

Rittal – The System.

Faster – better – everywhere.

► Świat infrastruktury IT

Informacje ogólne i podstawy podejmowania decyzji





Autor Martin Kandziora, urodzony w 1967 r., od 2004 roku kieruje działem komunikacji z rynkiem w firmie Rittal w Herborm. Swoją karierę jako inżynier-projektant rozpoczął po zakończeniu studiów elektrotechnicznych w Stuttgarcie. Następnie przeszedł do mediów i jako dziennikarz przez pięć lat z powodzeniem rozwijał czasopismo fachowe „Elektro Automation”. W roku 2000 zajął się marketingiem w firmie informatycznej w Monachium. Martin Kandziora współpracuje z różnymi organizacjami branżowymi i gremiami. Ponadto jest autorem licznych publikacji w prasie niemiecko- i angielskojęzycznej.

Biblioteka techniczna Rittal, Tom 4

Wydawca: Rittal GmbH & Co. KG
Herborn, czerwiec 2014

Wszelkie prawa zastrzeżone.
Wszelkiego rodzaju powielanie i rozpowszechnianie bez wyraźnej zgody jest zabronione.

Wszystkie teksty i ilustracje zostały opracowane przez wydawcę i autorów z najwyższą starannością. Niemniej jednak, nie możemy zagwarantować prawidłowości, kompletności i aktualności tych treści. Wydawca i autorzy w żadnym przypadku nie odpowiadają za jakiegokolwiek szkody pośrednie i bezpośrednie wynikające z zastosowania tych informacji.

Copyright: © 2014 Rittal GmbH & Co. KG

Realizacja:
Rittal GmbH & Co. KG
Martin Kandziora, Dagmar Liebegut
Grafika: Günter Muhly Grafik, Marketing- und Werbeberatung GmbH, Allendorf (Lumda)



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Słowo wstępne

Wraz z rozwojem przedsiębiorstwa i wzrostem cyfryzacji procesów biznesowych rośnie również zapotrzebowanie na fizyczny sprzęt IT. Do rozwoju technicznego musi się dopasować także infrastruktura IT oraz pomieszczenia, w których znajdują się komputery lub systemy pamięci masowych. Jednocześnie w nowoczesnych centrach danych rośnie potrzeba zapewnienia większego bezpieczeństwa i dostępności, a także wyższej efektywności energetycznej. Poza tym od infrastruktury budowanych lub modernizowanych centrów danych oczekuje się, aby sprostała ona przyszłym wymaganiom. Realizacją tych wymagań są skalowalne, modułowe i efektywne rozwiązania infrastruktury IT. W określeniu indywidualnych potrzeb pomoże Państwu niniejszy zarys, mogący służyć jako katalog kryteriów i poradnik. Ten zwarty przewodnik rozważa różne aspekty infrastruktury IT, m.in. zasilanie elektryczne i rozdział mocy, technologia sieciowa i efektywne metody chłodzenia wraz z parametrami, monitoring i szafy stosowane w centrum danych. Przykłady różnych rozwiązań mogą być przydatne i przyszłościowe dla Państwa własnej infrastruktury IT.

My – eksperci IT firmy Rittal – życzymy Państwu przyjemnej lektury.

Szczególne podziękowania za cenne wsparcie fachowe i konstruktywne uwagi należą się Panom: Heinrichowi Styppie, Hartmutowi Lohreyowi i Berndowi Hansteinowi a także Michaelowi Nicolaiowi, Günterowi Muhly'emu i Burkhardowi Weberowi.

Serdecznie pozdrawiam
Martin Kandziora

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Spis treści

	Strona
Podstawy infrastruktury IT	21
Komponenty systemowe dla infrastruktury IT	65
Rozwiązania dla infrastruktury IT	95
Wiedza ekspertów	111

Rittal – The System.

Faster – better – everywhere.

» nextlevel

for data centre

Rittal otwiera przed światem IT całkiem nowe perspektywy. Niezależnie od tego, czy chodzi o moduł standardowego centrum danych RiMatrix S, czy też efektywne komponenty – wszystkie elementy są dostępne w krótkich terminach, wprost z magazynu.

Rittal – The System.

- Rittal – modułowe i standardowe centra danych w produkcji seryjnej z RiMatrix S
- Rittal – komponenty dla indywidualnych rozwiązań IT



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL



nextlevel

for data centre

IT INFRASTRUCTURE

SOFTWARE & SERVICES



Rittal – The System.

Faster – better – everywhere.

Infrastruktura IT od S do XXL

- RiMatrix S
- Systemy szaf IT
- Obudowy IT
- Zasilanie IT
- Klimatyzacja IT
- Monitoring IT
- Rozwiązania bezpieczeństwa IT



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

- RiMatrix S – pierwsze produkowane seryjnie centrum danych jako gotowe rozwiązanie dla infrastruktury
- Pomieszczenia bezpieczeństwa IT – z certyfikatem ECB-S



IT INFRASTRUCTURE

SOFTWARE & SERVICES



Zalety RiMatrix

Dzięki jedynym w swoim rodzaju rozwiązaniom systemowym IT Rittal, mogą Państwo korzystać z nowoczesnej infrastruktury centrów danych. Swobodny wybór standardowych komponentów systemu RiMatrix, systemów szaf i obudów, zasilania, chłodzenia, monitoringu i bezpieczeństwa IT, umożliwia dopasowanie infrastruktury IT dokładnie do potrzeb przy jednoczesnych elastycznych możliwościach rozbudowy.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Faster – dopasowana infrastruktura centrów danych dzięki „Rittal – The System.“

Better – standardowe, wzajemnie dopasowane komponenty systemu

Everywhere – możliwość instalacji i uruchomienia przez 1000 techników serwisu na całym świecie



IT INFRASTRUCTURE

SOFTWARE & SERVICES



Zalety RiMatrix S

RiMatrix S jest rewolucyjnym alternatywnym podejściem do budowy centrów danych. Wstępnie skonfigurowane, kompletne moduły centrum danych umożliwiają zbudowanie jego standaryzowanej infrastruktury. Moduły centrum danych zawierają wszystkie niezbędne komponenty, jak systemy szaf IT, zabezpieczenie i rozdział zasilania, chłodzenie, monitoring oraz rozwiązania dotyczące bezpieczeństwa. Wszystkie moduły centrum danych są prefabrykowane, dostępne w magazynie, co pozwala na szybkie skompletowanie elementów dopasowanych do potrzeb klienta.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Faster – prefabrykowane moduły centrum danych dostępne w magazynie
Better – sprawdzone i wstępnie certyfikowane moduły centrum danych o doskonałej efektywności
Everywhere – montaż w posiadających atest systemu pomieszczeniach bezpieczeństwa, pomieszczeniach standardowych lub w kontenerach



IT INFRASTRUCTURE

SOFTWARE & SERVICES



Rittal – The System.

Faster – better – everywhere.

Selektor RiMatrix S

Indywidualne rozwiązanie dla centrum danych konfigurowane jest na bazie standardowych modułów.

- Faza projektowania, dostawa oraz czas uruchamiania ulegają znacznemu skróceniu.
- Dzięki karcie produktu dokładna kalkulacja opłacalności (z uwzględnieniem parametrów zużycia) staje się oczywistością już na etapie doradztwa.
- Standaryzacja daje możliwość znacznej oszczędności kosztów.
- Moduły centrum danych są kompletnymi jednostkami funkcyjnymi (łącznie z zasilaniem elektrycznym, chłodzeniem i monitoringiem).
- Moduły są całkowicie wymiarowane, posiadają kartę produktu i są dostępne w magazynie pod jednym numerem katalogowym.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Pierwsze seryjne centrum danych. Po prostu – podłączyć i gotowe.

Aplikacja RiMatrix S

Konfigurator standardowych centrów danych dla średnich przedsiębiorstw, koncepcji oddziałów i elastycznych aplikacji chmurowych.

Łatwy w obsłudze interfejs prowadzi do kompletnego centrum danych w zaledwie pięciu krokach:

1. Wymagania i warunki brzegowe
2. Dane techniczne
3. Wybór standaryzowanych modułów
4. Pakiety opcjonalne
5. Indywidualne rozwiązanie RiMatrix S



IT INFRASTRUCTURE

SOFTWARE & SERVICES

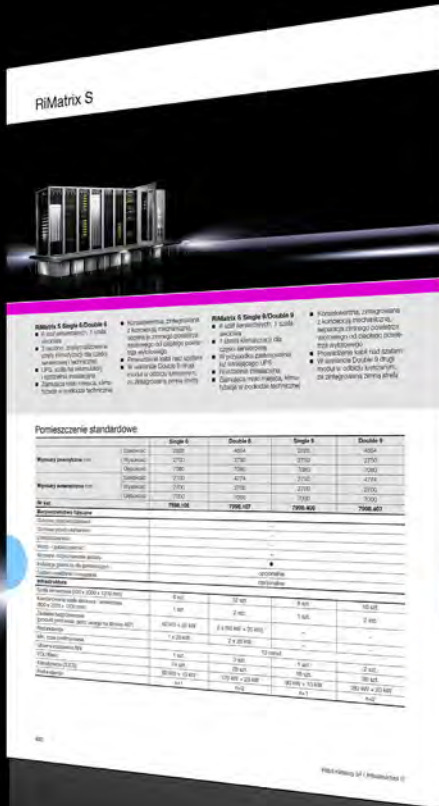


Rittal – The System.

