Large Transformer Criticality, Threats, and Opportunities

George Baker,[1, 2] Ian Webb,[3] Klaehn Burkes,[4] Joseph Cordaro[5]

[1]Professor Emeritus, James Madison University

[2]Corresponding Author, bakergh@jmu.edu

[3] Research & Development Engineer, Savannah River National Laboratory

[4] Senior Engineer, Savannah River National Laboratory

[5] Laboratory Fellow, Savannah River National Laboratory

[*see author capsule bios below*]

Abstract

Large power transformers (LPTs) represent a critical "tent-pole" in national electric power grid, and national resiliency. They are essential to both the generation and transmission sectors of our electric power grid. They are known to be targets in adversaries' plans to debilitate our critical infrastructures. Their high cost and supply chain issues involving months to years of replacement times dictate the importance of survivability assurance. Transformer vulnerability and protection are addressed for physical attacks, cyber, and electromagnetic effects, including solar weather geomagnetic disturbance (GMD) and high altitude burst nuclear electromagnetic pulse (EMP) effects. Programs have been underway to improve transformer and transformer substation cyber and physical resiliency. Similar programs are lagging for electromagnetic threats. Transformer vulnerability to EMP remains a subject of conjecture since no large power transformer has undergone threat-level EMP testing. Prevalent claims that LPTs are immune to EMP are premature.

The Savannah River National Laboratory has developed a test program and designed a test bed to complete testing on LPTs including physical set-up, injection sources, and measurement equipment to enable transformer testing under real load conditions without harming the larger power grid. The SNRL test bed will enable tests to determine both transformer vulnerability thresholds and the effectiveness of protection devices. A concerted national effort is needed to determine LPT vulnerabilities and to expeditiously develop and certify effective EMP and GMD protection approaches.

Keywords: Large transformers, electric power grid, electromagnetic threats, EMP, GMD, HEMP, grid vulnerabilities

 doi: 10.18278/jcip.2.2.5

Introduction

The demand for electricity continues to expand both in kilowatt hours and the diversity of applications. The electric power grid is the engine that that drives our economy and is essential for our critical services including communication and data networks, financial transactions, transportation, health and emergency services, water, and food supply. The dark side of our growing dependence on electricity is the grid's increasing vulnerability to hackers, physical saboteurs, and high-power electromagnetic debilitation from space weather and nuclear devices.

The electric lines that traverse the landscape are analogous to the blood vessels within our bodies that keep us alive. Continuing this analogy, generator stations function as the heart, providing blood pressure for the system of electric line arteries. In the electricity flow system, at the beginning and end of each electric line supplying the network is an organ needed to match the generator output pressure to the resistance (load) of the rest of the network. Failure of these organs stops the flow of the energy necessary for life and enterprise. If debilitated, these organs become choke points in our electric "circulatory system." These organs are called transformers.

Transformers are known targets of adversaries seeking to harm the nation's life-support infrastructure. They are "single-point failure" components whose debilitation brings down large numbers of other dependent critical infrastructure systems. They are easy targets—transformer yards or "substations" are quite accessible to the public and can be debilitated by objects as simple as a high-power rifle bullet. They are also susceptible to natural disruption from weather, rodents, and solar storms. Of particular concern are large power transformers, or LPTs, that sit at each end of the high voltage lines (analogous to coronary arteries) comprising the electric transmission system.[1] While the U.S. electric grid consists of thousands of transformers, the high voltage transformers make up less than three percent. Nonetheless, they transport 60 to 70 percent of our electricity. The largest of these transformers are the size of a house and weigh hundreds of tons.

LPTs are mostly custom-designed and cost in the range of $2-10M. They take a long time to replace due to custom-manufacturing timelines and special transportation requirements. Procurement delays beyond 20 months are possible. The LPT replacement time has extended up to five years in extreme cases.[2] Should multiple units fail simultaneously, limitations of the existing supply chain capacity would lead to much longer delays in restoring the grid.

The estimated total number of LPTs in the United States ranges into the of

1 The Department of Energy (DOE) defines LPTs as transformers with a maximum capacity power rating greater and or equal to 100 MVA.

2 DOE Office Of Electric Reliability, Large Power Transformers and the U.S. Electric Grid, 2012 Report.

tens of thousands, including LPTs that are located on high voltage (115 - 345 kV) and extra high voltage (> 345 kV) transmission lines. The United States domestic LPT manufacturing can produce high voltage LPTs, but there are no manufacturing facilities in the country that produce extra high voltage (EHV) transformers. The national capacity to meet normal demand for new LPT units is very limited. Therefore, the majority of installed transformers come from overseas. Key industry sources have flagged the limited availability of spare LPTs as a driving issue for critical infrastructure resilience.[3] Some utility companies keep spare transformers on hand. Because of the custom nature and complexity to transport, these spares are normally stored in the same substation as the in-service LPT. The U.S. LPT fleet is aging with an average time in-place of 40 years. Older power transformers exhibit an increased mean time between failures and are more susceptible to damage from transient over-voltages due to lightning, switching transients, ground faults, solar storms, and nuclear electromagnetic pulses.

Discussion

Transformer Threats

Threats to transformers can be grouped into three general categories: physical, cyber, and electromagnetic. Scenarios exist in each category where large portions of the North American electric power grid could fail simultaneously for indefinite periods.

Physical Threats

Transformers are vulnerable to weapons as common as a hunting rifle. Based on comments by former Federal Energy Regulatory Commission (FERC) chair, Jon Wellinghoff, a small number of coordinated physical attacks can shut down the national power grid for months.[4] On April 16, 2013, snipers fired high-power rifles at transformers within the Pacific Gas & Electric Metcalf substation in San Jose, California, severely damaging seventeen transformers.[5] The substation was out of service for 27 days. Wellinghoff described the attack as "the most significant incident of domestic terrorism involving the grid that has ever occurred."[6] In the immediate aftermath of the Metcalf substation attack, three consecutive attacks

3 Industry source documents include the Energy Sector Specific Plan; the National Infrastructure Advisory Council's A Framework for Establishing Critical Infrastructure Resilience Goals; North American Electric Reliability Corporation's Critical Infrastructure Strategic Roadmap.

4 R. Smith, U.S. Risks National Blackout from Small-Scale Attack, *The Wall Street Journal*, 13 Mar 2014.

5 R. Smith, R. Assault on California power station raises alarm on potential for terrorism. *The Wall Street Journal*, 5 February 2014.

