Two Electrical Forensic Engineering Case Studies

Kurt Clemente, *Senior Member, IEEE*, and Erling Hesla, *Life Senior Member, IEEE*

***Abstract*—A utility interruption at a small data center resulted in failure of all computer racks despite power redundancy. The electrical forensic engineer investigated numerous accounts of the failure event, including interviews with data center personnel and data logs from the generator and uninterruptible power system. Initial conclusions from these accounts led to detailed verification of as-installed condition, revealing a seemingly innocuous deviation from construction plans. A code-required safety feature was determined to have been incorrectly installed, performing the desired safety feature but delivering an inadvertent system-wide shutdown signal upon loss of utility power. With permission from the owner, the safety system was modified to maintain the required operational safety feature without risking undesired operation during loss of utility power. A fire started in a potato warehouse, totally destroying the building and two trucks with trailers. The point of origin was determined to be the Foreman's office. The Insurance Company was concerned that it may have been arson, and payment to the owner was uncertain. An electrical forensic engineering investigation showed that, through a series of unlikely events, an electrical heater had started the fire, proving the fire was accidental and not arson. The Insurance Company paid the claim.**

***Index Terms*—Arson, data center, electrical forensic engineering, fires, generators, uninterruptible power systems (UPSs), utility.**

I. Introduction

FORENSIC electrical engineering is frequently discussed in legal terms, with courtroom evidence, testimony under oath, and engineers being deposed by attorneys while earning hourly fees [1], [2]. A frequent application of forensic electrical engineering in industry, however, does not involve litigation. Instead, this application identifies an undesired process or event that the electrical forensic engineer must address. Because most organizations possess some internal capability for maintenance, troubleshooting, and repair, the case that the forensic electrical engineer is called upon after the owner or operator has been frustrated by numerous unsuccessful attempts to identify, locate, and resolve the problem is frequent. The goal, then, is to identify a root cause, recommend a corrective action, and assist in a return-to-the-known and desired state. For our purposes, forensic electrical engineering may be suitably defined as the investigation of materials, products, structures, or components that fail to operate or function as intended. Whether this investigation is internal to the engineer's company or a company retains a consulting engineer to perform this investigation, the forensic electrical engineer's job involves determining the what, when, where, why, and how of the problem. Although the conclusions of such an investigation may describe a very simple root cause that is easily remedied, the forensics of determining the simple root cause is often quite complex.

Manuscript received January 30, 2014; accepted May 27, 2014. Date of publication August 8, 2014; date of current version November 18, 2014. Paper 2013-PSEC-1005, presented at the 2014 IEEE/IAS Industrial and Commercial Power Systems Technical Conference, Fort Worth, TX, USA, May 20–23, and approved for publication in the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS by the Power Systems Engineering Committee of the IEEE Industry Applications Society.

K. Clemente is with Clark Nexsen Architecture & Engineering, Norfolk, VA 23502 USA (e-mail: kurt.clemente@ieee.org).

E. Hesla is with Hesla & Associates, Camano Island, WA 98282 USA (e-mail: erling.hesla@ieee.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIA.2014.2346706

II. Electrical Forensic Engineering

Excellent treatments of electrical forensic engineering are available for the student or engineer who wishes to enter the field [2]. In many cases, however, the consulting engineer is called upon to investigate a time-critical failure where a period of formal preparation is not possible and a rapid solution to the problem is needed. In this case, a minimum of studied research and analysis is the norm and mostly conducted in the field during investigation. Formal processes for general forensic engineering in the broadest extent do exist and provide a framework for the investigation and thorough resolution of any problem. Accepting that clients who seek the consulting engineer's assistance may be anxious for rapid resolution, the authors suggest that IEEE consider development of a recommended practice for conducting electrical forensic engineering investigations. Such a document would provide a ready primer and guide for consulting engineers in this position, particularly when there is little time for formal preparation and study. This recommended practice would additionally benefit from an ongoing appendix documenting the lessons learned from previous electrical forensic investigations. Indexing the results from these investigations by key words would allow a new generation of engineers to benefit from previous work and prevent known problems from continuing to create problems in the industry.