Faster – better – everywhere.

Katalog 2014/2015

W Katalogu 2014/2015 znajdują Państwo aktualne informacje dotyczące zamówień, obejmujące pełną gamę produktów Rittal. Katalog wyróżnia się czytelnym podziałem oraz praktycznymi odnośnikami do pasujących akcesoriów, produktów alternatywnych i ważnych informacji. Warto się przekonać!



- Kompletne informacje przydatne przy składaniu zamówienia, dopasowane do Państwa potrzeb
- Jednoznaczne przyporządkowanie akcesoriów
- Dodatkowe informacje w Internecie

- RiMatrix S Single 6 i Double 6**
 - 6 szuflad w szerokości 12 szuflad
 - 2 szuflady instalowane w górze umożliwiają łatwy dostęp do urządzeń serwerowych
 - 3 płyty szkieletowe umożliwiają łatwą instalację i wymianę
 - Zamki i klucze umożliwiają ochronę przed nieautoryzowanym dostępem
- RiMatrix S Single 8 i Double 8**
 - Rozszerzenie, zintegrowane z kolumną instalacyjną, umożliwia łatwy dostęp do urządzeń serwerowych
 - 2 szuflady instalowane w górze umożliwiają łatwy dostęp do urządzeń serwerowych
 - 3 płyty szkieletowe umożliwiają łatwą instalację i wymianę
 - Zamki i klucze umożliwiają ochronę przed nieautoryzowanym dostępem
- RiMatrix S Single 9 i Double 9**
 - 9 szuflad w szerokości 12 szuflad
 - 2 szuflady instalowane w górze umożliwiają łatwy dostęp do urządzeń serwerowych
 - 3 płyty szkieletowe umożliwiają łatwą instalację i wymianę
 - Zamki i klucze umożliwiają ochronę przed nieautoryzowanym dostępem
- RiMatrix S Single 10 i Double 10**
 - Rozszerzenie, zintegrowane z kolumną instalacyjną, umożliwia łatwy dostęp do urządzeń serwerowych
 - 2 szuflady instalowane w górze umożliwiają łatwy dostęp do urządzeń serwerowych
 - 3 płyty szkieletowe umożliwiają łatwą instalację i wymianę
 - Zamki i klucze umożliwiają ochronę przed nieautoryzowanym dostępem

Pomieszczenie standardowe

	Single 6	Double 6	Single 8	Double 8
Wymiary zewnętrzne (mm)				
Wysokość	2100	4054	2100	4054
Szerokość	750	1500	750	1500
Głębokość	750	750	750	750
Wymiary wewnętrzne (mm)				
Wysokość	2100	4054	2100	4054
Szerokość	750	1500	750	1500
Głębokość	750	750	750	750
Do 6 szuflad	750 x 1500	1500 x 1500	750 x 1500	1500 x 1500
Do 8 szuflad				
Do 10 szuflad				
Wymiary wewnętrzne (mm)				
Wysokość	2100	4054	2100	4054
Szerokość	750	1500	750	1500
Głębokość	750	750	750	750
Do 6 szuflad	750 x 1500	1500 x 1500	750 x 1500	1500 x 1500
Do 8 szuflad				
Do 10 szuflad				
Wymiary zewnętrzne (mm)				
Wysokość	2100	4054	2100	4054
Szerokość	750	1500	750	1500
Głębokość	750	750	750	750
Do 6 szuflad	750 x 1500	1500 x 1500	750 x 1500	1500 x 1500
Do 8 szuflad				
Do 10 szuflad				

ENCLOSURES

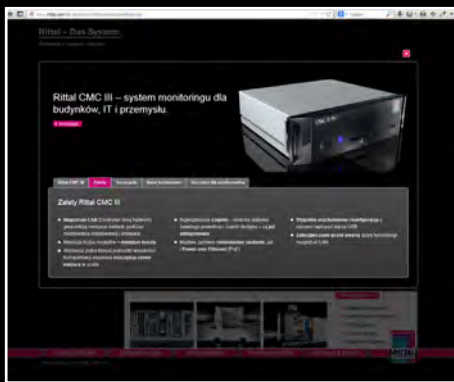
POWER DISTRIBUTION

CLIMATE CONTROL

Korzyści lepiej widoczne

Internet

Czasami jeden obraz mówi więcej niż tysiąc słów. Dlatego dla wielu produktów przygotowaliśmy strony internetowe lub narzędzia doboru i konfiguracji ułatwiające wybór oraz w czytelny i przejrzysty sposób przedstawiające korzyści. Naprawdę warto się przekonać!



Strony internetowe

- Czytelna wizualizacja korzyści
- Prezentacja zalet
- Informacje dodatkowe
- Wskazówki praktyczne



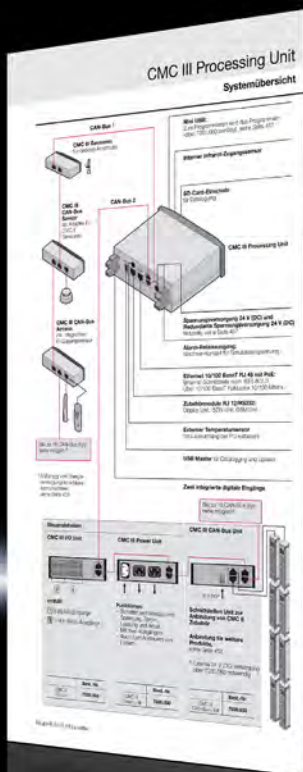
Narzędzia doboru i konfiguracji

- Łatwa konfiguracja
- Możliwość sprawdzenia różnych możliwych rozwiązań
- Łatwe zamawianie skojarzonych produktów

Podręcznik techniczny systemu Rittal

w formacie PDF

Szukasz prostego rozwiązania dla swoich zastosowań? Warto zajrzeć do naszego podręcznika technicznego, który jest dostępny na naszej stronie internetowej w formacie PDF. Umożliwia on szybkie zapoznanie się z nieskończonymi możliwościami rozwiązań oferowanych przez „Rittal – The System“.



- Czytelna prezentacja korzyści
- Jednoznaczne zalety produktów
- Zrozumiała prezentacja zasad
- Pomocne wskazówki dotyczące użycia

Rittal – The System.

Faster – better – everywhere.

Make **IT** easy.

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Podstawy infrastruktury IT

	Strona
Wstęp	22
Dostępność a koszty	24
Przykłady zależności mocy, dostępności i kosztów	25
Moc	26
Moc i bezpieczeństwo w przyszłości	26
Dostępność	28
Indywidualne wymagania odnośnie dostępności	28
Stopnie dostępności (Tier)	29
Klasy dostępności (VK)	30
Lista kontrolna dostępności IT wg TÜV Rheinland	32
Czynniki dostępności	34
Dostępność uwarunkowana bezpieczeństwem termicznym	35
Całościowe zasilanie w energię i zabezpieczenie	36
Dostępność uwarunkowana bezpieczeństwem fizycznym	45
Kryteria planowania dostępności	46
Efektywność	48
Czynniki efektywnego IT	48
Wzór obliczeniowy na efektywność energetyczną centrum danych	50
Drogi zwiększania efektywności centrum danych	52
Data Center Infrastructure Management System (DCIM)	54
Miejsce	56
Czynniki lokalizacji	56
Przyszłość	62
Opcje przyszłej infrastruktury IT	62

■ Wstęp

IT przedsiębiorstwa

Niezależnie od tego, czy firma jest mała, średnia, czy duża – prawie każde przedsiębiorstwo, organizacja usługowa czy instytucja publiczna potrzebuje sprawnej technologii informacyjnej. Centrum danych jest kompleksowe, gdyż musi nadążać za rozwojem technicznym i zmianami organizacyjnymi. Przed tym wyzwaniem stoi przyszłościowa infrastruktura IT, a jednocześnie musi ona sprostać wymaganiom odnośnie dostępności, bezpieczeństwa i większej efektywności energetycznej.



Infrastruktura IT

Niezależnie od rozmiarów centrum danych, infrastruktura IT dotyczy następujących obszarów:

- 1 Szafy i obudowy dla komponentów serwerowych i sieciowych
- 2 Rozdzielanie i zabezpieczanie energii
- 3 Wytwarzanie i rozdział chłodu
- 4 Monitorowanie i zdalne zarządzanie z komponentami sprzętowymi i oprogramowaniem
- 5 Komponenty bezpieczeństwa do wykrywania i gaszenia pożaru
- 6 Rozwiązania zabezpieczające, certyfikowane pomieszczenia bezpieczeństwa lub sejfy

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Współczesne trendy zmierzają w kierunku centrów danych all-in-one, np. w formie rozwiązania kontenerowego. Takie jednostki są skonstruowane elastycznie i modułowo, dają się szybko i sprawnie montować.

Jednak często rozróżnia się jednostki robocze i kontenery chłodnicze (przykład RiMatrix S, strona 100).



Czynniki ekonomiczne infrastruktury IT

Do kluczowych kwestii w nowoczesnej infrastrukturze IT należą moc, dostępność, bezpieczeństwo i efektywność energetyczna.

