/article/settinG-customer-service-standards. Accessed 25 Feb. 2017.

- “Smart Roads.” IoT Mashups. 2016. http://www.iotmashups.com/iot-examples/smart-roads/. Accessed 16 Mar. 2017.

- Walden, Leroy. The Internet of Things and Intelligent Facilities Management. HPAC Engineering. 7 Nov. 2016 http://hpac.com/internet-things/internet-things-and-Intelligent-facilities-management. Accessed 9 Mar. 2017.

- “When Cars Drive Themselves”. The New York Times. Updated 14 Apr. 2017. https://www.nytimes.com/interactive/2016/12/14/technology/how-self-driving-cars-work.html?_r=0. Accessed 7 Apr. 2017.

Disaster Network Security

by Ron Snyder

ABSTRACT
Protecting first responder and local user data is of critical importance, especially if data contains Personal Identifiable Information, or PII. The majority of humanitarian networks utilize ad hoc configurations in a disaster zone. When ad hoc networks are installed, little thought is given to the variety of cyber threats that are out in the field, ranging from malicious applications to denial of service. Technological advances in security features are constantly improving the cybersecurity landscape to include:

- Improved processing performance
- Rapid threat intelligence and remediation
- Portability of hardware
- Simplified security configuration management.

These advanced security features have been deployed in past disaster responses and can easily be implemented by today's disaster response teams in their communications solutions. Humanitarian cybersecurity practices must constantly evolve to protect against opportunistic threats. These practices must also be open to innovation that can detect and mitigate threats in real time with little human intervention, and ultimately eliminating these threats by early detection of damaging intent.

INTRODUCTION

Online connectivity during normal day-to-day life is important. We do ordinary tasks such as checking emails, checking the weather and traffic, and using social media to see what friends and family are doing. Additionally, we also use internet connectivity check more sensitive information such as our bank accounts, pay bills online, and transfer money. A natural disaster significantly disrupts our online life. Imagine a Category 4 or 5 hurricane ripping through a local area destroying infrastructure. When this happens, connectivity disappears in an instant, on top of electricity and water becoming unavailable, and homes damaged or destroyed. Of course in those critical moments, the humanitarian response efforts will focus on rescues and maintaining life. Communications play vital, high-level roles in synchronizing these efforts during a disaster response:

- Relay assessment information on affected areas
- Coordination medium for first responders
- Providing a means of communication for affected population

The scarcity of communications and energy resource in the aftermath of a disaster makes for constructing a robust, redundant, and highly secure network particularly challenging. Often the default mindset of relief workers trying to aid in IT connectivity, is to establish ad hoc data and voice networks as fast as possible. While any type of service that can be made available for communications is more desirable than no service at all, this should not preclude incorporating network security measures in the communications solution to protect the network clients.

For example, a municipal Emergency Operations Center (EOC) needs to report its status to the Regional Coordinating Center. When communication kits are installed to fulfill this purpose, there are key considerations during the setup and implementation of service availability. These include the operational responsibility of protecting data, its integrity, and availability, especially if it contains PII, or critical mapping and location information necessary for the continued operation of the EOC.