III. Case Study #1: Data Center Power Failure

A recently constructed small data center of approximately 5000 ft^2 was populated by fifty 19-in computer data racks. The data center provided network services for a large department of approximately 1500 personnel located in an approximately 300 000-ft^2 colocated building. The need for continuity of network services warranted a dedicated 500-kW diesel generator with 72 h of on-site fuel to power all loads within the data center. Computer loads were served through a 300-kVA uninterruptible power system (UPS) to carry these loads through possible loss of utility until the diesel generator could serve the load. The general design of the data center's electrical

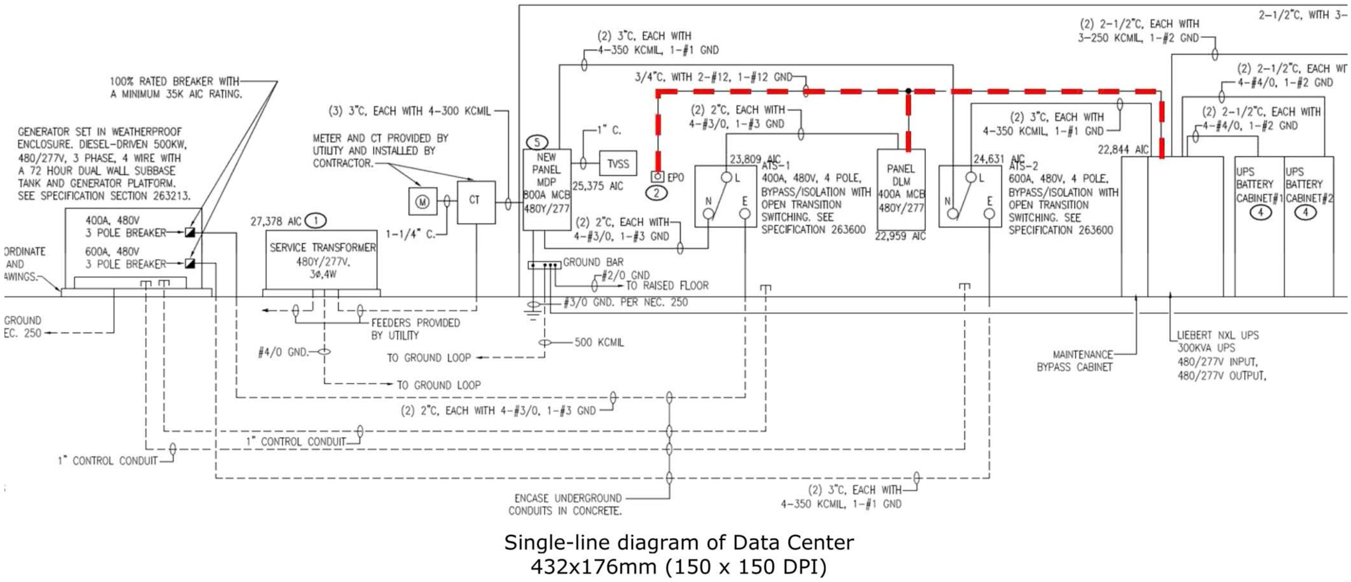

Fig. 1. Single-line diagram of the data center.

distribution system is shown in Fig. 1. The connection highlighted by a dashed line is intended to provide a Building Code-required emergency power-off (EPO) capability for equipment shutdown.

The owner requested an electrical forensic engineering investigation after the data center experienced a complete power failure. This caused computers to shut down for several hours until power was restored, resulting in loss of network services for the large department. Numerous internal efforts to identify, locate, and resolve the problem proved unsuccessful, and future data center power failures were possible. An engineer at the electrical forensic engineer's company had designed the data center; hence, rapid and thorough resolution of the problem was essential to prevent recurrence of the failures.