To wpływa na koszty zakupu i eksploatacji.

Decydujące dla budowy centrum danych są następujące czynniki:

- Elastyczność
- Wybór lokalizacji
- Rodzaj i rozmiar
- Bezpieczeństwo i dostępność
- Moc elektryczna
- Odprowadzanie ciepła
- Okablowanie
- Efektywność energetyczna
- Możliwości dostosowania do przyszłych potrzeb
- Koszty inwestycji i eksploatacji

Dostępność a koszty

Wzajemne oddziaływania

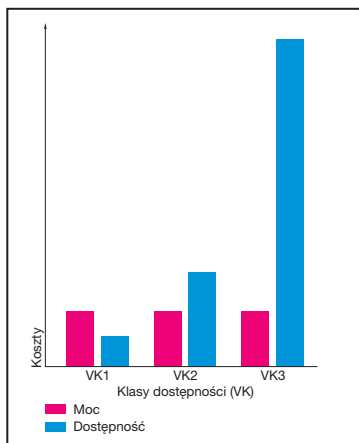
Decydujące dla niezawodności procesu przetwarzania informacji jest ciągłe podtrzymywanie pracy. Niedostatecznie chronione informacje stanowią często bagatelizowany czynnik ryzyka, który może zagrażać istnieniu centrum danych.¹⁾

Centra danych tworzą fizyczną podstawę infrastruktury IT. W dzisiejszych czasach główne filary gospodarki, jak np. banki, towarzystwa ubezpieczeniowe, producenci samochodów czy dostawcy, nie są już w stanie prowadzić swojej działalności bez trwale dostępnej i bezpiecznej

infrastruktury IT. Nawet jako taka sieć szkieletowa jest utrzymywana w centrach danych. Gospodarka rynkowa wymaga trwale dostępnych usług IT. Zadanie to realizują centra danych.

Głównym celem jest dostępność

Powiązanie fizycznej infrastruktury centrum danych z zarządzaniem serwerami i aplikacjami pozwala uzyskać kompleksową kontrolę nad usługami IT. Wczesne wykrycie awarii umożliwia odpowiednie szybkie działanie oraz utrzymanie określonej dostępności.

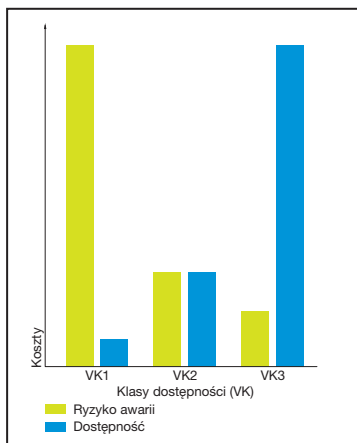


W przypadku większej dostępności, przy tej samej mocy centrum danych znacznie rosną koszty inwestycji i eksploatacji.

Jako wzór matematyczny na dostępność IT można użyć:

$$MTBF / (MTBF + MTTR)$$

Gdzie MTBF (Mean Time Between Failures) to czas upływający między jedną a następną awarią.



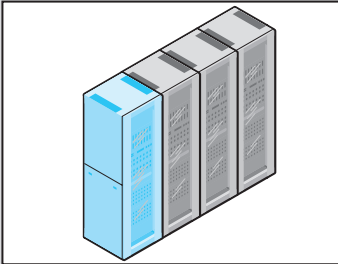
Zwiększanie dostępności minimalizuje ryzyko dużych strat produktywności.

Jako MTTR (Mean Time To Repair) rozumiemy średni czas potrzebny do naprawy centrum danych lub zainstalowanych w nim komponentów.

¹⁾ www.bsi.bund.de

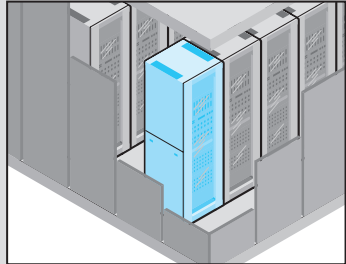
Przykłady zależności mocy, dostępności i kosztów

Tak jak w obu tych przykładach, decydujące jest dokładne określenie wymagań dostępności. Wzrost dostępności np. z 99% (VK 1) do 99,99% (VK 3) wiąże się ściśle z redukcją czasu przestoju. Jednakże wraz z dostępnością znacznie rosną koszty budowy infrastruktury IT oraz jej eksploatacji.



Przykład 1 (VK 1: 99%) Czas przestoju 88 godzin w roku

Gdy centrum danych jest budowane lub użytkowane przez np. firmę średniej wielkości, wówczas główny czas użytkowania z reguły przypada od poniedziałku do piątku, w godzinach pracy. W tym czasie wymagania dostępności są wysokie, częściowo również w nocy, w przypadku firm prowadzących działalność na płaszczyźnie międzynarodowej. W weekendy dostępność odgrywa zwykle mniejszą rolę.



Przykład 2 (VK 3: 99,99%) Czas przestoju 52 minuty w roku

Natomiast gdy np. bank lub sklep internetowy planuje własny klaster IT lub klaster tradingowy, wówczas absolutny priorytet ma niezawodność.

Cała infrastruktura musi umożliwiać maksymalną dostępność. Niezbędne do tego utrzymanie redundancji naturalnie winduje koszty inwestycji. Redundancja to adekwatna do możliwych kosztów awarii, opłacalna i sensowna inwestycja.

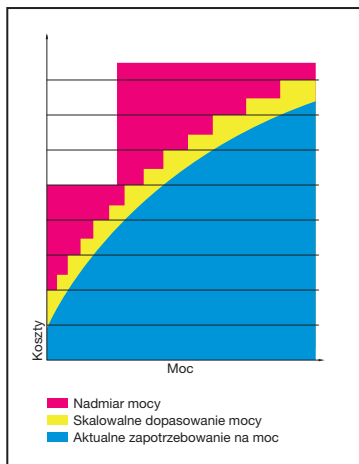
■ Moc

Moc i bezpieczeństwo w przyszłości

Czy to małe, średnie, czy duże przedsiębiorstwo – wymagania dotyczące wydajności IT stale rosną:

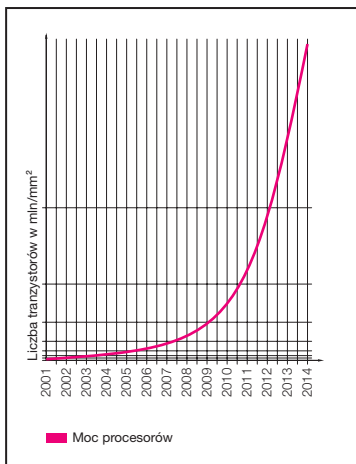
- Rozwój i konsolidacja serwerów
- Implementacja nowych aplikacji do automatyzacji procesów biznesowych wiążąca się ze zwiększeniem obciążenia sieci IT
- Wprowadzanie nowych technologii i centralizacja zasobów IT, a przez to „IT-traffics“
- Zwiększanie liczby użytkowników
- Wirtualizacja rozwiązań IT
- Użytkowanie i modernizacja aplikacji chmurowych, a przez to rozłożenie obciążenia
- Wymagania dostępności

Celem jest zastosowanie do budowy centrum danych rozwiązania skalowalnego i elastycznego, które umożliwi bardzo dynamiczny rozwój samego IT.



„Pay as you grow” – rozwiązanie dopasowane do potrzeb

Należy uwzględnić, że centrum danych musi sukcesywnie dostosowywać się do rosnącego zapotrzebowania na moc ze strony sprzętu. Duże nadwyżki mocy generują koszty.



Dynamika rozwoju

Aktualna dynamika rozwoju wskazuje, iż co 18 miesięcy podwaja się moc procesorów. Nowe centra danych powinny uwzględniać trendy rozwoju poprzez elastyczne i modułowe koncepcje rozbudowy.



Najbardziej kompaktowa jednostka centrum danych:
szafa IT z chłodzeniem, monitoringiem, UPS, serwerami i siecią

■ Dostępność

Indywidualne wymagania odnośnie dostępności

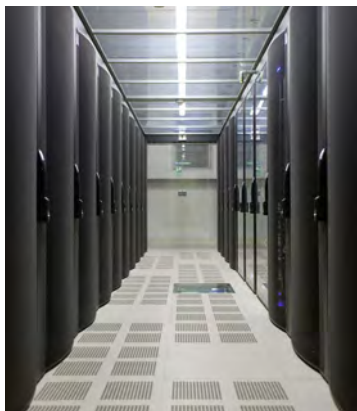
Opracowanie skutecznego planu przywracania w sytuacjach awaryjnych wymaga gruntownych przemyśleń i decyzji. Zalicza się do nich dostępność i potencjalne skutki czasów awarii systemu dla pracy przedsiębiorstwa.

