Transient Currents and Their Impact on Data Center Outages

Datacenters are critical infrastructures that rely on stable and reliable electrical systems to ensure continuous operation. However, transient currents—short-lived spikes in electrical current or voltage—can pose serious risks to the operation of datacenters, potentially causing outages, damaging equipment, and compromising data integrity. Understanding transient currents' nature, causes, and effects is essential for implementing effective protective measures in datacenter environments.

What Are Transient Currents

Transient currents are sudden, short-duration increases in electrical current that can occur in electrical systems due to various factors. These transients can arise from several sources, including:

1. **Lightning Strikes**: Direct or indirect lightning strikes can induce large voltage spikes in electrical systems, leading to transient currents.
2. **Switching Operations**: The operation of electrical equipment, such as circuit breakers, transformers, or motors, can cause transient currents during switching events. For example, when a device is turned on or off, the sudden change in load can create a surge.
3. **Power Faults**: Short circuits or faults in the electrical distribution system can generate transient currents, affecting equipment connected to the power supply.
4. **Electromagnetic Interference (EMI)**: Nearby electrical devices or systems can cause interference that leads to transients, affecting sensitive electronic equipment within the data centre.

Impact of Transient Currents on Data Centres

Equipment Damage

Transient currents can lead to immediate damage to electrical components and sensitive electronic equipment within the data centre. This damage can manifest in several ways:

1. **Component Failure**: Excessive transient currents can exceed the voltage ratings of electrical components, leading to failures in servers, switches, and other IT equipment.
2. **Degradation of Components**: Repeated exposure to transient currents, even if they do not cause immediate failure, can lead to the gradual degradation of components, reducing their lifespan and reliability.

Data Loss and Corruption

When transient currents disrupt the power supply to servers and storage systems, it can lead to data loss or corruption. The sudden loss of power can cause:

- **Unfinished Transactions**: In environments processing large volumes of transactions, sudden outages can lead to incomplete operations, resulting in data integrity issues.
- **File System Corruption**: Abrupt power loss can corrupt file systems, causing critical data to become inaccessible.

3. System Outages and Downtime

Transient currents can trigger protective devices such as circuit breakers or relays, leading to unplanned outages. Such outages can result in:

- **Operational Downtime**: Extended outages can disrupt business operations, leading to financial losses and reduced productivity.

Mitigating the Effects of Transient Currents

To protect datacenters from the adverse effects of transient currents, several mitigation strategies can be employed:

1. Surge Protection Devices (SPDs)

Surge Protection Devices (SPDs) are essential for protecting electrical systems and sensitive equipment from transient voltage spikes caused by lightning strikes, switching operations, and other sources of electrical disturbances.

SPDs can be classified based on their type:-

installation location, and operational principles.

1. Types of SPDs by Installation Location

a. Type 1 SPDs

- **Location**: Installed at the service entrance of a building.

- **Function**: Protects the entire electrical system from external surges, such as those caused by lightning strikes.
- **Characteristics**: Connected between the utility service entrance and the building's electrical panel. Must be installed on the line side of the service disconnect. Typically designed for high surge current capacity.

b. Type 2 SPDs

- **Location**: Installed at the distribution panel or sub-panel within the building.
- **Function**: Provides additional protection to downstream circuits and equipment.
- **Characteristics**: Connected on the load side of the service disconnect. Offers a second line of defense against residual surges that may pass through Type 1 SPDs.

c. Type 3 SPDs

- **Location**: Installed at the point of use, such as on individual devices or receptacles.
- **Function**: Protects sensitive equipment from localised surges.
- **Characteristics**: Typically includes plug-in or hardwired devices. Provides the highest level of protection for specific devices, like computers, servers, or telecommunications equipment.

2. Types of SPDs by Operating Principle

a. Metal Oxide Varistor (MOV) SPDs

- **Function**: Utilises metal oxide varistors to absorb and divert surge energy.
- **Characteristics**: MOVs change resistance based on voltage; they are high-resistance under normal conditions but become low-resistance during a surge. Commonly used in various types of SPDs, especially in Type 1 and Type 2 devices.

b. Transient Voltage Suppressor (TVS) Diodes

- **Function**: Quickly responds to voltage spikes and clamps the voltage to a safe level.
- **Characteristics**: Offers fast response times, making them suitable for protecting sensitive electronic circuits. Can be used in both Type 2 and Type 3 SPDs.

c. Gas Discharge Tubes (GDT)

- **Function**: Protects against high-voltage surges by ionising the gas within the tube, allowing current to flow through and diverting the surge.
- **Characteristics**: Effective for high-energy surges, often used in combination with MOVs or TVS diodes. Common in Type 1 SPDs.