Prior to visiting the data center site, the engineer analyzed the design documents, construction product data submittals, and as-constructed/record drawings to understand the electrical system and identify potential areas for power failure. Of particular interest was a lack of thorough electrical commissioning testing for the diesel generator and UPS. Post-installation vendor checkout testing of each individual component was conducted, but thorough installation and system-wide testing of the complete electrical system (e.g., "pull-the-plug" testing) was not performed. An additional area of significance was an EPO control circuit for the UPS and heating, ventilation, and air conditioning (HVAC) dedicated to the data center. This relatively new Building Code requirement addresses an emergent problem for firefighters responding to an incident within a data center, whereas, it is straightforward to remove utility power to a building, and procedures are additionally well understood to disconnect on-site generators for the same purpose, the trend toward large UPS unit in data centers presents further challenges for firefighters' attempt to remove all sources of power prior to applying water or other means for fighting a fire. The EPO circuit not only provides a manual button for firefighters to remove this additional source of electrical power in data centers but is also code required to remove power from all dedicated HVAC in the data center. These computer room air conditioners or other devices are typically not powered from the UPS. The specific intent of the code requirement for HVAC disconnection is beyond the scope of this paper, but this additional requirement would prove crucial to the understanding of the failures experienced at this site.

After analyzing design documents and other archived information about the data center, a list of possible root causes was assembled to guide the forensic electrical investigation:

- lightning surge (the event coincided with a storm event);
- data center loading in excess of power system rating;
- design error (for example, an improper transfer switch scheme that would fail to switch loads);
- manual operation of the EPO circuit button;
- spurious automatic operation of the EPO circuit via electronic signals from the fire alarm control panel or clean agent control panels;
- malfunctioning equipment.

Upon arriving at the data center, site interviews were conducted with operators present at the time of failure, managers of the data center, and generator maintenance personnel. Subsequent discussions were conducted with the manufacturers of both the generator and the UPS, with follow-up inquiries to obtain data logs from the date of the incident from each of these devices. Accounts from eyewitnesses varied, with reports of loss of utility power, generator operation without switch transfer operation, and HVAC operation with UPS failure. All eyewitnesses agreed that no one had manually activated either of the EPO control circuit activation buttons at the entrances to the data center. The data center manager confirmed that no fire alarm signal had been sounded at the time of failure, and the clean agent control panel was not yet operational as the system was not charged with clean agent. Further comparison of numerous first-hand accounts revealed reports of conflicting and mutually exclusive events, winding down the useful portion of the initial phase of the forensic electrical investigation.

Interviews with personnel and preliminary equipment inspection ruled out a number of possible root causes. The service entrance equipment surge protective device did not indicate a surge from lightning had occurred, and the device was still operable (the building was further protected by lightning protection air terminals). Metering at the service entrance equipment and automatic transfer switches revealed loading well below design limits, suggesting that the data center equipment had not exceeded design parameters to trigger overload protective devices. A review of the construction documents did not reveal any apparent design errors, although it was noted that the Building Code-required EPO circuit was noted with only cursory design information (see Fig. 1). The EPO manual switches were not of the type providing positive indication of operation, but the agreement of all interviews suggested this was not likely. Spurious automatic activation of the EPO circuit was strongly suggested by interviews with personnel, to the point where electronic connections to the fire alarm and clean agent discharge control panels had been disconnected (the local fire department was notified of this temporary condition). The likelihood of this cause compelled the investigation to retain it as a possibility and would help shape the later equipment testing that later identified the proximate root cause. Lastly, field inspection of all electrical equipment revealed no obvious equipment malfunction. Further investigation of equipment malfunction as a possible root cause would require detailed inspection of equipment data logs but would prove critical to the identification of the root cause.