Poniższe pytania pomagają w określeniu wymaganej dostępności:

- Jak brzmią wymagania odnośnie dostępności? W jakim przedziale czasu usługa client security musi być codziennie online?
- Jakie koszty powodują awarie dla przedsiębiorstwa?
- Jaki czas przestoju byłby akceptowalny, gdyby było niedostępne jedno z mediów (np. nośnik danych)?
- Jaki czas przestoju byłby akceptowalny dla usługi client security w przypadku wystąpienia sytuacji awaryjnej, np. utraty serwera w wyniku pożaru?
- Jak ważne jest, aby dane nigdy nie ulegały utracie?
- Jak łatwe byłoby odzyskanie utraconych danych?
- Czy w przedsiębiorstwie są administratorzy systemu i jaką mają funkcję?
- Kto odpowiada za procesy zabezpieczenia i odzyskiwania?
- Jakie kwalifikacje mają odpowiedzialni pracownicy?¹⁾

Postępujący rozwój i integracja technologii informacyjnej we wszystkich obszarach działalności oznacza także, iż żadne – nawet małe – przedsiębiorstwo nie może sobie dzisiaj pozwolić na awarię firmowego IT.

Jeszcze przed paroma laty kilkugodzinną awarią IT w firmie była do zaakceptowania. Dzisiaj rośnie ilość takich



Wymagania dostępności różnią się w zależności od użytkownika i aplikacji.

przedsiębiorstw, dla których ciągła dostępność IT stała się nieodzowna.

Dlatego dla sporządzenia i rozszerzenia lub kontroli koncepcji IT decydujące znaczenie ma dostępność, jaką musi dysponować infrastruktura IT przedsiębiorstwa. Wynikające z tego pytanie brzmi:

„Ile wynoszą maksymalne akceptowalne czasy awarii IT przedsiębiorstwa?”²⁾

¹⁾ Biblioteka TechNet Microsoftu

²⁾ BITKOM, *Betriebssicheres Rechenzentrum* (Bezpieczne w eksploatacji centrum danych)

Stopnie dostępności (Tier)

Centra danych to skomplikowane systemy, które w połączeniu ze wszystkimi aktywnymi i pasywnymi komponentami IT definiują wpływ na dostępność. W fazie koncepcji musi zostać oszacowana faktycznie niezbędna dostępność infrastruktury IT. Należy więc założyć dla firmy wielkość

maksymalnego tolerowanego czasu awarii infrastruktury IT w roku.

Renomowany instytut US Uptime zdefiniował klasy dostępności, tzw. Industry Standards Tier® Classification¹⁾:

Tier I

Lata 60-te:
pojedyncza ścieżka zasilania elektrycznego, pojedyncze źródło chłodzenia, brak redundantnych komponentów

Dostępność
99,671%

Tier II

Lata 70-te:
pojedyncza ścieżka zasilania elektrycznego, pojedyncze źródło chłodzenia, redundantne komponenty

Dostępność
99,741%

Tier III

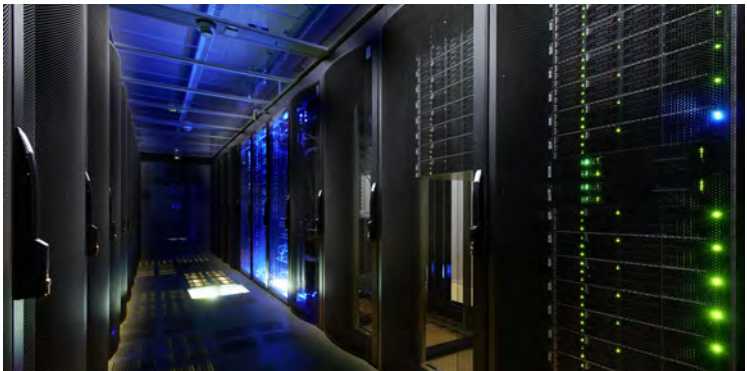
Koniec lat 80-tych:
obecność kilku ścieżek, ale tylko jedna aktywna, redundantne komponenty, możliwość konserwacji bez przerywania

Dostępność
99,982%

Tier IV

1994:
kilka aktywnych ścieżek rozdziatu prądu i wody lodowej, redundantne komponenty, odporność na błędy

Dostępność
99,995%



Procesy bazujące na komunikacji on-line oraz procesy IT drastycznie zwiększają wymagania dostępności.

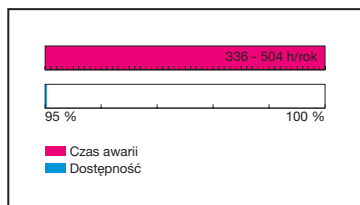
¹⁾ BITKOM, *Betriebssicheres Rechenzentrum*
(Bezpieczne w eksploatacji centrum danych)

Klasy dostępności (VK)

Rosnące wymagania dostępności infrastruktury IT spowodowały również zwiększenie wymagań dotyczących systemów IT. W wysokodostępnych strukturach IT przyjęła się redundancja klimatyzacji i zasilania elektrycznego uzyskiwana przez podwójne źródła oraz bezprzerwową konserwację systemów. Dostępność oblicza się z czasu awarii (czasu przestoju) i całkowitego czasu pracy systemu (centrum danych).

Dostępność = $(1 - \text{czas awarii} / \text{czas produkcji} + \text{czas awarii}) \times 100$

System IT jest określany jako dostępny, gdy jest w stanie wykonywać zadania, do których został przewidziany. Dostępność jest podawana w procentach i dzieli się na klasy dostępności.

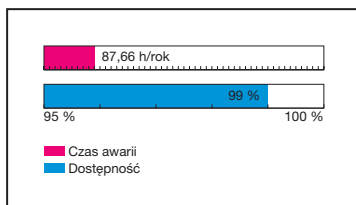


VK 0: ~ 95%
czas awarii = 2 – 3 tygodnie

- Brak wymagań odnośnie dostępności.
- Pod względem dostępności nie należy podejmować żadnych środków.
- Realizacja ochrony podstawowej IT dla innych wartości podstawowych działa korzystnie na dostępność.

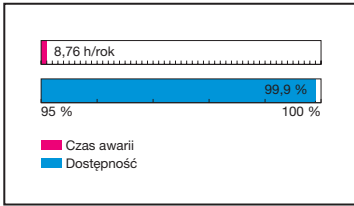
BSI, Federalny Urząd ds. Bezpieczeństwa Techniki Informatycznej:

- BSI opracował system oceny centrów danych VAIR (analiza dostępności infrastruktury w centrach danych). Pod adresem www.vair-check.de operatorzy centrów danych mogą anonimowo i bezpłatnie wprowadzić parametry infrastruktury i sprawdzić odporność na awarię swojego data center.
- BSI definiuje:
 - klasę dostępności,
 - oznaczenie,
 - skumulowany, prawdopodobny roczny czas awarii/skutki.



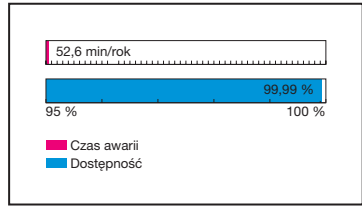
VK 1: 99,0%
czas awarii = 87,66 h/rok

- Zwykła dostępność.
- Pod względem dostępności warunki spełnia zastosowanie ochrony podstawowej IT (BSI 100-1 i BSI 100-2).



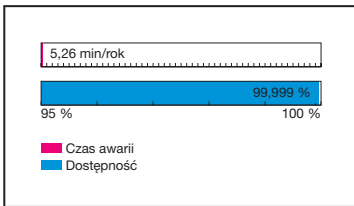
VK 2: 99,9% czas awarii = 8,76 h/rok

- Wysoka dostępność.
- Prosta ochrona podstawowa IT musi być uzupełniona o realizację komponentów zalecanych dla wysokiego zapotrzebowania na dostępność, np. zapobieganie awariom, obsługa incydentów dotyczących bezpieczeństwa i analiza ryzyka na bazie ochrony podstawowej IT (BSI 100-3).



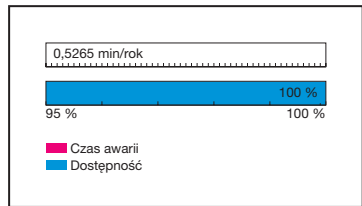
VK 3: 99,99% czas awarii = 52,6 min/rok

- Bardzo wysoka dostępność.
- Realizacja środków zalecanych przez ochronę podstawową IT dla wybranych obiektów ze szczególnym uwzględnieniem dostępności, np. w postaci UPS (zasilanie bezprzerwowe) w serwerowni lub wtórne zasilanie elektryczne w centrum danych, uzupełnione przez inne środki z kompendium wysokiej dostępności.



VK 4: 99,999% czas awarii = 5,26 min/rok

- Najwyższa dostępność.
- Ochrona podstawowa uzupełniona przez modelowanie wg kompendium dostępności.
- Ochrona podstawowa IT jest w coraz większym stopniu zastępowana i uzupełniana poprzez środki wysokiej dostępności.



