WHITEPAPER

SmartPDU – The central system component in the server rack

Secure power supply, load management, operational efficiency and physical security in modern data centers

Executive Summary

Data centers are undergoing fundamental change: increasing power densities, AI workloads with dynamic load profiles, stricter compliance requirements, and growing threats from physical manipulation and operational errors are necessitating new concepts in racks.

The classic PDU as a “power strip” is no longer sufficient for this. The SmartPDU, on the other hand, is becoming a central system component in the rack, as it combines high-availability power distribution, energy and power quality measurement, precise load management, early fault detection, rack access, and physical security in a single system.

This white paper describes the SmartPDU as a “rack backbone” and shows how it meets the most important requirements of modern data centers:

- Ideal and highly secure power supply
- Load management & utilization planning
- Highest possible physical security
- Optimization of operational processes
- Early fault detection & predictive maintenance
- Central system component for rack access (including rack lever/locking)
- Integration via REST API, SNMP v2/v3, and webhooks

Content

1. Starting point: Why the PDU must become a SmartPDU

1.1. Power density, dynamics, and complexity are increasing

Developments in recent years show a clear shift in power densities in racks: While classic enterprise racks were often operated in the range of 3 to 10 kW, modern virtualization and storage racks typically range from 10 to 20 kW, and AI racks with GPU/accelerator infrastructure already reach 30 to 80 kW and beyond. This development is changing the nature of rack operation because power distribution and contact points not only have to transmit more power, but are also subjected to greater stress from dynamic load changes, power-up processes, and nonlinear consumers. Modern server power supplies generate high inrush current peaks, which place greater strain on protective devices and switching components and can lead to false trips in unfavorable constellations. At the same time, nonlinear loads lead to harmonics, increasing THD, and higher neutral conductor loads, which increases the thermal and electrical stress profile in the rack.

In addition, the operational situation is exacerbated because remote hands, outsourcing, and tightly scheduled maintenance windows increase the likelihood of human error, and because energy transparency and billable measurements are increasingly required in the context of MID *(Measuring Instruments Directive)* und ESG (*Environmental, Social, Governance).*

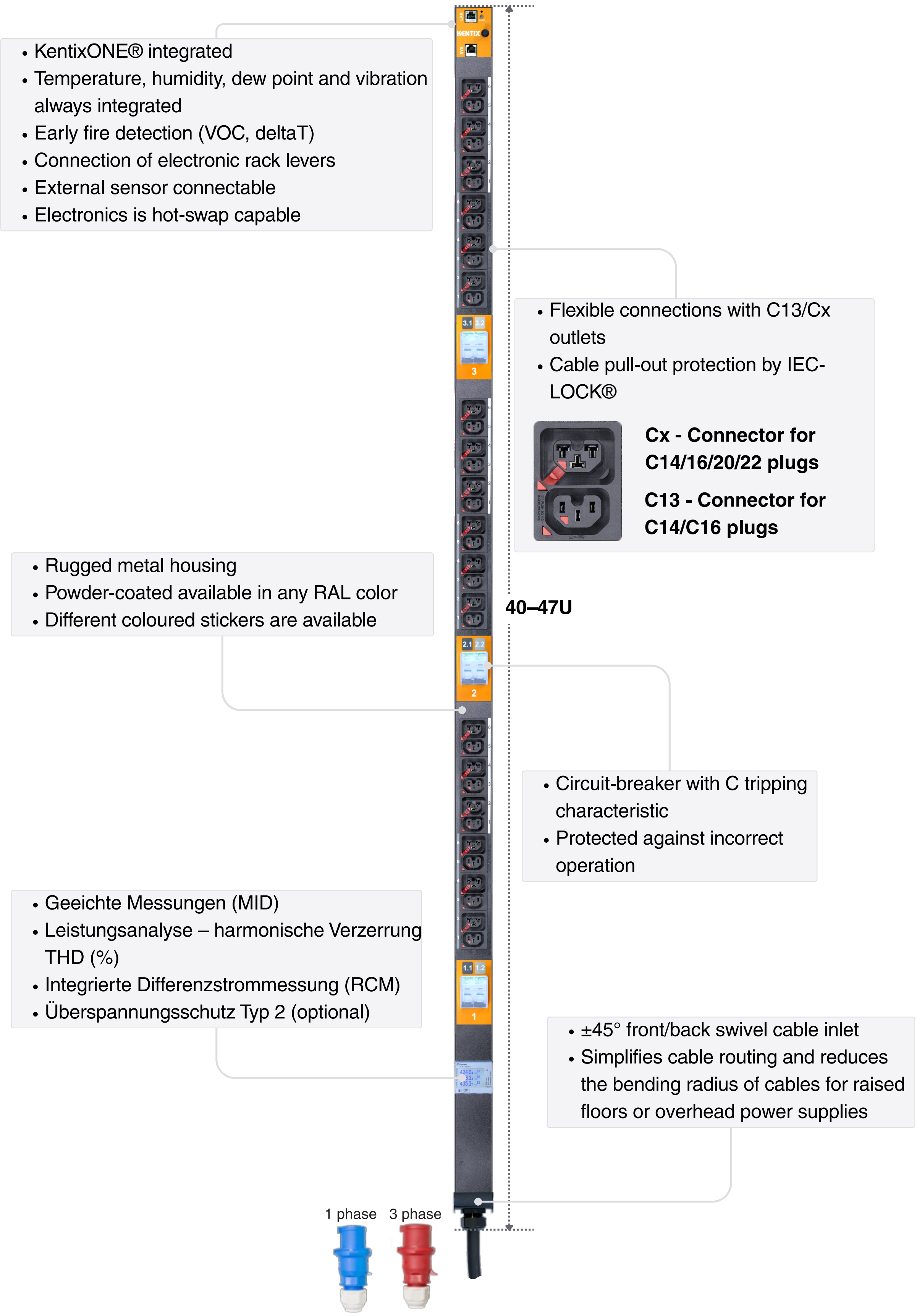
All in all, this creates an environment in which power distribution can no longer be “passive,” but must be actively monitored, understood, and made controllable.

