



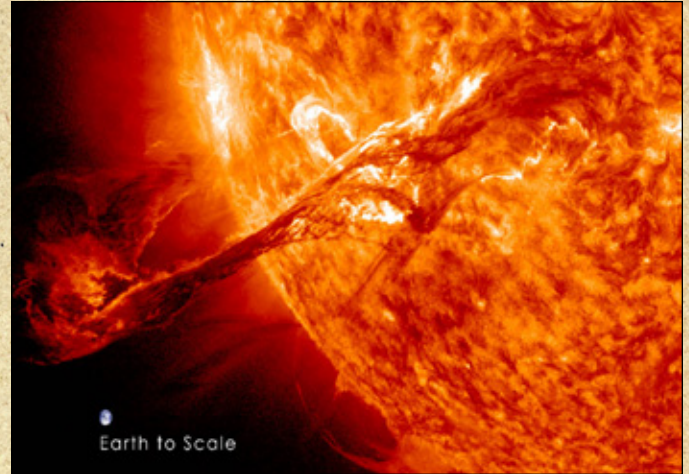
DomPrep Journal

[Subscribe](#)

Volume 14, Issue 5, May 2018



Turning Five Crisis Leader Pitfalls Into Opportunities
By Eric J. McNulty



Cascading Consequences: Electrical Grid Critical Infrastructure Vulnerability
By George H. Baker & Stephen Vollandt



Detecting & Preventing Nuclear/Radioactive Materials
By Ian Pleet



A Race Against Time: Canine/Handler Teams Prep for Disaster
By Omar Bourne

Also inside...

White Paper: Orthogonal Detection Can Help Save Firefighters Lives in the Overhaul Stage of Operations

Our commitment to **BioDefense**
has allowed us to be ready
for the **Ebola outbreak**
in West Africa.

Now, with the **FilmArray system**
and our reliable **BioThreat Panel**,
we are able to test for 16
of the worlds deadly
biothreat pathogens
all in an hour.

Now That's Innovation!



Learn more at www.BioFireDefense.com



Business Office

P.O. Box 810
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff

Martin Masiuk
Founder & Publisher
mmasuk@domprep.com

Catherine Feinman
Editor-in-Chief
cfeinman@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

BioFire Defense

Emergency Management Leaders
Conference (EMLC)

Environics

FLIR Systems Inc.

International Association of Fire Chief's
(IAFC) Hazardous Materials Response
Teams Conference

PROENGIN Inc.

Serious Play Conference

© Copyright 2018, by IMR Group Inc. Reproduction
of any part of this publication without express
written permission is strictly prohibited.

DomPrep Journal is electronically delivered by
the IMR Group Inc., P.O. Box 810, Severna Park,
MD 21146, USA; phone: 410-518-6900; email:
subscriber@domprep.com; also available at www.
DomPrep.com

Articles are written by professional practitioners
in homeland security, domestic preparedness,
and related fields. Manuscripts are original work,
previously unpublished, and not simultaneously
submitted to another publisher. Text is the opinion
of the author; publisher holds no liability for their use
or interpretation.



Featured in This Issue

Averting Disaster – A Multi-Tier Approach
By Catherine Feinman5

Turning Five Crisis Leader Pitfalls Into Opportunities
By Eric J. McNulty6

Cascading Consequences: Electrical Grid Critical Infrastructure
Vulnerability
By George H. Baker & Stephen Vollandt10

Detecting & Preventing Nuclear/Radioactive Materials
By Ian Pleet20

A Race Against Time: Canine/Handler Teams Prep for Disaster
By Omar Bourne22

White Paper: Orthogonal Detection Can Help Save Firefighters
Lives in the Overhaul Stage of Operations26

Pictured on the Cover: (top row) McNulty, Source: iStock.com/z_wei; Baker & Vollandt, Source: NASA/SDO/AIA; (second row) Pleet, Source: www.fuji.marines.mil; Bourne, Source: NYC Emergency Management, 2018

INTERNATIONAL
**HAZARDOUS
MATERIALS**

Response Teams Conference

2018



REGISTER NOW!

Conference: **June 7-10, 2018**

Exhibits: **June 8-9, 2018**

Hilton Baltimore | Baltimore, Maryland

IAFC.org/HazmatConf

Presented by the IAFC
in partnership with



Premier Media Partner



Powered by the IAFC



Averting Disaster – A Multi-Tier Approach

By Catherine Feinman



Disasters can take many forms – naturally occurring like a volcanic eruption or solar flare, human-caused like a terrorist attack or radioactive material release, or technological like a cyberattack or data breach. Although a specific threat or hazard may be unavoidable, whether it eventually becomes a “disaster” is not a certainty. Averting disaster requires making the right decisions at the right time – from the crisis leaders to the boots on the ground.

Starting at the top, crisis leaders need to be aware of and make every effort to avoid common pitfalls: thinking too narrowly, not adapting to change, not communicating effectively, being a single point of failure, and not performing adequate self-care. By considering ways experienced crisis leaders have [turned these pitfalls into opportunities](#), other leaders can take steps to avoid an even greater catastrophe when a threat emerges.

Equipped with the knowledge of what could happen without effective leadership skills and preparedness efforts, other stakeholders are better positioned to make their own crisis management decisions and implement threat barriers. For example, rapidly recovering from a widespread power outage, which many experts believe is inevitable, requires thoughtful planning on the part of each community member. Perhaps the greatest pitfall in this scenario is not understanding the [numerous vulnerabilities and cascading consequences](#), which can lead to many smaller disasters within the larger disaster.

Even with the right decisions and knowledge about potential crises, threats persist. Detecting these threats in advance – whether through [effective emergency management efforts](#) or [sophisticated detection equipment](#) – can isolate the threat and avert disaster. For example, chemical, biological, radiological, nuclear, and high-yield explosive devices pose significant risk for deliberate or accidental release. Being able to detect such threats before or immediately following the release mitigates the consequences.

Finally, when disaster does strike, highly skilled and trained response teams rescue survivors and reduce casualties. These responders – both human and [animal rescue teams](#) – provide another tier for minimizing the consequences of a disaster. The faster the response, the more lives can be saved. From leadership to management to boots on the ground, each stakeholder provides a layer of protection to avert disaster when prepared, trained, and ready to make the right decisions at the right time.

Turning Five Crisis Leader Pitfalls Into Opportunities

By Eric J. McNulty

Crises are among the most daunting challenges for leaders. The very nature of true crises – complex, high-consequence events that threaten physical, emotional, economic, and/or reputational health – test a leader’s ability to discern what is happening and what is to be done. The word “crisis” derives from the Greek “krisis” or decision. The contemporary understanding of the word stems from Middle English usage of the medical Latin variant that means “the turning point in a disease,” when the patient either lives or dies. These are the types of decisions today’s crisis leaders are asked to make in situations ranging from forest fires to active shooter incidents.



Faculty at the National Preparedness Leadership Initiative (NPLI) at Harvard have studied leaders in crisis situations for the past 15 years. The first field research was conducted in the aftermath of Hurricane Katrina in 2005 and has continued through Harvey, Irma, Jose, and Maria, the sequential hurricanes of 2017. Between those events were a variety of incidents – natural and manmade – ranging from infectious disease outbreaks to terror attacks as well as National Special Security Events (NSSE) with high potential as crisis situations. Five common pitfalls emerged from a meta-analysis of those events. In response, tools and techniques to turn each into an opportunity have been developed. These tools are now the foundation of NPLI educational curricula to help prepare leaders to make better decisions and take more effective action during crises.

Pitfall #1: Becoming Locked in a Narrow View

Many emergency management leaders have risen through the ranks. Along this journey, they have developed great operational experience and expertise. In routine emergencies, this serves them well as they grasp the contours of the incident and the steps to take. In a true crisis where much is unknown, however, such rapid certainty can create blind spots that obscure important information, the concerns and needs of certain stakeholders, and clues to how the event may unfold.

Further, leaders may revert to their operational comfort zone because it fosters a sense of certainty amid chaos and provides the satisfaction of taking action. In interviews after the Boston Marathon bombings on 15 April 2013, several senior first responders related that they felt drawn to help treat the wounded. It took intentional effort for them to pull themselves back because, in their leadership roles, it was necessary for them to leave some tasks to subordinates in order to grasp the big picture and see as many of the moving pieces as possible.