Inspection of the data logs was significantly more time consuming but represented a highly reliable source of information. Entries from the generator revealed that utility power was interrupted around the reported time of the incident, but the generator had been inoperable for the previous 14 days due to loss of fuel system prime. While this failure was a frustrating missed opportunity (an annunciator alarm panel providing visual and audible alerts to data center personnel was believed to have been silenced), this enabled the engineer to rule out the generator as a root cause for the failure. Inspection of the UPS data log proved more helpful, documenting events with millisecond precision immediately prior to the event, during the event, and after the event (the UPS control logic is operated separately from the power portion of the device, which ultimately failed to maintain power to the computer racks). This log showed normal operation of the system under utility voltage, loss of utility voltage, and the desired load transfer to battery. The data log then documented receipt of a shutdown signal from the EPO circuit, triggering the opening of numerous ac and dc circuit breakers within the UPS and affecting a loss of power to all 19-in rack loads in the data center. A follow-up discussion with UPS manufacturer revealed that he responded to the data center within approximately 4 h of the incident, resetting the system by closing circuit breakers and initializing the logic board. Due to the fact that this UPS reset restored system operation with no additional intervention to other power system devices, spurious automatic operation of the EPO control circuit was suspected by operators as the cause of the failure. A key factor in determining the root cause lies in the 4-h lapse from failure event to the UPS manufacturer's arrival at the scene to perform this reinitialization. During this time, utility power was restored to the data center. This change in state for the power system was to prove crucial in determining the ultimate root cause of the failure; if utility power had not yet been restored, reinitialization of the UPS would have led to a second immediate shutdown of the system, although the unit was sufficiently sized to power all connected loads without external power.

Having determined the proximate cause of the data center failure was the deactivation of the UPS by receipt of an EPO shutdown signal, the engineer focused his attention on the design of the EPO control circuit. The circuit collected shutdown signals from multiple input sources, including two manual pushbuttons at the building entrances, a fire alarm control panel, and a clean agent control panel. Shutdown by manual pushbutton is a code requirement [4], whereas shutdown upon activation of a fire alarm or clean agent discharge is a recommended practice for data centers [5]. Upon receiving any shutdown input signal, the circuit operated a 120-VAC power circuit to accomplish necessary equipment shutdown. The EPO circuit distributed this shutdown signal to the stored energy of the UPS and to the dedicated HVAC units in the data center. While the HVAC circuit breakers were factory-equipped with a shunt trip coil operated directly from the 120-VAC shutdown signal, the UPS required a "dry contact" activation signal for shutdown. While code requirements do not prevent using two separate EPO control circuits to deliver these two very different activation signals, the contractor for the data center elected to use a single circuit to deliver both signals by means of a relay. Design documents were unclear on how the contractor was to activate the dry contact from a 120-VAC activation signal, and the contractor selected a Form "B" normally open relay in a "fail-safe" configuration; the contacts were held open during normal operation (absence of a shutdown signal), but if the EPO circuit itself were to de-energize, the relay contacts would close. Design documents provided UPS-protected power for the EPO circuit to ensure circuit behavior would be independent of power outages, but field inspection during the investigation revealed that the contractor had installed the EPO circuit with non-UPS-protected power. "Fail-safe" operation therefore should not have been an issue as designed, but a seemingly innocuous field wiring change exposed this issue.

This clue provided sufficient insight into the probable root cause for the development of a detailed testing protocol that was able to reproduce the failure in the controlled environment of a planned weekend network outage. At considerable cost to the owner, a series of component and system-level tests were conducted to determine whether the suspected failure mode constituted the root cause of the failure. The testing confirmed the mode and root cause of the failure, and with the owner's concurrence, the relay circuit was modified to eliminate the "fail-safe" feature and return the EPO circuit to UPS-protected power. This corrective action addressed two aspects of the installation that led to the failures. The customer elected to not separate the 120 VAC and dry-contact shutdown circuits, as this work would have extended the network outage duration more than desired. As this dual-circuit configuration is permitted by the Building Code, it is recommended that designers strongly consider the separation of HVAC and UPS controls when these require different input types. While accidental manual activation of the EPO switch was not a factor in this failure, as an initially suspected root cause, it consumed time and resources during the investigation. Several manufacturers provide EPO switches with positive verification of manual activation (e.g., a placard reading "Activated" is exposed when the switch is pressed). We recommend this type of EPO be used for data centers to immediately rule out this mode of failure.

