

WHITE PAPER

Accelerating the transition to next-generation data center power architectures

Lessons learned from the
development of 800 VDC
electric vehicles

flex



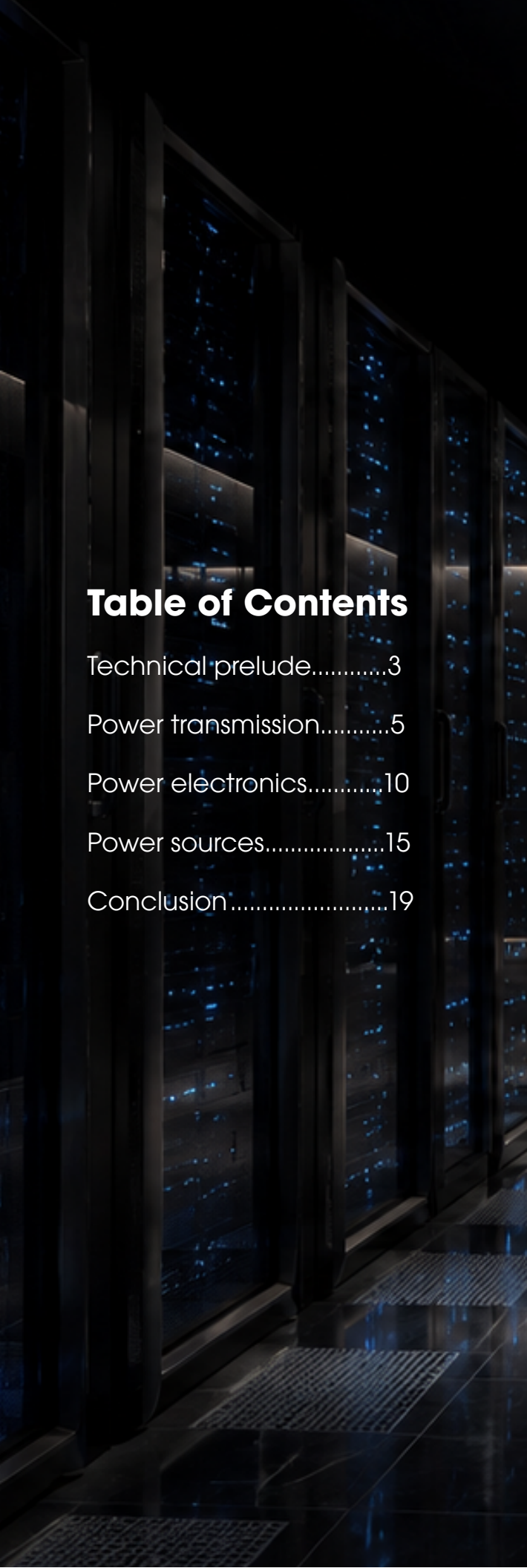


Table of Contents

Technical prelude.....	3
Power transmission.....	5
Power electronics.....	10
Power sources.....	15
Conclusion	19

Abstract

It is a pivotal moment for the data center industry. The rapid growth of AI-driven computing is forcing a fundamental re-evaluation of data center power architecture. Operators are under pressure to move quickly, reduce uncertainty and scale confidently. But as rack densities climb and energy demand escalates, traditional 48-54 V in-rack power distribution frameworks are reaching their practical limits. Emerging 800 VDC power architectures, including both 800 VDC and +/-400 VDC, are a logical next step in streamlining grid-to-chip power delivery for greater efficiency, fewer losses and faster growth.

While 800 VDC architectures are still being defined in the data center sector, they are far enough along that deployment timelines are accelerating under intense demand for capacity. The question is how quickly data center operators can make the transition while improving safety, uptime and long-term flexibility. To meet the demands of accelerated computing and dynamic AI workloads, a more efficient, scalable 800 VDC distribution system integrated with energy storage is essential.

Leveraging technology and experience from the automotive sector can help ease and accelerate the transition. Manufacturers of hybrid and electric models adopted 800 VDC platforms years ago to improve vehicle efficiency, thermal performance and charging speed — advancing power electronics, battery systems, connectors, insulation systems and global manufacturing processes along the way. Robust safety standards are also well-established for automotive applications. Today, millions of electric vehicles (EVs) operate worldwide, driven and charged daily by people with little to no technical knowledge of the energy systems they are dealing with. Safety incidents arising from user interaction are notably rare.

There are technical similarities, differences and lessons to be learned from the automotive industry's adoption of 800 VDC architectures, provided data center operators move forward with a clear understanding of the differences between the two as well. This white paper examines which lessons from the automotive sector can be directly applied to hyperscale environments, where adaptation is required, and how standards and safety frameworks must evolve.

Drawing on Flex's cross-sector expertise and UL Solutions' leadership in safety science and certification, we outline a practical path for organizations seeking to accelerate transformation.

Technical foundations of next-generation DC architectures

The 800 VDC adoption timeline for data centers is compressed, as seen in the graph below (Fig. 1), driven by the accelerated deployment of AI-ready facilities. At the same time, exploration of 1,500 VDC and beyond has already begun, making forward-compatible design essential. Organizations must move quickly.

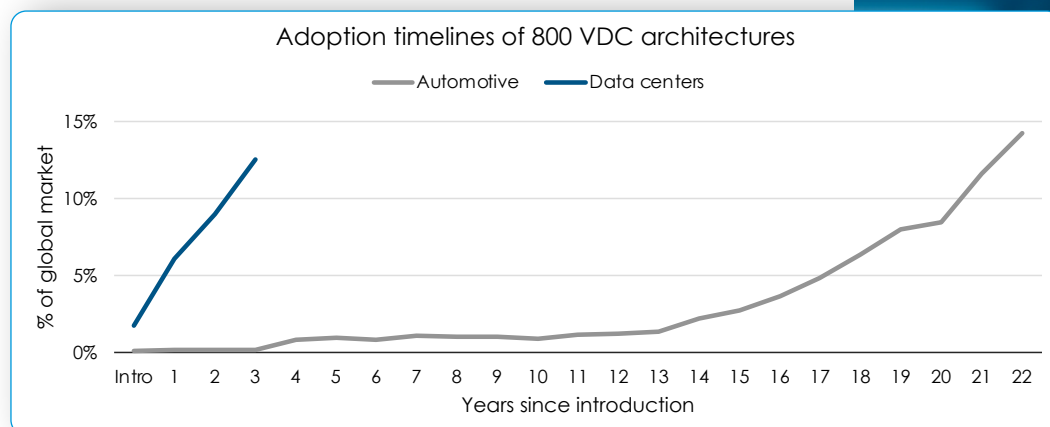


Fig. 1: Adoption timelines of 800 VDC architectures, via [Mobility Global](#) and Flex analysis

In the automotive sector, 800 VDC architectures have progressed through multiple generations of development and large-scale production. Today, the industry is defined by a mature ecosystem of 800 V components, design practices and safety standards. As data center operators proceed with their own transition, it is worth noting that both industries are grounded in the same principle: Operators must be able to work safely around high-voltage, high-current DC systems as part of routine operations and maintenance.