The tool to stimulate such mental positioning is a “situation map.” This is a simple visual depiction of the central incident – for example, a bombing, tornado touchdown, or cyberattack – surrounded by the secondary and tertiary situations likely to unfold. In the case of the Boston Marathon, the bombings were at the center. Around them were the medical, investigation, political, media, runners and families, business continuity, and other situations.

When mapped against each of these stakeholders, connections and interdependencies would emerge. Such a map may be sketched quickly on a piece of paper at the beginning of an incident. Over time, people may be assigned mapping responsibilities, which may take over a white board in the emergency operations center. No matter how sophisticated, a situation map helps the leader orient to the larger picture and identify critical gaps in the response.

Pitfall #2: Failure to Adapt Over Time

Even with a situation map, leaders may fail to grasp the evolution of a crisis over time and thus fail to adapt their thinking and actions as well as those of their teams. The classic example is Hurricane Katrina. Initially a wind event, Katrina became a water event in New Orleans once the levees broke. The dynamics of those two contingencies are divergent. The failure of leaders to make the mental shift from one to the other distorted their perceptions and priorities. It slowed the decision-making process, and gaps in the response became chasms.

An effective leader employs a disciplined process to continually test assumptions and recalibrate activities as necessary. For example, [wildfire fighters have adopted a system](#) to ensure that anomalies are rapidly and accurately reported up the chain of command. This helps leaders understand when a fire is behaving as expected – and when it is not. The NPLI tool is the POP-DOC Loop. Initially based on [Boyd's OODA Loop](#), which is used in air forces and other organizations around the world, the POP-DOC Loop is tailored to the needs of leaders.

The OODA Loop has four steps: observe, orient, decide, and act. The POP-DOC Loop has six steps, each aligned with a distinct cognitive function essential to effective leadership. *Perceive* is a more active version of observe, involving data gathering. *Orient* is common to both models and refers to pattern-finding and meaning-making – turning the relevant data into useful information. Once a pattern is identified and verified, it is possible to *predict* what is likely to happen next. In a complex event, several possible scenarios may present. POP is the thinking half of the loop. After predicting and assigning probabilities, the leader can *decide*, the first stop on the acting half of the loop. Decisions alone are not sufficient. The leader must next *operationalize* those decisions. This may entail marshalling resources, forging connectivity with other entities, and securing authorization for activities. This step turns intentions into realities on the ground. The final step is to *communicate* with all relevant stakeholders to ensure that they understand the leader's intent, their role, and the ramifications.

The steps of POP-DOC are arrayed along a figure-8 loop because the leader must return to the beginning to perceive whether decisions and actions are having their intended effect. The leader reorients to see if patterns have shifted and so on back around the loop. Leaders have used POP-DOC to discipline their individual activities and serve as a guide for team meetings in the midst of crisis.

Pitfall #3: Failure to Communicate Effectively

The C in POP-DOC is significant as communication failures are perhaps the most common pitfall for crisis leaders. These failures have occurred both internally and externally, involved all levels of leadership up to political leaders, and expanded out to the general public through the media (traditional and social). Some leaders become so focused on the operational aspects of a crisis that they fail to communicate and thus leave people unsure of what is happening and what they should do. Other leaders become extremely cautious, insisting that all communications go through multiple rounds of checks and double-checks. This can slow messaging such that it fails to keep pace with events.

One of a crisis leader's principle duties is what Karl Weick of the University of Michigan calls "sensemaking" – that is, understanding the dimensions and dynamics of the incident and ensuring that others understand them along with the credible plan for moving forward. [Weick wrote](#) in a 1988 article in the *Journal of Management Studies*, "The less adequate the sensemaking process directed at a crisis, the more likely it is that the crisis will get out of control."

The technique here is to make the mental shift from control to flow. Many emergency management leaders and first responders operate in formal chains of command. In a crisis, they situate in a formal management structure such as Incident Command Structure (ICS) or the National Incident Management System (NIMS). Each of these serves a useful purpose. However, within these environments, the pace of a crisis requires that information, decisions, and resources flow so that appropriate action can be taken when and where the appropriate people need it. One global organization with which NPLI faculty have worked has implemented an online system and repository to capture information, analysis, decisions, and actions for each of the emergencies and crises it faces. Automatic alerts are sent up the chain of command when triggered by the incident leader and the repository allows responders to consult detailed notes and outcomes from similar prior events. That is flow.

Pitfall #4: Becoming a Single Point of Failure

Another observation is that leaders think that their executive position requires that they have all of the answers and make every call. They aggressively assert control over every decision, expense, and media release. Although some assume this posture as a signal of heightened accountability, the message sent is one of distrust in those around the leader. Such an attitude limits the capacity and capability of the overall response enterprise. In an environment overly reliant on control, people can be paralyzed waiting for permission to do something.

Effective crisis leaders instead seize the opportunity to assemble and utilize a competent, empowered team and delegate decision-making except for those decisions that only they, as the top person, can make. When speaking at the NPLI, former U.S. Coast Guard Commandant Thad Allen called such team members, "dogs that hunt" – loyal, smart, mission-focused problem-solvers.

Such a team can mitigate risk and increase the odds of success when the incident commander's intent, organizational values, and operational principles are clear. The result is having one commander, with many people acting as leaders – that is, thinking and acting proactively within the parameters of intent, values, and principles to resolve or even preempt problems.

Pitfall #5: Failure at Self-Care

Related to becoming a single point of failure is the tendency of crisis leaders to act like superheroes who need no rest or recuperation time. It is possible to go around-the-clock for a day or two. After that, leaders become more likely to lose the ability to regulate their emotions leading to shortness of temper and impaired judgment. The leader also becomes vulnerable to [decision fatigue](#), a well-documented phenomenon in which the ability to make good decisions degrades over time.

In the response to the H1N1 pandemic, the Acting Director of the Centers for Disease Control and Prevention (CDC) [Dr. Richard Besser](#) made sure to take a day off from time-to-time. When he did so, he did it publicly so that his example would cascade down through the

ranks. He knew that others would be leery of stepping away from the emergency operations center or other response duties if he did not do so himself. The move also provided Besser the opportunity to express his confidence in his second-in-command, whom he left in charge while he took a break.

Self-care is not a sign of weakness. It is an expression of commitment to a positive outcome and acknowledgment that one's physical, mental, and emotional endurance have limits. No one person can do it all. Self-care shows respect for oneself and the others who need and expect the leader to be at his or her best. [Research from Northeastern University](#) has shown that workplaces with compassion outperform those that focus solely on technical expertise. The goal is to be kind to oneself and to others. Even brief breaks to meditate or walk in nature have been shown to [have restorative benefits](#). Make them a priority.

This is not an exhaustive list of the perils of leading through crises. However, understanding the most common ones and mastering ways to overcome them equips the leaders to handle most situations. The people who do so – those NPLI calls “[meta-leaders](#)” – are true assets to their organizations and communities.

Eric J. McNulty is associate director of the [National Preparedness Leadership Initiative](#), a joint program of the Harvard T.H. Chan School of Public Health and the Center for Public Leadership at Harvard's John F. Kennedy School of Government. Many of the program's more than 750 executive education alumni hold senior preparedness and response positions across the public, private, and nonprofit sectors.



EMERGENCY MANAGEMENT LEADERS CONFERENCE
PREPARE ♦ RESPOND ♦ RECOVER ♦ MITIGATE

**JUNE 12 - 13, 2018
AT SADDLEBROOK
IN TAMPA, FLORIDA**

REGISTRATION NOW OPEN, SIGN UP TODAY!

