Omnion POWER

WHITE PAPER

QUANTIFYING THE IMPACT OF QUALITY & RELIABILITY



By Susan Chorrushi

Director of Quality

QUANTIFYING THE IMPACT OF QUALITY & RELIABILITY

The Real Cost Of Downtime – And How To Avoid It

Across today's increasingly digitized landscape, entire industries are being built on foundational, always-on infrastructure. Whether it be rapidly evolving AI data center facilities in the high-volume computing space, industrial automation systems in manufacturing, or the deployment of 5G and even 6G wireless networks, operating these systems requires one core, common denominator: an immense amount of high-quality, reliable power.

Telecommunications: The Gold Standard for Reliability

Nowhere is this more apparent than in telecommunications, where network operators are expected to deliver continuous connectivity and maintain constant, around-the-clock service availability. The telecom industry has some of the most rigorous standards for quality, reliability, and uptime, requiring power systems that can deliver consistent performance over long operational lifecycles. In the industry, reliability is often mentioned as "five-nines". What this means is that the network is designed to be up and running 99.999% of the time, which equates to an implied downtime of less than 5.3 minutes per year.

In mission-critical environments, power is crucial for ensuring uninterrupted operations, system resilience, and overall business continuity. Even a momentary disruption in operations—an outage, a production line shutdown, a brief gap in wireless capabilities—can have broad, cascading effects across interconnected systems.



This unplanned downtime can cause equipment and/or critical systems to remain out of commission for an uncertain period of time. Given the "unplanned" nature of these outages, they're often lengthy and costly. One survey of manufacturing professionals found that **nearly half experience 6-10 incidents per week**, with the **average outage lasting up to 12 hours**. What's more, the **average cost of these incidents can reach $1.7 million per hour**. These costs quickly compound when downtime stretches from hours to days.

On its own, this would be a high economic cost for the organization to bear. But increasingly often, new types of digital infrastructure are subject to the rules and penalties of evolving power regulations and standards. These standards, along with sustainability and regulatory mandates, make power reliability a compliance necessity instead of solely a financial goal.

Given these economic and regulatory factors, supporting performance, avoiding downtime, and maintaining compliance are critical in always-on digital infrastructure. Meeting these needs requires solutions that are high-quality, durable, and designed for resilience. This white paper examines the varied causes and costs of downtime and highlights quality and reliability best practices and solutions to help create resilient infrastructure and prevent costly outages.

Downtime Causes & Risk Factors

To best understand how today's organizations can prevent unplanned downtime, it's necessary to examine the conditions that often lead to these disruptions. While outages may seem unpredictable, most downtime incidents can be traced back to a defined set of risk factors that impact system performance and reliable operations. These common root causes include:

Human Error

This can include errors such as misconfiguration, user oversight, inadequate maintenance, and human susceptibility to phishing and other social engineering attacks. These kinds of errors are more common than you might think. They often reflect opportunities to strengthen communication and enhance training effectiveness, as well as to implement robust system controls that reduce reliance on manual actions and minimize the potential for human error.

Hardware/Equipment Failure

This may include the failure of worn-down or unrepaired parts and components, the results of general wear-and-tear, or unnoticed flaws in the original manufacturing. These kinds of failures often snowball into larger system malfunctions, causing general disarray and unexpected downtime.

Environmental Factors

These can include extreme conditions such as temperature fluctuations, high humidity, corrosive environments, and exposure to factors like dust, vibration, or rapid environmental changes. They may also include unexpected power spikes, severe weather events, or natural disasters. If hardware is not built to withstand expected conditions and potential fluctuations, it can easily malfunction and lead to additional downtime.

Security Breaches

These breaches can include cyberattacks such as phishing and credential theft, malware infections, ransomware attacks, data breaches involving unauthorized access or data exfiltration, and distributed denial-of-service (DDoS) events, as well as insider threats, system compromises, and other malicious activities. These attacks may target humans or technical systems, exploiting vulnerabilities to cause unexpected outages.