The engineering challenges — isolation, protection, thermal management, fault detection and serviceability — are more alike than they may first appear. We will consider the transition to 800 VDC data center architectures through that lens, beginning with an overview of the electrical systems of modern 800 V EVs and future 800 VDC data centers, followed by a closer look at the technologies and safety considerations for:

- **Power transmission**
- **Power electronics**
- **Power sources**

Comparing 800 VDC operating environments

The chart below (Fig. 2) provides a simplified look at the topologies of 48 V and 800 VDC architectures in both the automotive and data center industries. To be clear, there are crucial differences between the two sectors, and lessons learned will require thoughtful consideration from a technical and safety perspective as data center operators move forward. Of note:

- The grid is a much larger and more powerful source of energy than the battery in an EV. This means when an arc flash event happens, the vehicle’s power source will quickly sag in voltage and reduce the overall arc reach. Although datacenter short-circuit current is limited by converters, the presence of capacitance may provide significant transient fault current and may sag only for very short durations during an arcing event and quickly recharge. It is as yet unclear what effect such a temporary sag may have on arcing behavior and incident energy.
- EVs must be designed to support safe use by untrained users in publicly accessible environments, accounting

for intentional or accidental access to 800 VDC systems despite physical protections and interlocks. Data centers will be manned by trained operators, and only technicians with relevant electrical certifications should be able to access high-risk areas and equipment.

- EVs operate in extreme conditions (temperature, dirt, moisture, vibration, crashes), requiring more robust safety systems. Data centers exist in a much more controlled environment by comparison, though it is an ever-evolving landscape with rising thermal loads and shifting technology ecosystems.
- During EV maintenance, repair or service, electrical systems can often be partially disconnected or fully powered off for extended periods. Data centers, by contrast, are expected to operate continuously to maximize uptime, which may limit when equipment can be placed in an electrically safe work condition.

We will explore what these differences mean in the following sections.

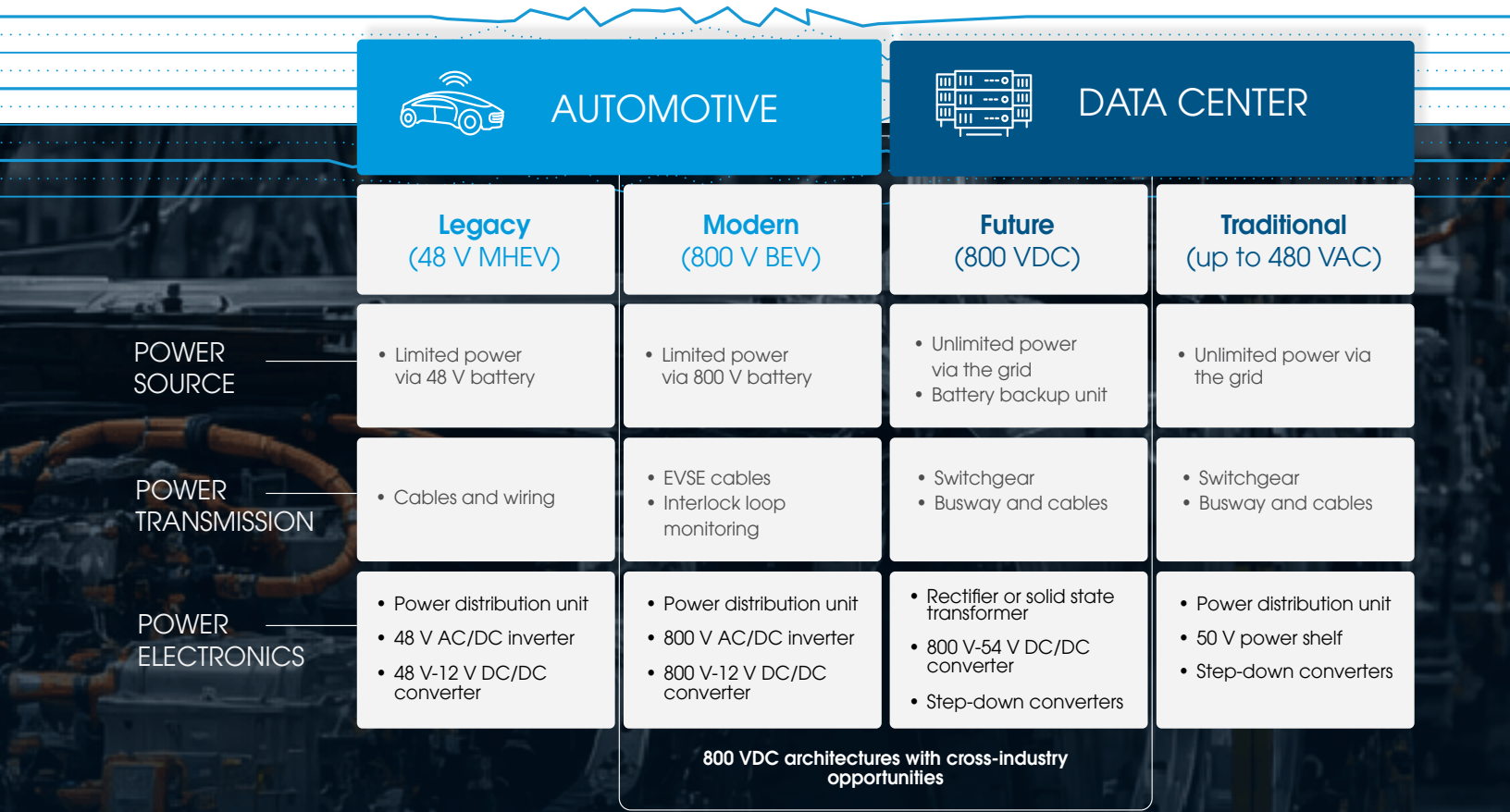


Fig. 2: Comparing simplified automotive and data center topologies

Power transmission

Power transmission considerations across sectors

The transition to 800 VDC introduces new challenges in power transmission, requiring careful consideration of distribution architectures, fault protection, insulation strategies and serviceability across both EV and data center environments. As power densities increase and electrical systems become more centralized, even minor faults can result in significant thermal and operational consequences if not rapidly isolated. At the same time, the need to maintain efficiency, uptime and safe maintenance practices is driving the development of new approaches to power distribution, protection coordination and system design.