KEYNOTES:

- Craig Fugate • FEMA Deputy Administrator Daniel Kaniewski, PhD

PLENARY SPEAKERS:

- Dr. Stephen Flynn • Mike Martinet

6 PANEL DISCUSSIONS:

- Homeland Security, moderated by Jim Featherstone; featuring Peter Neffenger, Arif Alikhan, Eileen Decker
- Perspectives on Emergency Management, moderated by Carolyn Harshman; featuring Chauncia Willis, Barg Graff, Mike Sprayberry, Matt Campbell, Lanita Lloyd
- Funding, Resources and the PPP, moderated by Shandi Treloar; featuring David Lusk, Rob Glenn, Tristan Allen, Rick Nuedorff, Greg Forrester, Persia Payne-Hurley
- EMAC Case Study, moderated by Trina Sheets; featuring Michael Dossett, Angee Morgan
- FEMA Regional Administrators, moderated by Bryan Koon; featuring Gracia Szczech, James Joseph, Tony Robinson, Mike O'Hare
- Aid & Logistics, moderated by Kathy Fulton; featuring Jeff Dorko, Bleu Hilburn, Colonel George Vogel, Patrick Crawford



\$100 OFF
FULL CONFERENCE REGISTRATION

**EMLC PROVIDES A
DISCOUNTED REGISTRATION
ENTER PROMO CODE**

DPJ-EMLC

#EMLC2018

CONTACT INFORMATION REGARDING HOW YOU CAN PARTICIPATE IN EMLC:
T: 470-344-2400 | W: EMLC.US | E: INFO@EMLC.US

Cascading Consequences: Electrical Grid Critical Infrastructure Vulnerability

By George H. Baker & Stephen Vollandt

If there were a prolonged nationwide, multi-week or multi-month power failure, neither the federal government nor any state, local, tribal, or territorial government – acting alone or in concert – would be able to execute an effective response. This bleak outlook results from understanding that so many critical infrastructures depend on electricity. As such, effective recovery cannot be expected through top-down assistance alone. Without electric power, the goods and services essential to protect life and property would be at risk by day three or perhaps longer depending on preparedness levels. Consequently, it is vital that citizens, households, communities, businesses, and governments be as informed and prepared as possible.



Citizens of the United States are dependent on secure and reliable electric power for their current way of life. If electric power were not available for weeks, months, or even a year, then cascading impacts would degrade multiple critical infrastructures, for example:

- Water supply and wastewater treatments; Telecommunications and the internet;
- Food production and delivery;
- Fuel extraction, refining, and distribution;
- Financial systems;
- Transportation and traffic controls;
- Government, including public works, law enforcement, and emergency services;
- Hospitals and healthcare;
- Supply chains; and
- Other critical societal processes.

Loss of life could be catastrophic. Life itself would change.

The recently published InfraGard community preparedness guide, *Powering Through: From Fragile Infrastructures to Community Resilience* (hereafter *Powering Through*), states that no post-industrial society has yet experienced a widespread and prolonged electric blackout. Thus, nations that develop resilience and recovery plans for long-term, wide-area electric power blackouts are in uncharted territory. Although there may be unforeseeable points of failure, cascading effects, and barriers to recovery, plans can still be made for prevention, mitigation, adaptation, and recovery. Imperfect plans, thoughtfully developed, are far better than no plan at all.

This article examines the national power grid and the most significant threats to it. Of particular note, Dr. George Baker developed and others helped refine an important matrix of impacts from five threats to the grid and other key infrastructures. Threats evaluated include:

- Coordinated physical attacks;
- Cyberattacks against industrial control systems and/or other cyber-enabled technology;
- An electromagnetic pulse (EMP) generated by detonation of one or more nuclear warheads in the upper atmosphere over the United States;
- An EMP caused by a coordinated attack using radio frequency weapons; and
- A severe solar storm caused by an Earth-directed coronal mass ejection (CME).

Some human-caused threats might utilize a natural disaster to mask and extend infrastructure damage.

High-Impact Risks to the Electric Grid & Other Critical Infrastructures

There are two types of hazards: *naturally occurring events*, such as a solar geomagnetic storm, a pandemic, or other random events; and acts of *human volition*, such as a human-caused electromagnetic pulse (EMP) attack, a coordinated cyberattack, or a coordinated set of physical attacks on critical grid equipment or related critical infrastructures. This article, drawn from *Powering Through*, presents a summary of the risks associated with dependencies on technologies that are increasingly vulnerable to the “triple threat” of cyber, solar geomagnetic storms (GMD), and electromagnetic pulse (EMP) weapons (see Table 1).

Comments From Powering Through on Equipment at Risk

Transformers – Transformers are vulnerable to EMP, solar GMD, or physical attacks. Because [unprotected relays](#) supporting transformers can be rapidly opened and closed, transformers may be damaged or destroyed via remote manipulation. Radio frequency weapons can be used to disable substation controls, but are unlikely to affect the transformers themselves directly unless targeted substation supervisory control and data acquisition (SCADA) systems cause secondary damage. If these are attacked and disabled, then the time to replace high-voltage and ultra-high-voltage transformers is likely to be lengthy, and often dependent on overseas manufacturers. There are smaller transformers, designed to serve the residential and small business consumer, that are generally less vulnerable, more easily transportable, and manufactured in the United States. Hence, these transformers might be replaced relatively quickly.

Generator Stations – Unless protected, grid generators at electrical power stations may be disabled by an EMP. Generator control electronics are highly susceptible to EMP. If there is a severe solar storm, there is evidence that the [generators themselves could be harmed](#). Cyber, physical, or radio frequency weapon attackers may target grid generator stations.

SCADA/Industrial Control Systems (ICS) – These industrial control devices regulate the operation of machinery, breakers, and transformers. SCADA systems are vulnerable to EMP and radio frequency weapons (RFWs). Solar GMD could debilitate SCADA operations if SCADA electronics are connected to long landlines. Since they are accessible from the internet, they may be targeted in cyberattacks. They also may be targets of physical and RFW attacks.

Grid Control Centers – Control facilities vary in size and are the hubs for grid communication and SCADA networks. They provide important situational awareness for directing both

Table 1. Potential Impacts on Critical Infrastructure Affecting the Electric Grid

Equipment at risk	EMP (nuclear)	Solar storm	Cyber	Physical attack	Radio frequency weapons
Transformers	R	R	R-Y	R	R
Generator Stations	R	G	R	R	R
SCADA/Industrial Controls	R	R	R	R	R
Utility Control Centers	R	R	R	R	R
Telecommunications including cellphones	R	R	R	Y	Y
Radio Emergency Communications	R	P	Y	Y	Y
Emergency SATCOM Communications	R	P	Y	Y	Y
Internet	R	R	R	Y	Y
GPS	R	P	Y	Y	Y
Transportation	R	Y	Y	Y	Y
Water	R	Y	R-Y	Y	Y

Legend: **Red** = direct permanent effects. **Yellow** = Cascading effects if no backup power. **Pink** = temporary effect (0.5-36 hours) assuming backup power. **Gray** = direct effects uncertain. **Red-Yellow** = potential permanent effects plus cascading effects.

normal grid operation and grid reconstitution following a blackout. Because of their long-line interfaces, they are highly susceptible to EMP and GMD effects. If communications lines going into or out of the center were disabled, SCADA functions would be disabled. A cyberattack could target the SCADA devices used in the control center. The facilities could be targets for physical and RFW attacks.

Cellphones – Although many individual cellphones may be unharmed, the phones depend on cell towers interconnected with the local and long-haul telecommunications networks, which are vulnerable to EMP, GMD, RFW, cyberattacks, and physical attack.

Radio Emergency Communications – Some of the emergency radio systems – such as the Federal Emergency Management Agency, National Radio System – continue to work if they are hardened. However, in an EMP, public radio stations and their power sources may not be hardened and may fail. In a solar storm, this communication may be temporarily disabled by atmospheric conditions, but could return in hours to days. The other threats would not affect radio systems if the attack were focused on the grid.

SATCOM – The military’s Military Strategic and Tactical Relay, MILSTAR system is EMP protected and will continue to operate. Some additional military portable UHF SATCOM radios that link through high-orbit geo-stationary satellites may also continue to function. Unhardened ground stations may fail in an EMP environment. Commercial satellite phones rely on satellite and ground stations that are likely to fail under EMP stress.

Internet – An EMP would disable key elements of the internet and users’ IT equipment. A cyberattack on the grid taking out the generators, SCADA devices, and control centers would also have a cascading effect on internet data centers depending on the capacity and longevity of their back-up power resources. A solar storm can damage long-haul internet interconnects including both metallic and fiber optic links (the latter due to the vulnerability of optical fiber regeneration equipment). Physical or RFW attacks targeting grid assets would disable local internet equipment within Endpoint Group data centers and substation control facilities, but leave the larger internet intact.