3. Specialised SPDs

a. Communication SPDs

- **Function**: Protects communication lines, such as telephone, Ethernet, and coaxial cables, from surges.
- **Characteristics**: Designed to prevent surges from damaging data and communication equipment. Often installed at the entry point of data lines into buildings.

b. Integrated SPDs

- **Function**: Combines multiple surge protection technologies into a single unit.
- **Characteristics**: Offers comprehensive protection by utilising MOVs, TVS diodes, and GDTs in one device. Suitable for various applications, from general electrical systems to sensitive electronic devices.

4. Industrial SPDs

- **Function**: Designed specifically for industrial environments where equipment may be exposed to higher levels of electrical noise and surges.
- **Characteristics**: Often ruggedised for harsh conditions, with higher surge ratings. Suitable for protecting motors, drives, and other industrial machinery.

2. Uninterruptible Power Supplies (UPS)

Uninterruptible Power Supplies (UPS) are critical components in data centres, providing backup power and protecting sensitive equipment from power disturbances such as surges, sags, and outages. Implementing **Multi-Stage UPS Systems** with advanced filtering capabilities can help to minimise the impact of transients and maintain system stability.

Here are the main types of UPS used in datacenters:

1. Offline/Standby UPS

- **Description**: The simplest and most cost-effective type of UPS.
- **Operation**: In normal operation, the power from the utility flows directly to the connected equipment, while the UPS remains on standby. If a power failure occurs, the UPS switches to its battery to provide power.
- **Advantages**: Cost-effective for small setups or environments with low power requirements. Easy to install and maintain.
- **Disadvantages**: Switch-over time (typically 5-20 milliseconds) may not be suitable for critical applications requiring uninterrupted power.
- **Applications**: Small servers, desktop computers, and home office equipment.

2. Line-Interactive UPS

- **Description**: A more sophisticated UPS that can provide voltage regulation along with battery backup.
- **Operation**: Uses a transformer to adjust the voltage in real time, compensating for sags and surges. In the event of a power outage, it switches to battery power.
- **Advantages**: Provides better protection against power fluctuations than an offline UPS. Typically has a faster response time (less than 5 milliseconds).
- **Disadvantages**: Less protection compared to online UPS in terms of complete isolation from power anomalies.
- **Applications**: Small to medium-sized data centres, networking equipment, and server rooms.

3. Online (Double-Conversion) UPS

- **Description**: The most advanced and comprehensive type of UPS.
- **Operation**: Converts incoming AC power to DC and then back to AC, providing a clean, stable output regardless of input fluctuations. The connected equipment always receives power from the inverter.
- **Advantages**: Provides the highest level of protection against power disturbances, including surges, sags, and outages. Zero transfer time since the equipment is always connected to the inverter.
- **Disadvantages**: Generally more expensive and has higher operational costs due to continuous energy conversion. Requires more space and cooling because of the heat generated during the conversion process.
- **Applications**: Critical data centres, large server rooms, and environments where power quality is paramount (e.g., financial institutions, hospitals).

4. Delta Conversion Online UPS

- **Description**: A variant of the online UPS that incorporates a unique power conversion method.
- **Operation**: Uses a two-stage conversion process, similar to traditional online UPS, but adds a delta converter to improve efficiency and reduce energy losses.
- **Advantages**: Higher efficiency than standard online UPS, reducing energy costs and heat generation. Provides superior protection against all types of power disturbances.
- **Disadvantages**: Generally more complex and expensive than standard online UPS systems.
- **Applications**: Large-scale data centres and environments with high energy efficiency requirements.

5. Modular UPS

- **Description**: A scalable UPS solution composed of several smaller, independent modules that can be added or removed as needed.
- **Operation**: Each module can operate independently, allowing for power capacity adjustments based on current needs.
- **Advantages**: Flexible and scalable, enabling easy capacity expansion as demands grow. Reduces initial investment by allowing data centres to start with lower capacity and add modules later.
- **Disadvantages**: Higher initial setup complexity and cost. Requires careful planning to ensure compatibility and optimal performance.
- **Applications**: Large data centres, cloud computing environments, and organisations with rapidly changing power needs.

6. Flywheel UPS

- **Description**: An innovative UPS technology that uses a flywheel to store energy mechanically rather than in batteries.
- **Operation**: During normal operation, the flywheel spins at high speed to store kinetic energy. In the event of a power outage, the kinetic energy is converted back to electrical energy to provide backup power.
- **Advantages**: Longer lifespan compared to traditional battery systems (often 20 years or more). Rapid response time and high efficiency. Minimal environmental impact due to the absence of toxic materials.
- **Disadvantages**: Generally lower energy storage capacity compared to battery-based systems. Requires more space and mechanical infrastructure.

- **Applications**: Data centres with short-duration power interruptions, mission-critical applications, and environments focused on sustainability.