6 A. Follet, "Lights out: The top 7 threats to America's power grid," http://dailycallernewsfoundation.org, 10 January 2016.

occurred on Entergy Arkansas substations and transformers during August and September of 2013.[7]

Cyber threats

The cyber defense community is particularly concerned about attacks on critical infrastructures. The electric grid is at the top of the list because it supplies all other infrastructure sectors and features the largest industrial control system in the U.S. Insuring cyber resilience is more challenging because the electric power grid is not self-sufficient. It relies on other infrastructures, notably communication and data networks, for its operation. Thus, the electric power grid is susceptible to debilitation through multiple cyber-attack entry points.

Cyber-attacks on electric power grid infrastructure in other countries have already had serious consequences.[8] According to *The Wall Street Journal*, "the threat to the U.S. electric grids is so serious that … a group of presidential advisers warned that the country needs to prepare for a 'catastrophic power outage' possibly caused by a cyberattack.[9] A 2018 DHS report indicated that hackers working for the Russian government gained access to U.S. electric utility control rooms and had had the ability to trigger blackouts using a cyber-attack tool known as Crash Override malware. As of 2020, it has been estimated that cyber-attacks on industrial control equipment worldwide have caused "more than 1,250 actual … incidents with more than 1,500 deaths and more than $70 Billion in direct damage."[10]

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards require certain utility companies, based on their functional capabilities, to inform the Electricity Information Sharing and Analysis Center (E-ISAC) and the United States National Cybersecurity and Communications Integration Center (NCCIC) of reportable cybersecurity incidents. NERC defines a cyber security incident as a malicious act or suspicious event that compromises or was an attempt to compromise the electronic security perimeter or disrupts or attempts to disrupt operation of a basic cyber asset. However, NERC leaves defining a cybersecurity incident up to the individual utility company. The cyber standards are some of the most violated NERC standards and have resulted in millions of dollars in penalties.[11] Unfortunately, most cyber incidents are not

7 K Melligan, https://www.academia.edu/40393187/The_Vulnerability_of_the_United_States_Electrical_Power_Grid?email_work_card=reading-history; 2019.

8 White House Council of Economic Advisors, The Cost of Malicious Cyber Activity to the U.S. Economy, 2018.

9 Rebecca Smith, The Wall Street Journal (August 5, 2018). See also: Staying wary of cyber-attacks shows vision (8/22/2018), Altoona Mirror.

10 Joe Weiss, Cyber Security of Control Systems – What Needs to be Done, CERIAS Security Seminar, 15 July 2020, Applied Control Systems, LLC.

11 Energy Policy Update: NERC fines utility $2.7 million for cyber breach

reported directly to the public—much effort has been required to access this information.

Transformer cyber vulnerabilities accrue from the grid's dependence on electronic sensors, controllers, and network connectivity. Many transformers have programable logic controlled "tap changers" that are remotely controlled to adjust transformer output voltage in response to changes in user load. These PLCs are networked to allow for a central control room operator to change the physical tap location if needed. Interference with the functioning of these devices can destabilize the grid and cause overheating of transformer coils. In addition, LPTs are connected and disconnected from the grid by high voltage circuit breakers that are also remotely operated through computer controlled protective relays. If these devices are not configured properly, cyber attackers have the ability to open and close high voltage breakers to induce multiple abnormally high-power line voltage spikes capable of damaging transformers.[12]

A recently developing concern stems from the U.S. import of large numbers of transformers from China. These transformers arrive with Chinese-installed sensors and control systems that can provide a cyber "backdoor" into the electric grid control system. The U.S. discovery of backdoor electronics in a Chinese-made transformer contributed to White House Executive Order 13920 that banned "… the acquisition, importation, transfer, or installation" of any bulk-power systems from foreign adversaries.[13] This executive order was cancelled in February 2021.

Electromagnetic Threats

The most common electromagnetic threat to transformers is lightning. Lightning effects on unprotected transformers can be severe.[14] Lightning has caused transformers to explode and ignite fires resulting in collateral physical damage to adjacent substation equipment. Most utilities protect their LPTs against this threat.

Less frequent effects relevant to transformers include abnormally high line currents induced by solar-caused geomagnetic disturbances (GMDs) and nuclear high altitude burst Electromagnetic Pulse (EMP). However, where lightning effects are highly localized, GMD and EMP can debilitate systems and networks over large multi-state regions. The experience with these effects is highly limited since no Carrington-class solar storms or HEMP events have occurred over the North American continent during the relatively short history of an interconnected

12 C. Evanich, Grid Improvements Needed to Prevent Transformer Failures and Power Outages, Electrical Business, April 2019.

13 White House Executive 0rder 13920, https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/, 1 May 2020.

14 Lightning Eliminators, Damages Rise when Substations Don't Invest in Lightning Protection, https://www.lightningprotection.com/damages-rise-when-substations-dont-invest-in-lightning-protection/, August 2012.

North American power grid. The event with the most severe effects on the North American grid to date was a moderate solar storm that occurred in March 1989. This storm shut down the Hydro Quebec grid for 12 hours.[15] The 1989 geomagnetic storm demonstrated that magnetic field intensities of ~300-550 nT/min in the area around the Salem nuclear plant in New Jersey caused permanent damage to two single phase transformers.[16] The peak energy of the 1989 storm geo-electromagnetic fields was roughly 1 percent of a Carrington-class event. A partial compendium of observed transformer problems due to GMD is shown in Table 1.

On July 23, 2014, NASA released a report warning that in July 2012, the Earth narrowly missed a geomagnetic super-storm that could have collapsed electric grids worldwide and risked the lives of billions. NASA estimates that the likelihood of a catastrophic geo-storm incident over the next decade is 12 percent.[17] In 2016, the White House issued an executive order acknowledging that natural EMP from a geomagnetic super-storm could have catastrophic effects to the nation's electric power and communication networks.[18] In 2019, the White house issued a similar executive order to prepare the nation for the effects of a nuclear EMP on critical national infrastructure.[19] Because of transformers' regular exposure to space weather, GMD effects have received considerably more attention from policy, scientific and electric power communities than has EMP. Similarities in system effects argue for addressing both GMD and EMP in a combined fashion.

Past solar storm, atmospheric nuclear tests and simulated GMD and HEMP tests reveal that systems connected to long lines are especially vulnerable to electromagnetic threats because the long transmission lines act as large antennas that allow large electromagnetic fields to couple to them. Transformers are the most important example of these vulnerable systems. The HEMP environment is divided into three time domains: a high amplitude broad band early time E1 waveform, an intermediate time E2 waveform similar in effects to nearby lightning strikes, and a late time E3 waveform similar in spectrum to space weather GMD, but with a considerably greater amplitude and shorter duration.