Whatever the root cause, unplanned downtime disrupts operations and can lead to high costs that spread well beyond the initial incident.

The True Costs of Downtime

As mentioned, the impact of downtime extends far beyond just the immediate interruption of service. It can have financial, technological, legal, reputational, and logistical impacts on both the original equipment manufacturer (OEM) and the end user or end application. Regardless of who experiences the impact, the consequences are often shared, interconnected, and compounding. Common categories of downtime consequences include:

Direct Financial Losses

These may include lost OEM revenue due to halted operations or unavailable services, service level agreement (SLA) penalties and contractual fines, or emergency repair costs for labor, replacement components, and expedited logistics.

Significant Operational Disruption

Downtime is likely to cause delays in production or coverage, increasing the pressure on internal teams to make up for lost time. It also increases strain on those handling incident response and can have cascading impacts on dependent systems, teams, services, and partners.

Field Service, Logistics, and Inventory Costs

Businesses will need to dispatch technicians to diagnose, repair, and/or replace broken infrastructure to bring systems back online. In a production scenario, they'll also need to facilitate returns and replacements from dissatisfied customers, handling additional warehousing, shipping, and fullfillment tasks.

Engineering and Remediation Time and Effort

Teams must set aside time and resources to conduct root cause analysis, which in turn will help identify and resolve failures and prevent future outages. This may involve the total redesign and requalification of outdated or inadequate systems and components, which in turn necessitates more testing, certification, and compliance verifications.

Reputation and Customer Satisfaction

Significant downtime events are likely to damage customer relationships, leading to lost trust and the potential for churn. This may extend to a more significant negative brand perception or reputation, and in some cases, may reduce shareholder confidence and market competitiveness for the business.

Legal and Compliance Risk

Disruptions can expose businesses to liability claims or regulatory penalties, especially if they endanger or otherwise significantly harm customer well-being. This may involve additional costs stemming from legal disputes, audits, or compliance issues, as well as heightened regulatory scrutiny in regulated industries.

Internal Resource Strain

Solving unexpected downtime is a group effort that requires cross-functional coordination across engineering, operations, supply chain, and service teams. Companies will be forced to place an increased workload on these staff, diverting resources from other projects or initiatives for an extended period of time.

These combined impacts reinforce a critical point: downtime is not just a single event, but a chain reaction of costs, consequences, and remediation efforts. Organizations that rely on always-on infrastructure must shift from reactive downtime response to proactive mitigation, investing in strategies and technologies that reduce risk and strengthen system resilience and reliability.

Key Strategies for Mitigating Downtime

While the risk of downtime can never be eliminated entirely, it can be reduced significantly through a proactive, structured approach to designing and supporting always-on infrastructure. Addressing the root causes outlined earlier—human error, equipment reliability, environmental exposure, and cybersecurity threats—requires a comprehensive strategy and intentional deployment. By combining robust system design, disciplined operational practices, and proven, high-quality hardware solutions, organizations can invest in a reliable foundation that minimizes the likelihood and costs of unplanned outages.

Pre-Deployment Strategies

Designing for reliability is at the root of any effective downtime mitigation strategy. This includes implementing redundancy and critical power paths to help ensure continuity in the event of component failure or malfunction. Modular system designs can also enhance system reliability by enabling more efficient maintenance, simplified upgrades, and reduced disruption during service or replacement. Incorporating these principles from the start helps improve uptime while supporting long-term scalability as infrastructure and demands evolve.

It's equally important that infrastructure adheres to rigorous quality and design standards developed and maintained by governing bodies and industry peers. These include:

IPC-9592

IPC-9592, an industry standard that establishes requirements for power conversion devices used in computing and telecommunications applications. Co-developed by Lineage Power (now OmniOn Power), the standard provides a unified framework for evaluating power supplies across four critical areas: design for reliability, qualification testing, manufacturing conformance testing, and quality processes.

