Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 19 — Issue 22 | June 27, 2019

New tool detects DC voltage hazards, helps prevent on-scene injuries

First responders encounter Direct Current (DC) more often thanks to the growing use of electric vehicles, fuel cells and solar power systems. The increase in DC use requires better ways of detection to protect personnel against electrical exposure, injuries and fatal shocks. DC detectors currently exist, but are bulky, unreliable and unsuitable for field use.

The U.S. Fire Administration (USFA) is working with Oak Ridge National Laboratories to develop a better DC hotstick technology. Currently this prototype is still undergoing testing, but the patent has been licensed.

The DC hotstick handheld prototype shows whether the electricity source is hot or not. At a vehicle collision involving an electric car, for example, the battery system could still be energized. Detecting this hazard more easily and quickly will save lives.

As the availability and use of DC power increases, it is important for firefighters to get proper training on managing the life safety risks.

- For electric vehicle hazards, visit the National Fire Protection Association website on Alternative Fuel Vehicle Safety, which includes Emergency Response Guides for 30 vehicle manufacturers.
- Underwriters Laboratories created "Firefighter Safety and Photovoltaic Systems" training to give firefighters tools to minimize the hazards of solar power systems.

(Source: USFA)

NIST camera shows 360-degree view of fires

In fire research, you can gather data, crunch numbers, run simulations and observe, but usually only at a distance. Getting a close-up look is difficult because of life safety dangers and technology challenges.

The National Institute of Standards and Technology (NIST) now has the ability to put a camera right inside the fire, capturing stunning 360-degree video. Using technology that circulates water around the camera to keep it cool, they are now able to get a view of fires not easily seen before.

The Burn Observation Bubble (BOB) allows the viewer to shift the scene around and look at the fire from different angles. You can see the fire coming toward you, moving above you, and watch it go past.

So far, they have video of a forest fire, a burning room, a kitchen fire and a mock-up of a museum collection storage room.

Researchers continuously work to improve video and photographic technology so researchers can better study fire behavior. This new tech "is a significant step to communicate the challenges in understanding wildfires and the risks they present."

(Source: NIST)

Highlights

U.S. Fire Administration

The U.S. Fire Administration operates the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC).

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.

Subscribe here

FirstNet buildout likely to be 60 percent complete this fall

AT&T, the company responsible for building and maintaining the FirstNet nationwide public safety broadband network, expects to see 60 percent deployment this fall and 80 percent deployment by fall 2020.

FirstNet development and implementation must meet certain deadlines. So far, the buildout is ahead of schedule.

Recent FirstNet speed tests show it is 25 percent faster than any commercial network, a fantastic achievement which will greatly benefit first responder communications.

AT&T must meet specific benchmarks in both urban and rural areas during the buildout – including tribal lands. To achieve this, FirstNet added mobile Satellite Cell on Light Trucks (SatCOLTs) and Cell on Wheels (COWs) to its toolbox. SatCOLTs and COWs are housed strategically around the country and are deployable during emergencies or planned events. These deployable assets made a significant difference for first responders during events in the National Capital Region.

FirstNet supports exercise programs and provides FirstNet-related exercise injects so jurisdictions can see how the network will help first responders during an emergency. One example of this is showing how network access provides better device connectivity. First responders will not have to compete with the public for signal.

Authorized by Congress in 2012, FirstNet is an independent authority within the Department of Commerce. Its mission is to develop, build and operate the nationwide broadband network for first responders.

(Source: FirstNet)

SAMHSA Disaster App

The Substance Abuse and Mental Health Services Administration (SAMHSA) offers a Disaster App to give first responders immediate access to behavioral health information for every phase of response, delivered right to your smartphone.