VK 5: 100% czas awarii = 0,5265 min/rok

- „Disaster tolerant“.
- Modelowanie wg kompendium dostępności. Ochrona podstawowa IT nadal służy jako baza dla ww. obszarów oraz innych kluczowych kwestii, takich jak integralność i poufność.¹⁾

¹⁾ BITKOM, *Betriebssicheres Rechenzentrum*
(Bezpieczne w eksploatacji centrum danych)

Lista kontrolna dostępności IT wg TÜV Rheinland

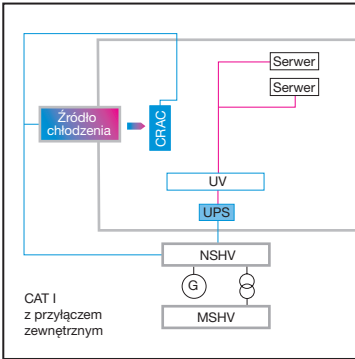
Serwerownia / centrum danych	n	n+1	2n	2(n+1)
< 400 kVA/do 320 kW/200 m ² CAT	1	2	3	4
Zasilanie elektryczne				
Zasilanie / przewód zasilający średniego napięcia	■	■	■	2
Transformatory	■	■	■	2(n+1)
Główna rozdzielnia niskiego napięcia	■	■	■	2(n+1)
Układ zasilania awaryjnego (Diesel)	–	■	■	2(n+1)
Zasilanie bezprzerwowe (UPS)	■	■	2	2(n+1)
Rozdzielnie elektryczne centrum danych	■	n+1	2	2(n+1)
Zasilanie szaf	■	2	2	2
Zasilanie klimatyzacji				
Chillery (chłodziarki / wytwarzanie chłodu)	■	n+1	2n	2(n+1)
Klimatyzatory centrum danych	■	n+1	2n	2(n+1)
System pomp	■	2	2n	2(n+1)
Przewody rurowe	■	■	pętla	pętla
System zarządzania budynkiem				
Robocza wartość progowa wskaźnik/komunikat	–	■	■	■
Komunikaty alarmu przez e-mail, SMS, tablicę sygnalizacyjną	–	■	■	■
Zapis danych	–	–	–	■
Możliwość analizy (ISO 50 001)	opcja	opcja	opcja	opcja
Konserwacja				
Redundancja	–	■	■	■
Redundantne drogi zasilania	–	–	■	■
Konserwacja podczas eksploatacji	–	–	■	■
Okno konserwacji	■	■	–	–

Źródło: TÜV Rheinland: www.tuv.com

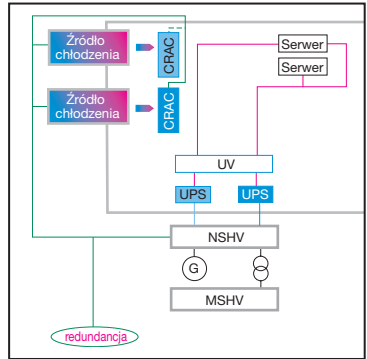
Na schematach blokowych przedstawiony został przegląd kategorii CAT I do CAT IV. Na tych schematach widać, jak musi być zrealizowane centrum danych zgodnie z profilem

wymagań dostępności w odniesieniu do zasilania, zasilania elektrycznego, klimatyzacji, systemu budynku i redundancji, aby spełnić wymagania bezpieczeństwa i otrzymać certyfikat TÜV.

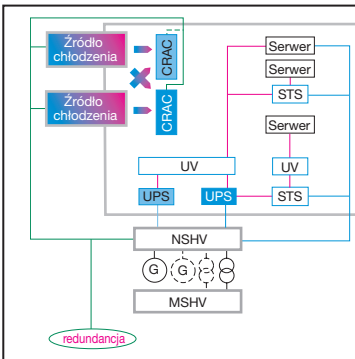
CAT I



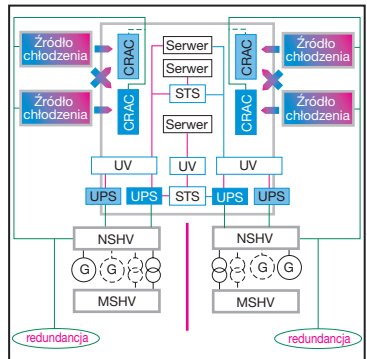
CAT II



CAT III



CAT IV



Wyjaśnienie

- CRAC = urządzenie powietrza obiegowego w centrum danych
- UV = podrozdzielnia
- UPS = zasilanie bezprzerwowe
- NSHV = główna rozdzielnia niskiego napięcia
- MSHV = główna rozdzielnia średniego napięcia
- MS = zasilanie / średnie napięcie
- CAT = kategoria pomiarowa

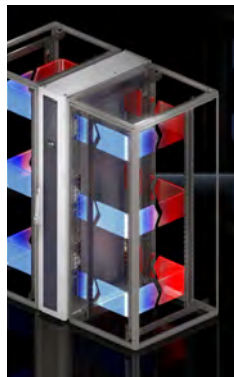
Czynniki dostępności

Nie ma jeszcze krajowej lub międzynarodowej normy bezpieczeństwa centrum danych. W obszarze niemieckojęzycznym korzysta się z protokołów

kontrolnych TÜV lub TSI, które służą do oceny wymagań dotyczących fizycznej infrastruktury IT.

Redundantna moc obliczeniowa i infrastruktura IT dla:

optymalnej temperatury pracy



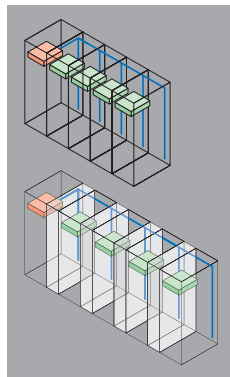
- Normy ASHRAE (temperatura/wilgotność)
- Bezpieczeństwo termiczne: zapewnienie wystarczającego odprowadzania ciepła (klimatyzacja)

zabezpieczenia energii



- Bezpieczeństwo zasilania elektrycznego
- Zapewnienie zasilania elektrycznego także w przypadku awarii – przez UPS lub zasilanie awaryjne

bezpieczeństwa fizycznego



- Dla szaf serwerowych i sieciowych
- Wykrywanie i wcześnie wykrywanie pożaru, instalacja gaśnicza
- System sygnalizacji włamania i kontroli dostępu

Dostępność uwarunkowana bezpieczeństwem termicznym

Prawie cały prąd zużywany przez szafę serwerową lub centrum danych ostatecznie zamienia się w ciepło. Ciepło to musi być z kolei odprowadzone z szafy serwerowej lub centrum danych. Tylko tak można zagwarantować trwałą dostępność systemów IT. Bezpieczeństwo termiczne osiąga się przez następujące koncepcje:

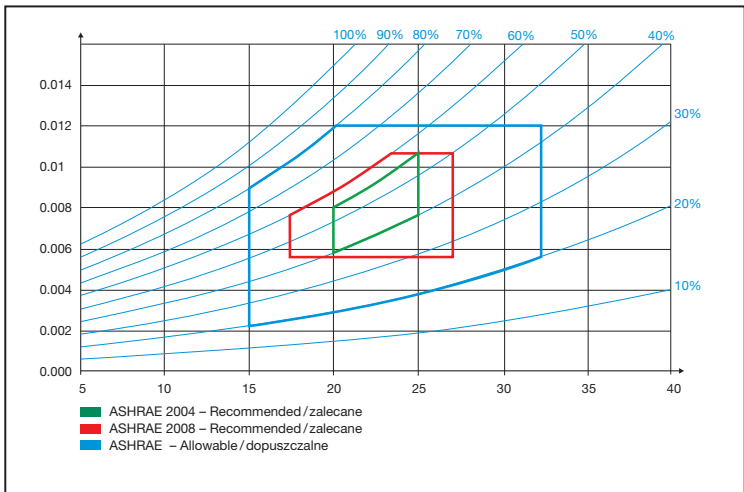
- Koncepcja klimatyzacji dopasowana do szafy IT lub centrum danych
- Zapewnienie koncepcji sprawnej wentylacji w szafie IT
- Funkcjonalność i bezpieczeństwo pracy w odniesieniu do odpro-

wadzenia ciepła (klimatyzacja precyzyjna)

- Zapewnienie niezmienniej temperatury i wilgotności powietrza przez klimatyzację precyzyjną
- Modułowość rozbudowy w przypadku poszczególnych serwerów, jak też centrów danych

Zalecenia klimatyczne (w oparciu o ASHRAE) w szafie IT:

- Dopuszczalna temperatura pracy krótkotrwała 5°C do 40°C, zalecana 18°C do 27°C, dopuszczalna 18°C do 32°C
- Zalecana względna wilgotność powietrza: od 20% do 80%

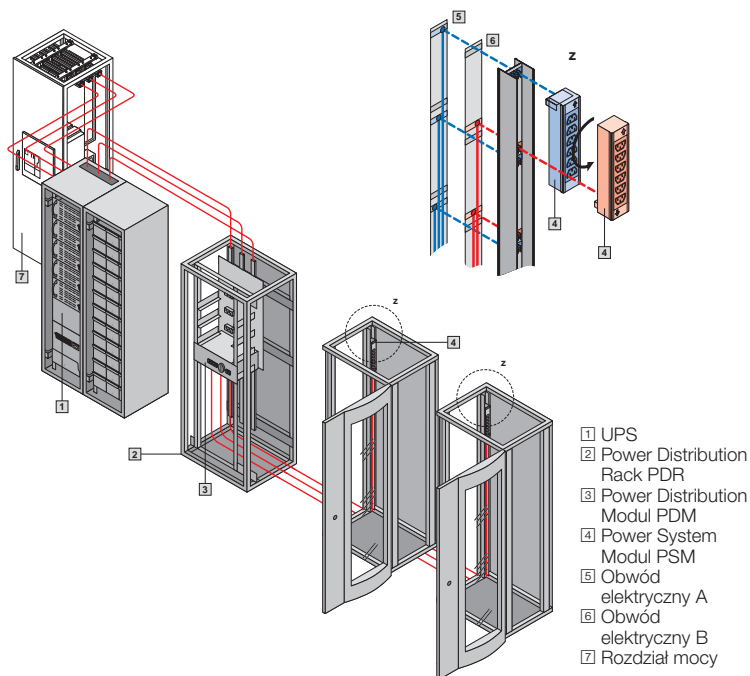


Wykres ASHRAE hx przedstawia zmiany wartości granicznych dla wymagań technicznych odnośnie klimatyzacji serwerów od roku 2004 do 2012.