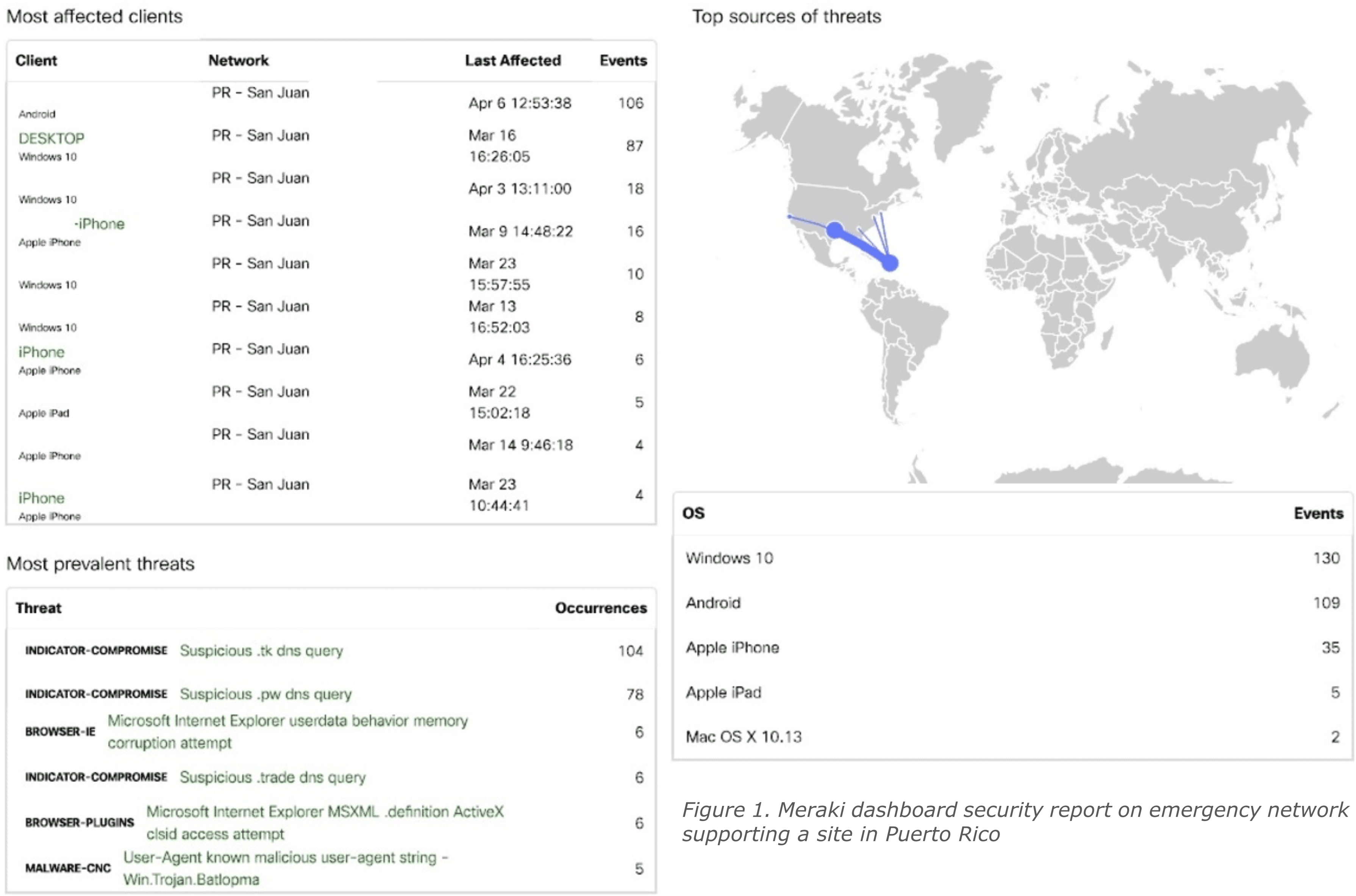
Further complicating service availability are highly latent and very expensive satellite uplinks that must be protected from unauthorized intrusion or worse, a denial of service attack. Limited bandwidth from satellite links also requires prioritization of data traffic types on the network as a standard practice, to allow important services such as Voice over IP unabated access. Content filtering of non-critical internet traffic categories may be necessary to prevent network congestion that could result in severe degradation of accessibility and quality of service.

This paper will discuss the two concepts that all disaster relief agencies must consider when setting up their communication networks in disaster areas:

- INTEGRATING SECURITY
- REAL-WORLD DEPLOYMENT

INTEGRATING SECURITY

According to an Office for the Coordination of Humanitarian Affairs (OCHA) policy paper Humanitarianism in the Age of Cyber-Warfare, humanitarian organizations need to recognize information security as a fundamental aspect of operations. These organizations need to work more closely with data security experts when setting up networks and other tools, and ensure regular reviews of vulnerabilities and breaches [1]. Security must be incorporated at multiple levels within the network. This 'defense-in-depth' approach offers layers of security for a multitude of threat vectors, beginning with end user devices. Smartphones, tablets, and laptops are assumed to be vulnerable if updates or patches are not installed. Risky user activity and phishing can also compromise not only the user device but other devices on the local area network. Modern networking tools allow for a generalized assessment of potential threats to vulnerable devices, and corresponding Advanced



Most affected clients

Client	Network	Last Affected	Events
Android	PR - San Juan	Apr 6 12:53:38	106
DESKTOP Windows 10	PR - San Juan	Mar 16 16:26:05	87
Windows 10	PR - San Juan	Apr 3 13:11:00	18
-iPhone Apple iPhone	PR - San Juan	Mar 9 14:48:22	16
Windows 10	PR - San Juan	Mar 23 15:57:55	10
Windows 10	PR - San Juan	Mar 13 16:52:03	8
iPhone Apple iPhone	PR - San Juan	Apr 4 16:25:36	6
Apple iPad	PR - San Juan	Mar 22 15:02:18	5
Apple iPhone	PR - San Juan	Mar 14 9:46:18	4
iPhone Apple iPhone	PR - San Juan	Mar 23 10:44:41	4