1.2. The greatest danger arises in the rack at the power distribution point

Many critical incidents in the rack do not originate in the server itself, but rather in plug connections, contacts, contact resistance, local heat input, incorrect fusing, or overloading of individual paths. The underlying physical principle is power dissipation $P = I^2 \cdot R$, which illustrates that even low resistance at contact points leads to significant heat input at high currents. Since the current is squared, the risk grows disproportionately with increasing rack power, making power distribution in the rack one of the most important risk factors.

This is precisely why the PDU is the most natural location for early thermal and chemical indicators, differential current monitoring, power quality measurement, tamper detection, and automated responses such as load switching or defined shutdowns. The SmartPDU is therefore not just an “upgrade,” but a functional necessity for managing the risks of modern rack power.

1.3. Typical SmartPDU Setup



- KentixONE® integrated
- Temperature, humidity, dew point and vibration always integrated
- Early fire detection (VOC, deltaT)
- Connection of electronic rack levers
- External sensor connectable
- Electronics is hot-swap capable

- Flexible connections with C13/Cx outlets
- Cable pull-out protection by IEC-LOCK®

Cx - Connector for C14/16/20/22 plugs

C13 - Connector for C14/C16 plugs

- Rugged metal housing
- Powder-coated available in any RAL color
- Different coloured stickers are available

- Circuit-breaker with C tripping characteristic
- Protected against incorrect operation

- Geeichte Messungen (MID)
- Leistungsanalyse – harmonische Verzerrung THD (%)
- Integrierte Differenzstrommessung (RCM)
- Überspannungsschutz Typ 2 (optional)

- ±45° front/back swivel cable inlet
- Simplifies cable routing and reduces the bending radius of cables for raised floors or overhead power supplies

2. SmartPDU as a central rack system component (system definition)

2.1. Architectural principle: “Power + Security + Monitoring + API”

A SmartPDU is not just a power distributor, but a critical rack management platform that connects multiple subsystems in a consistent architecture. In the **power path layer**, the SmartPDU forms the secure electrical basis through A/B feed, switching and protection devices, measuring transformers, MID meters, and IEC 60320 socket modules.

The **Measurement & Quality Layer** extends this basis with precise measurement functions for current, voltage, power, and energy, as well as power quality parameters such as THD, frequency, Cos ϕ, and crest factor, supplemented by residual current measurement (RCM) as a safety and status indicator.

In the **Environmental & Safety Layer**, the rack is monitored in its physical reality by monitoring temperature, humidity, and dew point, and safety-related events can be detected through early fire detection using VOC and temperature sensors as well as vibration detection.