The E1 and E3 aspects of the EMP waveform couple the most efficiently to long lines and would induce thousands of amperes on overhead transmission and distribution lines.[20] The quasi-DC currents of E3 are very damag-

15 https://www.nasa.gov/topics/earth/features/sun_darkness.html

16 J. Kappenman, An Analysis of the Equipment Vulnerability from Severe Geomagnetic Storms, Storm-R-112, August 2011.

17 https://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm

18 White House Executive Order 13744 – Coordinating Efforts to Prepare the Nation for Space Weather Events, 13 October 2016.

19 White House Executive Order 13865 – Coordinating National Resilience to Electromagnetic Pulses, 26 March 2019.

20 The HEMP E2 field is much lower amplitude than E1 and is nearly vertically polarized such that it doesn't couple efficiently to the horizontal lines of the electric transmission system.

ing to magnetic devices such as transformers and can cause hotspots, thermal runaway, and large amounts of reactive power consumption leading to grid instability. Mitigation of GMD effects on transformers will reduce the effects of the late time (E3) aspect of HEMP. Lightning protection reduces or eliminates HEMP's intermediate time (E2) HEMP effects. However, HEMP E3 levels theoretically approach 100 V/km – peak GMD levels are 3-4 times lower. Note that the 1989 Hydro Quebec grid blackout was the result of a 2 V/km solar storm.

In the case of HEMP, the E3 slow-pulse waveform is preceded by E1 fast-pulse which can pre-emptively debilitate the control systems necessary for isolating transformers and generators from the large follow-on E3 currents in the grid to prevent damage and achieve safe shut-down. Note that solar storm GMD waveforms do not exhibit a high frequency fast-pulse waveform precursor. Thus, protection against geomagnetic storms does not protect against E1 HEMP or guarantee E3 survivability.[21]

Table 1. Partial EMPIRICAL GMD Record: Transformer Problems Due to GMD[22]

Date	Location Name	Category of Impact (transformer, SVC, Generator, Down Rating, Congestion)	Measured GIC (A)	Measured dB/dt (nT/m)	Source Document Reference
March 13, 1989	Maine Yankee	GSU Transformer 345 kV damage; backup GSU request to NRC in 2 wks		574	Resilient Societies Letter to Dean Curtland, 18 June 2015
March 13, 1989	Salem I	SVC and 500 kV transformer - melting of low voltage windings	224	574	NERC filing on 13MAR89 storm
March 13, 1989	Contra Costa	Transformer			
September 19, 1989	Buchanan,	SVC' & 500 kV GSU partial damage 12 Mar 1989; explosion 19 Sep 1989	90		NERC filing on 13MAR89 storm
April 29, 1991	Maine Yankee, Wiscaset, ME	Transformer 345 kV GSU gassing; nighttime explosion 29 Apr 1991		80	Resilient Societies Letter to Dean Curtland, 18 June 2015
March 24, 1994	Waukegon Coal, IL	500 kV GSU transformer fire, during 23 -24 Mar 94 Coronal Hole solar storm, evening			
April 3, 1994	Zion Nuclear Unit 1, IL	500 kV GSU transformer explosiopn during Coronal Hole solar storm, CommEd evening			
April 5, 1994	Braidwood Nuclear	500 kV GSU transformer explosion during Coronal Hole solar storm, evening			
April 13, 1994	Custom Cogeneration	500 kV GSU transformer explosion during Coronal Hole solar storm, evening			
15-Apr-94	Powerton Generating,	500 kV GSU transformer fire during Coronal Hole solar storm, evening			
November 10, 1998	Seabrook Station	CME overtake by 2d event, bolt vibration;345 kV /24kV Phase A transformer windings melt	200		Resilient Societies Letter to Dean Curtland, 18 June 2015
July 15, 2000	Hope Creek	Downrating		300	Letter From William Harris, FRS. NRC ADAMS Database reference #ML12167A289
October 29, 2003	Seabrook Station	SVC	98		Resilient Societies FERC Docket 12-22
October 29, 2003	Point Beach	500 kV GSU transformer fire during CH 64 with CMEs	98		Resilient Societies FERC Docket 12-22
August 17, 2008	Diablo Canyon Unit 2, CA	500 kV GSU transformer fire during Coronal Hole 338 .			Solen (Norwegian) CH database
November 7, 2010	Indian Point Unit 2, NY	345 kV unit 2, GSU transformer explosion 6:39 pm during CH 429; prior MVAR alarms			Exelon contract engr rpt to NRC
December 15, 2015	South Texas Nuclear Unit 2	500 kV GSU transformer fire during Earth impact of Coronal Hole 705			
Date	Location Name	Category of Impact (transformer, SVC, Generator, Down Rating, Congestion)	Measured GIC (A)	Measured dB/dt (nT/m)	Source Document Reference
March 13, 1989	Maine Yankee	GSU Transformer 345 kV damage; backup GSU request to NRC in 2 wks		574	Resilient Societies Letter to Dean Curtland, 18 June 2015
March 13, 1989	Salem I	SVC and 500 kV transformer - melting of low voltage windings	224	574	NERC filing on 13MAR89 storm
March 13, 1989	Contra Costa	Transformer			
September 19, 1989	Buchanan,	SVC' & 500 kV GSU partial damage 12 Mar 1989; explosion 19 Sep 1989	90		NERC filing on 13MAR89 storm
April 29, 1991	Maine Yankee, Wiscaset, ME	Transformer 345 kV GSU gassing; nighttime explosion 29 Apr 1991		80	Resilient Societies Letter to Dean Curtland, 18 June 2015
March 24, 1994	Waukegon Coal, IL	500 kV GSU transformer fire, during 23 -24 Mar 94 Coronal Hole solar storm, evening			