Źródło: www.ashrae.org

Całościowe zasilanie w energię i zabezpieczenie

Bezpieczeństwo zasilania elektrycznego ma decydujące znaczenie dla dostępności centrum danych. Zaczyna się ono już na etapie doprowadzenia i rozdziału zasilania. Jeżeli budynek jest połączony przez przewód pętlowy, wówczas zasilanie elektryczne odbywa się poprzez dwa przewody średniego napięcia, a więc redundantnie. Zalety: nawet w przypadku awarii przewodu zasilającego, zasilanie będzie zapewnione przez drugi przewód średniego napięcia. Transformatory redukują średnie napięcie w zakresie od 3 do 30 kV na niskie napięcie do 400 V.



Zasilanie elektryczne jest integralną częścią składową komponentów infrastruktury w centrum danych.

Parametry napięcia zasilającego w publicznych sieciach rozdzielczych wg EN 50 160

Cecha	Wymagania	Odstęp pomiarowy	Rozważany okres
Częstotliwość sieci	Sieć sprzęgowa: 50 Hz + 4%/- 6% stale; 50 Hz ± 1% podczas ≥ 99,5% roku Tryb wyspowy: 50 Hz ± 15% stale; 50 Hz ± 2% podczas ≥ 95% tygodnia	Średnia 10 s	1 rok
Wolne zmiany napięcia	$U_{z\text{nam}} + 10\%/- 15\%$ stale $U_{z\text{nam}} \pm 10\%$ podczas ≥ 95% tygodnia	Średnia 10 min	1 tydzień
Migotania/szybkie zmiany napięcia	Długookresowe migotanie światła $P_{\text{fl}} < 1$ podczas ≥ 95% tygodnia i $AU_{10\text{ms}} < 2\% U_{z\text{nam}}$	2 h (miernik migotania światła wg EN 61 000-4-15)	1 tydzień
Asymetria napięć	U (system przeciwny) / U (system zgodny) < 2% podczas ≥ 95% tygodnia	Średnia 10 min	1 tydzień
Harmoniczne $U_{n2} \dots U_{n25}$	< wartość graniczna wg EN 50 160 i THD < 8% podczas ≥ 95% tygodnia	Średnia 10 min każdej harmonicznej	1 tydzień
Interharmoniczne	w trakcie opracowania		1 tydzień
Napięcia sygnałizacyjne	< charakt.norm. – f(f) podczas ≥ 99% dnia	Średnia 3 s	1 dzień
Zapady napięcia	Ilość < 10 ... 1000/rok; z tego 50% z t < 1 s i $AU_{10\text{ms}} < 60\% U_{z\text{nam}}$	10 ms wartość skuteczna $U_{10\text{ms}} - 1 \dots 90\% U_{z\text{nam}}$	1 rok
Krótkie przerwy w zasilaniu	Ilość < 10 ... 1000/rok; z tego > 70% trwające < 1 s	10 ms wartość skuteczna $U_{10\text{ms}} \geq 1\% U_{z\text{nam}}$	1 rok
Długie przerwy w zasilaniu	Ilość < 10 ... 50/rok trwające > 3 min		1 rok
Przepięcia dorywcze (L-N)	Ilość < 10 ... 1000/rok; z tego > 70% trwające < 1 s	10 ms wartość skuteczna $U_{10\text{ms}} \geq 110\% U_{z\text{nam}}$	1 rok
Przepięcia przejściowe	< 6 kV; $\mu\text{s} \dots \text{ms}$		b. d.

Rozdzielnie niskiego napięcia w centrum danych

Ekonomiczne zwymiarowanie rozdzielni niskiego napięcia dla centrum danych wymaga uwzględnienia warunków panujących na miejscu, zadań rozdzielni i wymagań dotyczących dostępności. Bezpieczeństwo ludzi i wykluczenie uszkodzeń urządzeń są na pierwszym miejscu. Dlatego przy doborze właściwej rozdzielni należy zwrócić uwagę na to, aby zastosowana została rozdzielnia z badaniem typu (świadczenie weryfikacji wg IEC 61 439-1/-2, VDE 0660-600-1/-2), z poszerzoną kontrolą zachowania w warunkach łuku elektrycznego (por. IEC/TR 61 641, VDE 0660-500, załącznik 2). Rozdzielnice i urządzenia zabezpieczające muszą być zawsze dobierane pod kątem obowiązujących przepisów określających wymagania odnośnie całej sieci (pełna selektywność, częściowa selektywność). Zalecenia brzmią następująco: Rozdzielnię niskiego napięcia z izolacją szyn zbiorczych przy zasilaniu należy połączyć przez systemy szyn zbiorczych ze standardowymi komponentami przyłączeniowymi. W ten sposób minimalizuje się błędy. Rozdzielnie niskiego napięcia muszą być instalowane z zachowaniem podanych przez producenta minimalnych odległości rozdzielni od przeszkód. Minimalne wymiary korytarzy obsługowych i serwisowych należy zaprojektować zgodnie z IEC 60 364-7-729 (VDE 0100- 729).

Ogólnie rzecz ujmując, rozdział mocy wymaga maksymalnego bezpieczeństwa zasilania i pełnej, wysokiej przejrzystości, np. poprzez system zarządzania energią. Ponadto do niezawodnej pracy IT niezbędne jest również niewielkie obciążenie ogniowe oraz niskie oddziaływanie pól elektromagnetycznych.

Do obszarów zasilania i zabezpieczania energii należą:

- Jedno lub kilka niezależnych źródeł zasilania, w zależności od wymaganej dostępności
- Przejrzyste, mający jasną strukturę energetyczną podział pomiędzy rozdzielnią główną a podrozdzielnią
- Zabezpieczenie zasilania poprzez zasilanie bezprzerwowe (systemy UPS)
- Zabezpieczenie obwodu prądu stałego za pomocą baterii i alternatywnych źródeł prądu, jak system fotowoltaiczny lub energia wiatrowa
- Włączanie i odłączanie obciążenia IT przez inteligentne systemy gniazdek zasilających

Niezawodny rozdział energii

Wymagania dotyczące zasilania elektrycznego w każdym centrum danych są inne i zależą od wyposażenia. Główne zasilanie jest jednak takie samo w każdym centrum danych. Oznacza to, że wiele centrów danych jest wyposażonych w zasilanie sieciowe od dostawców energii, jeden lub kilka zasilaczy bezprzerwowych (UPS), a także w generator.

Budowę bezpiecznego i niezawodnego rozdziału mocy przedstawia przykład rozwiązania Rittal i Siemens, patrz s. 75.

Zaliczają się do nich:

- Główna rozdzielnia niskiego napięcia
- Data centre backbone
- Podrozdzielnia
- Systemy gniazdek zasilających

Poprzez normalną podrozdzielnię sieciową zasilany jest także UPS.



Zasilanie bezprzerwowe (UPS)

Do podstawowego wyposażenia centrum danych należy zasilanie bezprzerwowe: Uninterruptable Power Supply – UPS. Ich początki sięgają wież wiertniczych ropy naftowej, gdzie były stosowane od połowy lat sześćdziesiątych. UPS jest jednym z krytycznych czynników powodzenia dla dostępności infrastruktury IT. W Europie systemy UPS uregulowane są standardem EN 50 091 i spełniają następujące warunki:

- Zapewnienie stałego napięcia wyjściowego także po przekroczeniu (skok napięcia, plus, spike) lub spadku (zapad napięcia, sag) napięcia sieciowego w zakresie milisekundowym
- Zapewnienie czystego jakościowo, sinusoidalnego przebiegu napięcia wyjściowego
- Odfiltrowanie niebezpiecznie wysokich przepięć (np. spowodowanych uderzeniem pioruna)
- Pojemność rezerwowa w przypadku awarii zasilania, wystarczająca do zapewnienia kontrolowanego wyłączenia zabezpieczanych systemów, względnie do załączenia długotrwałych systemów rezerwowych, jak generatory prądotwórcze

Systemy UPS z reguły posiadają dwie jednostki funkcyjne:

- Wygładzanie uderów napięcia, np. wskutek uderzeń piorunów i zapadów napięcia
- Przełączanie na tryb awaryjny w zakresie milisekundowym

Tryb awaryjny trwa zwykle 10 do 15 minut. W zależności od kraju, może być wymagany dłuższy tryb bateryjny. Następnie możliwe jest dołączenie innych awaryjnych agregatów prądowych lub baterii w systemie hot-swap. Określony czas podtrzymania, typy odbiorników oraz zużycie definiują system UPS i pojemność baterii. W tym czasie systemy po stronie obciążenia powinny się wyłączyć lub zostać odłączone.