It breaks down expectations based on equipment class:

Class	Description	Expected Life
Class 1	General or standard personal computing devices (PCDs), including consumer computers, peripheral devices, and standard telecom equipment.	5 years
Class 2	Enhanced or dedicated service equipment, including carrier-grade telecom hardware, network-grade computers, and high-reliability system infrastructure.	15 years

Before IPC-9592 was introduced in 2008, individual OEMs often relied on their own qualification requirements and standards, resulting in duplicated testing efforts and inconsistent quality benchmarks across the power industry. Today, this standard serves as a common foundation for qualifying AC/DC adapters, DC/DC converters, and embedded power modules, helping manufacturers deliver the consistent reliability and performance that mission-critical infrastructure demands.

ISO 9001 and TL 9000

ISO 9001 and TL 9000 are globally recognized quality management standards that help organizations establish consistent processes, prevent defects, improve customer satisfaction, and drive continuous improvement.

ISO 9001

The world's most widely adopted quality management standard, providing a framework for developing, maintaining, and continually improving a quality management system.

TL 9000

TL 9000 expands on this foundation with additional requirements developed specifically for the information and communications technology (ICT) industry, including product reliability measurements, lifecycle management processes, supplier-customer communication requirements, and quality performance metrics.

Achieving and maintaining certification to these standards is not a one-and-done process. It requires ongoing audits, documented quality processes, performance measurement, and a demonstrated commitment to improvement. OmniOn Power and its predecessor operations have maintained a Quality Management System certification in accordance with ISO 9001 and TL 9000 since 2001, reflecting more than two decades of continuous adherence to the standards which are designed to promote consistency, reliability, and long-term product performance.

UL Total Certification Program

The UL Total Certification Program is a rigorous certification framework designed to accelerate product certification by integrating testing, validation, and quality control directly into the product development process. Under the program, qualified manufacturers can perform approved testing in their own facilities, enabling faster authorization from UL to use the UL certification mark on compliant products and reducing time to market without sacrificing compliance with stringent safety requirements. The Total Certification Program requires both initial and ongoing responsibilities and actions from a participant to maintain its standing. To participate in the program, an organization must have a comprehensive quality management system, demonstrated testing expertise, and ongoing technical oversight from UL engineers.



SINCE 2004

MAINTAINING UL'S HIGHEST ACCREDITATION

OmniOn Power's Plano, Texas-based R&D lab has maintained **UL's highest product safety data acceptance accreditation since 2004**, reflecting decades of commitment to rigorous testing, validation, and product safety excellence. Achieving this highest level within the UL Total Certification Program is particularly challenging because it requires organizations to demonstrate **lab capabilities, engineering competency, and quality controls** comparable to those maintained by independent certification labs. To maintain this status, participants must undergo continuous assessments, third-party verification, and regular compliance reviews. This includes quarterly technical oversight assessments and annual assessments for the test methods and product categories covered by the Total Certification Program.

OmniOn POWER

OMNIONPOWER.COM

Testing and Validation

After standards-based design comes testing and validation processes. These tests must be comprehensive and detail-oriented, not just to ensure compliance with standards but to help ensure that hardware is prepared to operate as intended across a range of environments, conditions, and applications. For example, OmniOn Power completes a variety of in-house testing on its power conversion products.

OmniOn Power's In-House Testing Capabilities

Electromagnetic Compatibility (EMC) Validation, which leverages a three-meter semi-anechoic EMC test chamber to ensure that systems operate correctly without emitting, or being disrupted by, excess electromagnetic interference.

Design Verification Testing (DVT), which confirms that products meet technical specifications across expected input line, output loading, and temperature operating ranges.

System Integration Testing (SIT), which verifies seamless performance of controllers, rectifiers, converters, inverters, distribution, batteries, and user interfaces across interconnected system components.

Highly Accelerated Life Testing (HALT), which identifies potential failure modes by exposing products to extreme stress conditions that go beyond normal operating limits.

Temperature Humidity Bias (THB) Testing, which includes operating a product at max operating temperature and 85% relative humidity for 1,000 hours to simulate long-term exposure.