Arc flash and electrical shock

Arc flash events at 800 VDC can expose individuals to significant incident energy, expressed in calories per square centimeter (cal/cm^2), with the potential to cause serious injury or loss of life. An arc flash may produce intense thermal radiation, a high-pressure wave, and plasma ejection, resulting in burns, ignition or melting of clothing, high velocity debris, hearing damage, vision impairment, and other severe effects. Unlike AC systems, DC systems lack a sinusoidal current zero crossing, which makes arc interruption more challenging and places greater demands on protective systems to rapidly clear localized faults.

Significant arc flash events can cause damage to the affected equipment and potentially to surrounding equipment, often requiring repair or complete replacement. The timeline for repairs or replacement can vary. However, it is not uncommon for impacted facilities to experience several months of downtime to safely access, remediate, and recommission the affected areas.

To mitigate shock and arc flash hazards during EV charging, electric vehicle supply equipment (EVSE) incorporates multiple layers of protection. EVSE cables remain de-energized until the connector is fully inserted into the EV and the vehicle control system confirms a valid and safe connection. If abnormal conditions are detected, including damaged conductors, incomplete connector insertion or overcurrent conditions, the EVSE automatically de-energizes the cable and connector. EVSE connectors further enhance safety through recessed contact pins

for touch protection, weather-resistant construction, and grounding conductors designed to make first and break last, thereby reducing shock risk.

Beyond connector-level protections, EVSE installations incorporate isolation monitor interrupters, overcurrent protection and short-circuit protection, as mandated by applicable installation codes, such as the [NFPA 70 National Electrical Code \(NEC\) Article 625](#). The isolation monitor interrupters disconnect power when an ungrounded, isolated system has lost isolation within the AC-to-DC power conversion stage from primary to secondary circuits, reducing the likelihood and severity of hazardous energy events.



Connectors, power electronics, batteries and associated wiring within the vehicle are also actively monitored for abnormal conditions through the use of what is known in automotive as a “high voltage interlock loop” or “HVIL.” The interlock loop is designed to detect unintended access, unexpected open circuits or operating parameters outside defined thresholds. When such conditions are identified, the 800 V system is rapidly isolated using contactors, switches or other disconnect mechanisms. This approach is conceptually similar to the self-monitoring fault mitigation used in Class 4 systems (as covered by [UL 1400](#)) and supports compliance with safety standards such as [ISO 6469-3](#), which are intended to help protect users, technicians and first responders from shock, fire and arc flash hazards following a vehicle accident or unauthorized access. Technicians and first responders working on EVs will follow established safety practices that may include de-energizing 800 V systems and wearing appropriate personal protective equipment.



In contrast, a data center’s connection to the utility source or other high-capacity power supplies typically results in higher available fault currents and incident energy levels than those encountered in EV architectures. Incident energy levels in DC systems is currently being investigated through a [research consortium](#) led by the NFPA. Data centers are subject to similar installation code requirements, such as the NEC and other local codes, and must incorporate appropriate personal, overcurrent and short-circuit protection.

Additional safety measures are commonly integrated into data center equipment to help reduce shock

and arc flash risk. Interlocking features that prevent the insertion or withdrawal of removable components while the component is in the closed position, such as low-voltage power circuit breakers, help prevent arcing during installation or removal of the component and are critical where arc flash events could be severe. Physical barriers may also be used to prevent falling tools or conductive objects from landing on energized components. Additionally, barriers may be used to minimize inadvertent contact with live parts by maintenance personnel. Most data center distribution equipment is dead front when fully assembled, with all exposed metal surfaces bonded to the grounding system to further limit user exposure to hazardous energy.

Data center maintenance personnel are similarly required to be qualified and trained. However, unlike EV systems that are not typically connected to the utility and may have the battery system electrically isolated during maintenance, data center equipment often must remain energized to maintain system uptime. This operational requirement increases the risk of shock and arc flash events, particularly where connections may be made while energized, such as the installation or removal of busway plug-in fittings or IT racks. When an electrically safe work condition cannot be established by the removal of electrical power, safety-related work practices, assessments and precautions outlined in local safety standards, such as the Standard for Electrical Safety in the Workplace [NFPA 70E](#), must be followed. These practices would typically include performing a hazard risk assessment to determine available incident energy and shock hazards, applying lockout/tagout (LOTO) procedures and selecting appropriate personal protective equipment, such as calorie-rated clothing and face protection.

Identification of hazardous voltages

EVs provide a clear visual identification of conductors that may be energized at hazardous voltage levels, such as 800 VDC. These conductors are typically orange in color, which gives an immediate visual indication of potential electrical hazards. This standardized color identification reduces the risk of inadvertent contact during maintenance, service and emergency response activities by clearly distinguishing 800 V circuits from 12 V or 48 V systems.

Data centers manage exposure to hazardous electrical energies primarily through controlled installation environments and restricted access. Interaction with energized equipment is generally limited to qualified personnel operating under established site safety procedures and applicable worker safety standards, such as NFPA 70E. In addition, data center equipment is typically supplied with detailed wiring diagrams and warning labels, such as those found in the American National Standard for Product Safety Signs and Labels, [ANSI Z535.4](#) or IEC standards. These labels provide clear notification of hazardous energy locations and other electrical risks and must be used by maintenance and servicing personnel to identify areas of hazardous electrical energies. The qualifications for technicians working on 800 VDC systems may be different from previous 48 VDC systems.

Use and application

EVs are inherently required to operate under a wide range of environmental and mechanical stressors, including vibration, humidity, contamination, crash-induced deformation, and other variable conditions that can loosen electrical connections, degrade battery systems, or impact power electronics performance. During normal operation, EVs continuously monitor for abnormal system conditions related to temperature, voltage, current and insulation resistance. Cell balancing algorithms, predictive diagnostics and other power electronic control functions may be employed as preventive measures to identify and mitigate emerging issues. These electrical monitoring capabilities are further complemented by reinforced battery enclosures, shock-resistant mounting structures and deformation-resistant pack architectures designed to withstand mechanical stress. Due to exposure to extreme temperature variations, additional mitigation techniques such as

active battery heating, load shedding algorithms, energy limiting strategies and supplemental cooling are often necessary to maintain safe and reliable operation.

By contrast, data centers are permanently installed, stationary systems that are not subject to many of the dynamic environmental challenges encountered by EVs. However, data centers have a separate set of environmental stressors, largely associated with the significant heat generation resulting from concentrated processing loads and power consumption. While external mechanical vibration is typically minimal, internal stresses may arise from rapid load cycling and associated thermal expansion effects. Elevated operating temperatures necessitate robust thermal management strategies to help protect equipment and prevent premature component aging or loss of function. Techniques such as forced air cooling and liquid cooling systems are commonly employed to manage system heat. Inadequate maintenance conditions, including dust accumulation or obstructed airflow due to clogged fans, can exacerbate thermal stress, accelerate component degradation and increase the likelihood of premature component failures. To address these risks, data centers routinely incorporate thermal monitoring and mitigation strategies to reduce the likelihood of unplanned outages and equipment damage.