21 Baker, G. Testimony Before the U.S. Senate Committee on Homeland Security and Government Affairs, February 27, 2019.

22 Table compiled by William R. Harris, National Disaster Resilience Council, 2019.

April 3, 1994	Zion Nuclear Unit 1, IL	500 kV GSU transformer explosiopn during Coronal Hole solar storm, CommEd evening			
April 5, 1994	Braidwood Nuclear	500 kV GSU transformer explosion during Coronal Hole solar storm, evening			
April 13, 1994	Custom Cogeneration	500 kV GSU transformer explosion during Coronal Hole solar storm, evening			
15-Apr-94	Powerton Generating,	500 kV GSU transformer fire during Coronal Hole solar storm, evening			
November 10, 1998	Seabrook Station	CME overtake by 2d event, bolt vibration;345 kV /24kV Phase A transformer windings melt	200		Resilient Societies Letter to Dean Curtland, 18 June 2015
July 15, 2000	Hope Creek	Downrating		300	Letter From William Harris, FRS. NRC ADAMS Database reference #ML12167A289
October 29, 2003	Seabrook Station	SVC	98		Resilient Societies FERC Docket 12-22
October 29, 2003	Point Beach	500 kV GSU transformer fire during CH 64 with CMEs	98		Resilient Societies FERC Docket 12-22
August 17, 2008	Diablo Canyon Unit 2, CA	500 kV GSU transformer fire during Coronal Hole 338 .			Solen (Norwegian) CH database
November 7, 2010	Indian Point Unit 2, NY	345 kV unit 2, GSU transformer explosion 6:39 pm during CH 429; prior MVAR alarms			Exelon contract engr rpt to NRC
December 15, 2015	South Texas Nuclear Unit 2	500 kV GSU transformer fire during Earth impact of Coronal Hole 705			

There are four possible EMP/GMD-caused effects on transformers. The consequences of these effects can be temporary or permanent and affect the transformers themselves, elements of the surrounding grid, control systems, and customer loads.

A. Transformer line harmonics and reactive power consumption caused by transformer core saturation from HEMP-E3 and GMD quasi-DC current distortion of the normal 60Hz sine wave current. Line harmonics effects can be permanent but are most often temporary including tripped breakers, upset of communication and control electronics, and lock up of uninterruptable power supply units. The associated line harmonics and reactive power consumption can cause frequency and voltage instability that lead to blackouts throughout a large geographical area and cause damage to generators and power plants. Transformer line harmonics in some cases have damaged facility uninterruptable power supplies (UPS).

B. Transformer overheating caused by HEMP-E3 and GMD quasi-DC core saturation. Quasi-DC transformer overheating effects can cause immediate damage or delayed, cumulative damage. Effects are manifest as distortion/warping of transformer windings and/or hotspots in transformer structural elements.

C. Transformer voltage breakdown effects caused by EMP-E1 fast transients. Voltage breakdown effects are permanent in case of insulation pin holes and can be catastrophic if grid power flows through breakdown electrical arc paths ("power follow" effect).

D. Transformer cooling control system failures due to EMP-E1 effects on electronics. E1 debilitation of electronic cooling controls cause overheating of transformers and/or tripping of generators in some installations.

Transformer Protection Strategies

Cyber Protection

A new paradigm is needed for effective cyber protection of transformers. In the past, the personnel who operate heavy duty equipment such as machinery, circuit breakers and transformers have not been involved in the cyber protection process. Sensors are essential for monitoring and control of such equipment by measuring and providing data on the operational status or "state" of the controlled systems. These sensors and their data feed links are principal targets of cyber-attacks. The historic approach has been to delegate cyber security to network personnel unfamiliar with heavy duty equipment operation and control systems. Unfortunately, trying to solve grid cyber vulnerability from a network point of view has proved ineffective. The new paradigm must start at the frontline equipment "edge" by protecting the monitoring and control sensors themselves. It is important to involve equipment control experts because many of the sensors were manufactured years before cyber security was a problem. Sensors must be continuously surveilled in real time and off-line to detect any process anomalies.[23] Sensor surveillance schemes must be able to detect abnormal and unexpected changes in "set points" (temperature, pressure, voltage thresholds where operation becomes unsafe) and equipment operational states. Sensor monitoring communication links should employ high security optical fiber rather than radio, microwave, or Wi-Fi (use of nonconducting optical fiber assists with EMP/GMD immunity as well).

Sensor monitoring schemes should be integrated with operational technology (OT) network monitoring. It is important to avoid storing monitoring and data on the cloud. Technologies for monitoring control sensors in electrical systems are now only at the "proof of concept" stage. Comprehensive cyber protection of industrial control systems will also require corporate oversight by including operational executives as part of cyber security policy development and providing cyber and OT network training for control system engineers.[24]

Physical Protection

Physical attack protection of transformers and substations is challenging but straightforward, involving well known and tested techniques. In 2014, NERC established a physical security risk assessment standard for transmission stations and substations, CIP-014-1.[25] Note that this document does not specify protection engineering methods or requirements.

---

23 J. Funk, Electrical Grid, Power Plants, Pipelines Vulnerable to Cyber Attack: Interview with Joe Weiss, The Plain Dealer, October 2018.

24 J. Weiss, personal email communication.

25 https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-1.pdf

The Institute for Electrical and Electronic Engineers (IEEE) issued a new edition substation physical protection engineering guide, IEEE 1402-2021 in September 2021.[26] The IEEE guideline addresses threats that include unauthorized access to substation facilities, theft of material, and vandalism. The guide provides design options for positive access control, monitoring of facilities, and delay/deter features. Hopefully, this guide, although not mandatory, will become widely used by electric utilities for retrofitting existing substation protection engineering and the design of new substations.

Electromagnetic Protection

Transformer lightning protection is a mature engineering discipline. Air terminals on overhead structures are installed to divert lightning strikes away from transformers. Lightning currents induced on lines connected to transformers are diverted to ground using surge arrestors that include spark gaps and solid-state metal oxide varistors.

Lightning arrestors in general are not designed to react quickly enough to arrest the E1 portion of a HEMP waveform—special devices are needed. Test programs to date have addressed only small distribution transformers but reveal that transformers can be damaged by E1. The damage observed was caused by dielectric breakdown within the windings that resulted in insulation perforations. Damage mechanisms included turn-to-turn failures, line-to line failures, and primary-to-secondary winding failures.27 There has been speculation that E1 is not a problem for higher voltage LPTs due to their normal high voltage handling capability. E1 modeling predicts peak levels of megavolts on some lines. Testing is needed to certify whether LPT E1 immunity is real. Until testing occurs, LPT E1 immunity cannot be assumed.