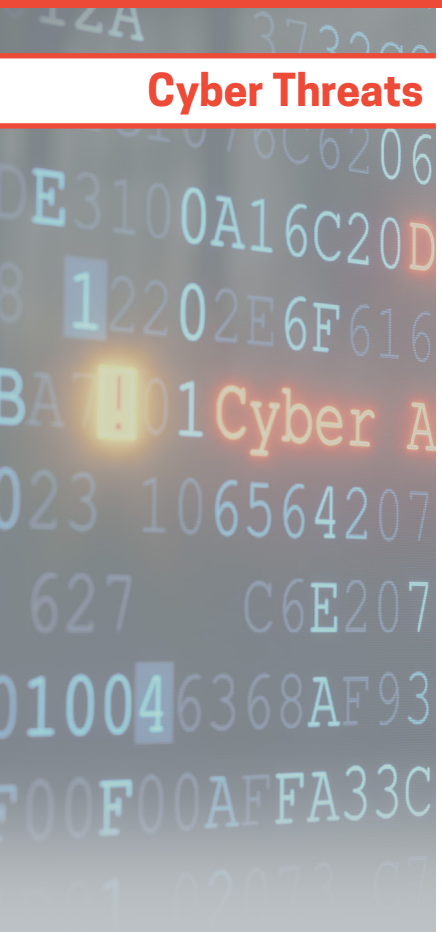
Through this app, you can:

- Access tip sheets; guides for responders, teachers, parents, and caregivers; and a directory of behavioral health service providers in the impacted area.
- Download information on your phone before deployment in case of limited Internet connectivity in the field.
- Review key preparedness materials to help you provide the best support possible.
- Send information to colleagues and survivors via text message, email, or transfer to a computer for printing.
- Find interventions to help survivors of infectious disease epidemics.
- Access resources for self-care and returning home from deployment to everyday life.

The SAMHSA Disaster App is based on the SAMHSA Disaster Kit, a go-to toolkit of crisis intervention resources. You can either order copies of the Disaster Kit to be sent by mail or download the electronic version in sections.

(Source: SAMHSA)

Cyber Threats



Hackers may be targeting power grid

Those behind the epic 2017 Triton/Trisis attack that targeted and shut down a physical safety instrumentation system at a petrochemical plant in Saudi Arabia now have been discovered probing the networks of dozens of Unites States and Asia-Pacific electric utilities. **The findings follow speculation and concern among security experts that the group would expand its scope into the power grid**.

Attackers actually began scanning electric utility networks in the United States and Asia-Pacific regions in late 2018 using similar tools and methods attackers used in targeting oil and gas companies in the Middle East and North America.

(Source: DarkReading.com)

Visualization of the world's largest data breaches and hacks

You can get a better idea of the data breaches greater than 30,000 records from the past 10 years thanks to this **interactive data visualization tool displaying the world's biggest data breaches and hacks**.

Data can be sorted and filtered based on the sector (e.g., healthcare, government, military) and method (e.g., hacked, inside job, poor security). You can also search for specific incidents and sort it based on either year or data sensitivity.

(Source: Information is Beautiful)

Webinar: Detecting Cyber Incidents in Your Small Business

On June 11, 2019, the National Cyber Security Alliance (NCSA) held a webinar on how to detect and respond to cyber incidents in small businesses. The webinar recording and presentation slides are now available online.

Many departments and agencies within the Emergency Services Sector operate similar to small businesses and could benefit from this information. **It is important to detect a cyber incident as soon as you can to limit the amount of damage**.

So, what signs do you look for? What are methods of detecting an incident? Speakers from the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Trade Commission discussed methods for incident detection and ways to limit or contain the impact of a potential cybersecurity event.

(Source: StaySafeOnline.org)

Old web scam on the rise again: fake domains and misspelled URLs

Cyber criminals are going back to the future by conducting attacks utilizing various kind of domain fraud – and **almost all organizations with an online presence are potentially at risk**. These campaigns were quite common in the early days of the web, but domain fraud is now stronger than ever, taking advantage of the sheer variety of top level domains available to choose from.

Attacks using fraudulent domains can include typosquatting on domains that capitalize on traffic meant for other websites, or domains and websites designed to look like the real deal. For example, the letter "m" can be replaced by the letters "r" and "n" to give the appearance of "m" and it's something that many users won't notice at first glance.

(Source: zdnet)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.