IV. Case Study #2: Potato Warehouse Fire

A fire destroyed a potato warehouse after everyone had left for the day. The sheet metal building housing machinery for sorting and washing potatoes had a lunchroom, foreman's office, machine shop area, storage area for bins of potatoes, and parking space for the two trucks with open trailers that were used for collecting potatoes from the surrounding fields. Firemen who fought the blaze concluded that the fire originated in the foreman's office, caused by a space heater on the wall. A *cause-and-origin* investigator was retained to establish for certain the cause and origin of the fire. The *electroforensic* investigator was tasked with determining details of electrical involvement. Both investigators were advised to be watchful for any indication of arson.

The investigation followed the systematic approach described in guide National Fire Protection Association 921 [3] with particular attention to the basic methodology described in Chapter 2 and to information in Chapter 14.4 to 14.7 covering electricity and fire. For this investigation, the two investigating engineers worked together closely during examination of the site.

The service entrance and exterior of the remains of the building were conventional good design and construction; hence, investigation turned to the interior of the building. The building was not sprinklered.

Photos, nameplate data, and information of details of the electrical installation were collected, working from the perimeter toward the origin of the fire. Although the two trucks and trailers clearly contributed greatly to the fire when fuel and tires ignited, the only wiring in the vicinity was a bit of overhead lighting that showed no indication of being a source of ignition. Suffice it to say that electrical systems in this major area of the installation appeared to have been satisfactory. Finally, close attention was directed to the office, its contents, and its electrical installation.

The office was wood frame construction, approximately 12 ft × 16 ft with an 8-ft ceiling. Walls and ceiling had heavy thermal insulation. The tight door in the 16-ft wall provided good thermal and sound insulation. At one end of the room, a large, tight, and fixed-sash window looked out on the machine shop area. At the other end was a large desk and a chair on casters, and low on the nearby wall is the electric heater. File cabinets, shelving, and normal office furniture occupied the remaining space. The foreman, a Jack of all trades, built this comfortable office for himself more than a year earlier.

The door still was locked. The "cause-and-origin" engineer concluded that the office had become very hot that pressure built up inside until the big window blew out in an explosion that then ignited the contents of the building. The question became, why and how did the office become very hot?

Careful observation showed that the chair was pushed back close to the heater. On the back of the chair were the charred remains of a heavy cloth jacket that had been hanging very near the heater, perhaps touching the heater. The heater with a nameplate reading of 3000 W, 240 V, and 1 PH was connected correctly to a 240-V breaker. Examination of the remains of the heater, the integral thermostat, and the wiring showed that, despite the fact that the heater was unusually large for the insulated room, the installation met code requirements and was installed in a workman-like manner. These observations led to the initial theory of the sequence of events.

Initial Theory: The cloth jacket was close to or touching the heater; the heater turned on when the evening turned cold and ignited the jacket. The burning jacket generated sufficient heat to ignite other combustibles in the office, creating heated gasses that built up pressure inside the tight office. Finally, the big window exploded outward, releasing superheated gasses into the oxygen-rich air. The fire spread from there, quickly involved diesel fuel and tires, and the building was destroyed. However, the nagging question remained, why was the jacket against the heater?

Further Investigation: Investigators interviewed several people who worked in the warehouse or were familiar with the facility. Their recollections were consistent, seemed honest and not contrived, and led to a revised theory with the following sequence of events.

Revised Theory: The foreman wore a jacket when he came to work because it was a cold morning. The day grew hot toward midday so he took off his jacket and hung it over the back of the chair. The thermostat did not turn on because the day was too hot. At the end of the shift in the late afternoon, the foreman pushed back his chair, forgot his jacket, closed and locked the door, and left in shirtsleeves. During the cool of the evening, the thermostat turned on the heater, starting the sequence of events described above.

Conclusion: Physical events happened as described under "revised theory". The foreman never thought of the risk of having combustible clothing close to the heater and simply forgot his jacket on the chair.

This case describes how the electroforensic engineer, working closely with the cause-and-origin engineer, determined the what, when, where, why, and how of this problem. An electroforensic engineering investigation has shown that, through a series of unlikely events, a properly installed electrical heater started the fire, showing that the fire was accidental and not arson. The Insurance Company accepted this conclusion as "more likely than not" based on the thorough and analytical investigation.