Liquid cooling

The use of liquid cooling methods introduces additional risk considerations. The introduction of the coolant medium within the electrical system could present a significant shock, fault or arc flash hazard, particularly at elevated voltage levels such as 800 VDC. In addition, active cooling systems require ongoing operational surveillance to identify potential defects and periodic maintenance activities, which may require equipment to be taken out of service while repairs are performed.

In pressurized liquid-cooled systems, factors such as aging seals and gaskets, sustained exposure to heat and pressure, and vibration may degrade piping integrity over time. This degradation can result in unexpected coolant leakage onto electrical components and data center structures. Small leaks in pressurized systems may produce sprays or mists that are not immediately detected by pressure-monitoring systems. Furthermore, inadequately isolated cooling systems may cause condensation to form around or within electrical equipment. Preventive design measures, such as cooling components placement with respect to electrical equipment, dedicated condensation collection areas, and drainage provisions, are necessary to help minimize risks.

Immersion cooling introduces additional considerations. The long-term effects of submerging insulating materials or support materials in nonconductive cooling fluids may not be known. Prolonged immersion may result in degradation of dielectric strength or mechanical properties. Material compatibility must be carefully evaluated where insulating or support materials are critical to system performance and safety.

Another important consideration in high-power DC installations is current stability when supplying dynamic processing loads. Variability in load demand can produce power consumption characteristics that resemble those of high-frequency alternating currents, with frequencies potentially extending into the kilohertz range. The suitability of equipment used in these applications and their response to such high frequencies must be carefully considered. Accordingly, the use of appropriate mitigation strategies or components evaluated for these types of operating conditions is necessary to address and reduce the impact of these high-frequency dynamic loading effects.

Selective coordination considerations for DC data center power systems

Selective coordination of protective devices is critical to the operational resilience of the data center. A fault at an individual device or load within the data center has the potential to escalate into a systemwide loss of power if upstream protective devices, such as feeder or main protective devices, respond to a localized fault condition. An effective selective coordination strategy helps ensure that the protective device closest to the fault will clear the condition before the fault duration or energy level reaches the thresholds that would initiate upstream device operation. This coordination helps preserve service to unaffected loads.

Under fault conditions, components such as AC/DC converters or battery energy storage systems (BESSs) may cease exporting power when subjected to extended voltage depressions or abnormal system instability. Prolonged equipment faults can result in a systemwide loss of power. Rapid protection operation at or near the onset of a fault event is critical to maintaining system energization.

As data center power architectures evolve beyond 48 V distribution systems, including deployments at 800 VDC and beyond, the implementation of selective coordination introduces a distinct set of technical challenges. DC systems' lack of sinusoidal current zero crossing complicates arc extinguishment and reduces the predictability of interruption duration

for traditional air gap mechanical contact devices. Under low to intermediate DC fault current conditions, interruption times may be significantly longer than those associated with comparable AC protective devices or higher-magnitude DC faults. These characteristics can erode coordination margins and increase the likelihood of upstream device operation.

Modern data center designs also increasingly incorporate battery-based energy sources while minimizing AC-to-DC conversion stages. These architectures are capable of delivering substantial fault currents over very short time intervals. Conventional protective devices are typically designed and evaluated for inductive or general-purpose circuits. In contrast, DC data center systems frequently exhibit strongly capacitive behavior due to the presence of BESSs, uninterruptible power supplies (UPSs), converters and other capacitance components. During fault conditions, these elements can contribute high inrush and discharge currents, further complicating coordination strategies.

To address these limitations, contemporary DC power system designs are increasingly adopting alternative protection and coordination approaches. These approaches include the application of fast-acting protective devices with predictable interruption behavior, such as current limiting fuses at the equipment or the use of solid-state or solid-state hybrid circuit breakers.



Power electronics

Advanced safety protocols for power electronics systems

One of the primary advantages of adopting a centralized 800 VDC architecture in data centers is the opportunity to reduce the number of low-efficiency AC/DC power conversion stages between facility AC input power and the IT load. At the IT rack level, a highly efficient 800 V-to-48 V DC/DC converter input stage must be added (Fig. 3) to deliver power to the 48V DC/DC step down cascade toward 0.8 V GPU input voltage.

New challenges arise for the DC/DC converter operating from an 800 VDC bus, including:

- Operation from an 800 VDC bus increases galvanic isolation requirements between the 800 VDC domain and protective earth (PE). Unintended energization during service must be prevented to protect people from electrical shock. This is particularly challenging under demanding thermal and power density constraints.

- The 800 VDC circuit must incorporate stringent short-circuit protection in case of a control fault or power semiconductor failure, particularly due to higher device stress than in 48 VAC systems.
- The additional DC/DC power stage negatively affects the availability and reliability of power delivery toward the IT load side. This may require redundant system architectures to allow continued power delivery if one subsystem fails.

The automotive industry encountered similar challenges during its transition to 800 V EV platforms over the past 10 years. The primary DC/DC converters used to step down traction battery voltage for 12 V or 48 V auxiliary systems required advances in converter topologies, semiconductor devices and integrated protection strategies. The design practices developed to safely manage 800 V DC/DC conversion in EVs provide a valuable reference point for the development of rack-level 800 V input DC/DC converters in emerging data center architectures.