Transportation – Railroad signals and highway traffic signals could be directly damaged by an EMP and cause significant delays. Controls and communications elements that use rails for transmitting communications signals are in great jeopardy if not protected and tested. A solar storm should not disable these transportation items if backup power is available for the duration of the grid failure. Likewise, a cyberattack or RFW attack on the grid would not disable transportation systems if backup power is available. In a widespread grid blackout, standard operating procedures to close ports safely could result in delays in prioritized reopening of U.S. ports that are essential for throughput of disaster relief supplies. Chemicals or liquefied natural gas facilities within ports could benefit from backup power capabilities that prevent hazardous chemical releases due to loss of external power. In turn, preventing these chemical releases could avert extended port shutdowns after regional grid blackouts and help to re-establish priority supply chains and accelerate lifesaving and recovery operations.

Water – Because water purification and wastewater purification plants are controlled by SCADA devices, these could be disabled by EMP. Backup emergency diesel generators and solar panels are also vulnerable to E1 pulses (the first of three electromagnetic pulses created by an EMP) unless the generators and the solar panel inverters and controllers are EMP-protected. A cyberattack or RFW attack on the grid would not directly disable the water/wastewater systems if protected backup power were available. Nevertheless, if electric substations continue to be exempt from cyberprotection standards for “high-impact” grid assets, adversary takeover of substation controls could disable aqueduct pumps and locks, as well as other water and wastewater pumps and motors that provide essential water pressure and that process and manage wastewater products.

Probability

Powering Through states:

The likelihood of natural event hazards is generally independent of efforts to prevent, mitigate, or recover from such events. Solar storms cannot be deterred, though the consequences can be mitigated. In contrast, the likelihood of volitional acts may be affected by both preventive measures and by the deterrent effects of initiatives to mitigate and recover.

Powering Through continues:

Severe solar geomagnetic storms have been recorded over recent millennia, but their impact on electrical systems has been measured with increasing accuracy only since the August-September 1859 Carrington event. Various models in the past decade estimate the probability of severe solar geomagnetic storms – of the magnitude of the Carrington event or the May 1921 New York Central Railroad storm – as approximately 8% to 12% per decade.

It is very important to examine the consequences of a long-term power outage and not to concentrate on the probability.

In more than seven decades since nuclear weapons were employed in World War II, a high-altitude electromagnetic pulse (HEMP) attack has not occurred. EMP-optimized atmospheric testing occurred before a Limited Test Ban Treaty, a ban on testing in outer space, the atmosphere, or underwater, took effect in 1963. Deterrence of nuclear weapon use has been successful to date. However, the past may also be a prologue.

Even if most nation states are deterred, not *all* nation states (including failed states) and all subnational groups will be deterred if EMP vulnerabilities are not addressed and diminished. There is no credible way to assign a probability to HEMP attack or to ground-based or cruise missile radiofrequency weapons employment that may not violate the Environmental Modification Convention. However, it is reason for concern that approval for asymmetrical warfare, including a HEMP attack, is found in foreign military literature.

With these diverse hazards in mind, it is essential to recognize that government entities at the federal and state levels cannot protect critical infrastructures by themselves. Public-private partnerships will be necessary, and planning concepts and suggestions for broader audiences must extend beyond government.

Readiness Gap

The authors have considered various scenarios that range from two to three weeks without power on a regional basis, to continent-wide loss of power for over one year. It is certainly possible for an adversary or solar weather to disrupt electrical power for longer than a year. Accepting this possibility is the first major step in readiness planning. Aiming for readiness that can address a one-year outage is daunting; however, that effort will do much to provide for limited-term outages of up to two-three months. Recent events in Puerto Rico caused by Hurricane Maria make it obvious how challenging it can be to restore electrical power even with the remainder of the nation providing assistance.

As of [26 September 2017](#), 95% of the island was without power and, due to the cascading effects of power loss, less than half the population had tap water and 95% had no cellphone service. Two weeks after the hurricane, 89% of the population was still without power, 44% without water service, and 58% without cell service. One month after the hurricane, there was only slight improvement as 88% of the population lacked power, 29% lacked tap water, and 40% lacked cell service. Three months after the hurricane, 45% of the population still had no power (1.5 million people) and 14% had no tap water; cell service was returning, with over 90% of service restored and 86% of cell towers functioning.

Powering Through observed:

On its [Ready.gov website](https://www.ready.gov), the U.S. Department of Homeland Security advises the American public to store food and water for at least three days. As useful as that is for a starting point, high-impact events must also be considered. Many who assume that the government will provide support as soon as day four may think that they do not need to plan for extended emergencies at all.

In the West now, they are encouraging their citizens to be prepared for two weeks. This is significantly better than three days.

Powering Through continues to illustrate that:

In the event that a widespread failure of electrical power, which takes down critical infrastructures for a much longer duration, sufficient relief, whether from government and/or other sources, probably will not be available. Depending on the duration of the infrastructure failure, consequences for unprepared citizens could go well beyond economic loss to include sickness and death from dehydration, disease, pollution, exposure, starvation, fire, and civil unrest. Consequences for the nation could include a breakdown of coherent central government (local, state, and federal), leading to possible loss, at least temporarily, of effective sovereignty: the full right and power of governing bodies to govern themselves without outside interference. There could also be unacceptable delays in recovery, resulting in extensive loss of life and property. All of these are unacceptable risks.

The U.S. House of Representatives has passed several bills that address U.S. electric power grid vulnerabilities. The Federal Energy Regulatory Commission sponsored research at Oak Ridge National Laboratories to characterize EMP effects on the national power grid. There are several indications that these threats are being taken seriously by federal officials. For example, the White House National Science and Technology Council's [National Space Weather Strategy](#) and [National Space Weather Action Plan](#) are strong indicators. In addition, the [Defense Threat Reduction Agency](#) has recognized the EMP effects on the national electric power grid in a request to strengthen the critical civil infrastructure on which military facilities in the United States depend for at least 98% of their electricity. The Department of Energy and Electric Power Research Institute issued a [Joint Electromagnetic Pulse Resilience Strategy](#) in July 2016. The Department of Homeland Security Office of Infrastructure Protection explicitly noted the EMP threat to the cyber industry in the public and more detailed "For Official Use Only" [reports issued in 2016](#) by the Regional Resiliency Assessment Program. All of the foregoing initiatives validate the threat.

However, no plan or preparation exists at the national level that addresses long-term electrical power outages that span large regions or the continent. In such a case, there would be no neighboring state or region that could provide the depth of assistance required to promptly assist the general public, businesses, and local or state governments. Each region would be grappling with its own problems (see Figure 1).