High Temperature Operating Bias (HTOB) Testing, which operates and power cycles products at max operating temperatures for 1,000 hours to simulate long-term exposure.

Non-Operating Temperature Cycle (TC) Testing, which subjects devices to 700 accelerated thermal cycles from minimum to maximum storage temperatures to simulate excessive fluctuations in temperature.

Powered Thermal Cycling (PTC) Testing, which tests products operating at nominal conditions with thermal cycling over the typical operating temperature range.

Shock and Vibration Testing, which ensures products' mechanical robustness and resilience under the physical stress of real-world conditions.

These design and validation practices are critical to achieving measurable reliability outcomes. For example, representative products from OmniOn Power that have been engineered and tested to these standards have demonstrated calculated Mean Time Between Failure (MTBF) values exceeding one million hours.

Quality & Manufacturing Excellence

OmniOn Power and its predecessor operations have received numerous renowned quality and manufacturing awards.

1992

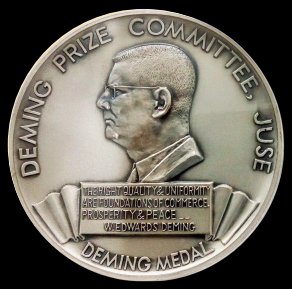
The Shingo Prize for Excellence in Manufacturing

The Shingo Prize is widely regarded as one of the highest honors in manufacturing and operational excellence, often referred to colloquially as the “Nobel Prize of Manufacturing.” Awarded by the Shingo Institute, it recognizes organizations that demonstrate world-class performance through a deeply embedded culture of continuous improvement, principle-based leadership, and sustainable operational excellence.

Consideration for the award involves an exhaustive on-site evaluation of day-to-day operations and sustained, long-term success over multiple years. Unlike many other industry awards, the Shingo Prize evaluates more than just business results, including the behaviors, systems, and organizational culture that help create and maintain operational success.

1994

The Deming Prize for Total Quality Management



Managed by the Union of Japanese Scientists and Engineers (JUSE), the Deming Prize is a global quality award that recognizes organizations and individuals that have implemented Total Quality Management (TQM) processes with exceptional and sustainable results.

It is one of the most respected honors for quality and operational excellence, requiring organizations to establish a company-wide culture of quality, continuous improvement, data-driven decision-making, and customer focus. This makes the Deming Prize—and those organizations that earn it—globally recognized benchmarks for excellence in quality management.

By winning these prestigious awards, OmniOn Power demonstrates its capacity to support the long-term durability and performance required of power equipment in mission-critical environments.



Post-Deployment Strategies

Once proven hardware has been tested and integrated into system infrastructure, teams can extend reliability through continuous monitoring. Employing real-time monitoring across power systems enables proactive, predictive maintenance and early identification of potential failure risks. Advanced system controllers such as OmniOn Power's Pulsar 200 and Millennium X can add this monitoring and control capability to both new equipment and retrofit into existing systems to improve visibility and control for DC systems and beyond. This kind of monitoring helps teams shift from reactive to proactive maintenance, reducing the likelihood of unplanned downtime while improving overall efficiency.

At the operational level, standardizing processes and employee training can help to minimize the risks of human error. Establishing clear procedures for installation, maintenance, and change management helps reduce reliance on manual intervention and ensure consistent execution across teams. By improving communication and accountability, teams can prevent common failures caused by misconfiguration or oversight.

Finally, integrating cybersecurity into infrastructure is essential for hardening power management systems against evolving security threats. By adopting a Zero Trust security approach and aligning with standards such as IEC 62443 and FIPS 140-3, systems can incorporate advanced protections like Secure Boot, EdgeLock®, and hardware-protected cryptographic keys. Together, these measures help enhance system integrity, safeguard critical data, and support secure, resilient operation across power environments.

When combined, these best practices help form a holistic approach to mitigating downtime—one that addresses risk at every level, from hardware design to overall system operation. By investing in quality, validation and testing, continuous monitoring, and robust security, organizations can build always-on infrastructure that performs reliably in any conditions.

