KENTIX
ASSA ABLOY

WHITEPAPER

SmartPDU – Die zentrale Systemkomponente im Serverrack

Sichere Stromversorgung, Lastmanagement, Betriebseffizienz und physische Sicherheit in modernen Data Centern

WHITEPAPER

Executive Summary

Rechenzentren unterliegen einem fundamentalen Wandel: Steigende Leistungsdichten, KI-Workloads mit dynamischen Lastprofilen, strengere Compliance-Anforderungen sowie wachsende Bedrohungen durch physische Manipulation und operative Fehler machen neue Konzepte im Rack erforderlich.

Die klassische PDU als „Steckdosenleiste“ ist dafür nicht mehr ausreichend. Die SmartPDU hingegen wird zur zentralen Systemkomponente im Rack, da sie hochverfügbare Stromverteilung, Energie- und Netzqualitätsmessung, präzises Lastmanagement, Fehlerfrüherkennung sowie Rackzugriff und physische Sicherheit in einem System verbindet.

Dieses Whitepaper beschreibt die SmartPDU als „Rack-Backbone“ und zeigt, wie sie die wichtigsten Anforderungen moderner Rechenzentren erfüllt:

- ideale und hochsichere Stromversorgung
- Lastmanagement & Auslastungsplanung
- höchstmögliche physische Sicherheit
- Optimierung des operativen Betriebs
- Fehlerfrüherkennung & Predictive Maintenance
- zentrale Systemkomponente für den Rackzugriff (inkl. Rackhebel/Locking)
- Integration über REST API, SNMP v2/v3 und Webhooks

WHITEPAPER

Inhaltsverzeichnis

WHITEPAPER

1. Ausgangslage: Warum die PDU zur SmartPDU werden muss

1.1. Leistungsdichte, Dynamik und Komplexität steigen

Die Entwicklung der letzten Jahre zeigt eine eindeutige Verschiebung der Leistungsdichten im Rack: Während klassische Enterprise-Racks häufig im Bereich von 3 bis 10 kW betrieben wurden, liegen moderne Virtualisierungs- und Storage-Racks typischerweise bei 10 bis 20 kW, und KI-Racks mit GPU-/Accelerator-Infrastruktur erreichen bereits heute 30 bis 80 kW und darüber hinaus. Mit dieser Entwicklung verändert sich die Natur des Rackbetriebs, weil Stromverteilung und Kontaktstellen nicht nur mehr Leistung übertragen müssen, sondern auch stärker durch dynamische Lastwechsel, Einschaltvorgänge und nichtlineare Verbraucher belastet werden. Moderne Servernetzteile erzeugen hohe Einschaltstromspitzen, die Schutzorgane und Schaltkomponenten stärker beanspruchen und in ungünstigen Konstellationen zu Fehlauslösungen führen können. Gleichzeitig führen nichtlineare Lasten zu Oberwellen, steigender THD und höheren Neutralleiterbelastungen, wodurch das thermische und elektrische Stressprofil im Rack zunimmt.

Ergänzend dazu verschärft sich die operative Situation, weil Remote Hands, Outsourcing und eng getaktete Wartungsfenster die Wahrscheinlichkeit menschlicher Fehler erhöhen und weil Energie-Transparenz und abrechnungsfähige Messungen im Kontext von MID *(Measuring Instruments Directive)* und ESG (*Environmental, Social, Governance)* zunehmend gefordert werden.

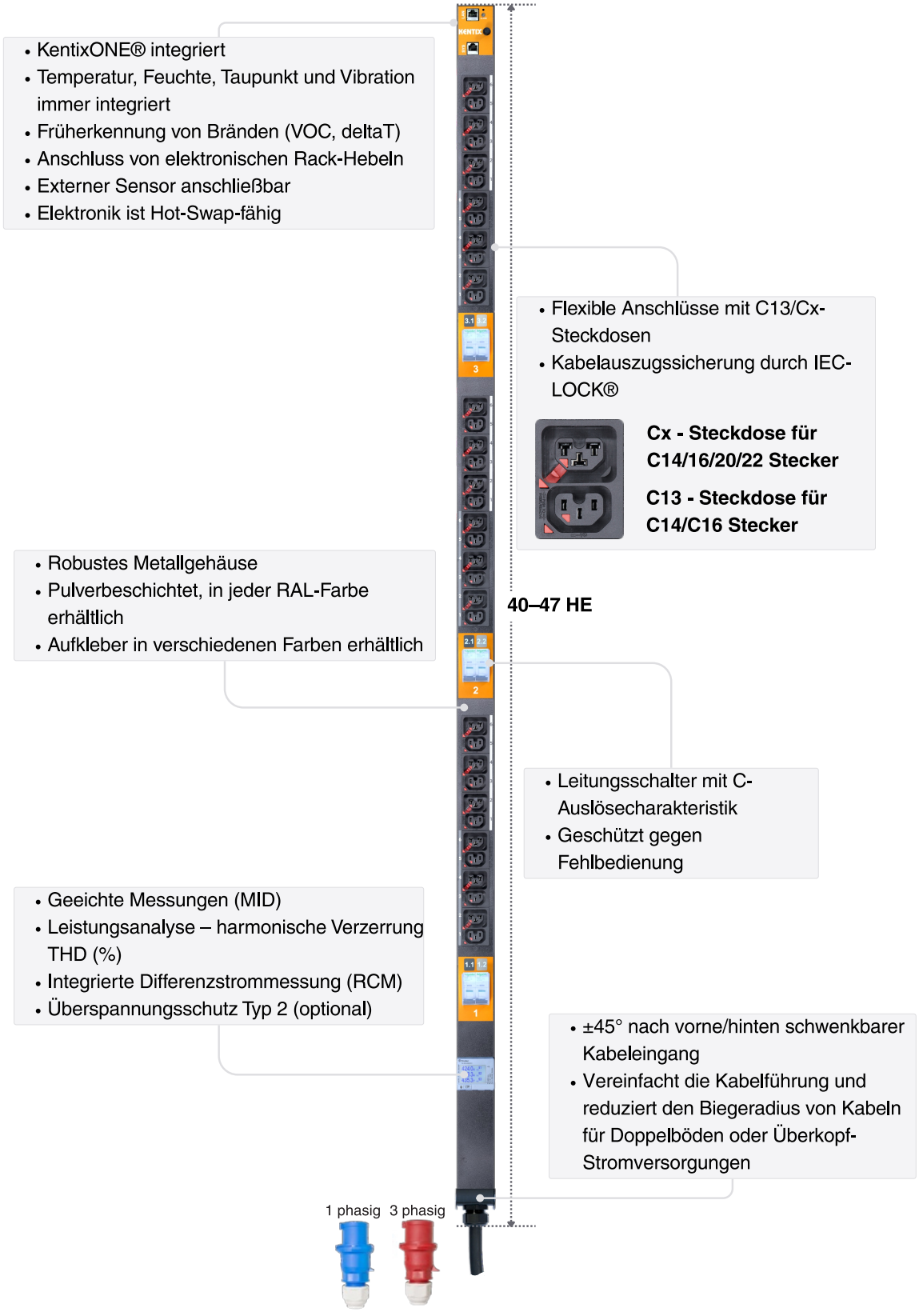
In Summe entsteht ein Umfeld, in dem die Stromverteilung nicht länger „passiv“ sein darf, sondern aktiv überwacht, verstanden und steuerbar gemacht werden muss.