The **Control & Access Layer** enables the SmartPDU to act by allowing outlets to be switched selectively, loads to be prioritized, and physical rack access to be controlled via electronic handles or rack levers.

Finally, the **Network & Integration Layer** ensures that the system does not remain isolated: PoE-powered electronics increase resilience, while REST API, SNMP v2/v3, webhooks, and optional Syslog/SIEM connections *(Security Information and Event Management)* enable deep integration into operational and security processes. The combination of these layers creates a central rack component that brings together power, operation, security, and automation in a single system.

3. Highly secure power supply – “ideal supply” in the rack

3.1. Requirements of modern data centers

Modern data centers are designed for availability, which is why redundancy concepts such as N+1 or 2N must be implemented not only at the building or UPS level, but consistently down to the rack. This includes the clear separation of two supply paths, the selective design of protective devices, safe operation in the event of a feed failure, and fast and clear fault localization. In addition, the communication and controllability of power distribution is becoming increasingly important because a PDU must not itself become a single point of failure in the event of a fault, for example by monitoring and access breaking down as soon as the main supply fails. An ideal rack supply is therefore not only redundant, but also measurable, diagnosable, and operatively controllable.

3.2. Two separate power supply paths (PSU feed): correct connection & load

The basic principle of A/B redundancy is that a rack is supplied via **feed A** (PDU A) and **feed B** (PDU B) and two power supplies are connected so that PSU1 is connected to feed A and PSU2 to feed B (PSU = power supply unit, e.g., the UPS). Only then can it be guaranteed that if one feed fails, the remaining path will take over the power supply and that maintenance can be carried out on one path without interrupting operation. In practice, however, errors often occur, for example when both power supplies are connected to the same feed and redundancy only appears to exist, or when an asymmetrical load causes one path to operate close to its limit load while the other remains underutilized. Another common misconception is the assumption that the load is always distributed exactly 50/50 between both power supplies, although this can vary depending on the power supply type, firmware, temperature, and load condition.

A resilient design therefore takes into account that both feeds should typically operate in the range of 40–60% during normal operation, while in the event of a fault, one feed must be able to carry the entire rack load.

It has become established planning practice to limit the maximum continuous load per feed to around 80% in order to accommodate thermal reserves, standard reserves, and short-term peaks, such as during boot processes. The SmartPDU supports this concept by measuring current, power, and energy per feed, providing trends over defined periods, displaying reserve capacities in kW, and implementing warning thresholds that indicate compromised N redundancy at an early stage.

In the event of an incident, it can automatically alert, trigger webhooks, prioritize non-critical consumers, or shut down defined outlet groups to ensure stability.

4. Load management & operational efficiency

4.1. Load management in the rack

Load management means not only avoiding overload, but also controlling operations in such a way that power paths remain stable, protective devices are not subjected to unnecessary stress, and critical consumers continue to be supplied even in fault situations. In practice, this includes dynamic load distribution, defined start sequences (staggered startup), prioritization of consumers according to criticality, and remote power cycling per outlet.

Load management is particularly crucial in AI environments because GPU clusters can jump from low utilization to high power consumption within seconds and because highly efficient power supplies optimize energy consumption but create new stress factors in power distribution due to switch-on and harmonic components. A SmartPDU makes these dynamics transparent and controllable, thereby reducing the risk of uncontrolled shutdowns and thermal overloads.

4.2. Capacity planning

Capacity planning is the operational prerequisite for scalability in the rack because it prevents capacity limits from only becoming apparent in the event of a malfunction. The SmartPDU acts as a “rack capacity planner” by recording load values per phase including neutral conductor, and per feed, and deriving reserve capacities from this data.

Trend analyses and simulations provide reliable answers as to how much additional power can be integrated into a rack without compromising redundancy concepts or exceeding thermal limits. This transforms capacity planning from a gut feeling to a data-based decision.

5. Optimal circuit breakers taking into account inrush currents

5.1. Problem: Inrush currents of modern server power supplies

Modern server power supplies, especially those with active PFC, have large input capacitors and generate high inrush currents when switched on. These currents can trip circuit breakers, stress relays and switching components in PDUs, and cause thermal stress on contact points, especially when multiple systems are started simultaneously, such as after a power failure or during maintenance windows. The challenge is to design protective devices that provide reliable protection and selective tripping on the one hand, but tolerate the dynamic power-up processes of modern IT loads on the other.