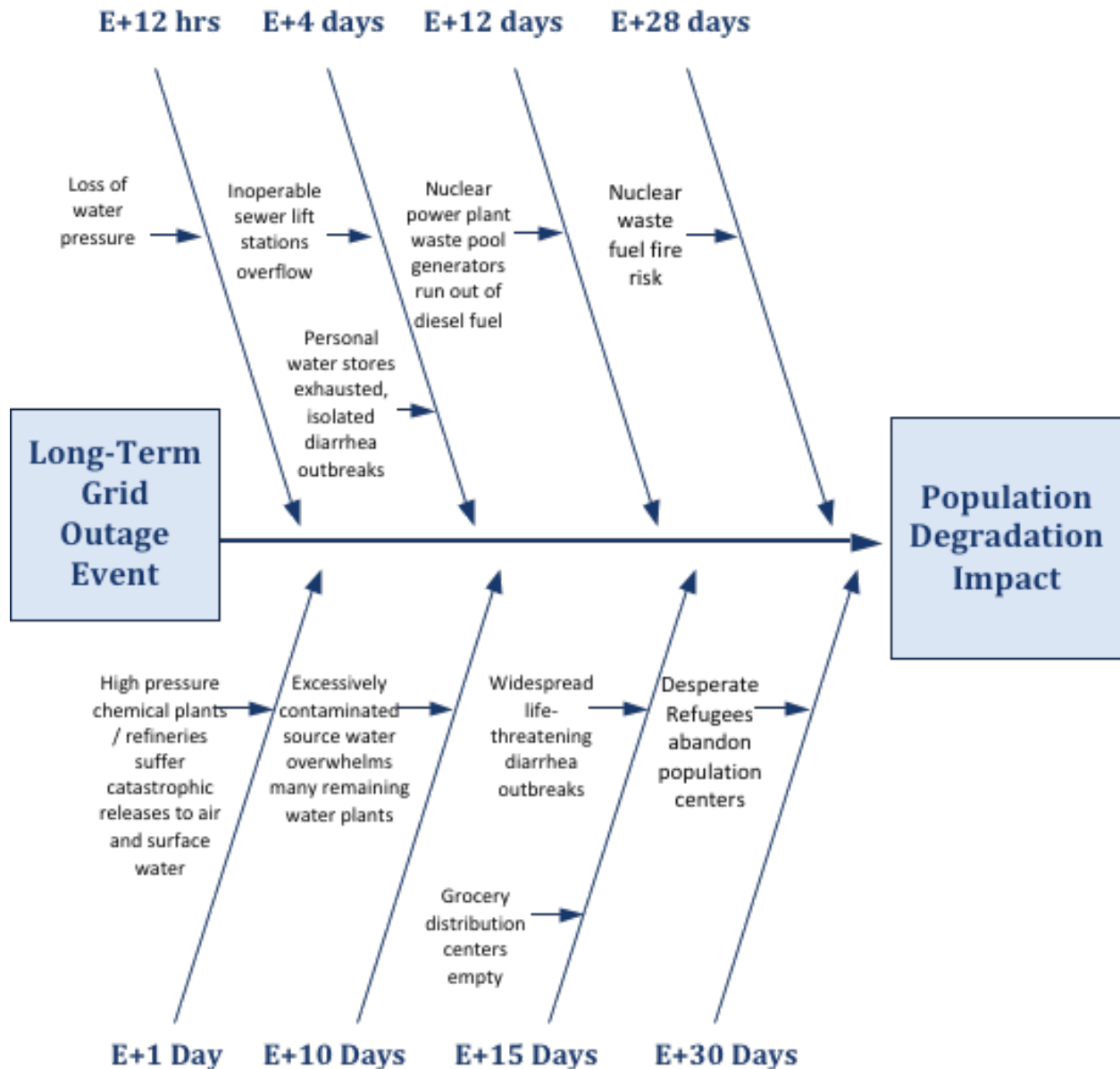


Fig. 1. Long-Term Power Outage Worst Case Timeline, as shown in *Powering Through*, p. 166 (Source: Stephen Vollandt, Auroros Incorporated).

Recommendations

Acceptance of the threats presented in this article as being credible is the first step in any recommendation. For example, Section 1913 of The 2018 [National Defense Authorization Act](#) addresses EMP specifically. Additionally, The Congressional EMP Commission has been granted permission to publicly release two reports regarding EMP:

- EMP Commission, Volume I, Assessing the Threat from EMP Attack – Executive Report, July 2017, publicly released April 2018 and available at: dtic.mil; and
- EMP Commission, Volume II, Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures, July 2017, publicly released April 2018 and available at: dtic.mil

Overall, a strategy to protect and rapidly restore lifeline sectors – including water, electricity, food, medical and emergency services, and telecommunications – offers the potential to maximize “shelter in place” capabilities and minimize uncoordinated evacuations. Uncoordinated evacuations have the potential to escalate threats to public safety, protection of supply chains, and equitable distribution of life-essential goods and services.

As stated in the *Powering Through* preparedness guide:

The United States needs to augment the planning and investments that are essential to cope with extended duration catastrophes. Whole community participation in both planning and recovery must be the new norm, and this vital process needs to start now and continue. The fundamental criterion for success should be prepared individuals and communities capable of surviving long-term infrastructure failure, while at the same preserving families, assisting others in their communities, and defending the nation.

The White House National Science and Technology Council in October 2015 issued the National Space Weather Strategy and the National Space Weather Action Plan, calling for the “[whole of community](#)” to plan for a severe solar storm and noting that other threats could cause similar effects. In 2016, the Department of Energy and the Electric Power Research Institute issued a [Joint Electromagnetic Pulse Resilience Strategy](#) for the national electric power grid. Also in 2016, the Defense Threat Reduction Agency recognized the [operational importance of grid survivability](#) in the event of an EMP, and requested proposals to strengthen the private sector and military critical infrastructure upon which defense missions depend. The Department of Homeland Security Office of Infrastructure Protection specifically noted the EMP threat to the telecommunications industry in a 2016 report prepared for the [Regional Resiliency Assessment Program](#). Finally, the 2018 National Defense Authorization Act calls out the vulnerability of military bases caused by their dependence on the electrical power grid instead of relying on locally produced electricity. The foregoing documentary findings validate the threat and underscore the urgent need for infrastructure planning and protection. Assessments are still needed for households, communities, and organizational readiness to manage the risks described in this article.

*InfraGard, more formally the InfraGard National Members Alliance is a nonprofit consisting of more than 50,000 volunteers committed to assessment and protection of critical infrastructures throughout the United States. InfraGard sponsored the December 2016 publication of *Powering Through: From Fragile Infrastructures to Community Resilience, an Action Guide Powering Through, Version 1.0*, which was researched and prepared by InfraGard’s Electromagnetic Pulse Special Interest Group (EMP-SIG) volunteers. *Powering Through* examines actions that could be taken now to be more resilient, protect life and property during grid outages, and prepare for expedited recovery. Most of the content of this article is taken from this action guide, which is available at: <https://www.amazon.com/Powering-Through-Infrastructures-Community-Resilience/dp/0998384402>*

Dr. George H. Baker (pictured above), is a professor emeritus at James Madison University, where he directed the JMU Institute for Infrastructure and Information Assurance. Previously, he led the Defense Nuclear Agency’s Electromagnetic Pulse (EMP) program, directed the Defense Threat Reduction Agency’s assessment arm, and served as a senior scientist for the Congressional EMP Commission. He is a member of the Foundation for Resilient Societies’ board of directors. He holds an M.S. in Physics from University of Virginia, and a Ph.D. in Engineering Physics from the U.S. Air Force Institute of Technology. Currently, he is CEO of BAYCOR, LLC – a consulting

company primarily devoted to preparedness for and protection against major electromagnetic threats to critical infrastructures including nuclear EMP, solar storms, and radio frequency weapons.

Stephen Volandt, vice president of Auroros Inc., currently serves as a vice-chair of the FBI's InfraGard Electromagnetic Special Interest Group (EMP-SIG). He has over 30 years of experience leading projects that assess and transform critical operations with focus on capability portfolio management and cascading consequence management. He has led teams for the FBI, Headquarters Army, and Headquarters Marine Corps to address enterprise-wide operations and systems improvement. His experience spans operations in austere locations, weapons of mass destruction neutralization, nuclear terrorism, cybersecurity, and infrastructure readiness and protection. His current passion is the establishment of vibrant, resilient, and self-sustaining communities.

Significant contribution to this article was provided by:

William R. Harris is an international lawyer specializing in arms control, nuclear nonproliferation, energy policy, and continuity of government. He is a member of the board, secretary, and a principal investigator involved in reliability standard development for critical infrastructures for the Foundation or Resilient Societies. He formerly served as a space operations lawyer for reconnaissance and communication systems of the United States government. He served as a senior (legal) advisor to the Commission on Electromagnetic Pulse (EMP) in January-December 2017. Since September 2017, he has been a vice chair of the EMP Special Interest Group of InfraGard, a nonprofit committed to protection of critical infrastructures. He holds a B.A. from Harvard College and a J.D. from Harvard Law School.

Mary D. Lasky is the chairman of the InfraGard Electromagnet Pulse Special Interest Group (EMP SIG). She is the lead editor and author of "Powering Through: From Fragile Infrastructure to Community Resilience" an action guide on being prepared if there is grid failure. She is a Certified Business Continuity Professional (CBCP). She has been the program manager for business continuity planning for the Johns Hopkins University Applied Physics Laboratory (JHU/APL). She is a past president of the Community Emergency Response Network Inc. (CERN) in Howard County, Maryland. She is a past president of the Central Maryland Chapter of the Association of Contingency Planners (ACP). At APL, she has held a variety of supervisory positions in Information Technology and in business services.