1.2. Die größte Gefahr entsteht im Rack an der Stromverteilung

Viele kritische Vorfälle im Rack beginnen nicht im Server selbst, sondern an Steckverbindungen, Kontakten, Übergangswiderständen, lokalem Wärmeeintrag, falscher Absicherung oder durch Überlastung einzelner Pfade. Das zugrunde liegende physikalische Prinzip ist die Verlustleistung $\mathbf{P = I^2 \cdot R}$, die verdeutlicht, dass schon geringe Widerstände an Kontaktstellen bei hohen Strömen zu starkem Wärmeeintrag führen. Da der Strom quadratisch eingeht, wächst das Risiko mit steigender Rackleistung überproportional, wodurch die Stromverteilung im Rack zu einem der wichtigsten Risikofaktoren wird.

Genau deshalb ist die PDU der natürlichste Ort für frühe thermische und chemische Indikatoren, für Differenzstromüberwachung, für Messung der Netzqualität, für Manipulationserkennung und für automatisierte Reaktionen wie Lastumschaltungen oder definierte Abschaltungen. Die SmartPDU ist somit nicht nur ein „Upgrade“, sondern eine funktionale Notwendigkeit, um die Risiken moderner Rackleistungen beherrschbar zu machen.

1.3. Typischer SmartPDU Aufbau



WHITEPAPER

WHITEPAPER

2. SmartPDU als zentrale Rack-Systemkomponente (Systemdefinition)

2.1. Architekturprinzip: „Power + Security + Monitoring + API“

Eine SmartPDU ist nicht nur ein Stromverteiler, sondern eine kritische Rack-Management-Plattform, die mehrere Subsysteme in einer konsistenten Architektur verbindet. Im **Power Path Layer** bildet die SmartPDU die sichere elektrische Basis durch A/B-Einspeisung, Schalt- und Schutzorgane, Messwandler, MID-Zähler und IEC-60320-Steckdosenmodule.

Der **Measurement & Quality Layer** erweitert diese Basis um präzise Messfunktionen für Strom, Spannung, Leistung und Energie sowie um Netzqualitätsparameter wie THD, Frequenz, Cos ϕ und Crest-Faktor, ergänzt um Differenzstrommessung (RCM) als Sicherheits- und Zustandsindikator.

Im **Environmental & Safety Layer** wird das Rack in seiner physischen Realität erfasst, indem Temperatur, Luftfeuchte und Taupunkt überwacht werden und durch Brandfrüherkennung mittels VOC- und Temperatursensorik sowie durch Vibrationserkennung sicherheitsrelevante Ereignisse erkannt werden können.

Der **Control & Access Layer** macht die SmartPDU handlungsfähig, indem Outlets gezielt geschaltet, Lasten priorisiert und physischer Rackzugriff über elektronische Griffe oder Rackhebel kontrolliert werden kann.

Der **Network & Integration Layer** schließlich stellt sicher, dass das System nicht isoliert bleibt: PoE-gespeiste Elektronik erhöht die Resilienz, während REST API, SNMP v2/v3, Webhooks und optional Syslog/SIEM-Anbindungen *(Security Information and Event Management)* eine tiefe Integration in Betriebs- und Sicherheitsprozesse ermöglichen. Aus der Kombination dieser Schichten entsteht eine zentrale Rack-Komponente, die Strom, Betrieb, Sicherheit und Automatisierung in einem System zusammenführt.

3. Hochsichere Stromversorgung – „ideale Versorgung“ im Rack

3.1. Anforderungen moderner Rechenzentren

Moderne Rechenzentren sind auf Verfügbarkeit ausgelegt, weshalb Redundanzkonzepte wie N+1 oder 2N nicht nur auf Gebäude- oder USV-Ebene, sondern konsequent bis ins Rack umgesetzt werden müssen. Dazu gehört die klare Trennung zweier Versorgungspfade, die selektive Auslegung von Schutzorganen, der sichere Betrieb bei Ausfall eines Feeds sowie eine schnelle und eindeutige Fehlerlokalisierung. Zusätzlich gewinnt die Kommunikations- und Steuerbarkeit der Stromverteilung an Bedeutung, weil eine PDU im Fehlerfall nicht selbst zum Single Point of Failure werden darf, etwa indem Monitoring und Zugriff zusammenbrechen, sobald die Hauptversorgung ausfällt. Eine ideale Rackversorgung ist daher nicht nur redundant, sondern auch messbar, diagnosefähig und operativ beherrschbar.

WHITEPAPER

3.2. Zwei getrennte Versorgungspfade (PSU-Feed): korrekter Anschluss & Belastung

Das Grundprinzip der A/B-Redundanz besteht darin, dass ein Rack über **Feed A** (PDU A) und **Feed B** (PDU B) versorgt wird und mit zwei Netzteilen so angeschlossen werden, dass PSU1 an Feed A und PSU2 an Feed B liegt (PSU = Power Supply Unit, z.B. die USV). Nur dann ist gewährleistet, dass beim Ausfall eines Feeds der verbleibende Pfad die Versorgung übernimmt und dass Wartungen an einem Pfad ohne Betriebsunterbrechung möglich sind. In der Praxis treten jedoch häufig Fehler auf, etwa wenn beide Netzteile am selben Feed hängen und Redundanz nur scheinbar existiert, oder wenn eine asymmetrische Belastung dazu führt, dass ein Pfad nahe Grenzlast betrieben wird, während der andere unterfordert bleibt. Ein weiterer häufiger Irrtum ist die Annahme, dass sich die Last immer exakt 50/50 auf beide Netzteile verteilt, obwohl dies je nach Netzteiltyp, Firmware, Temperatur und Lastzustand variieren kann.

