D32 Data Center Failures and Outages

Helmut G. Brosz, BASc, PEng, Brosz Forensic Services, 64 Bullock Drive, Markham, ON L3P 3P2, CANADA*

After attending this presentation, attendees will understand the critical importance of preventing data losses in today's information society, the causes of such data losses, and the preventative measures available to avert such losses.

The presentation will impact the forensic science community by: (1) exploring the causes, mitigation, and prevention of power failures and accompanying data losses; and, (2) discussing power failures and outages and the potential for litigation involving data center losses.

Data centers are the hub of communication networks. They are powered by electricity from local utilities, back-up generators, and Uninterruptable Power Supply (UPS) systems. Despite power supply redundancies and proper maintenance, total or partial outages occur and can be a costly disaster for users. Outage costs or penalties in the one-million-dollar-per-minute range have occurred. Litigation can ensue as one or more parties invariably are held responsible. Four cases are presented.

Case 1: Defective switchgear — 480-volt switchgear and circuit breakers are essential components of a UPS distribution system. In-plant inspection at the time of manufacture and proper commissioning are important to achieve the high degree of reliability required. Good electrical connections are necessary to prevent overheating and failure. Thermography is a useful tool for detecting incipient faults and preventing power failures and data losses.

Case 2: Defective Diesel engine overrunning clutches on UPS — Overrunning clutches are used to transfer electro-mechanical power from a motor generator set to a diesel engine during a power failure. Although this transition may last only a few seconds, during this time the clutch is exposed to the harmonic vibrations produced by a large (3,000kw) reciprocating diesel engine. Some types of clutches can fail during these circumstances. This potential source of failure can be averted by proper in-plant inspection and pre-equipment purchase vetting.

Case 3: Improper Maintenance — An establishment's computer and scanners tasked with reading paper credit card receipts were continually failing. The onsite service contractor would replace various printed circuit boards in this equipment using bare-hand handling methods in a service environment that was not designed to safely discharge accumulated static electricity. Upon touching the terminals of the exposed printed circuit board, the technicians would discharge static electricity to sensitive circuit components, ultimately resulting in computer malfunction. Costly arrangements had to be made to have the credit card data read by a competitor.

Case 4: Improper grounding systems — A cold war-era communication center on a hilltop was converted to a data center. The secure 1,000-foot vertical steel well water supply pipe of this center was used as the main building ground. The soil conditions in the vicinity of the center were very dry. The 1,000-foot steel well pipe was connected to the electric utility neutrals and ground. Thus, during utility ground faults, high-fault currents flowed toward the best ground in the area, which happened to be the 1,000-foot well casing. The rise in potential caused failures and outages in the data center. Rearrangement and redesign of the grounding system was necessary.

Data Centers, Failures, UPS Systems

*Presenting Author