SERIOUS PLAY
CONFERENCE

at George Mason University
Science & Tech Campus
Manassas, VA

REGISTER NOW

www.seriousplay-dc.com

Use **DOMPREP** for \$100 discount

3 day conference:

Leadership Training for First Responders

Practical Sessions by FEMA, DHS,
Dept of Health, DOD Contractors

Full track for police, fire, govt emergency workers



WE STEPPED UP SO YOU CAN STEP BACK.

The new **FLIR identiFINDER® R440** lets you scan for radiological threats from farther away to keep you and your community safe.

The new R440 is a lightweight, sourceless RIID that can be operated with one hand and is IP67-rated to survive tough missions. Not only does the 2x2 NaI detector deliver sensitive and fast detection, but it also provides accurate identification during secondary screening. The new 360° EasyFinder™ Mode expedites decision-making to keep you safe.

[Learn more at flir.com/R440](https://flir.com/R440)



FLIR identiFINDER R440
Highly Sensitive, Sourceless Handheld RIID



Detecting & Preventing Nuclear/Radioactive Materials

By Ian Pleet

This case study from a 2015 deployment to the U.S. Marine Corps (USMC) Combined Arms Training Center (CATC) Camp in Fuji, Japan, demonstrates effective ways to detect and prevent unwanted nuclear and radioactive materials from being brought aboard an overseas USMC installation. The author was deployed as the emergency manager (EM) with the collateral duty of being the chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) protection officer (CPO). Upon arrival, the commanding officer also appointed him to serve as the alternate antiterrorism officer, with full support from his contracting company, Camber Corporation.



The immediate challenges for the EM/CPO involved establishing peer networks and conducting a mission assurance assessment to determine protection needs for the CATC. The first step was to reach out to the emergency managers at other bases in the Kanto Planes: Camp Zama, Atsugi Naval Airfield, Yokota Air Base, and Yokosuka Naval Station. If one of the bases faced an emergency, they may need assistance from the other installations. If one of their EOCs was activated, the EM/CPO would stand up the CATC's EOC as well. Networking also involved reaching out to fellow emergency managers and CPOs aboard Marine Corps Base Okinawa and asking the base fire chief, who was bilingual, to accompany when visiting the base fire department at the Takigahara Garrison, which was located literally across the street from the CATC.

The other key challenge for the EM/CPO was to protect the CATC from radiological threats as well as to be able to assist the host nation, Japan, respond to and mitigate a radiological threat, should leaders ask for assistance. The U.S. Marines assigned to the CATC helped during operation Tomodachi following the earthquake and tsunami in 2011 and the goal was for the CATC to be ready to respond if Japan needed help again. A combination of training, equipment, and exercises were used to accomplish this goal.

Established Practices

Prior to arrival of the EM/CPO, there was not a consistent emergency management presence aboard the CATC for a variety of reasons. The commanding officer and the other stakeholders – explosive ordnance disposal (EOD) officer, provost marshal (similarly to a civilian chief of police), safety officer, and base fire chief – were not used to working with a proactive emergency manager. The installation emergency management plan was outdated and had not been exercised regularly.

Every military base has a cache of CBRNE equipment including bomb suits, atmospheric meters and monitors, chemical protective outer garments, respiratory protection, and CWA detectors assigned to it based on the threats identified in its hazard and vulnerability assessment. However, in the CATC's case in 2015, its cache of CBRNE equipment was stationary, nicely stored on shelves. After the EM/CPO had time to assess the situation and meet with stakeholders, a plan was established to issue out the CBRNE equipment to better protect

the CATC. The equipment was assigned to specific personnel who were responsible for training on it and maintaining it to ensure it was ready at all times.

New Practices

Because the security forces are the primary deterrent for CBRNE threats, they were issued personal handheld radiation detectors to be worn while on duty. If the handheld detectors alarm, the base fire department would respond and utilize several different radiation detectors to confirm (or deny) the initial radiation alarm and identify specific radioactive isotopes. If further analysis were needed, the CPO, the safety officer, and the EOD officer would determine the best course of action. The EOD unit assigned to the CATC were already issued the regular suite of radiation detectors as well as the established reach-back capabilities to request further analysis, personnel, and assets to respond to and mitigate any radiological threat. Fixed radiation detectors were also placed at the entry control points to screen vehicles and personnel entering and leaving the CATC.



Source: fuji.marines.mil

Coordinating with Marine Corps Installation Command, a semi-annual schedule was established for its Regional CBRNE Equipment Training Team to visit the CATC. Its cadre of instructors provided the security forces (both U.S. and local Japanese) 40 hours of CBRNE training, which included interactive, classroom lectures, hands-on practice with the CBRNE meters, monitors, and detectors, as well as functional exercises. It was important for the CPO to be present during the classes and help design the exercises. Because they taught both U.S. Marines and local nationals, an interpreter also accompanied the Regional CBRNE Equipment Training Team.

Monthly exercises – both tabletop and functional – were established to include radiological threats, like radiological dispersal devices. The EOD unit served as a “red cell” and helped create realistic, safe, and functional exercises to test and evaluate the CATC’s response to all-hazards threats, like suspect mail received in the mailroom. With the support of Marine Corps Installation Command and a newly established network, there was buy-in from the commanding officer and other stakeholders to mature the emergency management plan and heighten the security posture of the CATC in Fuji.

The CATC Since 2015

Since departing in 2015, the changes made are still in place. Fortunately, the succeeding CPO from Marine Corps Base Okinawa continues to evolve the program. The lessons learned from this were to establish a network of peers and empower first responders by equipping and training them.

In 2015, Ian Pleet served as the installation emergency manager and CBRNE protection officer for the U.S. Marine Corps Combined Arms Training Center (CATC) Camp Fuji, Japan. Since his return from Japan, he has been accepted into the EMI’s Emergency Manager Basic Academy train-the-trainer course and looks forward to sharing his experiences with the next generation of emergency managers. He currently works as an emergency manager for the U.S. Department of Defense and is contract CBRN Operations instructor for the State Department’s Global Antiterrorism Assistance (GATA) Program.

A Race Against Time: Canine/Handler Teams Prep for Disaster

By Omar Bourne

New York City has various disaster preparedness teams that are specially equipped to manage many types of threats. One such team involves canines trained to perform search and rescue tasks. Canines have helped save lives at critical times following disasters such as 9/11, when finding survivors among rubble and debris is especially challenging. A Dutch Shepherd named Diesel is one responder who currently works with New York City Police Department to prepare for the next disaster.



Canine certification is important to the emergency management field. According to the Federal Emergency Management Agency (FEMA), all of the 28 FEMA Urban Search and Rescue (US&R) task forces have canine/handler teams trained in urban search and rescue strategies and tactics. Each canine/handler team undergoes a rigorous certification and must re-certify every three years in order to participate in search and rescue operations.

“Our certification process assesses skills that we have found to be necessary to do this job. While there is no training or test that can truly replicate a deployment, we have found that a team that successfully completes the certification process is successful on deployment,” said Teresa MacPherson, former chair of FEMA’s Canine Work Group, on 3 May 2018. “For example, we cannot train on trapped infants among thousands of deceased bodies, yet the dogs were able to find babies among the death and destruction in Haiti (earthquake 2010).”

According to FEMA guidelines, the [canine certification](#) “includes proper command control, agility skills, a focused bark alert to indicate a live find, and a willingness to persist to search for live victims in spite of possible extreme temperatures and animal, food, and noise distractions.... The team tests on two large rubble piles for an unknown number of victims, implementing all of their knowledge, skills, and abilities acquired from years of training.” The canine must be at least 18 months old to attempt the test.



Fig. 1. NY-TF1 canine searches for live victims during a recent certification examination at the NY-TF1 US&R Canine Training Facility in Staten Island, New York (Source: NYC Emergency Management, 2018).

“Ours is a specialized job and it takes a very special dog to do it,” MacPherson said. “There is an extremely small percentage of dogs that are born with the right stuff. The rest is up to us – the training.”