Most prevalent threats

Threat		Occurrences
INDICATOR-COMPROMISE	Suspicious .tk dns query	104
INDICATOR-COMPROMISE	Suspicious .pw dns query	78
BROWSER-IE	Microsoft Internet Explorer userdata behavior memory corruption attempt	6
INDICATOR-COMPROMISE	Suspicious .trade dns query	6
BROWSER-PLUGINS	Microsoft Internet Explorer MSXML .definition ActiveX clsid access attempt	6
MALWARE-CNC	User-Agent known malicious user-agent string - Win.Trojan.Batlopma	5

Top sources of threats

OS	Events
Windows 10	130
Android	109
Apple iPhone	35
Apple iPad	5
Mac OS X 10.13	2

Figure 1. Meraki dashboard security report on emergency network supporting a site in Puerto Rico

Malware Protection systems from security appliances can mitigate the threat until security updates are applied.

By carefully integrating security features into your network configurations before disasters happen, these functionalities become available for rapid deployment into the disaster zone and scalable to support an increasing number of users.

REAL-WORLD DEPLOYMENT

It is impractical to assume all users of the disaster networks are technically proficient in advanced security practices. Engineers designing and configuring these disaster response solutions must consider the evolving threats during analysis, and include advance security throughout the design of communications solution. Management of security controls should be simplified and self-evident on a streamlined user interface.

During the Hurricane Maria disaster response, a site in Puerto Rico served by NetHope's emergency network had numerous queries to compromised DNS servers, malicious browser plugin activities, and malware being blocked by a Meraki MX (Figure 1). These security events happened during users' normal online activity, perhaps running in the host's background, and sometimes without any obvious signs of security threats or malicious activity from programs and applications.

Disaster response teams such as Cisco Tactical Operations (TacOps) utilize compact, easily configurable, and highly secure Meraki MX security appliances in field deployments as recently as the Hurricane Maria response in Puerto Rico. The Meraki MX security appliance is at the heart of almost every network deployed across the island. Not only does it perform the basic routing and switching but more importantly, it protects the communication path. Meraki implemented and maintains a security program that leverages the ISO/IEC 2700 series of control standards as its baseline [2].

The dynamic situations at disaster sites typically result in significant and continuous changes in communication requirements. In most disasters, by the time the humanitarian response teams arrive for network installation, the service needs will most likely be different than what was requested initially. Disaster response teams, as well as the equipment used in establishing connectivity, need to be flexible and adapt to the reconfiguration needed, while also meeting the changing requirements in a secure manner. Within all the modifications, conforming security measures need to be mindful of the type of data transmitted and received, in order to properly separate and prioritize critical and non-critical information, software, and applications. The same level of data protection built in the original network design should be afforded to any redesign done in the field.

CONCLUSION

We are in an era where advanced security is becoming more intelligent, faster, less complex to configure, and less resource intensive. All of these characteristics are enabling quicker deployment in locations closer to the affected population.

Industry disaster response groups and all humanitarian networks must incorporate updated security to protect the integrity, privacy and confidentiality, and availability of information. The pace of technological advancement means that engineers have more tools available to design innovative security practices. Ultimately all the innovation, implementation, research and development are geared towards protecting critical first responder and user data.

References

[1] UN Office for the Coordination of Humanitarian Affairs (OCHA), Humanitarianism in the Age of Cyberwarfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies, Policy and Studies Series, October 2014, available at http://www.unocha.org/about-us/publications/policy-studies