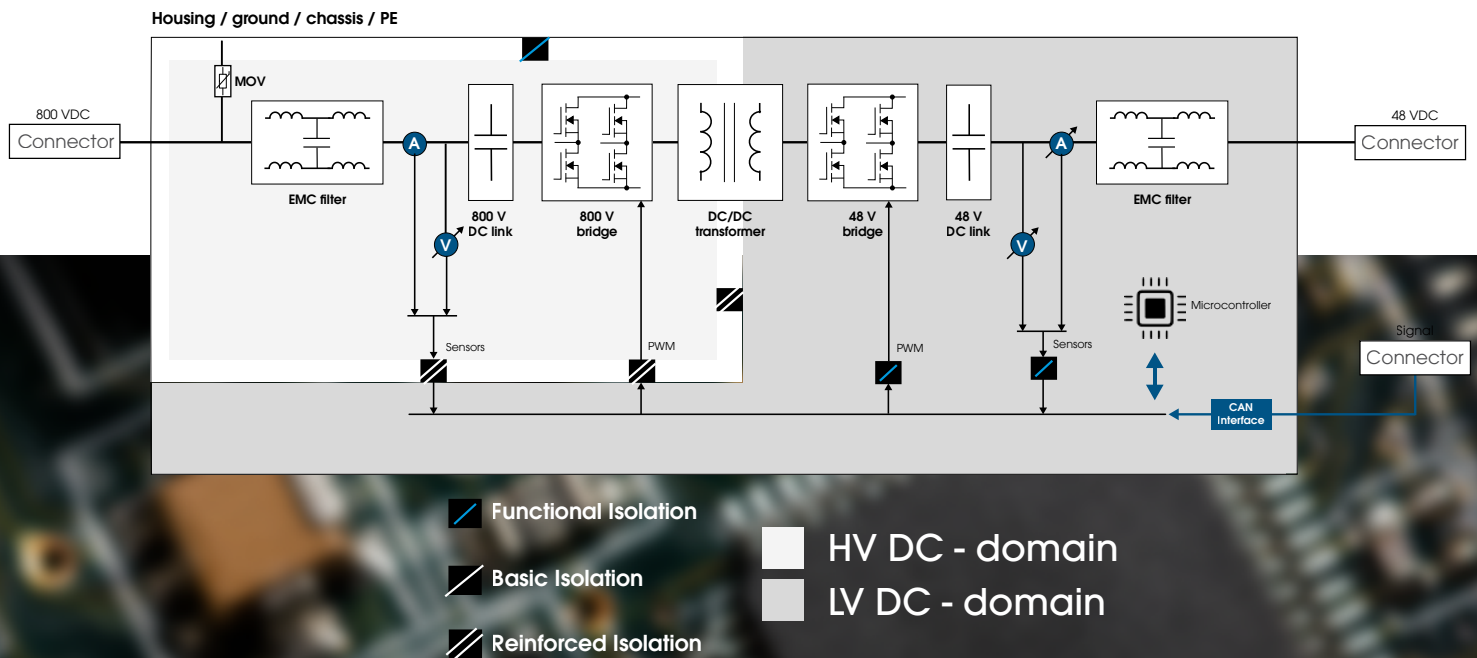


Fig. 3: Comparing simplified automotive and data center topologies

State-of-the-art automotive safety concepts

Electrical shock protection is essential for 800 VDC converters, where insulation failure or accidental contact with energized conductors may cause severe injury. To help ensure safety, automotive systems apply a multilayered protection strategy combining robust electrical design, continuous monitoring and controlled system reactions. This architecture must remain effective under harsh conditions such as vibration, humidity, contamination, crash deformation and interaction with nonexpert users.

Non-earthed 800 VDC bus operation

At high power levels, ground-fault current sensing becomes increasingly challenging to use without compromising system availability. Normal leakage currents resulting from long 800 V cable lengths, electromagnetic interference (EMI) filters and high-frequency inverter switching can approach or exceed typical protection thresholds, making the system vulnerable to nuisance tripping. This is especially problematic in architectures that rely on ground-fault detection for personnel protection, such as terra-neutral (TN) grounded systems.

To avoid these availability limitations, the DC/DC converter instead operates from a floating 800 V insulated terra (IT) battery system, where no intentional connection exists between the 800 VDC bus and the chassis. This architecture inherently provides single-fault tolerance; a first insulation fault cannot create a hazardous return path, allowing the system to remain functional.

Insulation monitoring

To supervise insulation degradation caused by cable damage, coolant ingress, connector contamination or internal DC/DC faults, an insulation monitoring device (IMD) continuously measures resistance between the 800 V bus and chassis. If insulation falls below the threshold (typically 100 Ω /V), the DC/DC converter is de-energized, and the 800 V battery is commanded to disconnect, preventing continued energy delivery into a fault.

Unlike ground-fault circuit interrupters (GFCIs) or residual-current devices (RCDs) that react to abnormal residual current, an IMD in an IT architecture is less susceptible to nuisance trips caused by normal converter switching and responds only when an actual insulation fault is

detected. This approach, widely used in EVs for more than a decade, pairs isolated DC/DC converters with continuous insulation supervision to deliver reliable fault detection, high system availability and consistent protection under demanding automotive conditions.



Isolation barriers in the DC/DC converter

800 V DC/DC converters must provide galvanic isolation between the 800 V traction bus and the 12 V or 48 V vehicle network. This isolation prevents direct-contact hazards and 800 V fault propagation into safety critical electronics. Early EV converter generations (2000–2015) lacked integrated reinforced isolation components. As a result, isolation was achieved using optocouplers, magnetic transformers and large creepage/clearance distances with double basic insulation, increasing converter size and reducing long term reliability.

With the shift to 800 VDC buses and the demand for improved reliability, the automotive sector drove and accelerated significant innovation in semiconductor-reinforced isolation technology. These devices integrate a robust isolation barrier directly into semiconductor packages, reducing dependence on magnetic components for signal-level isolation. They provide higher voltage margins, strong common mode transient immunity (CMTI) for SiC/GaN switching, better electromagnetic compatibility (EMC) robustness and more predictable long-term insulation performance. Consequently, they now dominate voltage interfaces such as gate drivers, current sensors and communication links.

Despite this evolution, the high-frequency transformer remains the essential isolation component for power transfer. It provides the mandatory galvanic barrier between the 800 V domain and the 12 V or 48 V network and plays a critical role in electrical safety. Its insulation between windings, core, shields and enclosure must prevent 800 V faults from reaching the chassis or accessible conductive parts. Proper transformer design limits leakage paths, avoids 800 V-to-core failures, and helps maintain isolation between the 800 V return and the chassis or ground, supporting IT system protection against direct and indirect contact.

Environmental constraints for an 800 V DC/DC converter, such as overvoltage category, pollution degree, altitude operation, and high power-density operation, require a tightly coordinated set of insulation and segregation practices. To withstand these conditions, the converter architecture combines several protective layers:

- Basic and reinforced insulation per IEC 60664 and ISO 6469
- Clearance and creepage distances sized for 800 VDC, as shown in **Table 1**

- Partial-discharge-free design under operating voltage and dv/dt stresses
- Mechanical segregation using barriers, sealed enclosures and touch-safe 800 V connectors
- Conformal coating to strengthen dielectric withstand in high-density PCB regions
- Strict cleanliness control to limit particle contamination throughout manufacturing and lifecycle
- Robustness against temperature cycling, humidity and vibration to maintain insulation integrity

Groups	Clearance	Creepage
800 V to 12 V or 48 V (reinforced)	6.5 mm	11.2 mm
800 V to ground (basic)	4.2 mm	6.6 mm

Table 1: Typical clearance/creepage isolation air distances in 800 V DC/DC converters



Interlock

To prevent personnel injury or equipment damage during service or unintended access, an interlock loop is present to monitor 800 V connectors and service covers, as shown in the diagram below (Fig. 4). Any opening or intrusion triggers immediate converter shutdown and capacitor passive and active discharge of 800 VDC links, reducing voltage to Class B limits (<60V) and residual energy to <0.2 J within the specified safe time interval of approximately 60 seconds.