5.2. Requirements for protective devices in PDUs

Protective devices must be selective in order to provide upstream protection so that faults are localized and entire supply lines do not fail. At the same time, they must be inrush-tolerant, thermally stable, easy to maintain, and clearly documented so that operating and service processes can be carried out safely. In highly compacted racks, the thermal reserve of the protective devices is a decisive factor because continuous load and ambient temperature can influence the tripping characteristics.

5.3. Selection of characteristics (B/C/D)

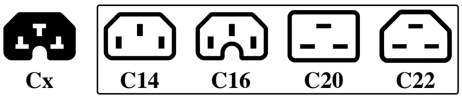
When selecting the characteristic, it is generally apparent that B characteristics are often unsuitable due to their sensitivity to high inrush currents, while C characteristics often form the standard for many IT loads. D characteristics offer higher inrush tolerance, but require consideration of network impedances and shutdown conditions in order to trigger safely in the event of a fault. In data centers, C or D characteristics are therefore often appropriate, depending on the network structure, protection concept, and verification. The SmartPDU increases operational reliability by logging inrush events, correlating switching operations, recommending or automating start sequences, and providing early warnings when protective devices are approaching their thermal limits.

Copyright Kentix GmbH 2026

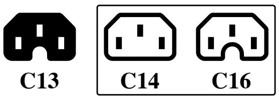
6. Sockets according to IEC 60320 – New Cx sockets

6.1. IEC 60320 overview

IEC 60320 is the established standard for rack connectors, with C13/C14 typically used for standard IT loads up to 10A and C19/C20 for higher power and currents up to 16A, as found in blade systems, high-end servers, or GPU nodes. Standardization reduces complexity and the risk of errors and forms the basis for serviceability in heterogeneous environments.



The Cx standard integrates several plug types into a single socket, essentially replacing C19 sockets.



6.2. Advantages in rack operation

The advantages of IEC 60320 connector systems lie in their standardized geometry and safety, defined current carrying capacity and temperature limits, and clear connector compatibility. At the same time, they enable high packing density, which is particularly important for vertical rack PDUs. The worldwide availability of standardized cables greatly simplifies logistics and remote hands, while robust connectors and optional locking mechanisms increase operational reliability and minimize accidental pulling as a common source of error.

6.3. Operational reliability: Contact quality and hotspots

Since contact points in high-performance racks become critical points, the SmartPDU should be able to detect hotspot risks not only indirectly via load values, but also via environmental and safety data. If rising temperatures or VOC anomalies (air quality) are registered while the current remains constant, this can be an indication of increasing contact resistance and serve as an early warning signal for preventive maintenance. In addition, recording plug cycles and load profiles can help evaluate the stress on individual outlets and identify weak points.

7. Residual current measurement (RCM) in the PDU

7.1. What is RCM?

RCM (Residual Current Monitoring) measures the differential current between the forward and return conductors. In ideal conditions, the sum of the currents is zero; deviations indicate leakage currents or faults, such as insulation problems, defective mains filters, moisture, contamination, or cable and connector problems. RCM is therefore a highly effective indicator of electrical risks that are not visible in conventional current measurements.

7.2. Why RCM in the rack is crucial

IT power supplies generate system-related leakage currents, and when device density is high, these currents add up, which can lead to unexpected shutdowns of RCD/FI protective devices or safety risks. RCM therefore enables early detection before critical thresholds are reached and supports condition-based maintenance planning. In OT and industrial environments, RCM is becoming even more important because insulation conditions, environmental conditions, and safety certifications are often evaluated more strictly, and RCM can serve as a measurable indicator in protection and compliance concepts.

7.3. SmartPDU functions related to RCM

A SmartPDU should record RCM per feed or phase, support multi-level alarms (warning/critical), analyze trends over weeks and months, and correlate events with outlets or operating states. This transforms a pure measurement function into an operational early warning system that translates technical risks into concrete instructions for action.

8. THD measurement (Total Harmonic Distortion) – real-time power quality

8.1. Why THD is mandatory today

Data centers consist mainly of non-linear consumers such as switching power supplies, UPS rectifiers, and—depending on the architecture—frequency-controlled drives in the cooling system. AI clusters amplify these effects through dynamic load profiles. High THD can cause transformers and cables to heat up more, overload neutral conductors, affect protective devices, distort measured values, and reduce the service life of infrastructure components in the long term. Power quality thus becomes a direct factor in operational reliability and efficiency.