The proceedings of a 2011 NERC GMD workshop identified three methods for eliminating ground induced currents (GIC) from both solar GMD and E3:

a. eliminating one of the neutral ground connections at one end of the transmission line,

b. inserting series compensation into the transmission line, or

c. using a blocking capacitor on the neutral-ground connection[28, 29]

26 IEEE Approved Draft Guide for Physical Security of Electric Power Substations, IEEE 1402-2021; 23 September 2021.

27 E. Savage, J. Gilbert, W. Radasky, The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid, Meta-R-320, 2010.

28 NERC, "Geo-Magnetic Disturbances (GMD): Monitoring, Mitigation, and Next Steps," Atlanta GA, 2011

29 EPRI, "Monitoring and Mitigation of Geomagnetically Induced Currents," December 2008.

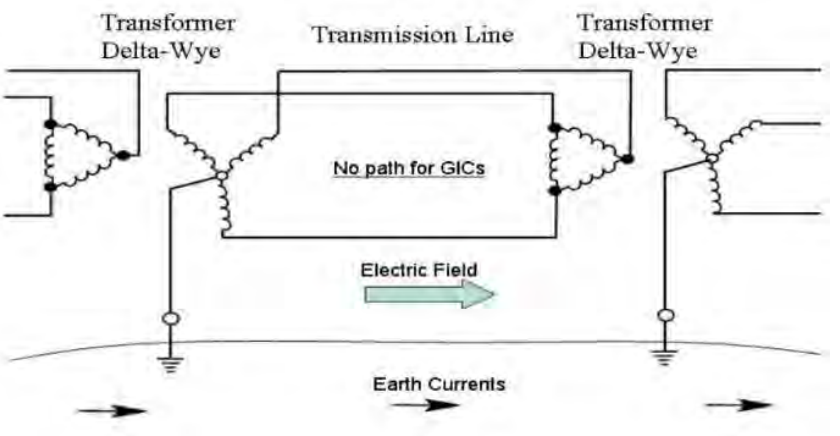

Figure 1. Removing Ground from Transmission Line[20]

Removal of the neutral ground connection (Figure 1) creates more serious issues than it resolves because the neutral ground connection is needed for fault protection, which is a more likely and more serious event. Also, the majority of EHV LPT are autotransformers, which cannot be designed in a delta connection and require neutral grounded to limit over-voltage problems.[30] Finally, this protection approach makes design of the interconnected transmission system more difficult because of the phase shift from a delta wye transformer requires more coordination and engineering to keep phasing consistent between interconnections.

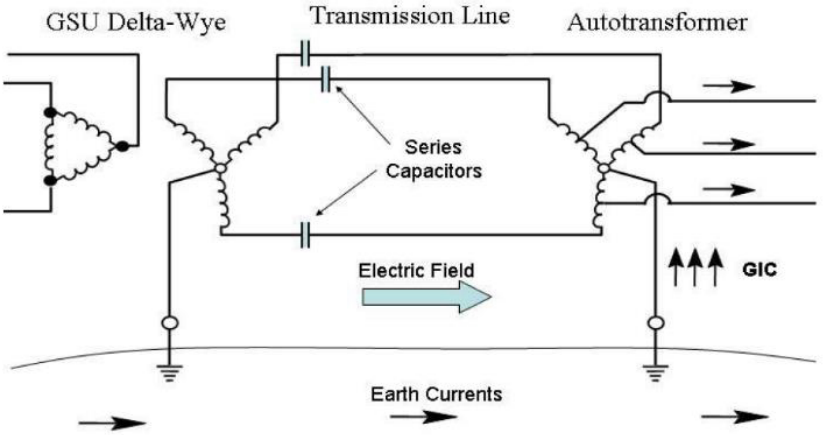

Figure 2. Series Capacitor Method to Block GIC [20]

Series capacitor compensation (Figure 2) under quasi-DC currents operates as an open circuit and can be used for blocking GIC. This approach is mainly employed to help with power flow control and is one of the Flexible AC Transmis-

30 R. Girgis and K. Vedante, Writers, *Effect of GIC on Power Transformers & Power systems.* [Performance]. ABB Power Transformers, PSRC Meeting May 14, 2014.

sion System (FACTS) methods. However, this method is not widely implemented because of cost. These capacitors also take up a large amount of substation real-estate. Series capacitors also produce issues with line impedance, load impedance, and system stability from resonance issues.[10] Nonetheless, this method is widely used by the Western Electricity Coordinating Council (WECC) which uses series capacitors on about 55% of its 500-kV lines. However, studies have shown that its reduction of GIC is between 12-22 percent.[31] Therefore, these devices must be implemented more widely throughout the network to fully protect from GIC.

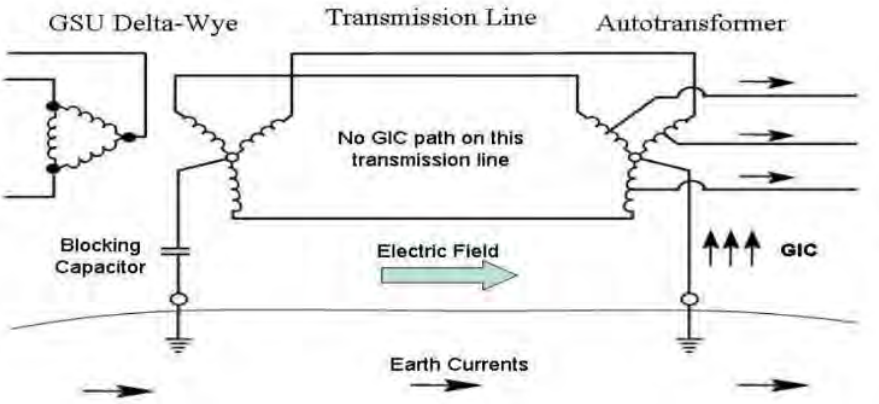

Figure 3. Blocking Capacitor Implementation[20]

Similar to the series compensation method, a transformer neutral blocking capacitor has been proposed to eliminate geomagnetically induced current (GIC) from the transmission line (Figure 3). An advantage of this scheme is that the capacitor does not need to be capable of supporting the full transmission voltage. However, just as with series compensation, every neutral will require a blocking device to fully eliminate GIC. Also, the devices are not inexpensive because they must be utility grade and designed to handle fault currents. Furthermore, studies by the Electric Power Research Institute (EPRI) on the reliability of these types of devices in surviving typical operating conditions of the power system concluded that they did not survive many fault scenarios.[32] Also, researchers believe that these devices would bring considerable uncertainty and integration would introduce a risk from impedance changes. Finally, they may cause ferro-resonance instabilities in the power system.[32]

Improved transformer designs hold partial promise for eliminating GMD/EMP vulnerabilities. For example, ABB consulting services has developed and par-

31 J. Kappenman, "Low-Frequency Protection Concepts for the Electric Power Grid: Geomagnetically Induced Current (GIC) and E3 HEMP Mitigation," Metatech Corporation, Goleta, CA, January 2010.