Eine belastbare Auslegung berücksichtigt deshalb, dass beide Feeds im Normalbetrieb typischerweise im Bereich von 40–60 % betrieben werden sollten, während im Fehlerfall ein Feed die gesamte Racklast tragen können muss.

Als Planungsregel hat sich etabliert, die maximale Dauerlast pro Feed auf etwa 80 % zu begrenzen, um thermische Reserve, Normreserven und kurzzeitige Peaks – etwa bei Bootvorgängen – abzufangen. Die SmartPDU unterstützt dieses Konzept, indem sie pro Feed Strom, Leistung und Energie misst, Trends über definierte Zeiträume bereitstellt, Reservekapazitäten in kW sichtbar macht und Warnschwellen implementiert, die eine gefährdete N-Redundanz frühzeitig anzeigen.

Im Ereignisfall kann sie automatisiert alarmieren, Webhooks auslösen, nichtkritische Verbraucher priorisieren oder definierte Outlet-Gruppen abschalten, um Stabilität zu gewährleisten.

4. Lastmanagement & Betriebseffizienz

4.1. Lastmanagement im Rack

Lastmanagement bedeutet nicht nur, eine Überlast zu vermeiden, sondern den Betrieb so zu steuern, dass Strompfade stabil bleiben, Schutzorgane nicht unnötig beansprucht werden und kritische Verbraucher auch in Störsituationen versorgt bleiben. In der Praxis umfasst dies eine dynamische Lastverteilung, definierte Startsequenzen (Staggered Startup), Priorisierung von Verbrauchern nach Kritikalität und Remote Power Cycling pro Outlet.

Besonders in KI-Umgebungen ist Lastmanagement entscheidend, weil GPU-Cluster innerhalb von Sekunden von geringer Auslastung auf hohe Leistungsaufnahme springen können und weil hoch effiziente Netzteile zwar den Energieverbrauch optimieren, jedoch durch Einschalt- und Oberwellenanteile neue Stressfaktoren in der Stromverteilung erzeugen. Eine SmartPDU macht diese Dynamik transparent und steuerbar und reduziert dadurch das Risiko unkontrollierter Abschaltungen und thermischer Überlastungen.

4.2. Auslastungsplanung

Auslastungsplanung ist die operative Voraussetzung für Skalierbarkeit im Rack, weil sie verhindert, dass Kapazitätsgrenzen erst im Störfall sichtbar werden. Die SmartPDU fungiert als „Rack Capacity Planner“, indem sie Lastwerte pro Phase inklusive Neutralleiter und pro Feed erfasst und daraus Reservekapazitäten ableitet.

Durch Trendanalysen und Simulationen lässt sich belastbar beantworten, wie viel zusätzliche Leistung in ein Rack integriert werden kann, ohne Redundanzkonzepte zu gefährden oder thermische Grenzen zu überschreiten. Damit wird Kapazitätsplanung vom Bauchgefühl zur datenbasierten Entscheidung.

5. Optimale Leitungsschutzschalter unter Berücksichtigung von Einschaltströmen

5.1. Problem: Einschaltströme (Inrush) moderner Servernetzteile

Moderne Servernetzteile, insbesondere mit Active PFC, besitzen große Eingangskondensatoren und erzeugen beim Einschalten hohe Inrush-Ströme. Diese Ströme können Leitungsschutzschalter auslösen, Relais und Schaltkomponenten in PDUs belasten und Kontaktstellen thermisch stressen, insbesondere wenn mehrere Systeme gleichzeitig gestartet werden, etwa nach einem Stromausfall oder in Wartungsfenstern. Die Herausforderung besteht darin, Schutzorgane so auszulegen, dass sie einerseits zuverlässig schützen und selektiv auslösen, andererseits aber die dynamischen Einschaltvorgänge moderner IT-Lasten tolerieren.

5.2. Anforderungen an Schutzorgane in PDUs

Schutzorgane müssen selektiv zur vorgelagerten Absicherung sein, damit Fehler lokal eingegrenzt werden und nicht ganze Versorgungsstränge ausfallen. Gleichzeitig müssen sie inrush-tolerant, thermisch stabil sowie wartungsfreundlich und eindeutig dokumentiert sein, damit Betriebs- und Serviceprozesse sicher durchgeführt werden können. In hochverdichteten Racks ist die thermische Reserve der Schutzorgane ein entscheidender Faktor, weil Dauerlast und Umgebungstemperatur die Auslösecharakteristik beeinflussen können.

5.3. Auswahl von Charakteristiken (B/C/D)

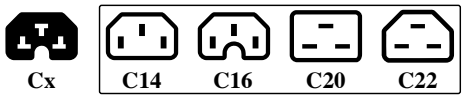
Bei der Auswahl der Charakteristik zeigt sich grob, dass B-Charakteristiken aufgrund ihrer Empfindlichkeit bei hohen Inrush-Strömen häufig ungeeignet sind, während C-Charakteristiken oft den Standard für viele IT-Lasten bilden. D-Charakteristiken bieten eine höhere Inrush-Toleranz, erfordern jedoch die Berücksichtigung von Netzimpedanzen und Abschaltbedingungen, um im Fehlerfall sicher auszulösen. In Rechenzentren ist daher häufig die C- oder D-Charakteristik sinnvoll, abhängig von Netzstruktur, Schutzkonzept und Nachweisführung. Die SmartPDU steigert hier die Betriebssicherheit, indem sie Inrush-Ereignisse protokolliert, Schaltvorgänge korreliert, Startsequenzen empfiehlt oder automatisiert und frühzeitig warnt, wenn sich Schutzorgane im Bereich thermischer Grenzbelastung bewegen.