“Training is key,” said Neal Campbell, New York City Police Department (NYPD) detective and canine search specialist, and Diesel’s handler, on 30 April 2018. “From the day you get certified as a search and rescue dog, your training has to be kept up. This is a perishable skill. If you do not use it, you lose it. You have to keep that dog hungry for that game. The reality is what he is doing is a game. He is playing canine hide and seek. We are telling him to go and play hide and seek, and when he finds somebody hiding, we tell him that he did a good job. You have to practice the way you play.”

Beep! The long blare of the facilitator’s horn interrupts the morning silence. Diesel, a Dutch Shepherd, scampers up the massive debris pile. He scurries from end to end, ears flapping in the wind on this brisk spring morning. Every second counts, and though no real lives are currently in danger, today is a certification examination, Diesel continues his desperate search for any scent or sign of life, knowing that one day real lives will be counting on these next few seconds.

Diesel darts toward the middle of the pile, abruptly stopping on top of a gargantuan block of concrete. He slowly circles his spot, strategically sniffing with each step. He halts again, this time standing erect, letting out four loud barks in the direction of Neal, his handler. Neal meets him on the pile, “good boy, good boy,” he cheers, while rubbing Diesel’s chin and stomach. Neal takes a piece of red tape from his pocket, marking the spot where the victim was located. He then sends Diesel back off into the rubble, in a race against time, knowing that one day, Diesel wouldn’t be chasing a certification – he would be racing to save a life.

Practice What Is Played

The New York City Emergency Management Department manages the team that is composed of specially trained personnel from the Fire Department of New York (FDNY) and the NYPD. US&R teams were established as a response system to natural disasters, but their roles have expanded. The team deployed in response to the 1995 Oklahoma City bombing, the Atlanta and Salt Lake City Olympic Games, the 1997 presidential inauguration, and the 2001 attacks on the World Trade Center. During 9/11, New York-Task Force 1 (NY-TF1) canine/handler teams worked for seven months, digging through mangled steel frames and concrete, searching for any trace of life.

The NY-TF1 canine training facility is located at the Fresh Kills Landfill in Staten Island New York, housed on the property of the city’s Department of Sanitation (DSNY). DSNY teamed up with FDNY, NYPD, and NYC Emergency Management nine years ago to construct two massive rubble piles used to conduct the canine trainings and certifications. These piles simulate a real-life structural collapse or disaster scene. They consist of reinforced concrete, structural steel, rebar, ads pipe, precast concrete, vehicles, and wood structures. To obtain the highest certification for their canine/handler teams, the NY-TF1 team uses the rubble piles to test in a limited access and full access environment to simulate a disaster.



Fig. 2. NY-TF1 Canine/handler team search for live victims during a recent certification examination at the NY-TF1 US&R Canine Training Facility in Staten Island, New York (Source: NYC Emergency Management, 2018).

“We recently changed our piles to offer the canines a search area offering more options to hide live human scent (people) in different scenarios,” NYPD Detective and NY-TF1 Canine Team Manager Scott Mateyaschuk said on 2 May 2018. “This process takes approximately 2 to 3 months with heavy equipment. During the certification exam, the canine team has 20 minutes to conduct a search one pile at a time, with a 10-minute travel and break before the next search. The handlers have no idea of the amount of victims buried in the pile, so the evaluators can give a blind assessment.”

Limited Access Vs. Full Access Sites

The limited access site tests the canine’s ability to work independently – outside the view of the handler. The handler can only access a limited access site after the canine indicates it has located the first victim. The signal – the canine must bark at least three times, making sure to stay with the victim until the handler arrives. Once the canine indicates the presence of live human scent, the handler rewards the canine, marks the victim location with a piece of tape, and deploys the canine in search of additional victims.

During a full access site test, the handler and canine are working together to locate victims. The NY-TF1 canine team trains continually. FEMA mandates that all certified canine teams train 16 hours per month, and NY-TF1 travels the country to practice on different rubble piles and disaster environments. During the 2017 Atlantic hurricane season, NY-TF1 deployed for search and rescue efforts in Texas and Puerto Rico. Their extensive training prepares them for their work in any environment.

“Our motto is: Don’t let the first time be the first time,” Mateyaschuk said. “I am very fortunate to have a group of dedicated men, women, and canines who share the same passion for this work that I do. I could not do this without them.”

Omar Bourne is the deputy press secretary at the New York City Emergency Management Department. He has responded to various disasters and emergencies in New York City, including the East Village building collapse 2015, a number of winter storms, and preparations for Hurricanes Joaquin, Matthew, and Jose, and Tropical Storm Hermine. He recently deployed to assist in the response efforts in Puerto Rico. As deputy press secretary, he assists the press secretary in day-to-day press operations and serves as one of the agency’s spokespersons, helping to develop and distribute information to the news media. He has spearheaded the creation of New York City’s emergency management podcast “[Prep Talk](#)” and serves as a writer and co-host for the show. Prior to joining NYC Emergency Management, he worked as an assignment editor at Fox 5 News WNYW.



What are you using
for **Overhaul?**



ChemPro100i Chemical Detector

Welcome to visit us!

Hilton Baltimore **Baltimore, MD** 7th - 10th Jun
Booth 503 together with our **Master Distributor in US**



International **Hazardous Materials** Response Teams Conference **2018**

For further information visit www.environicsusa.com

White Paper: Orthogonal Detection Can Help Save Firefighters Lives in the Overhaul Stage of Operations

Building materials, furnishings, paints, plastics, and electronics found in today's buildings have the potential to burn or decompose into acutely and chronically acting toxic gases and vapors. Studies have validated that toxic gases and vapors are not just present during suppression activities but also during the overhaul and investigation stages. The impact can be life threatening.

What Is the Overhaul Stage of Firefighting

Overhaul is the stage of firefighting when firefighters check for the presence of fire in both precontrol and postcontrol phases. Because of the lack of visible fire and smoke during this stage, firefighters are likely to remove Self Contained Breathing Apparatus (SCBA) and work "barefaced." The overhaul stage formerly was considered less toxic than suppression activities. However, the increased use of plastics as a construction material has increased the likelihood of complex inorganics toxic gases not detected by Carbon Monoxide (CO) and Hydrogen Cyanide (HCN) detectors.

Orthogonal Detection Can Provide More Complete Protection From Toxic Gases and Vapors

Building materials, furnishings, paints, plastics and the electronics used in today's buildings have the potential to burn or decompose into acutely and chronically acting toxic gases and vapors. Studies have validated that toxic gases and vapors are not just present during suppression activities but also during the overhaul and investigation stages. Many potentially toxic and carcinogenic gas and vapors can or will be present during the overhaul process. They include but are definitively not limited: Carbon Monoxide (CO), Hydrogen Cyanide (HCN), oxides of Nitrogen (NO and NO₂), Sulfur Dioxide (SO₂), Polycyclic Aromatic Hydrocarbons (PAHs), Aldehydes (like Formaldehyde), acids (like HCl), aromatics (like benzene) and Phosgene (from the thermal decomposition of refrigerants). Even a small kitchen fire can off-gas many toxic vapors from pots and pans when Teflon thermally decomposes including PFIB (perfluoroisobutane, similar to a chemical warfare agent) and HF (hydrofluoric acid).


CO and HCN Cannot Work as "Canaries"

Standard CO detectors have been used to indicate the presence of toxic gases. However, there is no significant correlation between CO levels and levels of other chemicals that may be present during overhaul. Electrochemical cells used to measure CO are also prone to give inaccurate readings in the presence of interferants or high humidity.

The Value of an "Orthogonal" Solution

"Orthogonal" is used to characterize vapor detectors that use multiple, non-redundant sensors to solve a detection problem. The Environics ChemPro100i is an orthogonal detector. The primary sensor is an open-loop Ion Mobility Spectroscopy (IMS) sensor. It uses data from the IMS sensor with additional sensors and computer "fuzzy logic" to classify chemicals. The ChemPro100i orthogonal system has the proven ability to give a warning for more threatening chemicals in the overhaul environment than any other handheld detection





technology. The ChemPro100i also does not have the calibration and sensor replacement costs that are associated with CO, HCN or similar sensors. The ChemPro100i also comes with a 5-year Guaranteed Cost of Ownership (GCO) program. Normal maintenance costs are completely covered for the first 5 years of ownership. The ChemPro100i represents a more systematic approach to monitoring the overhaul process for toxic gases and vapors. If a toxic gas or vapor is present, it alerts to “mask up” and defeats the desire to remove SCBA.