32 EPRI, "Geomagnetic Disturbance (GMD) Neutral Blocking Device Analysis," Electric Power Research Institute, Palo Alto, CA, April 2014.

tially tested improved LPT designs that demonstrate much higher levels of GMD induced currents. Grid resilience would be markedly improved if these designs are intentionally selected in new transformer installations. Note that these improved designs have yet to be tested to maximum Carrington-class GMD and HEMP E1/E3 currents. Even if more robust transformers are installed in new builds, because transformer lifecycles are 40–50 years, there will continue to be a large population of existing transformers that remain vulnerable. It is problematic that no industry "GIC-withstand" design or acceptance standard has been adopted.[33]

Importance of Testing

The need to protect transformers against cyber and physical threats is clear since these attack modes have been used in prior grid attacks. Substantive past and ongoing programs exist which have tested or are testing the efficacy of cyber and physical protection. Similar attention is lagging for electromagnetic threats to transformers. A concerted testing effort to determine the vulnerability or invulnerability of LPTs to peak GMD and HEMP currents has not occurred, much less grid-scale field testing to certify the effectiveness of proposed protection engineering solutions. Consequently, this section will focus on recommended testing for electromagnetic effects protection solutions.

Some analytical assessment GMD effects on transformers has occurred. For example, the American Electric Power Company (AEP) requires transformer manufacturers to show, *by calculations*, that when a candidate transformer is subjected to six 5-minute on/5-minute off cycles of 120 A/phase DC in the common and series windings, the transformer would not exceed specified transformer oil gassing values. These GMD current levels correspond to geomagnetic electric field strength in the range of 4 ~ 5 V/km.[34] However, GMD levels can reach 20-30 V/km which scale to 500-900 A/phase current levels. EMP-E3 reaches levels with a reasonable bound of 80 V/km, scaling to test levels of 2500 ~ 3000 A/phase. Clearly, analytical assessment values are inadequate for known threat values. Testing is needed to for reasonable confidence in transformer resilience.

Despite the absence of threat-level LPT test data, there have been strong assertions that GMD and HEMP effects on LPTs will be minimal to non-existent. These assertions are contradicted by DOD comparisons of systems' effects under threat-level tests with prior analytical system effects predictions. DOD found that methods used to predict EM effects in specific systems that are based on pure analysis and/or extrapolated low-level test results are not reliable. Furthermore, DOD determined that reliable results on probability of system effects requires threat-level testing on the specific system or system components of interest. Top

33 J. Kappenman, Op. Cit.

34 D. Ball, Q. Qiu, R. Girgis, & K. Vedante; Effect of GIC and GIC Capability of EHV Power Transformers – A Case Study on an AEP 765 kV Power Transformer Design; CIGRE US National Committee, 2013 Grid of the Future Symposium.

national analysts found that HEMP effects depend on fine, often trivial, details of system construction which are not obvious from drawings and specs and thus difficult to model. Some details such as parasitic capacitance and inductance effects and high voltage breakdown or hot spot locations defy the best available modeling techniques even when as-built engineering drawings are available since these details do not influence normal system operation. The bottom line is that system assessments based on paper studies, visual inspection, exact replication of circuit schematics, and even low-level testing are not reliable: analysts predicted failures where none occurred and predicted system survivability where failures occurred.

DOD test experience shows that both HEMP damage and upset occur in a high proportion of objects tested exhibiting a wide variation in environment thresholds. Observed damage and upset effects were highly repeatable for individual systems tested. Although effects are most pronounced for modern electronics, heavy duty components such as transformers are susceptible to damage, especially when energized. The DOD's findings have important implications for transformer effects predictions and testing, namely:

- Transformer vulnerability assessments using analysis that is based on system design drawings or analysis extrapolating low-level stress tests are not reliable.
- Decisions on whether protection is required should not rely on analytical assessments and/or low-level test-based assessments.
- Threat-level testing of transformers under normal operating conditions and load is necessary to ascertain survivability.
- To optimize the use of available test objects, HEMP and GMD testing should start at low levels and step up gradually, up to threat level, if necessary, to identify threshold and location of system failure. If signs of impending failure are discernable, stop tests and record vulnerability threshold.
- Similar testing is required to ascertain the absence of effects on systems with protective measures installed.

In the absence of threat level test results, statements about the vulnerability or invulnerability of LPTs is highly speculative. We have not developed the necessary EMP threat-level effects test data base on LPTs to rule out HEMP/GMD effects. EMP threat level testing of transformers has been limited to small distribution units.[35] Several recent analytical studies and low-level tests have yielded optimistic survivability prognostics, but as previously explained, experience dictates that conclusions on HEMP/GMD immunity based on analysis and low-level test-

35 E. Savage, J. Gilbert, and W. Radasky, "The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and its Impact on the U.S. Power Grid," (Metatech Corporation) Oak Ridge National Laboratory, Tennessee, January 2010.

ing are not reliable. While it would be wonderful if these systems are unaffected by HEMP and major solar storms, we cannot, at present, make that assumption. Unfortunately, some senior officials in government and industry have accepted and openly endorsed these analytical predictions as conclusive. If analytical studies that predict transformer EMP immunity prove to be incorrect, because of considerable replacement transformer procurement lead times, national recovery periods would be extended from an estimated 30 day minimum to in excess of one year.

Recommended test program

Based on the vulnerabilities stated above and the DoD requirements to test at threat level, several organizations have tested smaller distribution transformers by injecting quasi-DC currents. These tests were done to understand the effects of DC and determine scalability to LPTs. However, each one of these tests, when extrapolated, indicated that testing of grid-connected LPTs at threat level would risk major problems (related to the four effects categories previously discussed) on the larger grid. To overcome this problem, Savannah River National Laboratory (SRNL) has designed a testbed to decouple the LPT under test from the power grid that enables testing transformers under normal load and operational conditions without the risk of grid failure. This test-bed concept allows testing LPTs at threat levels, enabling realistic determination of transformer failure mechanisms and certification of protection designs. Instructive examples of past test results are provided in the next two sections.