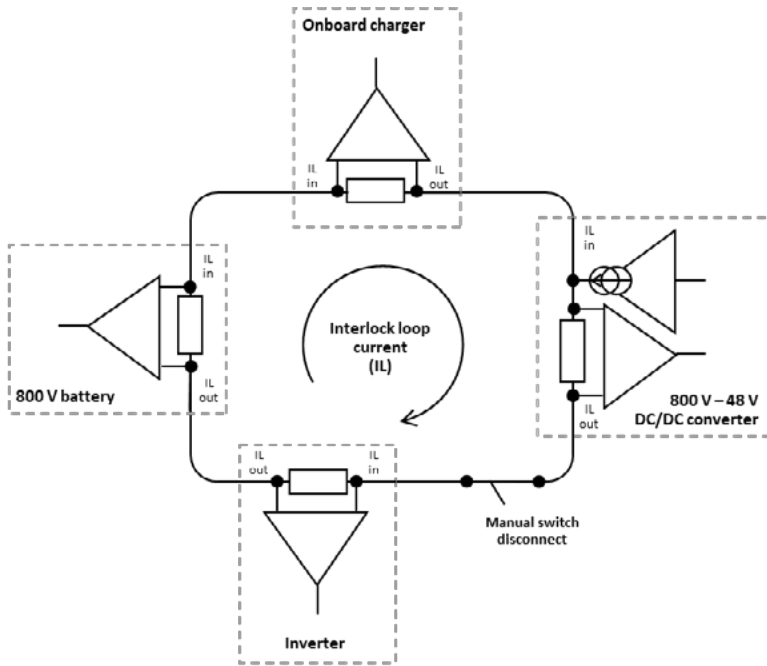


Fig. 4: A centralized interlock system with a common interlock loop shared with all 800 V components

Electrical shock protection is achieved through galvanic isolation, insulation monitoring, touch-safe design, interlock loop supervision and residual-energy management. Together, these measures provide comprehensive protection against direct and indirect contact hazards, consistent with [UNECE R100](#) and state-of-the-art safety practices for DC/DC converters in 800 VDC architectures.

Thermal incident considerations

Unlike many industrial power supplies, the 800 V battery can deliver extremely high fault current continuously. In case of an internal converter fault, the current is mainly limited by the electrical path impedance:

$$I_{fault} = \frac{V_{battery}}{R_{path}}$$

Because the total fault-loop resistance R_{path} , including both the battery internal resistance and the distribution network impedance, is typically only a few milliohms, fault currents I_{fault} can reach the kiloampere range. This can lead to very high power dissipation, due to the applied battery voltage $V_{battery}$.

A major concern is, therefore, short-circuited or partial “soft-short” failures within DC/DC components such as degraded MOSFETs, transformer insulation breakdown, capacitor dielectric failure, inductor insulation faults or PCB contamination, creating leakage paths. These faults often produce moderate overcurrent, which is insufficient to trip the 800 V fuse. Additionally, the battery management system cannot immediately disconnect, since contactors operate in tens of milliseconds and are not designed to open under DC current load conditions that can generate arcing and may weld contacts.

Conventional 800 V fuses are also too slow (millisecond blowing time) and rely on high I^2t energy, making them ineffective for soft-short conditions. As a result, the converter could continuously dissipate large amounts of power, potentially leading to overheating, insulation failure and fire. Fast electronic overcurrent protection (OCP) therefore acts as the primary protection layer, while the fuse remains a secondary, last-resort safeguard against catastrophic faults.

Short circuit fault protection

A DC/DC converter must be capable of managing internal faults locally to prevent damage or propagation of hazardous conditions. Modern 800 V converters implement fast OCP to mitigate this risk. By detecting abnormal current levels or semiconductor electrical overstress and disabling the pulse-width modulation (PWM) within microseconds ($\approx 1\text{-}10\text{ }\mu\text{s}$ using hardware comparators or desaturation detection), the converter interrupts energy transfer before thermal damage can develop. Table 2 provides a comprehensive comparison of short-circuit detection and protection methods for silicon carbide MOSFETs in EV applications.

Protection type	Reaction
Control loop OCP	10-100 μs
Hardware comparator current sensing	<1 μs
Gate driver desat	1-3 μs

Table 2: Typical reaction time vs. OCP implementation approaches

Automotive DC/DC converters must comply with [ISO 26262](#), which requires systematic identification and control of hazards. For internal electrical or thermal faults, the hazard analysis typically assigns an ASIL C safety goal: “Prevent thermal incidents caused by internal DC/DC converter faults.” When a short-circuit fault occurs, the converter must transition to a safe state within the fault tolerant time interval (FTTI), generally <10 μs . From a hardware safety perspective, the design must ensure that random hardware failures below 100 FIT (failures in time 10^9 operating hours) do not violate the safety goal. Compliance is demonstrated using ISO 26262 hardware metrics for probabilistic metric for random hardware failures (PMHF), single-point fault metric (SPFM) and latent fault metric (LFM), which are typically assessed through failure modes, effects, and diagnostic analysis (FMEDA) or fault tree analysis (FTA).

The architecture must ensure that single point faults in DC/DC components are controlled by fast OCP, while latent faults in protection circuits are detected by cyclic or start-up diagnostics.

The following EV safety solutions can be used to extend the scope of today’s data center equipment regulation and accelerate standardization toward 800 VDC.

- Isolate 800 V lines from the ground to inherently provide single-fault tolerance. This isolation concept does not exist in today’s 48 V data centers.
- Introduce fast short-circuit and overcurrent protections within the range of a few microseconds to prevent thermal incidents due to a slow relay or fuse opening mechanism. The initial current slope will be even higher for the data center as the short-circuit impedance R_{path} is expected to be lower.
- Interlock loops will be a practical mechanism for maintenance of the 800 V power system.
- IMDs already exist in some data center applications but may require broader adoption as 800 VDC architectures evolve to support detection of isolation faults and appropriate protective actions. Creepage and clearance distances are only considered up to 600 V and need to be extended to cover voltages up to 1,000 V.



Power sources

Power supply, storage and protection in 800 VDC systems

The transition to 800 VDC architectures is reshaping how power is sourced, stored and distributed in modern data centers. As AI workloads drive higher energy demands, operators are moving beyond traditional AC-based systems toward more efficient DC-based designs that integrate advanced battery storage and power management technologies.

Although EVs and data centers operate in different environments, both rely on power systems that must safely manage large amounts of energy. Lessons from EV charging, battery management and fault protection can help inform the development of next-generation data center infrastructure.

AC power distribution

EVs are routinely charged from the electrical grid via AC conductive charging, typically using an onboard charger (OBC). Depending on the region, the vehicle is supplied with a single-phase 120 V or 240 V AC (North American markets), or single- or three-phase 230 V/400 V AC (IEC markets). In this operating mode, the vehicle interfaces directly with low-voltage AC distribution systems, making it conceptually similar to server and data center equipment powered from utility AC front ends.