WHITEPAPER

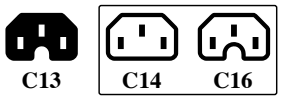
6. Steckdosen nach IEC 60320 – Vorteile der Cx-Steckdosen

6.1. IEC 60320 Überblick

IEC 60320 ist der etablierte Standard für Rack-Steckverbinder, wobei C13/C14 typischerweise für Standard-IT-Lasten bis 10A eingesetzt wird und C19/C20 für höhere Leistungen und Ströme bis 16A, wie sie bei Blade-Systemen, High-End-Servern oder GPU-Nodes auftreten. Die Standardisierung reduziert Komplexität und Fehlerrisiken und bildet die Grundlage für Servicefähigkeit in heterogenen Umgebungen.



Der Cx-Standard integriert mehrere Steckertypen in einer einzigen Steckdose und ersetzt damit im Wesentlichen die C19-Steckdosen.



6.2. Vorteile im Rackbetrieb

Die Vorteile der IEC-60320-Stecksysteme liegen in der normierten Geometrie und Sicherheit, definierten Stromtragfähigkeit und Temperaturgrenzen sowie klarer Steckkompatibilität. Gleichzeitig ermöglichen sie eine hohe Packungsdichte, was insbesondere für vertikale Rack-PDUs entscheidend ist. Die weltweite Verfügbarkeit standardisierter Kabel vereinfacht Logistik und Remote Hands erheblich, während robuste Steckverbindungen und optionale Verriegelungsmechanismen die Betriebssicherheit erhöhen und versehentliches Ziehen als häufige Fehlerquelle minimieren.

6.3. Betriebssicherheit: Kontaktqualität und Hotspots

Da Kontaktstellen in Hochleistungsracks zu kritischen Punkten werden, sollte die SmartPDU Hotspot-Risiken nicht nur indirekt über Lastwerte, sondern auch über Umwelt- und Sicherheitsdaten erkennen können. Werden steigende Temperaturen oder VOC-Anomalien (Luftqualität) bei gleichbleibendem Strom registriert, kann dies ein Hinweis auf zunehmenden Übergangswiderstand sein und als Frühwarnsignal für präventive Wartung dienen. Ergänzend kann die Erfassung von Steckzyklen und Lastprofilen helfen, die Beanspruchung einzelner Outlets zu bewerten und Schwachstellen zu identifizieren.

7. Differenzstrommessung (RCM) in der PDU

7.1. Was ist RCM?

RCM (Residual Current Monitoring) misst den Differenzstrom zwischen Hin- und Rückleiter. Im idealen Zustand ist die Summe der Ströme null; Abweichungen weisen auf Ableitströme oder Fehler hin, etwa Isolationsprobleme, defekte Netzfilter, Feuchtigkeit, Verschmutzung oder Kabel- und Steckerprobleme. RCM ist damit ein hochwirksamer Indikator für elektrische Risiken, die in klassischen Strommessungen nicht sichtbar werden.

WHITEPAPER

7.2. Warum RCM im Rack entscheidend ist

IT-Netzteile erzeugen systembedingt Ableitströme, und bei hoher Gerätedichte addieren sich diese Ströme, was zu unerwarteten Abschaltungen von RCD/FI-Schutzeinrichtungen oder zu Sicherheitsrisiken führen kann. RCM ermöglicht daher eine Früherkennung, bevor kritische Schwellwerte erreicht werden, und unterstützt eine zustandsbasierte Wartungsplanung. In OT- und industriellen Umgebungen gewinnt RCM zusätzlich an Bedeutung, weil Isolationszustände, Umweltbedingungen und Sicherheitsnachweise häufig strenger bewertet werden und RCM als messbarer Indikator in Schutz- und Compliance-Konzepten dienen kann.

7.3. SmartPDU-Funktionen rund um RCM

Eine SmartPDU sollte RCM pro Feed oder Phase erfassen, mehrstufige Alarmierung (Warnung/Kritisch) unterstützen, Trends über Wochen und Monate analysieren und Ereignisse mit Outlets oder Betriebszuständen korrelieren können. Dadurch wird aus einer reinen Messfunktion ein operatives Frühwarnsystem, das technische Risiken in konkrete Handlungsanweisungen übersetzt.

8. THD-Messung (Total Harmonic Distortion) – Netzqualität in Echtzeit

8.1. Warum THD heute Pflicht ist

Rechenzentren bestehen überwiegend aus nichtlinearen Verbrauchern wie Schaltnetzteilen, USV-Gleichrichtern und – je nach Architektur – frequenzgeregelten Antrieben in der Kühlung. KI-Cluster verstärken diese Effekte durch dynamische Lastprofile. Hohe THD kann Transformatoren und Leitungen stärker erwärmen, Neutralleiter überlasten, Schutzorgane beeinflussen, Messwerte verfälschen und langfristig die Lebensdauer von Infrastrukturkomponenten reduzieren. Netzqualität wird damit zu einem direkten Faktor für Betriebssicherheit und Effizienz.

8.2. SmartPDU als Netzqualitäts-Sensor im Rack

Eine SmartPDU mit THD-Messung liefert THD(U) und THD(I) pro Phase, erkennt Verschlechterungen („Power Quality Degradation“) und kann Grenzwertüberschreitungen alarmieren. Diese Daten bilden die Grundlage für Kapazitätsplanung, für die Optimierung von USV- und Filterkonzepten und für Predictive-Maintenance-Strategien, weil Netzqualität in vielen Fällen ein Frühindikator für überlastete oder ungünstig dimensionierte Infrastruktur ist.

WHITEPAPER

9. Integriertes Umgebungsmonitoring (Temperatur, Feuchte, Taupunkt)

9.1. Warum Taupunktmessung entscheidend ist

In modernen Rechenzentren ist nicht nur die absolute Temperatur kritisch, sondern auch das Risiko von Kondensation. Wenn der Taupunkt die lokale Temperatur erreicht, kann Feuchtigkeit ausfallen, was Korrosion, Kurzschlüsse und Isolationsverschlechterungen begünstigt und damit indirekt auch RCM-Werte beeinflussen kann. Insbesondere bei Luftstromveränderungen, Kaltgangeinhausungen, Leckagen oder falsch eingestellten Klimaparametern kann Taupunkt zum entscheidenden Risikofaktor werden.

9.2. SmartPDU als Rack-Klimamonitor

Die SmartPDU überwacht Temperatur oben und unten im Rack, erfasst Luftfeuchte, berechnet den Taupunkt und alarmiert, wenn sich Taupunkt und Racktemperatur kritisch annähern. Dadurch wird Klimarisiko messbar und kann präventiv adressiert werden, bevor es zu elektrischen Folgeschäden kommt.