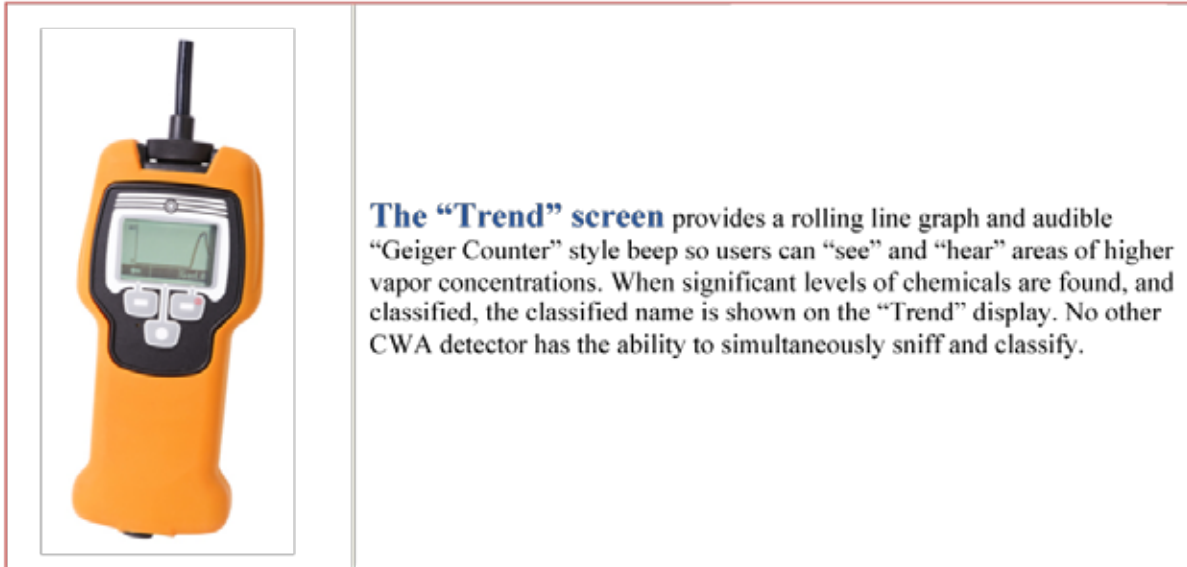
The ChemPro100i is a “PID on Steroids”. With its 60,000-eV ionization energy it allows detection of hundreds of dangerous chemicals and then sorts the ions, instead of counting them like a PID. Therefore, the ChemPro 100i is ideally suitable in Overhaul situations to warn the presence of dangerous gases. The detection technology is based on orthogonal sensors with a 16 channel IMS, 2 MOS and atmospheric sensors.

Overhaul Library

The Overhaul library in the ChemPro 100i has two “baskets” of data. “Mask Up” measures 19 of the most common Overhaul chemicals such as Acrolein, Benzene, Formaldehyde, CO, HCN etc. at TWA levels. The other “basket” is a generic “Chemical Detected” alarm for when the detector’s orthogonal sensors record a potentially dangerous chemical that is not in the “Mask Up” group. “Chemical Detected” covers hundreds of toxic chemicals, thus providing an extensive, additional, level of safety for the user.

What the ChemPro100i Tells You			What the ChemPro100i is Detecting	
Text/Icon	Audio	Visible	Chemicals	Alarm Limit ppm
Mask Up 		Red LEDs	Acetaldehyde (CH ₃ CHO)	Detectable mostly at TWA Levels
			Acrolein (C ₃ H ₄ O)	
			Acrylonitrile (C ₃ H ₃ N)	
			Ammonia (NH ₃)	
			Benzene (C ₆ H ₆)	
			Carbon monoxide (CO)	
			Formaldehyde (CH ₂ O)	
			Formic acid (CH ₂ O ₂)	
			Glutaraldehyde (CH ₂ (CH ₂ CHO) ₂)	
			Hydrogen bromide (HBr)	
			Hydrogen chloride (HCl)	
			Hydrogen cyanide (HCN)	
			Hydrogen fluoride (HF)	
			Isocyanates (TDI, MDI)	
			Naphthalene (C ₁₀ H ₈)	
			Nitrogen oxides (NO, NO ₂)	
			Sulphur dioxide (SO ₂)	
			Toluene (C ₆ H ₅ CH ₃)	
			Vinyl chloride (H ₂ C.CHCl)	
Chemical Detected 		Red LEDs	Generic alarm for chemicals in hazardous concentrations or chemical mixtures	

The Overhaul library provides a “Mask Up” (above Table) prompt for personnel to put on their self-contained breathing apparatus (SCBA). It is not meant for chemical classification. Advanced users may obtain additional information about the atmosphere by using the “TIC-Classifier” or “TIC Confirm” libraries.



Radiation Detector (RAD) Module and Other Accessories

The RAD module brings additional capability to the ChemPro 100i– it permits measuring hazardous gamma radiation at the same time as vapor monitoring. The ChemPro100i also can use a handy “Sampling Cap” that allows for collecting an air sample. The Sample Cap fills a Tedlar bag using the ChemPro air inlet.



About Us & ChemPro100i

ChemPro 100i is a product of Environics, fielded in more than 50 countries and widely used among Hazmat teams in the US and Canada. Environics has been present in the US since 1988 and now is represented by Gases101 LLC, Round Rock Texas. Please contact us for further information.

Master Distributor in the US
Gases 101 LLC
sales@gases101.com
1107 Wonder Dr, Round Rock
TX 78681
+1-512-436-8923

Environics Oy
Timo Jaakkola
timo.jaakkola@environicsusa.com
Sammonkatu 12
50100 Mikkeli – Finland
US Cell +1-443-703-8008

References

Dawn M. Bolstad-Johnson, Jefferey L. Burgess, Clifton D. Crutchfield, Steve Storment, Richard Gerkin, & Jeffrey R. Wilson, "Characterization of firefighter exposures during fire overhaul." AIHA Journal 9-10/2000, pp. 636-641.

Michael Donahue, "Occupational safety and health programs for fire investigators," Fire Engineering, 2/2001.

F.D.J.R. Feunekes, F.J. Jongeneelen, H. v.d. Laan, & F.H.G. Schoonhof, "Uptake of polycyclic aromatic hydrocarbons amount trainers in a fire-fighting training facility," AIHA Journal, 1/1997, pp. 23-27.

John R. Hall, "Whatever happened to combustion toxicity," NFPA Journal, 11-12/1996, pp. 90-101.

Gregory Kinnes & Greg Hine, "Health Hazard Evaluation Report 96-0171 Bureau of Alcohol, Tobacco, and Firearms," 11/1997.

Dennis L. Rogers, "Characterization of fire investigator's exposure during fire scene examination," DuPage County Arson Task Force, DuPage County, IL, March 18, 2005. Adapted from Chris Wrenn, Application Note 103, Environics USA Inc. 2012.

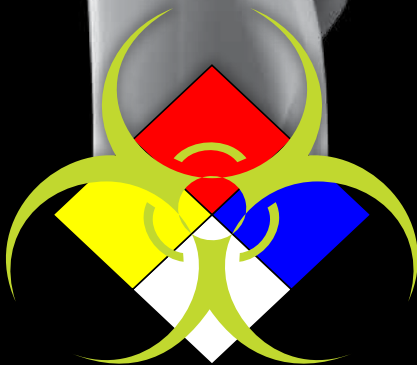
Invisible Threats Exposed



AP4C

**Portable Chemical Detection System
Protects First Responders, Military & Infrastructure**

- Fast, Reliable Analysis of Invisible Hazards Saves Time & Lives
- Unlimited Simultaneous Detection Exposes Unknown Agents
- Low Maintenance & Operation Costs Save Money
- Rugged Handheld Design is Easy-To-Use With Minimal Training
- Complete System Includes Accessories & Case for Easy Transport



[Learn More Online](#)

PROENGINE

Chemical and Biological Detection Systems