During AC charging, the same safety concerns described in the power electronics section apply, including electric shock protection, thermal hazards and fire risk. Personnel protection against electric shock is largely addressed by the building and charging infrastructure, typically based on terra-neutral (TN) or terra-terra (TT) earthing systems with residual current protection (RCD/GFCI). Fire protection on the AC side relies primarily on upstream overcurrent protective devices (fuses and circuit breakers), while the OBC itself incorporates internal overcurrent, short-circuit and thermal protection.



The transition from AC to DC power

Data centers are supplied from a medium- or high-voltage grid. Depending on the equipment being powered, this voltage is stepped down to lower voltage and distributed throughout the facility. The first phase of the 800 VDC transition in data centers will keep AC distribution and add a converter unit (power rack) to transform 480 VAC into 800 VDC for delivery to GPU racks (Fig. 5). In the final phase of this transition, rectification will be performed at the beginning of the installation inside a data center, and energy will be distributed at 800 VDC throughout the data center (Fig. 6).

Unlike EVs, data centers do not rely on a continuous supply of energy from batteries; they primarily rely on the grid. In situations of increased grid demand or grid instability, a generator may be used to provide AC voltage to the rectifier or transformer for the data center. BESSs can be used to provide temporary (seconds to minutes) 800 VDC power to the data center until the generator comes online and takes over. BESSs in data centers are used as a backup during grid voltage instability or a power outage. BESSs can also be used in conjunction with renewable energy sources such as wind and solar to store energy until it is needed by the data center. At the rack level, a variation on a BESS known as a battery backup unit (BBU) is used for power smoothing during load steps generated by GPU racks.

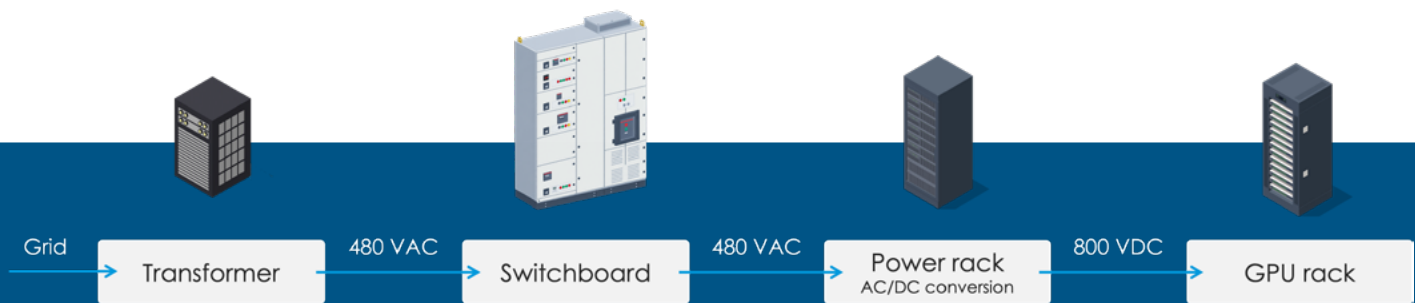


Fig. 5: Simplified model of power supply using power rack for 480 VAC to 800 VDC conversion

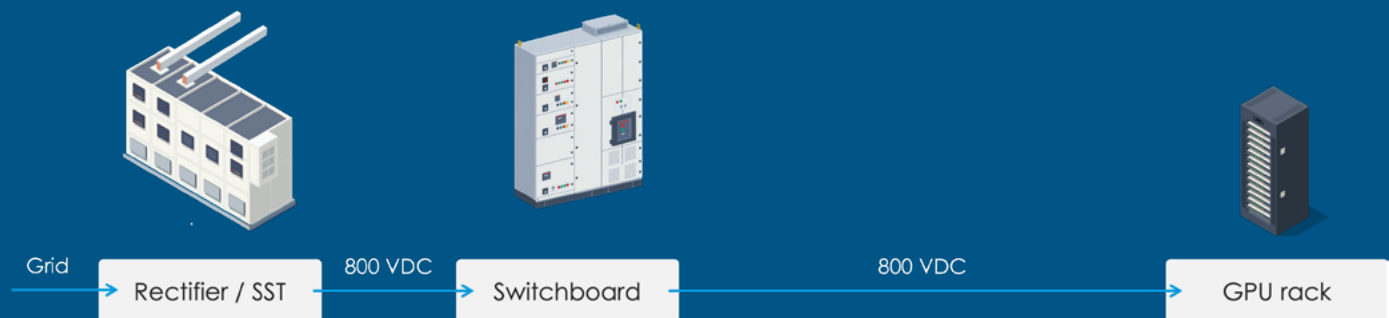


Fig. 6: Simplified model of power supply with 800 VDC

Battery safety risks and mitigation

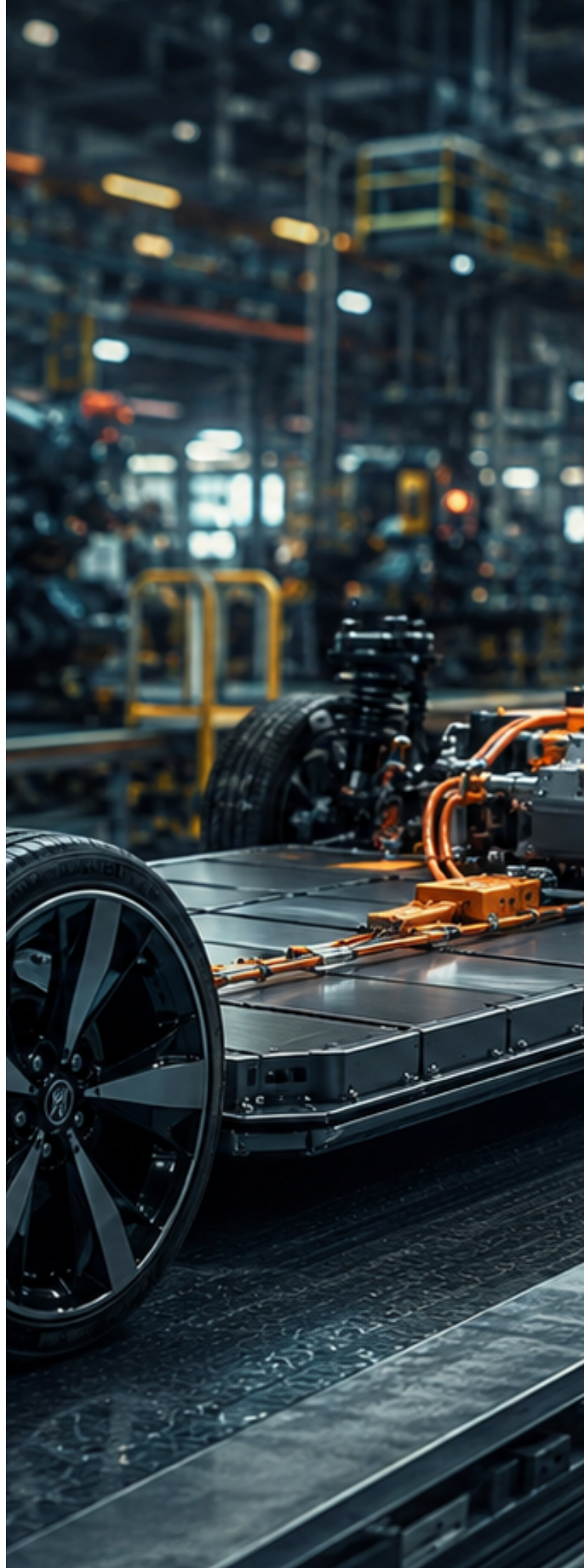
Batteries used in EVs and energy storage systems (ESSs), including those in data centers, must undergo rigorous testing to evaluate their ability to withstand electrical stresses, physical damage and environmental conditions encountered during normal operation and abnormal events. These tests help confirm that batteries will perform reliably and safely throughout their service life. In conjunction with testing, quality control of cell and battery manufacturers helps minimize risks due to manufacturing defects.