The Impact of Preparedness

To illustrate the value of reliability-centric design, consider the continued expansion of modern telecommunications networks. As service providers modernize communications infrastructure by deploying 5G capabilities and increasing network capacity, they face challenges that include aging power systems, geographically distributed assets, limited redundancy at remote sites, and growing demands for continuous network availability. Together, these factors can leave critical communications infrastructure particularly susceptible to unplanned downtime. In these always-on environments, even a single failure can trigger widespread disruption. An outage at a central office, network node, or cell site can impact connectivity for thousands of users and affect the systems and services that depend on the network. Without real-time visibility or built-in redundancy, response efforts are inherently reactive, increasing not just the downtime duration but its associated costs. As telecom networks grow in complexity and traffic volumes increase, the margin for error only continues to shrink. This highlights the importance of not only addressing failures when they occur, but proactively designing systems to prevent them.

Best Practices for Network Resilience

By applying reliability-centric best practices, network operators can significantly enhance resilience and mitigate downtime. Integrating validated, high-efficiency power systems and equipment—including modular, hot-swappable architectures and built-in redundancy—helps to establish a more stable infrastructural foundation. When this equipment has been rigorously tested and validated by the original equipment manufacturer, network operators can be more confident that communications infrastructure will maintain consistent performance across real-world operating conditions, from extreme environments at remote sites to periods of peak network demand.

Beyond hardware, integrated monitoring and control platforms help enable predictive maintenance by providing operators with real-time visibility and early anomaly detection across power systems, batteries, environmental controls, and other critical network infrastructure. Standardized installation and maintenance procedures reduce human error and help organizations translate lessons learned into repeatable deployment and service practices. Likewise, built-in cybersecurity protections help safeguard increasingly connected network infrastructure from evolving threats.

The result is a measurable improvement in reliability and network performance, even amid the challenges of modernizing legacy infrastructure. Reliability-centric telecommunications networks, supported by robust hardware and standards-based processes, are more likely to experience fewer unplanned outages, faster recovery times, and greater overall operational efficiency, helping service providers maintain the uptime and service levels their customers expect.



Maintaining Reliable Power Supplies

Downtime remains one of the most costly and disruptive threats to today's high-profile industries. And as digital infrastructure scales even further, the margin for error will only continue to shrink. With outages costing hundreds of thousands of dollars (if not millions) and having impacts that extend beyond financial losses, reliable power systems have never been more critical.

At OmniOn Power, we can identify the root causes of downtime and take proactive steps to mitigate its varied threats. By incorporating high-quality components, robust design and manufacturing controls, disciplined processes, and resilient hardware—supported by monitoring, testing, and maintenance best practices—teams can build sustainable operations, maximize uptime, and avoid costly outages.

If you'd like to discuss your critical infrastructure and how to help ensure uptime at your facility, contact OmniOn Power today.

About OmniOn Power

OmniOn Power designs and develops reliable, quality, and efficient power solutions for today's evolving data center, telecommunications, and industrial sectors. With a heritage that dates back more than 100 years, our deep domain expertise in mission-critical applications allows us to anticipate our customers' future power needs and help ensure their sustained success. We collaborate with customers to co-develop solutions that solve their power infrastructure challenges while optimizing uptime and efficiency.

Get In Touch

Visit omnionpower.com to learn more and to find the right solution for your power needs

OMNIONPOWER.COM
LINKEDIN.COM/COMPANY/OMNIONPOWER
1-877-546-3243

Disclaimer:

This white paper is provided for informational purposes only. Statements regarding performance, reliability, certifications, and product capabilities are based on available information at the time of publication and may vary depending on application, operating conditions, configuration, and maintenance practices. This document does not create any warranty, guarantee, or contractual commitment

We reserve the right to make technical changes or modify the contents of this document without prior notice. We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents - in whole or in parts - is forbidden without prior written consent of OmniOn Power Inc.

© Copyright 2026 OmniOn Power™