10. Vibrationserkennung: mechanische Einflüsse erkennen

Vibration und Schockereignisse können durch unsachgemäße Montage, Türschläge, Transport und Umsetzen, unautorisierte Manipulation oder strukturelle Probleme am Rack und Untergrund entstehen. In einem hochkritischen Rackbetrieb sind solche Ereignisse nicht nur „Mechanik“, sondern potenzielle Vorläufer für Kontaktprobleme, lockere Verbindungen oder physische Sicherheitsvorfälle. Eine SmartPDU mit Vibrationserkennung kann Ereignisse dokumentieren, korrelieren und als Security-Event an SIEM-Systeme melden, sodass physische Manipulation nicht unbemerkt bleibt und forensisch nachvollziehbar wird.

11. Brandfrüherkennung in der PDU (VOC + Temperatur)

11.1. Warum Brandfrüherkennung in die PDU gehört

Die meisten kritischen Brandursachen im Rack entstehen an Steckern, in der Stromverteilung und durch Übergangswiderstände. Aufgrund $\mathbf{P = I^2 \cdot R}$ steigt das Risiko mit der Leistung massiv an, was die Stromverteilung zum zentralen Ort für präventive Branddetektion macht. Klassische Rauchmelder reagieren häufig erst spät, wenn bereits Rauchpartikel entstehen, während thermische oder chemische Vorphasen früher messbar sind.

11.2. VOC (Volatile Organic Compounds) als Frühindikator

VOC-Sensorik erkennt thermische Zersetzungsprodukte, „Schmor“-Vorphasen und Ausgasungen aus Kunststoffen und Kabelmaterialien. In Kombination mit Temperaturprofilen ergibt sich eine deutlich frühere Detektion als bei rein rauchbasierten Verfahren, und Warnungen können lokalisierbarer gestaltet werden, weil sie racknah entstehen und mit Strom- und Lastdaten korrelierbar sind.

11.3. Reaktionskonzept

Eine SmartPDU sollte mehrstufig warnen (Pre-Alarm/Alarm), automatische Maßnahmen unterstützen und klare Integrationspfade in Incident-Prozesse besitzen. Dazu zählen definierte Abschaltungen von Outlet-Gruppen, das Auslösen einer Alarmkette und die automatisierte Ticket-Erstellung via Webhooks, damit aus einer Detektion ein kontrollierter Betriebsprozess wird.

12. Strom- und Energiemessung mit MID-geeichten Zählern

12.1. Warum MID wichtig ist

Abrechnung und Mandantenfähigkeit sind in Colocation- und gemischten Umgebungen zentrale Anforderungen, ebenso Auditfähigkeit, ESG- und Energieberichte sowie eine belastbare Kostenstellenrechnung. MID-geeichte Zähler (Measuring Instruments Directive) schaffen hier die Grundlage für abrechnungsfähige und nachvollziehbare Energiemessung, die in Prüfungen und Reports Bestand hat.

12.2. SmartPDU als Abrechnungs- und Transparenzsystem

Die SmartPDU ermöglicht kWh-Erfassung pro Feed, Phase unterstützt Export via API und liefert Langzeitdaten über Jahre. In idealer Ausprägung ist die Protokollierung manipulationssicher und revisionsfähig, sodass Energie-Transparenz nicht nur technisch, sondern auch kaufmännisch nutzbar wird.

WHITEPAPER

13. PoE-gespeiste Elektronik: Datenzugriff auch bei Feed-Ausfall

13.1. Problem: „PDU tot = Monitoring tot“

Wenn eine klassische PDU ausfällt oder beide Feeds unterbrochen sind, gehen häufig nicht nur Stromfunktionen verloren, sondern auch Monitoring, Diagnose und Steuerbarkeit. Genau in dieser Situation sind jedoch Daten und Zugriff besonders wertvoll, weil Fehleranalyse, Wiederanlauf und Sicherheitsprozesse davon abhängen.

13.2. Lösung: PoE als unabhängige Energiequelle

Eine SmartPDU mit PoE-gespeister Elektronik kann Messdaten und Logs weiterhin bereitstellen, Alarme senden und – je nach Architektur – Steuer- und Zugriffsmechanismen aufrechterhalten. Damit wird sie im Fehlerfall zur „letzten Instanz“ im Rack, was besonders für Wartung, Security/Forensik und KI-Racks mit sehr hohen Ausfallkosten entscheidend ist.

14. Kommunikationsschnittstellen: REST API, SNMP v2/v3, Webhooks

14.1. Anforderungen an die Systemintegration

Rechenzentren bestehen aus heterogenen Systemlandschaften wie DCIM *(Data Center Infrastructure Management)*, BMS *(Building Management)*, NMS *(Network Management System)*, SIEM *(Security Information and Event Management)*, ITSM *(IT Service Management)* und Automatisierungs-Workflows. Eine SmartPDU muss deshalb standardisierte und sichere Schnittstellen bieten, um Messdaten und Events nicht nur anzuzeigen, sondern in Prozesse zu integrieren, die automatisch eskalieren, dokumentieren und reagieren.

14.2. REST API

REST APIs ermöglichen eine moderne Integration für Konfiguration, Messwerte und Event-Daten, unterstützen rollenbasierte Authentifizierung und können idempotente Schaltbefehle bereitstellen. Strukturierte JSON-Events erleichtern die Integration in Automatisierungs- und Datenplattformen.

14.3. SNMP v2/v3

SNMP ist in vielen NMS-Umgebungen weiterhin Standard, wobei SNMPv3 für Security durch AuthPriv entscheidend ist. Hersteller-MIBs und standardisierte OIDs ermöglichen tiefe Überwachung, während Traps für kritische Ereignisse wie RCM, Temperatur, THD oder Feed-Ausfälle den Betrieb beschleunigen.

14.4. Webhooks

Webhooks sind ideal für event-getriebene Architekturen, da sie Echtzeit-Events direkt in ChatOps- oder Incident-Response-Prozesse leiten können. Damit wird aus Monitoring ein aktiver Reaktionsmechanismus, ohne dass Polling-Intervalle die Geschwindigkeit begrenzen.

15. Physische Sicherheit & Rackzugriff: SmartPDU als zentrale Sicherheitsinstanz

15.1. SmartPDU + Rackhebel = physische Root-of-Trust im Rack

Wenn Stromverteilung, Sensorik und Zugriffskontrolle in einem System zusammengeführt werden, entsteht ein neuer Ansatz: Die SmartPDU wird zur „Rack Security Control Unit“. Dadurch wird physische Sicherheit nicht als Add-on betrachtet, sondern als Kernfunktion am zentralen Punkt des Racks.