Lithium-ion batteries are widely used because they offer a strong balance between physical size and energy capacity. In simple terms, lithium-ion technology can store a large amount of energy in a relatively small and lightweight package. This compact design makes lithium ion batteries particularly attractive for applications where space is limited, such as data centers.

However, the same high energy density that makes lithium ion batteries attractive also introduces safety considerations. Lithium-ion batteries can be vulnerable to a phenomenon known as thermal runaway. Thermal runaway occurs when a battery begins to heat faster than it can cool itself. This condition may arise as batteries age, when dendrite formation within a cell can cause an internal short circuit. Thermal runaway can also be caused when a battery is overheated, physically damaged or affected by a manufacturing defect. When thermal runaway occurs, a battery cell can release hot gases, reach very high temperatures, and potentially catch fire.

Because battery cells are tightly packed together inside a battery system, a failure in one cell can spread to neighboring cells. This chain reaction can escalate quickly and affect an entire battery unit. In a data center environment, preventing such events is critical, as battery failures can result in equipment damage, service interruptions and costly downtime.

To manage these risks, lithium-ion batteries rely on a battery management system (BMS). The BMS constantly monitors and controls key operating conditions to ensure the battery stays within its specified temperature, voltage and current ranges. It also plays a crucial role in detecting abnormal conditions and triggering protective actions when necessary. These actions may include disconnecting the battery from the electrical system or placing it into a safe state.



To ensure protective systems work reliably, batteries used in EV and ESS applications follow established functional safety standards, such as ISO 26262, ISO 13849-1 and ISO 13849-2, IEC 61508-1 or CSA E60730-1. Testing the battery with its BMS helps assess whether safety components, such as contactors, fuses and protective circuits, operate as intended during fault conditions, including overheating, overcharging, overdischarging or electrical short circuits.

Modern lithium-ion battery systems used in data centers often operate at DC voltages, including at 800 V or higher. At these voltage levels, batteries are capable of delivering large amounts of electrical current in an extremely short time. Because lithium-ion cells have very low internal resistance, fault currents can reach many thousands of amperes. This makes careful coordination between the battery, protective devices, and power electronics essential.

Effective communication between the BMS and electrical components such as switches and protective disconnects is critical to ensuring that charging and discharging stop immediately when unsafe conditions are detected. This coordinated response helps reduce the likelihood of damage, limit fault energy, and lower the risk of thermal runaway.

All electrical connections associated with battery systems, including busbars and wiring, must be designed to safely handle these high currents. Proper sizing and insulation are necessary to prevent overheating, electrical failures, or loss of isolation between conductive parts.

Lithium-ion batteries are particularly well-suited for data center applications because they can deliver power very quickly when needed, such as during a utility outage. They can also remain in standby for long periods with minimal energy loss, requiring only occasional charging to maintain readiness. While they excel at supplying short-duration backup power, lithium-ion batteries are not intended to support long-duration outages lasting many hours or days. For extended outages, they must be paired with other power sources such as generators.

Temperature control is another critical consideration in data centers that use batteries. Most lithium-ion batteries are designed to operate continuously at temperatures up to approximately 40°C to 45°C. Higher temperatures may be tolerated for short periods, but sustained exposure to heat accelerates battery degradation, reduces performance and shortens battery life. As a result, environmental controls such as cooling systems are essential to support safe and reliable battery operation.

Finally, data centers deploying large quantities of lithium-ion batteries must comply with applicable fire and building codes, such as NFPA 855, Standard for Installation of Stationary Energy Storage Systems. These codes often place limits on how much battery energy can be installed within a given fire area and may require minimum separation distances between battery systems and other equipment. In some cases, these requirements are met by separating battery installations into dedicated rooms or locating BESSs outside the main data center space.



Accelerating the transition to 800 VDC data center infrastructures

The transition to 800 VDC architectures represents a fundamental shift in data center power design driven by the rapid expansion of AI workloads, increasing rack densities and the need for more efficient grid-to-chip power delivery. While the data center industry is only beginning its migration toward 800 VDC and beyond, other sectors — particularly automotive — have already demonstrated that these systems can be deployed safely, reliably and at scale.

EV manufacturers spent more than a decade refining the technologies, safety mechanisms and operational practices required to manage 800 VDC systems in demanding real-world environments. These advances include insulation monitoring, interlock loops, fast fault protection, thermal management strategies, reinforced isolation techniques and battery safety systems. Many of these technologies and lessons learned can accelerate the deployment of next-generation data center architectures while reducing technical risk and improving operational safety.

At the same time, data centers introduce unique challenges that require adaptation rather than direct replication of automotive solutions. Unlike vehicles, data centers operate continuously, are connected to potentially high-capacity utility power sources, and must maintain uptime during maintenance and fault conditions. As a result, arc flash hazards, selective coordination, grounding strategies, thermal management and serviceability requirements may become even more critical in high-density AI environments.

The evolution toward 800 VDC data centers will therefore depend on a combination of proven safety principles, new protection technologies and updated industry standards. Areas such as insulation coordination, high-speed fault interruption, battery integration, selective coordination and operational safety practices must continue to mature to support widespread adoption.

The broader lesson is clear: The transition to 800 VDC infrastructure is not unprecedented. The automotive, solar, industrial and energy storage sectors have already established practical pathways for safely deploying advanced DC systems. By leveraging cross-industry expertise and aligning around common technologies, standards and safety frameworks, the data center industry can accelerate the adoption of power architectures capable of supporting the future of AI and high-performance computing.

For more information, visit flex.com/connect

Flex (Reg. No. 199002645H) is the global manufacturing partner of choice that helps leading brands design, build, and manage products that improve the world. For more information, visit flex.com

©2026 FLEX LTD. All rights reserved. Flextronics International, LTD.

flex

