

STATUS:	UPDATE v.2.0
INCIDENT TICKET NUMBER:	IN25016208575
PROBLEM TICKET NUMBER:	PR25000162187
PRIORITY:	1

DESCRIPTION OF INCIDENT

The Little Rock Technology Data Center (LRTC) lost external power at 13:57 CT on January 15, 2025, and backup power failed to activate for one half of a data storage cabinet. In and of itself, this issue is one that could have been recovered from quickly with limited disruption to service. However, coincident with this power event, a Direct Access Storage Device (DASD) within the data storage cabinet suffered a hardware malfunction and became inaccessible, preventing cache data from being stored. This substantially complicated and delayed recovery from the incident.

For added clarity, this incident was not related in any way to a cyber or cyber-related security event.

ROOT CAUSE

A series of cascading events caused this incident, with the most significant event being the hardware failure of the DASD.

External Power: First, the LRTC lost external power at 13:57 CT on January 15, 2025. The voltage sagged for two to four seconds, and seconds later, a full loss of utility power to the LRTC occurred.

Loss of Backup Power Supply to One Half of a Data Storage Cabinet: The LRTC is equipped with redundant uninterrupted power supply (UPS) systems, referred to as UPS-A and UPS-B. UPS-A performed without incident, temporarily supplying power from its batteries while diesel-powered generators came online, and then transferring the power supply to those generators. UPS-B suffered an anomaly, and went into static bypass mode, which prevented it from supplying power when the second utility outage occurred. The cause of this anomaly is unknown and remains under investigation. Most systems were not affected by this anomaly, as they were redundantly wired to receive power from both UPS-A and UPS-B. However, one data storage cabinet was improperly wired so that, instead of both halves of the cabinet being wired to both UPS-A and UPS-B, one half was wired only to UPS-A and the other half was wired only to UPS-B. As a result, the second half lost power. We are still investigating the cause of this power cabling issue.

Hardware Failure of the DASD: Even with the loss of power to one half of the data storage cabinet, the incident would have caused limited disruption if not for the DASD hardware failure. The DASD has features designed to protect data and operational integrity following a power loss, including a back-up power module (BPM) meant to provide limited power to the system in the event of an external power failure. This limited power allows the DASD to write any recent cache data from volatile system random-access memory (RAM) to a static solid-state drive (SSD), so that the data can be stored persistently without external power. The DASD is designed to then power off until external power can be restored; once power is restored, it is designed to load the data from SSD into RAM and continue processing data updates. In this way, the DASD is designed to support a quick recovery of the DASD storage in the cabinet in the event that power is lost.

However, when the external power failure here occurred, the DASD BPM failed, and the data in the DASD cache was not written to SSD. This failure delayed overall recovery from the incident because of the manual effort required to ensure data integrity when clearing the transaction processing backlog.

As result of the BPM failure, the DASD was unable to come back online after power was restored to the DASD storage cabinet. FIS worked with the DASD supplier to replace the BPM in the affected DASD at which point the DASD started functioning as designed.

We have sent the failed component from the DASD to the manufacturer for investigation.