V. Conclusion

A recurring theme of these two case studies is the importance of independent verification of initial reports and observations [1]. In particular, eyewitness accounts reported honestly can be misleading or even incorrect, and frequently, a forensic breakthrough begins with the identification that an indication, report, or other information is erroneous. Detailed notes throughout the forensic investigation are critical; conflicting information can provide excellent suggestions for investigative focus. While the study of a formalized approach for electrical forensic engineering is beyond the scope of this paper, several recommendations may be helpful.

1) Interview eyewitnesses at the earliest opportunity, preferably in person but by phone if necessary. Make notes for later reference, paying key attention to speculations of a root cause. In my experience, a hint at the ultimate root cause is frequently found in these first interviews, concealed, quite often, by numerous incorrect speculations. Treat all eyewitness reports as unproven data, however. Verify all reports that appear to be relevant by using reliable data, engineering analysis, or recreations of the event.
2) Take the time to verify installed conditions against design documents. Deviations from the design that were considered minor by the contractor can create an undesired hazard. This verification step is recommended, particularly when field observations offer conflicting data, unexplained behavior, or illogical sequencing.
3) When available, retrieve and analyze data logs from power devices that record this information. The objective and precise data that may be available from these sources can help reconstruct the scene to an amazing degree. The same holds true for logs kept by operators.
4) Use manufacturer representatives as valuable resources for determining the specific causes and effects of evidence uncovered during the investigation. While no manufacturer wants their product's image to be tarnished by an unfortunate experience, their expertise in the detailed operation of the devices often proves crucial.

Acknowledgment

The first author would like to thank Dennis Marchant, his friend and mentor, for his technical assistance over the years and in particular during his portion of this forensic investigation of the data center. He is additionally grateful and appreciative to his wife, Julie, for her patience during his many long hours of work and for her assistance in proofreading this paper.

References

[1] K. Carper, *Forensic Engineering*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2001, pp. 5–6.
[2] R. E. Nabours, *Forensic Electrical Engineering & Liability*. Tucson, AZ, USA: Lawyers and Judges, 1994.
[3] *Guide for Fire and Explosion Investigations*, NFPA, Quincy, MA, USA, NFPA 921, 1995 ed.
[4] *National Electrical Code*, 2008 ed. Quincy, MA, USA, NFPA 70, Article 645 "Information Technology Equipment."
[5] *Standard for the Protection of Information Technology Equipment*, NFPA 75, 2003 ed.

Kurt Clemente (S'91–M'93–SM'06) received the B.S.E.E. degree from the University of Illinois at Chicago, Chicago, IL, USA, in 1993 and the M.S. degree from Old Dominion University, Norfolk, VA, USA, in 1995.

He is currently a Senior Electrical Engineer and Associate with Clark Nexsen Architecture & Engineering, Norfolk. He is the holder of three patents for fiber optic components and submersible LED lights.

Mr. Clemente is a Registered Communications Distribution Designer and a Licensed Professional Engineer in six states and the District of Columbia. He is a member of Standards Coordinating Committee 18 and the IEEE representative to Code-Making Panel #18 of NFPA-70 *National Electrical Code*.

Erling Hesla (S'46–M'48–SM'62–LSM'86) was born in Canada. He received the Bachelor of Applied Science degree in electrical engineering from The University of British Columbia, Vancouver, BC, Canada, in 1947.

He was with Canadian General Electric Company, Cobast in Brazil, and Scott Paper Company before moving into consulting practice. He is currently with Hesla & Associates, Camano Island, WA, USA. He established or helped establish three firms and holds three patents related to such "hearing aid" devices made by one firm.

Mr. Hesla is a Registered Professional Engineer in several states and has served as an Expert Witness. He has been active in AIEE and IEEE since his student years in the Seattle Chapter as Chair of the "Yellow Book" (902–1998), Chair of a chapter of the "Red Book" (141–1983), past Member-at-Large of the IEEE Industry Applications Society (IAS) Executive Board, and past Chair of the IAS Chapters Technical and Professional Outreach Committee. He received the RAB Larry K. Wilson Transnational Award (1998) for innovative promotion of IEEE globalization.