15.2. Funktionen

Ein elektronischer Rackhebel oder Griff ermöglicht kontrollierten Zugriff mit Rollen- und Rechteverwaltung, während ein manipulationssicheres Eventlog dokumentiert, wer wann und wie lange Zugriff hatte. Ergänzend kann die SmartPDU bei Manipulationen – etwa über Vibration oder Türkontakte – alarmieren und Ereignisse in SIEM-Systeme integrieren, wodurch physische Security in digitale Sicherheitsprozesse eingebunden wird.

16. Zukunftstrends: Was zeichnet eine SmartPDU der Zukunft aus?

16.1. KI-Rechenzentren

KI-DCs benötigen extrem hohe Leistungsdichte, sehr schnelle Laständerungen, maximale Verfügbarkeit und präzise Energie-Transparenz. Eine SmartPDU der Zukunft muss daher hochauflösend messen, THD und Power-Quality-Analysen in Echtzeit liefern, intelligente Lastpriorisierung unterstützen und Schnittstellen für automatisierte Orchestrierung bereitstellen, damit Stromversorgung und Betrieb mit der Dynamik moderner KI-Cluster Schritt halten.

16.2. Predictive Maintenance und digitale Zwillinge

Der nächste Schritt ist die Verbindung von Strom-, Umwelt- und Sicherheitsdaten zu Anomalieerkennungssystemen, die Alterungsprozesse sichtbar machen. Wenn Stromverlauf, Temperatur, VOC-Trends und RCM-Verhalten gemeinsam bewertet werden, lässt sich etwa prognostizieren, dass eine Steckverbindung altert oder ein Netzteil atypisch reagiert. Daraus entstehen digitale Zwillinge und Risikoscoring pro Rack, die präventive Wartung wirtschaftlich machen.

16.3. Security-by-Design

Mit wachsender Vernetzung muss eine SmartPDU Security-by-Design umsetzen, also Secure Boot, signierte Firmware, gehärtete Kommunikation (SNMPv3/TLS) und SIEM-native Events. Damit wird sie nicht nur funktional, sondern auch sicherheitstechnisch zu einer vertrauenswürdigen Infrastrukturkomponente.

17. Einsatz in OT-Anwendungen (Operational Technology)

OT-Umgebungen verlangen lange Lebenszyklen, robuste Funktion in schwierigen Umgebungsbedingungen, strengere EMV-Betrachtungen und Security-/Compliance-Anforderungen wie IEC 62443.

Gleichzeitig ist die Verfügbarkeit häufig produktionskritisch, und Eingriffe müssen besonders kontrolliert erfolgen, weil OT-Systeme nicht dieselbe Wartungsflexibilität wie IT-Systeme besitzen. Die SmartPDU bietet hier Energie-Transparenz in Schaltschränken, frühzeitige Brand- und Überhitzungsdetektion, RCM zur Isolationsüberwachung und robuste Alarmierung über etablierte Schnittstellen.

In vielen OT-Szenarien ist zudem die Anbindung über Gateways zu industriellen Protokollen sinnvoll, sodass SmartPDU-Daten in Leit- und Sicherheitssysteme integriert werden können.

WHITEPAPER

WHITEPAPER

18. Fazit

Moderne Rechenzentren – insbesondere High-Density- und KI-Rechenzentren – stellen deutlich höhere Anforderungen an die Infrastruktur im Rack: steigende Leistungsdichten, dynamische Lastprofile, strengere Compliance-Vorgaben sowie zunehmende Risiken durch operative Fehler und physische Manipulation. In diesem Umfeld reicht eine klassische PDU als reine Stromverteilung nicht mehr aus.

Die SmartPDU wird zur **zentralen Systemkomponente im Serverrack**, da sie weit über die reine Energieverteilung hinaus zentrale Funktionen für Sicherheit und Betrieb vereint: hochverfügbare Versorgung über zwei Feeds, präzises Lastmanagement, Auslastungsplanung, MID-konforme Energieerfassung sowie die Echtzeitüberwachung der Netzqualität (THD). Ergänzt durch Differenzstrommessung (RCM), Umgebungsmonitoring (Temperatur, Luftfeuchte, Taupunkt), Vibrationserkennung und Brandfrüherkennung mittels VOC- und Temperatursensorik entsteht ein umfassendes Sicherheits- und Diagnosesystem direkt an der kritischsten Stelle des Racks – der Stromverteilung. Dies ist besonders relevant, da elektrische Kontaktstellen und Übergangswiderstände bei hohen Strömen ein überproportional wachsendes Risiko darstellen ($P = I^2 \cdot R$).

Durch PoE-gespeiste Elektronik bleibt die SmartPDU auch bei Feed-Ausfällen kommunikationsfähig und stellt Messdaten, Ereignisse und Steuerfunktionen weiterhin bereit. Über offene Schnittstellen wie REST-API, SNMP v2/v3 und Webhooks wird sie zum Integrationshub für DCIM-, Monitoring-, ITSM- und SIEM-Prozesse.

Damit bildet die SmartPDU die Grundlage für einen sicheren, effizienten und zukunftsfähigen Rackbetrieb – sowohl im Rechenzentrum als auch in OT-Anwendungen. Sie ist ein zentraler Enabler für Verfügbarkeit, Betriebssicherheit und Automatisierung in der nächsten Generation von IT- und KI-Infrastrukturen.