Przegląd kodu klasyfikacyjnego wg EN 62 040-3

Kod klasyfikacyjny								
V	F	I	S	S	1	2	3	
Zależne od wyjścia			Krzywa napięcia wyjściowego		Dynamiczna charakterystyka wyjścia			
tylko w trybie normalnym			1. litera: normalny lub obejście 2. litera: tryb baterii		1. cyfra: przy zmianie trybu pracy 2. cyfra: przy liniowym skoku obciążenia (ang.: worst case) w trybie normalnym lub baterijnym 3. cyfra: nieliniowy skok napięcia (ang.: worst case) w trybie normalnym lub baterijnym			

Znaczenia kodu

VFI: Wyjście UPS niezależne od zmian napięcia sieciowego i częstotliwości. Napięcie zasilania jest w granicach wg IEC 61 000-2-2. Dzieje się tak, gdyż napięcie zasilające jest nieregulowane, a zgodnie z uwagą pod niniejszą tabelą IEC 61 000-2-2 określa tylko normalny poziom wyższych harmonicznych i poziom zniekształceń napięcia, a nie zmiany częstotliwości.

VFD: Wyjście UPS zależne od zmian częstotliwości i napięcia sieci.

VI: Częstotliwości wyjściowe UPS stabilizowane zależnie od częstotliwości sieci, napięcia (elektronicznie/pasywnie) w zakresie wartości granicznych dla trybu zwykłego.

S: Sinusoidalna krzywa napięcia wyjściowego. Współczynnik zawartości wyższych harmonicznych $D < 0,08$ < IEC 61 000-2-2 przy ref. obciążeniu liniowym i nieliniowym.

X: Sinusoidalna krzywa napięcia wyjściowego taka sama jak dla „S” przy obciążeniu liniowym. Przy obciążeniu liniowym i nieliniowym współczynnik zawartości wyższych harmonicznych $D > 0,08$ przy obciążeniu powyżej granic podawanych przez producenta.

Y: Krzywa napięcia nie jest sinusoidalna. Przekracza wartości graniczne wg IEC 61 000-2-2 (patrz dane producenta dot. rodzaju krzywej).

1: \leq rys. 1 w 5.3.1 (bezprzerwowo)

2: \leq rys. 2 w 5.3.1 (przerwanie napięcia do 1 ms)











3: \leq rys. 3 w 5.3.1 (przerwanie napięcia do 10 ms)

4. O właściwości należy zapytać producenta

Uwaga: IEC 61 000-2-2 określa normalny poziom wyższych harmonicznych i poziom zniekształceń napięcia, których można oczekiwać w sieciach publicznych na przyłączy odbiornika, przed podłączeniem układu odbiornika.

Przyporządkowanie błędów sieci do systemów UPS

Zgodnie z normą produktową dla UPS, EN 62 040-3 istnieje dziesięć różnych błędów sieci wyłapywanych przez UPS:

	Zakłócenia sieci	Czas	Np.	EN 62 040-3	Rozwiązanie UPS	Rozwiązanie ochronika
1.	Przerwy w zasilaniu	> 10 ms		VFD Voltage + Frequency Dependent	Klasyfikacja 3 Tryb pasywny standby (offline)	–
2.	Szybkie zmiany napięcia	< 16 ms				–
3.	Krótkotrwałe przebiegi	4 ... 16 ms				–
4.	Zapady napięcia	ciągłe		VI Voltage Independent	Klasyfikacja 2 Tryb line interactive	–
5.	Przebiegi	ciągłe				–
6.	Impulsy przebiegowe (surge)	< 4 ms		VFI Voltage + Frequency Independent	Klasyfikacja 1 Tryb konwersji	–
7.	Oddziaływanie przebiegów atmosferycznych	spora-dyczne				Ochrona odgromowa i przebiegowa (IEC 60 364-5-53)
8.	Odstąpienia krzywej napięcia (burst)	okresowo				–
9.	Wyższe harmoniczne napięcia	ciągłe				–
10.	Wahania częstotliwości	spora-dyczne		–		

Rodzaje zakłóceń sieciowych i odpowiednich rozwiązań UPS wg IEC 62 040-3 (VDE 0558-530) [12]

Tryby pracy UPS

■ Tryb normalny

Prostownik jest zasilany energią z sieci elektrycznej, więc baterie są ładowane z pośredniego obwodu prądu stałego.

■ Tryb bateryjny

W przypadku awarii zasilania elektrycznego z sieci publicznej. Falownik jest zasilany energią z baterii aż do momentu rozładowania baterii.

■ Tryb obejściowy

Gdy falownik jest przeciążony lub uszkodzony. Obejście włącza się również w przypadku awarii prostownika lub uszkodzenia baterii. UPS jest pomijany.

Wnioski

Poza zasilaniem w przypadku awarii, UPS ma za zadanie również ciągle polepszanie jakości zasilania elektrycznego.

Norma EN 62 040-3 została stworzona w celu sklasyfikowania systemów UPS. Wprowadziła ona trójstopniowy kod klasyfikacyjny, który jest podany w tej normie.



Redundancja systemów UPS

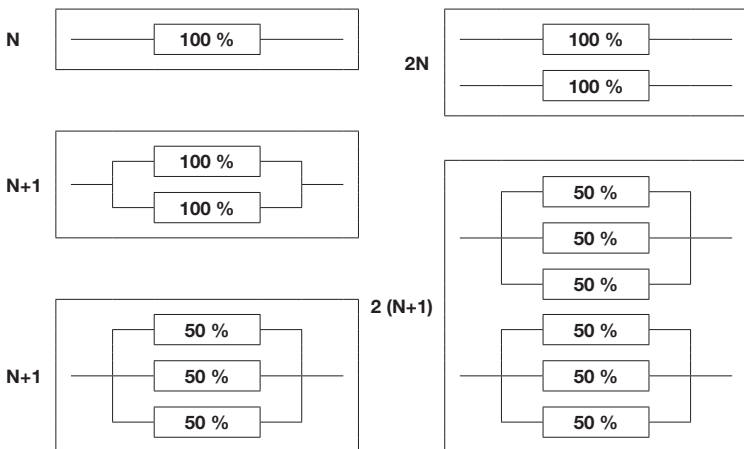
W celu zapewnienia bezpieczeństwa zasilania elektrycznego wskazane jest, aby systemy UPS były zrealizowane

redundantnie. Klasyfikacja centrum danych oraz dopuszczalny czas awarii decyduje o tym, od kiedy wymagana jest redundancja systemów UPS.

Kategoria centrum danych	UPS			Dopuszczalny czas awarii centrum danych
	Szafa serwerowa	Szafa serwerowa	Centrum danych / serwerownia	
	do 7 kW	od 7 kW do 40 kW	500 do 2500 W/m ²	
A	Standard, minimalny czas podtrzymania 10 min (z wentylacją), minimalny czas pracy zależny od kontrolowanego czasu wyłączenia serwerów		Standard, minimalny czas podtrzymania 10 min, minimalny czas pracy zależny od kontrolowanego czasu wyłączenia serwerów	12 h
B	Redundancja (N+1), minimalny czas podtrzymania 10 min			1 h
C	Redundancja (2N), minimalny czas podtrzymania 10 min			10 min
D	Redundancja 2 (N+1), minimalny czas podtrzymania 10 min			< 1 min

Źródło: Tabela BITCOM „Pomoc planistyczna w eksploatacji centrum danych”

Dla systemów UPS znajdują zastosowanie następujące redundancje:¹⁾



¹⁾ BITKOM, *Betriebssicheres Rechenzentrum* (Bezpieczne w eksploatacji centrum danych)

Dostępność uwarunkowana bezpieczeństwem fizycznym

(Streszczenie informacji BSI)

Katalogi ochrony podstawowej IT

Poszczególne elementy składowe katalogów ochrony podstawowej IT zawierają: krótki opis poszczególnych komponentów, zasad postępowania i systemów IT oraz przegląd sytuacji zagrożeń i zalecane środki zaradcze. Składniki są połączone w grupy na bazie warstwowego modelu ochrony podstawowej IT na następujące katalogi:

- B1: Ogólne aspekty bezpieczeństwa informacji
- B2: Bezpieczeństwo infrastruktury
- B3: Bezpieczeństwo systemów IT
- B4: Bezpieczeństwo w sieci
- B5: Bezpieczeństwo w aplikacjach

Katalogi zagrożeń

Ta część zawiera szczegółowe opisy zagrożeń, które zostały podane w poszczególnych częściach składowych. Zagrożenia są zgrupowane w pięciu katalogach:

- G0: Podstawowe zagrożenia
- G1: Siła wyższa
- G2: Braki organizacyjne
- G3: Błędy w działaniu człowieka
- G4: Awaria techniczna
- G5: Działania umyślne

Dodatkowo wprowadzony został katalog zagrożeń elementarnych G0 zawierający uogólnione i zredukowane do najistotniejszych zagrożenia elementarne. Katalog ten może być używany np. do analiz ryzyka.