8.2. SmartPDU as a power quality sensor in the rack

A SmartPDU with THD measurement provides THD(U) and THD(I) per phase, detects power quality degradation, and can alert when thresholds are exceeded. This data forms the basis for capacity planning, for optimizing UPS and filter concepts, and for predictive maintenance strategies, because in many cases, power quality is an early indicator of overloaded or poorly dimensioned infrastructure.

9. Integrated environmental monitoring (temperature, humidity, dew point)

9.1. Why dew point measurement is crucial

In modern data centers, not only is the absolute temperature critical, but also the risk of condensation. When the dew point reaches the local temperature, moisture can precipitate, promoting corrosion, short circuits, and insulation deterioration, which can indirectly affect RCM values. The dew point can become a decisive risk factor, especially in the event of airflow changes, cold aisle containment, leaks, or incorrectly set climate parameters.

9.2. SmartPDU as a rack climate monitor

The SmartPDU monitors the temperature at the top and bottom of the rack, records humidity, calculates the dew point, and alerts you if the dew point and rack temperature approach critical levels. This makes climate risk measurable and allows it to be addressed preventively before it causes electrical damage.

10. Vibration detection: detecting mechanical influences

Vibration and shock events can be caused by improper installation, door slamming, transport and relocation, unauthorized tampering, or structural problems with the rack and base. In highly critical rack operations, such events are not just “mechanical” issues, but potential precursors to contact problems, loose connections, or physical security incidents. A SmartPDU with vibration detection can document and correlate events and report them as security events to SIEM systems, ensuring that physical tampering does not go unnoticed and can be forensically traced.

11. Early fire detection in the PDU (VOC + temperature)

11.1. Why early fire detection belongs in the PDU

Most critical causes of fire in racks originate from plugs, power distribution, and contact resistance. Due to **$P = I^2 \cdot R$**, the risk increases significantly with power, making power distribution the central location for preventive fire detection. Traditional smoke detectors often react too late, when smoke particles are already present, whereas thermal or chemical precursors can be measured earlier.

11.2. VOC (volatile organic compounds) as an early indicator

VOC sensors detect thermal decomposition products, preliminary stages of smoldering, and outgassing from plastics and cable materials. In combination with temperature profiles, this results in significantly earlier detection than with purely smoke-based methods, and warnings can be made more localizable because they originate near the rack and can be correlated with power and load data.

11.3. Response plan

A SmartPDU should provide multi-level warnings (pre-alarm/alarm), support automatic measures, and have clear integration paths into incident processes. This includes defined shutdowns of outlet groups, triggering an alarm chain, and automated ticket creation via webhooks, so that detection becomes a controlled operational process.

12. Electricity and energy measurement with MID-calibrated meters

12.1. Why MID is important

Billing and multi-client capability are key requirements in colocation and mixed environments, as are auditability, ESG and energy reports, and reliable cost center accounting. MID-calibrated meters (Measuring Instruments Directive) provide the basis for billable and traceable energy measurement that stands up to scrutiny in audits and reports.

12.2. SmartPDU as a billing and transparency system

The SmartPDU enables kWh recording per feed and phase, supports export via API, and provides long-term data over years. Ideally, the logging is tamper-proof and auditable, making energy transparency usable not only technically but also commercially.

13. PoE-powered electronics: Data access even in the event of a power failure

13.1. Problem: “PDU dead = monitoring dead”

When a traditional PDU fails or both feeds are interrupted, not only are power functions lost, but also monitoring, diagnostics, and controllability. However, it is precisely in this situation that data and access are particularly valuable, because error analysis, restart, and security processes depend on them.

13.2. Solution: PoE as an independent power source

A SmartPDU with PoE-powered electronics can continue to provide measurement data and logs, send alarms, and—depending on the architecture—maintain control and access mechanisms. This makes it the “last resort” in the rack in the event of a failure, which is particularly crucial for maintenance, security/forensics, and AI racks with very high downtime costs.

14. Communication interfaces: REST API, SNMP v2/v3, webhooks

14.1. Requirements for system integration

Data centers consist of heterogeneous system landscapes such as DCIM *(Data Center Infrastructure Management)*, BMS *(Building Management)*, NMS *(Network Management System)*, SIEM *(Security Information and Event Management)*, ITSM *(IT Service Management)* and automation workflows. A SmartPDU must therefore offer standardized and secure interfaces in order to not only display measurement data and events, but also integrate them into processes that automatically escalate, document, and respond.