WHITEPAPER

19. Use-Case-Mapping: SmartPDU im IT-Betrieb

Use Case / Problem im Betrieb	Data Center	Serverraum (On-Prem)	Edge / Remote Standort	Typischer Nutzen
Energie-Transparenz & Abrechnung (kWh / Kostenstellen)	✔✔✔	✔✔	✔✔	Verbrauch je Rack/Abgang sichtbar, Energieberichte, Kostenumlage
Lastmanagement & Kapazitätsplanung (A-/B-Feed, Phase, Reserve)	✔✔✔	✔✔	✔	Verhindert Überlast, bessere Rack-Belegung, Planbarkeit
Früherkennung elektrischer Fehler (RCM / Differenzstrom)	✔✔✔	✔✔✔	✔✔	Erkennt defekte Netzteile/ Leckströme früh → weniger Ausfälle/Brandrisiko
DGUV-V3 / Compliance Unterstützung	✔✔	✔✔✔	✔	Hilft beim Nachweis elektrischer Sicherheit / Prüfpflichten
Remote-Power / Schalten von Ports (Reboot ohne Vor-Ort-Einsatz)	✔✔	✔✔	✔✔✔	Spart Fahrten, schnellere Entstörung (z. B. Router/Server hängt)
Umgebungsüberwachung im Rack (Temp, Feuchte, Taupunkt)	✔✔	✔✔✔	✔✔✔	Verhindert Hitze-/ Feuchteschäden, bessere Klimaführung
Brandfrüherkennung direkt am Rack	✔✔✔	✔✔	✔	Minimiert Ausfall-/Schadensrisiko, schnellere Alarmierung
Zentrale Überwachung & Alarmierung (KentixONE / SNMP/ Events)	✔✔✔	✔✔	✔✔	Einheitliches Monitoring statt Tool-Flickenteppich
Manipulationsschutz / Stecker-Sicherheit (IEC-Lock)	✔✔	✔✔	✔✔	Verhindert versehentliches Ziehen - weniger ungeplante Downtime
SLA-/Audit-Nachweise (Messwerte, Events, Historie)	✔✔✔	✔✔	✔✔	Reporting, Nachvollziehbarkeit, Betriebssicherheit

Legende:
✔ = relevant / häufig, ✔✔ = sehr relevant, ✔✔✔ = Top-Treiber

20. Glossar

Active PFC (Power Factor Correction)

Technologie in Netzteilen zur Verbesserung des Leistungsfaktors (Cos ϕ). Reduziert Blindleistung, kann aber hohe Einschaltströme verursachen.

A/B-Redundanz

Redundantes Versorgungskonzept mit zwei getrennten Strompfaden (Feed A und Feed B), sodass beim Ausfall eines Pfades der andere übernehmen kann.

Ableitstrom

Strom, der über Isolationsstrecken oder Entstörfilter gegen Erde abfließt. Kann sich bei vielen Geräten addieren und Schutzschalter auslösen.

API (Application Programming Interface)

Schnittstelle zur Integration in Software-Systeme. Ermöglicht automatisiertes Auslesen von Messwerten und Steuerung (z.B. Outlets schalten).

BMS (Building Management System)

Gebäudemanagementsystem zur Überwachung und Steuerung technischer Infrastruktur (z.B. Klima, Energieversorgung).

Brandfrüherkennung

Erkennung von Vorstufen eines Brandes (z.B. Überhitzung oder Schmorprozesse), bevor Rauch entsteht.

Cos ϕ (Leistungsfaktor)

Kennzahl für das Verhältnis von Wirkleistung zu Scheinleistung. Je näher an 1, desto effizienter wird elektrische Energie genutzt.

Crest-Faktor

Verhältnis von Spitzenwert zu Effektivwert eines Strom- oder Spannungssignals. Hohe Werte deuten auf nichtlineare Verbraucher hin.

Cx-Steckdose

Steckdosensystem, das mehrere IEC-Steckertypen unterstützen kann (z.B. kompatibel zu C13/C19). Reduziert Komplexität und erhöht Flexibilität.

DCIM (Data Center Infrastructure Management)

Software zur Überwachung und Verwaltung von Rechenzentrums-Infrastruktur (Strom, Klima, Kapazitäten, Racks).

Differenzstrom

Stromdifferenz zwischen Hin- und Rückleiter. Eine Abweichung weist auf Fehlerströme oder Ableitströme hin.

Dynamische Lastwechsel

Schnelle Änderungen der Leistungsaufnahme, typisch bei GPU- und KI-Systemen oder Virtualisierung.

Einschaltstrom / Inrush Current

Sehr hoher Strom beim Einschalten eines Netzteils (durch Ladung großer Kondensatoren). Kann Schutzorgane auslösen oder Bauteile belasten.

ESG (Environmental, Social, Governance)

Regulatorischer und unternehmerischer Rahmen für Nachhaltigkeit, soziale Verantwortung und Unternehmensführung. Erfordert oft Energie-Transparenz.

Feed

Versorgungspfad einer PDU, z.B. Feed A und Feed B als getrennte Stromzuführungen.

Fehlauslösung

Ungewolltes Auslösen eines Schutzorgans (z.B. Leitungsschutzschalter) ohne echten Fehler, häufig durch Inrush oder Oberwellen.

GPU-Rack

Serverrack mit hoher Leistungsdichte, typischerweise für KI-Training/Inference, mit GPU- oder Accelerator-Hardware.

WHITEPAPER

Hotspot

Lokale Überhitzung an Kontaktstellen oder Steckverbindungen, meist durch erhöhten Übergangswiderstand.

IEC 60320

Internationaler Standard für Steckverbinder in IT- und Rack-Infrastrukturen (z.B. C13/C14, C19/C20).

IEC 62443

Sicherheitsstandard für industrielle Automatisierungs- und Steuerungssysteme (OT-Security).

ITSM (IT Service Management)

Prozesse und Tools zur Verwaltung von IT-Services (Tickets, Incidents, Changes), z.B. ServiceNow.

KI-Rack

Rack mit sehr hoher Leistungsdichte und dynamischer Last, betrieben für AI-Workloads (GPU/Accelerator).

Leitungsschutzschalter (LS-Schalter)

Schutzorgan gegen Überlast und Kurzschluss. Charakteristiken (B/C/D) bestimmen Auslöseverhalten bei Stromspitzen.

Lastmanagement

Steuerung der Leistungsaufnahme im Rack, z.B. Priorisierung, Lastverteilung oder kontrollierte Startsequenzen.

MID (Measuring Instruments Directive)

EU-Richtlinie für Messgeräte. MID-konforme Zähler liefern abrechnungsfähige Energieverbrauchsdaten.

Monitoring

Überwachung von Betriebszuständen wie Strom, Spannung, Temperatur oder Sicherheitsevents.

N+1 / 2N

Redundanzkonzepte:

- **N+1**: ein zusätzliches Reserve-System
- **2N**: vollständige doppelte Auslegung aller Komponenten

Neutralleiterbelastung

Belastung des Neutralleiters, die bei Oberwellen und nichtlinearen Lasten stark ansteigen kann.