Oak Ridge Testing of Quasi-DC Effect on Distribution Transformers[36]

Reactive power draw and harmonics are known to be primary failure mechanisms for the electric power grid. During the early 1990s Oak Ridge National Laboratory (ORNL) tested the effect of Quasi-DC currents on three-phase distribution transformers. The project's objectives were to determine the effect of quasi-DC currents on the operation of three-phase transformer banks, measure voltage and current harmonics within the system and at the loads, assess the importance of the quasi-DC current duration, determine the change in reactive power demand as a function of the quasi-DC current, and determine if low level quasi-DC currents and the distorted AC current can cause primary fuses to blow. The results show that GICs can cause a dramatic increase in reactive power draw and very high current harmonics with large distortions of the current waveforms, with the harmonics generated being transmitted through the transformer to the load and, most likely, to the generation source. Figure 4 graphs the difference in the current absorbed by a transformer under test during normal conditions (left graph) and

36 B. W. McConnell, P. R. Barnes, F. M. Tesche, and D. A. Schafer, "Impact of Quasi-DC Currents on Three-Phase Distribution Transformer Installations," Oak Ridge National Laboratory, Oak Ridge, Tennessee, June 1992.

with 5.5 amperes DC injected (right graph) in the frequency domain. Notice the high amplitude of the harmonics generated by DC injection. Figure 5 plots the reactive power generated by the DC current injection during the ORNL tests. The "reactive power" is power mostly absorbed by the transformer causes abnormal heating of transformer components.

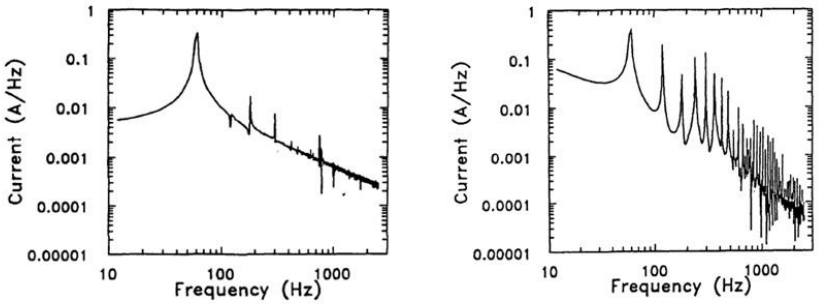

Figure 4. FFT of Current absorbed by Transformers Under Test at 0.0 ADV (left graph) and at 5.5 ADC (right graph)

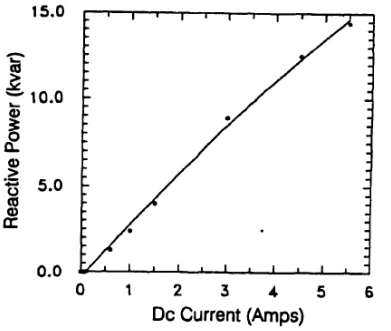

Figure 5. Reactive Power vs Neutral Current

The ORNL test imposed DC currents for only 10 seconds. If the DC current and associated reactive power and harmonics duration were extended to minutes on the larger scale electric grid, system instability and potential blackout would result. This would be caused by the voltage drop from the imbalance of reactive and real power, causing a frequency drop in the electric power system.

SRNL Distribution Transformer Testing Results

Based on the vulnerabilities noted above, SRNL tested the effect of DC injection on distribution transformers to evaluate if the predicted impact on the power grid was realistic. Figure 6 plots six cycles of data of the measured current flowing into two distribution transformers. This represents the current that the grid would have to supply to the distribution transformers in this test configuration. Notice that

there are two spikes of current on each waveform. These spikes lead and lag the fundamental waveform peak by 90 degrees. The two peaks are the half cycle saturation current absorbed by each transformer under test. They are in opposite polarities because the DC current is flowing in different directions within the two transformers, causing them to experience saturation at different locations on the transformer's hysteresis curve (B-H curve). The saturation current amplitude is linear as it increases with DC input once the transformer is saturated. As can be seen in this experiment, with minimal DC current injected into the neutral, the amplitude of the half cycle currents peak can exceed normal operation voltages by factors of 4 to 10.

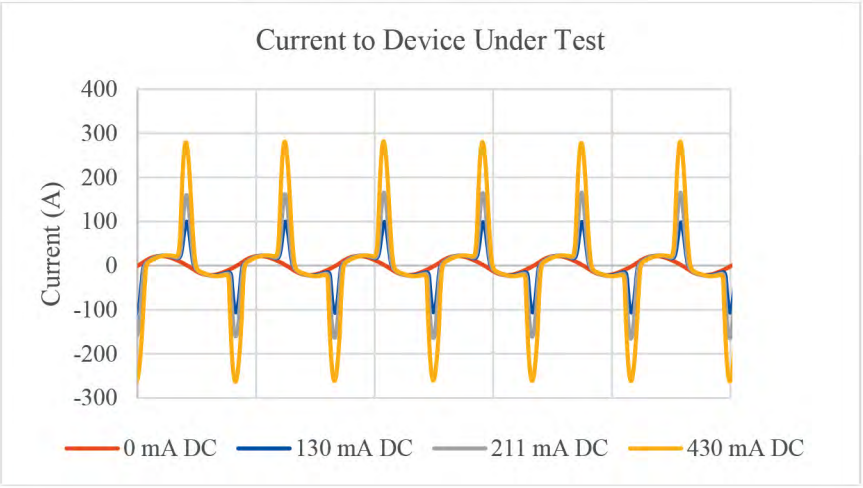

Figure 6. Current Draw from SST to Distribution Transformers

Solid State Power Substation

Based on the results from these ORNL and SRNL experiments, performing GIC testing on a megawatt scale with the LPT directly connected to the grid poses high risks to the operation of the rest of the grid. The scale of reactive power required for GIC injection at megawatt scale is likely to cause instability of the power system if directly connected and may cause the test bed substation to trip off. An engineering solution to circumvent this issue is use of a Solid-State Power Substation (SSPS) to imitate grid-power feeding the utility-scale test bed. An SSPS is a flexible, standardized power electronic converter that uses common modular, scalable, and adaptable power blocks.[37] They are flexible power routers or hubs that have the capability to electrically isolate system components. They can provide bidirectional AC and/or DC power flow control from one or more sources to one or more

37 https://www.energy.gov/sites/default/files/2020/07/f76/2020 Solid State Power Substation Technology Roadmap.pdf

loads. The power flow control is indifferent to magnitude and frequency, therefore, the input and output of a SSPS are decoupled. This protects the input from the test's effects on the output.