14.2. REST API

REST APIs enable modern integration for configuration, measured values, and event data, support role-based authentication, and can provide idempotent switching commands. Structured JSON events facilitate integration into automation and data platforms.

14.3. SNMP v2/v3

SNMP remains the standard in many NMS environments, with SNMPv3 being crucial for security through AuthPriv. Vendor MIBs and standardized OIDs enable deep monitoring, while traps for critical events such as RCM, temperature, THD, or feed failures speed up operations.

14.4. Webhooks

Webhooks are ideal for event-driven architectures because they can route real-time events directly into ChatOps or incident response processes. This turns monitoring into an active response mechanism without polling intervals limiting speed.

15. Physical security & rack access: SmartPDU as a central security authority

15.1. SmartPDU + rack lever = physical root of trust in the rack

When power distribution, sensor technology, and access control are combined in a single system, a new approach emerges: the SmartPDU becomes a “rack security control unit.” This means that physical security is no longer considered an add-on, but rather a core function at the central point of the rack.

15.2. Access functions

An electronic rack lever or handle enables controlled access with role and rights management, while a tamper-proof event log documents who had access, when, and for how long. In addition, the SmartPDU can alert you to tampering—for example, via vibration or door contacts—and integrate events into SIEM systems, thereby integrating physical security into digital security processes.

16. Future trends: What will characterize the SmartPDU of the future?

16.1. AI data centers

AI data centers require extremely high power density, very fast load changes, maximum availability, and precise energy transparency. A smart PDU of the future must therefore measure in high resolution, deliver THD and power quality analyses in real time, support intelligent load prioritization, and provide interfaces for automated orchestration so that power supply and operation can keep pace with the dynamics of modern AI clusters.

16.2. Predictive maintenance and digital twins

The next step is to combine power, environmental, and safety data with anomaly detection systems that reveal aging processes. When power history, temperature, VOC trends, and RCM behavior are evaluated together, it is possible to predict, for example, that a plug connection is aging or that a power supply is reacting atypically. This results in digital twins and risk scoring per rack, which makes preventive maintenance economical.

16.3. Security-by-Design

With increasing connectivity, a SmartPDU must implement security by design, i.e., secure boot, signed firmware, hardened communication (SNMPv3/TLS), and SIEM-native events. This makes it not only functional but also a trustworthy infrastructure component in terms of security.

17. Use in OT applications (operational technology)

OT environments require long life cycles, robust functionality in harsh environmental conditions, stricter EMC considerations, and security/compliance requirements such as IEC 62443.

At the same time, availability is often critical to production, and interventions must be particularly controlled because OT systems do not have the same maintenance flexibility as IT systems. The SmartPDU offers energy transparency in control cabinets, early fire and overheating detection, RCM for insulation monitoring, and robust alarming via established interfaces.

In many OT scenarios, connection via gateways to industrial protocols is also useful so that SmartPDU data can be integrated into control and safety systems.

18. Conclusion

Modern data centers—especially high-density and AI data centers—place significantly higher demands on rack infrastructure: increasing power densities, dynamic load profiles, stricter compliance requirements, and growing risks from operational errors and physical tampering. In this environment, a traditional PDU is no longer sufficient for pure power distribution.

The SmartPDU is becoming a central system component in the server rack, as it combines key functions for safety and operation that go far beyond pure power distribution: highly available power supply via two feeds, precise load management, utilization planning, MID-compliant energy metering, and real-time monitoring of power quality (THD). Supplemented by residual current measurement (RCM), environmental monitoring (temperature, humidity, dew point), vibration detection, and early fire detection using VOC and temperature sensors, this creates a comprehensive security and diagnostic system directly at the most critical point of the rack—the power distribution. This is particularly relevant because electrical contact points and contact resistances pose a disproportionately high risk at high currents ($P = I^2 \cdot R$).

PoE-powered electronics ensure that the SmartPDU remains communicative even in the event of feed failures and continues to provide measurement data, events, and control functions. Open interfaces such as REST API, SNMP v2/v3, and webhooks turn it into an integration hub for DCIM, monitoring, ITSM, and SIEM processes.

The SmartPDU thus forms the basis for secure, efficient, and future-proof rack operation—both in data centers and in OT applications. It is a key enabler for availability, operational reliability, and automation in the next generation of IT and AI infrastructures.