Nichtlineare Last

Verbraucher, deren Stromaufnahme nicht sinusförmig ist (z.B. Schaltnetzteile). Ursache für Oberwellen und THD.

NMS (Network Management System)

System zur Netzwerk- und Infrastrukturüberwachung, häufig via SNMP.

Outlet

Einzelne Steckdose innerhalb einer PDU, oft separat mess- und schaltbar.

Overload / Überlast

Betriebszustand, in dem Strompfade oder Komponenten oberhalb ihrer zulässigen Dauerlast betrieben werden.

OT (Operational Technology)

Industrie- und Produktionssysteme (Maschinensteuerung, Prozessanlagen), die andere Anforderungen als klassische IT haben.

PDU (Power Distribution Unit)

Stromverteiler im Rack zur Versorgung von IT-Geräten.

PoE (Power over Ethernet)

Stromversorgung über Netzwerkkabel. Ermöglicht Betrieb von Elektronik unabhängig von der Hauptstromversorgung.

Power Quality / Netzqualität

Qualität der Stromversorgung, beeinflusst durch Oberwellen, Frequenzabweichungen, Spannungsschwankungen und THD.

WHITEPAPER

Power Cycling

Gezieltes Aus- und Einschalten eines Outlets oder Verbrauchers (remote oder automatisch), um Systeme neu zu starten.

Predictive Maintenance

Vorausschauende Wartung durch Trend- und Anomalieanalyse, um Fehler vor Eintritt zu erkennen.

PSU (Power Supply Unit)

Netzteil eines Servers oder einer Infrastrukturkomponente. In Redundanzkonzepten meist doppelt vorhanden.

RCM (Residual Current Monitoring)

Differenzstromüberwachung zur Erkennung von Fehler- oder Ableitströmen. Frühwarnindikator für elektrische Risiken.

RCD / FI-Schalter

Schutzeinrichtung, die bei Fehlerströmen gegen Erde abschaltet. Kann durch hohe Ableitströme ausgelöst werden.

Remote Hands

Betriebsmodell, bei dem externe Techniker vor Ort einfache Tätigkeiten ausführen (Kabel stecken, reboot, Hardware tauschen).

REST API

Moderne HTTP-basierte Schnittstelle zur Integration und Automatisierung (meist JSON-basiert).

Rackhebel / elektronischer Griff

Mechanismus zur kontrollierten Öffnung eines Racks, oft mit Authentifizierung und Logging.

Schalt- und Schutzorgane

Bauteile wie Relais, LS-Schalter oder Sicherungen, die Strompfade absichern und schalten.

Schmorprozess

Thermische Überlastung von Kabeln/Steckern, oft Vorstufe eines Brandes. Erkennbar durch Temperaturanstieg und VOC-Ausgasungen.

Secure Boot

Sicherheitsmechanismus, der nur signierte und vertrauenswürdige Firmware/Software beim Start zulässt.

Security-by-Design

Ansatz, bei dem Sicherheitsmechanismen von Anfang an in die Systemarchitektur integriert werden.

SIEM (Security Information and Event Management)

System zur zentralen Sammlung und Analyse von Security-Events, z.B. für Alarmierung und Forensik.

Single Point of Failure

Komponente, deren Ausfall das gesamte System oder wesentliche Funktionen lahmlegt.

SmartPDU

Intelligente PDU mit Mess-, Monitoring-, Steuerungs- und Security-Funktionen inklusive Schnittstellenintegration.

SNMP v2/v3

Standardprotokoll zur Netzwerküberwachung. SNMPv3 bietet zusätzliche Sicherheit (Authentifizierung/ Verschlüsselung).

Staggered Startup

Gestaffeltes Einschalten von Geräten zur Reduktion von Inrush-Strömen und zur Entlastung von Schutzorganen.

THD (Total Harmonic Distortion)

Maß für Oberwellenanteile in Strom oder Spannung. Hohe THD bedeutet schlechtere Netzqualität und höhere Belastung.

THD(U) / THD(I)

THD bezogen auf Spannung (U) bzw. Strom (I).

WHITEPAPER

Taupunkt

Temperatur, bei der Luftfeuchtigkeit kondensiert. Kritisch im Rack wegen Korrosions- und Kurzschlussrisiko.

Übergangswiderstand

Widerstand an Kontaktstellen (Stecker, Klemmen). Steigt oft durch Alterung oder lockere Verbindungen und erzeugt Wärme.

VOC (Volatile Organic Compounds)

Flüchtige organische Verbindungen. Sensorik erkennt Ausgasungen, z.B. bei Überhitzung von Kunststoff oder Kabelisolierung.

Vibrationserkennung

Sensorik zur Detektion von Erschütterungen oder Schlägen, relevant für Manipulation, Montagefehler oder mechanische Schäden.

Webhook

Mechanismus zur automatischen Übertragung von Ereignissen an externe Systeme (event-getrieben statt Polling).

Wirkleistung / Scheinleistung

- **Wirkleistung (kW):** tatsächlich genutzte Leistung
- **Scheinleistung (kVA):** Gesamtleistung inklusive Blindanteilen

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

Über Kentix

Jedes Unternehmen hat einen Bedarf an physischer Sicherheit. Dieser muss schnell und skalierbar zu erfüllen sein. Darauf hat Kentix eine revolutionär einfache Antwort entwickelt: Diese heisst KentixONE, von der Zutrittskontrolle bis zur Alarm- und Videotechnik ist alles 100% IoT-basiert und in einer Plattform zusammengefasst. KentixONE verschmilzt 8 herkömmliche Sicherheitssysteme und erkennt vorausschauend über 40 Gefahren. Einfacher geht's nicht. Unternehmen aus allen Branchen sichern durch Produkte der Kentix GmbH ihr Geschäft und Infrastruktur gegen physische Gefahren sowie menschliches Fehlverhalten ab und halten gesetzliche Anforderungen ein. Die Entwicklung und Produktion erfolgt ausschließlich in Deutschland.

Als Teil der **ASSA ABLOY Group**, dem weltweit führenden Anbieter von Zugangslösungen, verbinden wir die Innovationskraft eines agilen Technologieunternehmens mit der Stärke einer globalen Unternehmensgruppe. Seit mehr als fünfzehn Jahren entwickeln wir digitale, intuitive Sicherheitstechnologie, die Menschen im Alltag entlastet – denn **Einfachheit ist der Schlüssel zu mehr Sicherheit.**