3. Proper Grounding and Bonding

Effective grounding and bonding techniques reduce the risk of transient currents affecting equipment. Proper grounding provides a low-resistance path for fault currents, while bonding ensures that all parts of the electrical system are at the same potential, minimising voltage differentials. Proper grounding in a data centre is vital for safety, equipment protection, and system reliability. Implementing a comprehensive grounding strategy that includes equipment grounding, system grounding, bonding, telecommunications grounding, static grounding, and lightning protection ensures that the data centre operates smoothly and minimises risks associated with electrical disturbances. By following industry standards and best practices, datacenter operators can create a safe and reliable environment for critical IT infrastructure.

Proper grounding helps mitigate electrical hazards, reduce electromagnetic interference (EMI), and protect sensitive equipment from transient voltage spikes. Here are the primary types of grounding used in datacenters:

1. Equipment Grounding

- **Description**: Equipment grounding involves connecting electrical equipment, such as servers, racks, and cooling units, to the ground to provide a safe path for fault currents.
- **Purpose**: It protects personnel and equipment from electrical shocks and helps ensure that fault currents are safely dissipated to the ground.
- **Implementation**: Grounding conductors (often green or green with yellow stripes) connect equipment to a common grounding system or grounding rod, typically located at the data centre's main electrical panel.

2. System Grounding

- **Description**: System grounding refers to the grounding of the electrical power system, such as the neutral point of transformers and generators.
- **Purpose**: It helps stabilise voltage levels within the electrical system, provides a reference point for voltage measurement, and facilitates the operation of protective devices.
- **Implementation**: The neutral conductor of the electrical system is connected to the ground at the transformer or generator. This creates a solid reference point for the entire electrical system.

3. Grounding Electrode System (GES)

- **Description**: A Grounding Electrode System consists of one or more grounding electrodes (such as ground rods, plates, or concrete-encased electrodes) connected to the grounding system.
- **Purpose**: It provides a physical connection to the earth, allowing for the dissipation of electrical energy into the ground.
- **Implementation**: Ground rods are typically driven into the ground, and the grounding conductors connect these rods to the main electrical system. The GES must meet local code requirements for size, depth, and materials.

4. Bonding

- **Description**: Bonding is the practice of connecting various metal parts (e.g., equipment, racks, piping) to ensure they are at the same electrical potential.
- **Purpose**: It reduces the risk of electrical shock and prevents differences in voltage that could lead to equipment damage.
- **Implementation**: Bonding conductors are used to connect various metal components within the data centre, including equipment racks, cable trays, and structural elements. This ensures a uniform ground potential.

5. Telecommunications Grounding

- **Description**: Telecommunications grounding focuses on grounding telecommunication equipment, such as network switches, routers, and communication lines.
- **Purpose**: It protects communication equipment from electrical surges and maintains signal integrity by reducing EMI.
- **Implementation**: Grounding and bonding of telecom equipment should follow standards such as the Telecommunications Industry Association (TIA) 607-C and ANSI/EIA-310. Equipment should be grounded to a common telecommunications grounding bus.

6. Static Grounding (ESD Grounding)

- **Description**: Static grounding is used to prevent the buildup of static electricity on sensitive electronic equipment and personnel.
- **Purpose**: It helps prevent electrostatic discharge (ESD), which can damage sensitive electronic components.
- **Implementation**: ESD grounding mats, wrist straps, and grounding points are used to connect sensitive equipment and personnel to a common ground, effectively dissipating static charges.

7. Lightning Protection Grounding

- **Description**: Lightning protection grounding systems are designed to protect the data centre from lightning strikes and related electrical surges.
- **Purpose**: It directs lightning energy safely to the ground, minimising damage to the structure and its equipment.
- **Implementation**: A dedicated lightning protection system, including air terminals (lightning rods), conductors, and grounding electrodes, is installed to intercept and divert lightning strikes safely to the ground.

4. Regular Maintenance and Testing

Routine inspection and maintenance of electrical systems help identify potential weaknesses in the infrastructure that could be exacerbated by transient events. Testing SPDs, UPS systems, and grounding integrity regularly ensures optimal performance.

5. Design and Layout Considerations

Data centre design should consider the placement of electrical equipment and cabling to minimise the risk of EMI and transients. Using shielded cables, maintaining proper distance from high-power devices, and organising cabling can help reduce exposure to transient currents. One should have Automation in place to ensure the

Conclusion

Transient currents can pose significant risks to data centres, leading to equipment damage, data loss, and unplanned outages. Understanding the sources and impacts of transient currents is essential for data centre operators to implement effective mitigation strategies. By utilising surge protection devices, UPS systems, proper grounding techniques, and regular maintenance, data centres can protect their critical infrastructure from the adverse effects of transient currents and ensure continued reliability and operational efficiency.