19. Use case mapping: SmartPDU in IT operations

Use case / operational problem	Data Center	Server room (On-Prem)	Edge / Remote Sites	Typical benefits
Energy transparency & billing (kWh / cost centers)	✓✓✓	✓✓	✓✓	Consumption per rack/outlet visible, energy reports, cost allocation
Load management & capacity planning (A-/B-feed, phase, reserve)	✓✓✓	✓✓	✓	Prevents overload, better rack utilization, predictability
Early detection of electrical faults (RCM / residual current)	✓✓✓	✓✓✓	✓✓	Detects defective power supplies/ leakage currents early - fewer failures/fire risk
DGUV-V3 / Compliance Support	✓✓	✓✓✓	✓	Helps with proof of electrical safety / inspection obligations
Remote power/port switching (reboot without on-site intervention)	✓✓	✓✓	✓✓✓	Saves trips, faster troubleshooting (e.g., router/server hangs)
Environmental monitoring in the rack (temperature, humidity, dew point)	✓✓	✓✓✓	✓✓✓	Prevents heat/moisture damage, better climate control
Early fire detection directly at the rack	✓✓✓	✓✓	✓	Minimizes risk of failure/damage, faster alerting
Early fire detection directly at the rack	✓✓✓	✓✓	✓✓	Uniform monitoring instead of a patchwork of tools
Tamper protection / plug safety (IEC lock)	✓✓	✓✓	✓✓	Prevents accidental pulling - less unplanned downtime
SLA/audit evidence (measurements, events, history)	✓✓✓	✓✓	✓✓	Reporting, traceability, operational safety

Legend:

✓ = relevant / frequently, ✓✓ = very relevant, ✓✓✓ = key drivers

20. Glossary

A/B Feed (Dual Feed / Redundant Feed)

Redundant rack power concept using two independent power supply paths (Feed A and Feed B) to ensure availability if one feed fails.

AI Rack

A high-density rack designed for GPU/accelerator systems, typically requiring extremely high power (30–80 kW and beyond).

API (Application Programming Interface)

A standardized interface enabling software systems to communicate with the SmartPDU (e.g., retrieving measurements or switching outlets).

Availability (Data Center Availability)

The ability of a data center or rack system to remain operational without downtime, often ensured by redundancy concepts like N+1 or 2N.

BMS (Building Management System)

A building automation system that monitors and controls infrastructure such as cooling, ventilation, and power.

Circuit Breaker Characteristics (B / C / D)

Tripping behavior categories for circuit breakers:

- **B** = sensitive, trips early
- **C** = standard for IT loads
- **D** = high inrush tolerance

Cos ϕ (Power Factor)

Measurement describing how efficiently electrical power is converted into useful work. Poor Cos ϕ indicates inefficiency and higher reactive power.

Crest Factor

Ratio between peak current and RMS current. Important for detecting stress caused by nonlinear loads.

DCIM (Data Center Infrastructure Management)

Software platform for monitoring and managing data center infrastructure (power, cooling, racks, capacity).

Dew Point

The temperature at which moisture condenses. If rack temperature reaches dew point, condensation risk increases significantly.

Digital Twin

A data-driven virtual representation of a rack/system used for simulations, anomaly detection, and predictive maintenance.

Differential Current

The difference between outgoing and returning current in a circuit. Deviations indicate leakage current or insulation faults.

Dynamic Load Changes

Fast changes in power consumption (common in AI/GPU systems), stressing power distribution and protective devices.

ESG (Environmental, Social, Governance)

A compliance and reporting framework increasingly requiring transparent and auditable energy measurements.

Feed Failure

Loss of one power path (Feed A or Feed B). Redundant design ensures the remaining feed can take over.

Harmonics

Electrical distortions caused by nonlinear loads, resulting in overheating and reduced infrastructure lifetime.

High-Density Rack

Rack operating at significantly higher power levels (10–80+ kW) compared to traditional enterprise racks.

Hotspot

A local overheating point often caused by increased contact resistance in connectors or plugs.

IEC 60320

International standard defining rack power connectors such as C13/C14 and C19/C20.

Inrush Current

A high short-term current peak occurring when devices power up (server PSUs), potentially causing false breaker trips.

ITSM (IT Service Management)

Service process systems (ticketing, workflows) integrating alarms and operational responses.

Leakage Current

Unwanted current flowing to ground due to filters, insulation faults, moisture, or contamination.

Load Management

Operational control of rack power usage, including prioritization, staggered startup, and outlet switching to avoid overloads.