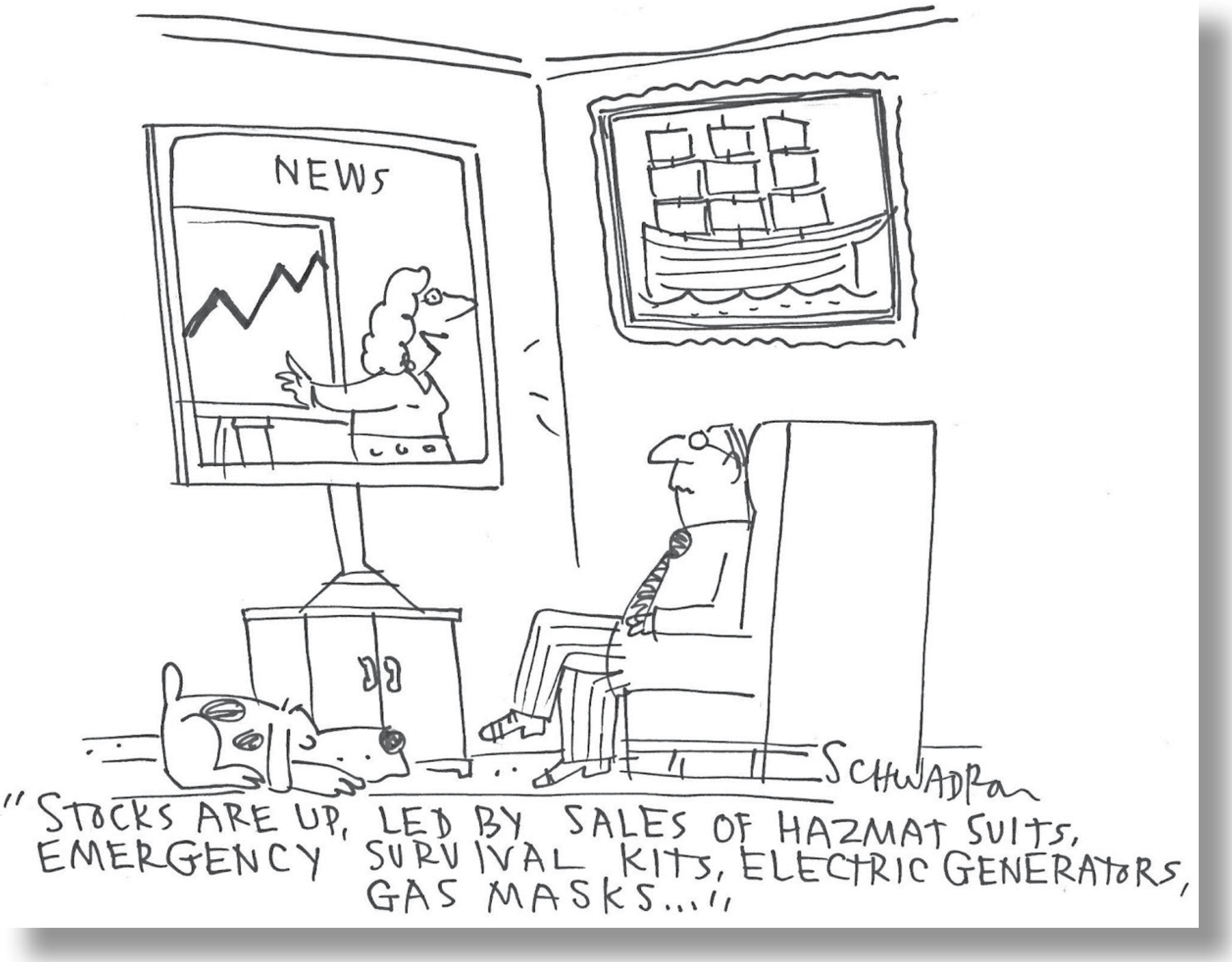
[2] Cisco Meraki Privacy and Security Practices, Cisco Meraki, February 19, 2018, available at https://meraki.cisco.com/lib/pdf/eu_technical_organizational_measures.pdf

Ron Snyder is a Solutions Architect for Cisco Tactical Operations, a dedicated crisis response team that establishes emergency networks in the aftermath of a disaster. A member of TacOps since May 2013, he is responsible for leading the strategy and technical direction of the team’s network infrastructure and deployable communications solutions. Ron also deploys and supports mobile communications platforms such as the Network Emergency Response Vehicle, a.k.a. the NERV, Mobile Command Vehicle, and smaller kits such as the Mesh Response Kits and Emergency Communications Kits. He has deployed to provide communications support in disasters such as the 2017 Hurricane Maria response in Puerto Rico, 2016 Ecuador earthquake, European Refugee Crisis in Slovenia, Cyclone Pam in Vanuatu, and Super Typhoon Haiyan in the Philippines. Ron previously worked at the Camp Roberts SATCOM facility in Paso Robles, creating the Standard Operating Procedures and training program for Regional Hub Node operators serving the US Army.

Funny Pages

Stocks Are Up

by Harley Schwadron



"STOCKS ARE UP, LED BY SALES OF HAZMAT SUITS, EMERGENCY SURVIVAL KITS, ELECTRIC GENERATORS, GAS MASKS..."