The SSPS includes functional control, communications, protection, regulation, and other features necessary for safe, reliable, resilient, and cost-effective operation of the test facility. An SSPS is comprised of several power electronic building blocks, which are programmable power electronic-based converters. It can protect the power system from excessive reactive power draw and harmonics when testing is being performed and will supply the reactive power needed for the transformers under saturation. Also, the SSPS system can supply a dedicated port to apply DC to the neutrals of the transformers to replicate the E3/GMD GIC on the transformers being tested. Figure 7 shows DOE's SSPS configuration concept for testing LPTs.

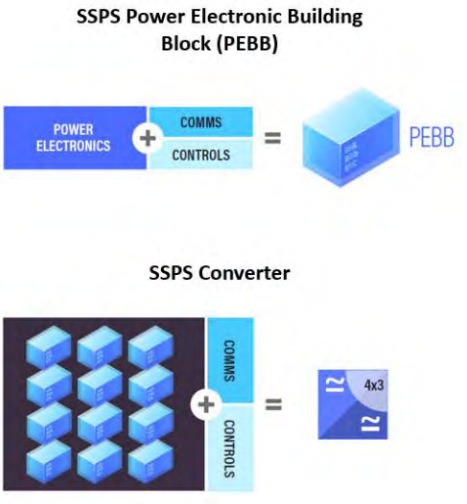

Figure 7. DOE Vision for SSPS Converters Employment for LPT Test Bed

Conclusion

LPTs represent a critical "tent-pole" in the national electric power grid and are integral to national resiliency. They are essential to both the generation and transmission sectors of the electric power grid. They are known to be targets of adversaries plans to debilitate national critical infrastructures. Their high cost coupled with months to years replacement time dictate the importance of survivability assurance. However, LPT vulnerability remains a subject of conjecture since no bulk-power transformer has undergone threat-level EMP testing. The high cost of test object hardware and transportation puts a premium on test optimization to produce the most information possible.

The Savannah River National Laboratory has developed a test program and designed a test bed to complete testing on LPT including physical set-up, injection

sources, and measurement equipment. To enable testing transformers under real load conditions, SRNL has devised a solid-state power substation to mimic the loading conditions of the larger grid. The SNRL test bed will enable tests to determine both transformer vulnerability thresholds and the effectiveness of protection hardware.

We recommend a concerted national test effort to determine LPT vulnerabilities and to expeditiously develop effective protection approaches.

Acronyms and Abbreviations

AEP	American Electric Power Company
CIP	Critical Infrastructure Protection
DOD	Department of Defense
DOE	Department of Energy
EHV	Extra High Voltage (Transformer)
E-ISAC	Flexible Alternating Current (AC) Transmission System
GIC	Geomagnetically Induced Current
GMD	Geomagnetic Disturbance
HEMP	High-Altitude Electromagnetic Pulse
IEEE	Institute for Electrical and Electronic Engineers
LPT	Large Power Transformer
NASA	National Aeronautics and Space Administration
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Electric Reliability Corporation
ORNL	Oak Ridge National Laboratory
PLC	Programmable Logic Controller
SSPS	Solid-State Power Substation
SRNL	Savannah Rover National Laboratory
WECC	Western Electricity Coordinating Council

Author Capsule Bios

Dr. George Baker is emeritus professor of applied science at James Madison University (JMU), where he also directed the University's Institute for Infrastructure and Information Assurance during 2000-2012. He recently retired from the National Security Council staff, where he coordinated federal interagency implementation of EMP executive order 13865 tasking. From 1999-2000 Baker served as a senior scientist at Northrop-Grumman, advising Defense Threat Reduction Agency (DTRA) nuclear effects R&D programs. He served as Director of DTRA's Springfield Research Facility from 1996–99, a national center for critical system all-hazards vulnerability assessment and protection guidance. Baker's organization developed the JCS Force Protection assessment program. From 1994–1996 he directed the Defense Nuclear Agency's Innovative Concepts Division, managing advanced weapon concept development and protection technology research. From 1987–1994 Baker led the Defense Nuclear Agency's electromagnetic effects programs to protect strategic systems and develop DOD's EMP guidelines and standards. He now applies lessons-learned from DOD experience to critical national infrastructure assurance and community resilience. He has consulted in the areas of critical infrastructure protection, EMP and geomagnetic disturbance (GMD) protection, nuclear and directed energy weapon effects, and risk assessment for customers including DOD, DOE, DHS, the White House, National Guard units, the National Park Service, SAIC, George Mason University, Oregon State University, and Defense Group Inc. During 2001–2008 and 2016–2017 he served as senior advisor to the Congressional EMP Commission. From 2011–2019 he served on the Board of Directors of the Foundation for Resilient Societies, the Board of Advisors for the Congressional Task Force on National and Homeland Security and the JMU Research and Public Service Advisory Board. Degrees include MS, Physics (University of Virginia) and PhD, Engineering Physics (U.S. Air Force Institute of Technology).

Ian Webb is a research and development engineer in the Cyber Security and Threat Assessments group in the Global Security Directorate at Savannah River National Laboratory. Before SRNL, he earned his B.S. in electrical engineering at Louisiana Tech University and is currently pursuing his M.S. in electrical engineering at Clemson University. His research focuses on cyber security vulnerabilities of critical infrastructure networks and the mitigations associated, integration of advanced grid sensors, solid state transformers, and large power equipment evaluation.

Klaehn Burkes is a Senior Engineer in the Cybersecurity and Threat Assessments group in the Global Security Directorate at Savannah River National Laboratory. He received a BS degree in electrical engineering and a MS degree in power systems from Clemson University, Clemson, SC, USA, in 2012 and 2014, respectively,

and he received the Laboratory Director's Award for Early Career Achievement in 2016 and 2021. His current research interests include industrial control systems, defense critical infrastructure, solid state technologies, large power equipment testing, Electric Grid SCADA Cybersecurity, and data acquisition.

Joseph Cordaro holds a senior technical leadership position within the Global Security section of SRNL supporting a wide variety of DOE/NNSA Missions. For more than 25 years, he has been internationally recognized in the areas of nuclear instrumentation, process control and high-speed data acquisition and control systems, particularly as they apply to the development of systems for nuclear component production and for the US Nuclear Stockpile Surveillance program. He was the recipient of the 2012 Don Orth Award and selected as a Laboratory Fellow in 2019, the highest technical achievement awards at SRNL and he has won multiple DOE/NNSA Awards of Excellence for his contribution to the safety and reliability of the U.S. Nuclear Stockpile. Mr. Cordaro is presently leading major National Security Programs for the Department of Defense and other U.S. Government Agencies.