Load Prioritization

Mechanism ensuring critical devices stay powered while non-critical loads can be shut down during incidents.

MID (Measuring Instruments Directive)

EU directive ensuring energy meters are calibrated and legally usable for billing and audits.

MID-Calibrated Meter

A certified energy meter suitable for billable kWh measurement and compliance reporting.

Monitoring Layer

A SmartPDU architecture component that measures power, environment, and safety parameters continuously.

N+1

Redundancy design where one additional component is available beyond what is required for normal operation.

2N

Full redundancy design where an entire second independent system exists (complete duplication).

Neutral Conductor Load

Current load on the neutral conductor, often increased by harmonics in nonlinear IT loads.

Nonlinear Load

Loads like switching power supplies that draw current unevenly and generate harmonics.

OT (Operational Technology)

Industrial and production systems (machines, control cabinets) requiring robust, long-lifecycle infrastructure monitoring.

Outlet Switching

Remote controlled switching of individual power outlets for rebooting, shutdown, or load shedding.

$P = I^2 \cdot R$

Power dissipation formula showing heat increases strongly with higher current and contact resistance, explaining hotspot/fire risk.

PDU (Power Distribution Unit)

Device distributing electrical power inside a rack, traditionally passive.

SmartPDU

An advanced PDU combining power distribution with monitoring, measurement, security functions, automation, and network integration.

PoE (Power over Ethernet)

Technology providing electrical power through Ethernet cabling, allowing SmartPDU electronics to stay alive even during feed failures.

Power Density

The amount of electrical power used per rack (kW). Rising density increases thermal and electrical risks.

Power Quality

Electrical stability indicators such as THD, voltage stability, frequency, harmonics, and crest factor.

Predictive Maintenance

Maintenance approach based on measured trends and anomalies to detect failures before they happen.

RCM (Residual Current Monitoring)

Monitoring method measuring leakage/differential currents to detect insulation faults, moisture, or filter issues early.

RCD / FI

Residual current protection device that trips when leakage current exceeds a threshold (safety shutdown).

Remote Hands

Technicians performing on-site actions for customers/operators, increasing the need for error-proof infrastructure.

REST API

Modern web-based API interface using HTTP and JSON for integration into automation systems.

Selective Tripping

Protection concept where only the faulty circuit trips, preventing full rack or upstream power loss.

SIEM (Security Information and Event Management)

Security platform collecting and correlating events (tamper, vibration, access logs, alarms) for incident response.

SNMP (v2/v3)

Network monitoring protocol widely used in data centers. SNMPv3 adds encryption and authentication (secure monitoring).

Staggered Startup

Controlled sequential startup of devices to avoid simultaneous inrush current peaks.

Switching Components

Relays, breakers, and switching mechanisms inside PDUs that can be stressed by high inrush currents.

Tamper Detection

Detection of unauthorized physical manipulation (rack door, vibration, access handle events).

THD (Total Harmonic Distortion)

Power quality metric measuring harmonic distortion in voltage (THD(U)) and current (THD(I)).

Thermal Stress

Heat load affecting components due to high current, ambient temperature, and poor contact resistance.

Trend Analysis

Evaluation of long-term measurement data to detect capacity limits, anomalies, and degradation patterns.

UPS (Uninterruptible Power Supply)

Backup power system ensuring power continuity during outages or instability.

VOC (Volatile Organic Compounds)

Gases released by overheated plastics/cables, used as an early indicator of smoldering and fire risk.

Webhook

Event-driven interface that automatically pushes SmartPDU alarms/events into ITSM, ChatOps, or automation systems.

Kentix GmbH
Carl-Benz-Straße 9
55743 Idar-Oberstein - Germany
kentix.com

About Kentix

Every company has physical security needs. These needs must be met quickly and scalably. Kentix has developed a revolutionary, simple solution: KentixONE. From access control to alarm and video technology, everything is 100% IoT-based and combined in a single platform. KentixONE merges eight conventional security systems and proactively detects over 40 hazards. It couldn't be simpler. Companies from all industries use Kentix GmbH products to protect their business and infrastructure against physical hazards and human error, while also complying with legal requirements. Development and production take place exclusively in Germany.

As part of the **ASSA ABLOY Group**, the world's leading provider of access solutions, we combine the innovative power of an agile technology company with the strength of a global corporate group.

Copyright Kentix GmbH 2026