Katalogi działań

Ta część szczegółowo opisuje środki bezpieczeństwa cytuwane w częściach składowych katalogów ochrony podstawowej IT. Środki te są zgrupowane w sześciu katalogach działań:

- M1: Infrastruktura
- M2: Organizacja
- M3: Personel
- M4: Sprzęt i oprogramowanie
- M5: Komunikacja
- M6: Zapobieganie awariom



Uprawnienia / dostęp do budynku, pomieszczenia, szafy

Kryteria planowania dostępności

	Definicja celu zastosowania
Planowanie i koncepcja	<ul style="list-style-type: none"> ■ Określenie scenariuszy działania ■ Ocena potencjału wystąpienia ryzyka ■ Dokumentacja decyzji o zastosowaniu ■ Sporządzenie koncepcji bezpieczeństwa ■ Określenie wytycznych do zastosowania
Zaopatrzenie (jeżeli jest wymagane)	<ul style="list-style-type: none"> ■ Określenie wymagań dotyczących nabywanych produktów (w miarę możliwości na bazie scenariuszy działania określonych w fazie planowania) ■ Wybór odpowiednich produktów
Realizacja	<ul style="list-style-type: none"> ■ Koncepcja i przeprowadzenie trybu testowego ■ Instalacja i konfiguracja zgodnie z wytycznymi bezpieczeństwa ■ Szkolenie i uświadomienie wszystkich zaangażowanych
Praca	<ul style="list-style-type: none"> ■ Środki bezpieczeństwa dla bieżącej eksploatacji (np. protokołowanie) ■ Ciągła dbałość i rozwój ■ Zarządzanie zmianami ■ Organizacja i przeprowadzenie prac konserwacyjnych ■ Audyt
Usuwanie (jeżeli jest wymagane)	<ul style="list-style-type: none"> ■ Odbieranie uprawnień ■ Usuwanie zbiorów danych i referencji do tych danych ■ Bezpieczna utylizacja nośników danych
Zapobieganie awariom	<ul style="list-style-type: none"> ■ Koncepcja i organizacja zabezpieczania danych ■ Użycie redundancji dla zwiększenia dostępności ■ Postępowanie z incydentami dotyczącymi bezpieczeństwa ■ Sporządzenie planu awaryjnego

Źródło: www.bund.bsi.de

Szafa IT jako baza dla bezpieczeństwa fizycznego

Podstawę do bezpiecznego umieszczenia serwerów i systemów IT w centrum danych stanowi szafa IT.

Wymagania bezpiecznej szafy serwerowej

- Skalowalność w montażu komponentów całowyc
- Możliwość rozbudowy w oparciu o inteligentny program akcesoriów
- Łatwość montażu przy jednoczesnym zredukowaniu złożoności akcesoriów

- Stabilność, czyli nośność do 1 500 kg, do dużej gęstości serwerów i serwerów typu blade
- Ochrona przed nieupoważnionym dostępem i systemy zamków z kontrolą dostępu
- Montaż systemów wczesnego wykrywania i gaszenia pożaru
- Zapewnienie rozbudowy (dodatkowe szafy IT)

W wysokowydajnych centrach danych szafy są ustawiane zarówno pojedynczo, jak i w szeregach. Modułową szafę serwerową można w razie potrzeby zdemontować lub przebudować – w tym także komponenty klimatyzacji.



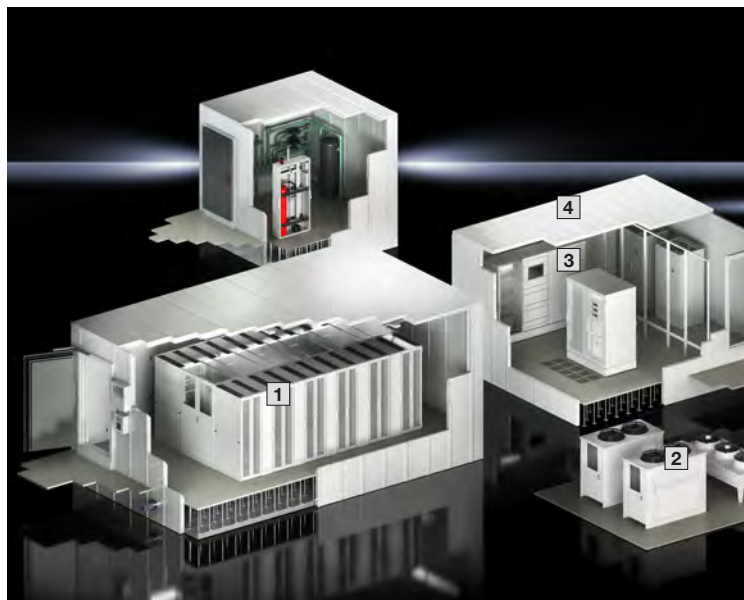
Bezpieczne, chronione przed pożarem centrum danych jako rozwiązanie systemowe: Rittal Micro Data Center

■Efektywność

Czynniki efektywnego IT

Zapotrzebowanie na energię w centrum danych jest tak jak wcześniej wysokie, – także po przeprowadzeniu różnych działań zwiększających efektywność. Dlatego podczas użytkowania centrum danych zapotrzebowanie energetyczne stanowi często najważniejszy czynnik generowania kosztów. Podzespoły elektroniczne i procesory w centrum danych produkują moc ciepłą, Thermal Design Power (TDP).

Na tej podstawie projektuje się chłodzenie systemów IT. W wyniku tego powstaje konflikt celów pomiędzy mocą obliczeniową, kosztami a klimatyzacją pomieszczeń. Dodatkowo poza dostępnością i bezpieczeństwem, efektywność energetyczna zalicza się do głównych wyzwań w nowoczesnych centrach danych.



1 Serwery IT

2 Chłodzenie

3 Rozdział mocy

4 Oświetlenie

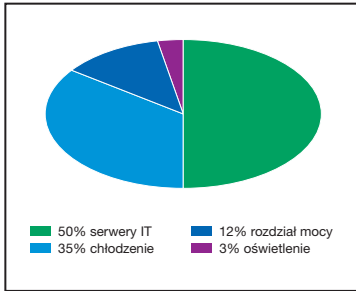
ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Według aktualnych pomiarów, zapotrzebowanie energetyczne dzieli się następująco: 50% serwery IT, 35% chłodzenie, 12% rozdział mocy oraz 3% oświetlenie.

Zależnie od wyboru lokalizacji, koszty energii wpływają na całkowite koszty eksploatacji.



Wielkości wpływające na efektywną infrastrukturę centrum danych

- Efektywne dostarczanie niezbędnej energii
- Efektywne odprowadzanie ciepła z serwerów
- Wybór architektury i lokalizacji
- Opcje dotyczące skalowania

Im wyższa jest temperatura powietrza wylotowego, tym efektywniej pod względem energetycznym zachodzi proces wytwarzania chłodu. Z tego wynika: im wyższa jest różnica temperatur (wylotu i wlotu powietrza), tym mniejsza ilość powietrza jest potrzebna do odprowadzenia obciążenia cieplnego z centrum danych.

Zasada ta jest identyczna w przypadku medium chłodniczego w postaci wody. Także w chłodzeniu cieczą obowiązują zasady: Im bliżej ogniska gorąca (serwera) odbywa się chłodzenie, tym jest efektywniejsze. Im wyższa jest temperatura powrotu wody, tym dłużej może być stosowany freecooler bez chłodziarki.



Energooszczędne chłodzenie (free cooling) można wykorzystać na wiele sposobów.

Poza tym w katalogu kryteriów efektywności należy uwzględnić następujące elementy:

Modułowość oraz monitorowanie i ukierunkowane sterowanie odbiornikami.

Obiektywna analiza ROI (Return On Investment), poza kosztami inwestycji, obejmuje także analizę szacowanych kosztów eksploatacji. Poza kosztami personelu, sprawdzenia i oceny wymagają przede wszystkim koszty zużycia energii.

Wszystkie kryteria efektywności dla komponentów, systemów, a przez to dla całej infrastruktury IT, decydują o stopniu efektywności całego centrum danych.

Efektywność energii używanej w centrach danych

Można ją analizować ilościowo na różne sposoby. Wariant wybrany przez organizację The Green Grid uwzględnia dwa parametry:

- Data Center Infrastructure Efficiency (DCIE)
- Power Usage Effectiveness (PUE)

DCIE ocenia sprawność zużytej w centrum danych energii w procentach.

Wzór obliczeniowy na efektywność energetyczną centrum danych

Data Center Infrastructure Efficiency (DCIE)

$$\text{DCIE} = \frac{\text{Zużycie energii przez IT}}{\text{Całkowite zużycie energii przez centrum danych}} \times 100\%$$

Power Usage Effectiveness (PUE)

$$\text{PUE} = \frac{\text{Całkowite zużycie energii przez centrum danych}}{\text{Zużycie energii przez IT}}$$

Obliczenie energii termicznej

(ciepło tracone lub potrzebna moc chłodnicza)

$$Q = c \times m \times (T_a - T_z)$$

Q > Energia cieplna
(ciepło/moc chłodnicza)

c > Specyficzny współczynnik przewodzenia ciepła
(powietrze/woda)

m > Masa medium
(powietrza lub wody)

T_a = Temperatura powietrza wylotowego

T_z = Temperatura powietrza wlotowego

Na często wymieniany **współczynnik PUE** składa się całkowita ilość energii zużytej w centrum danych w stosunku do zużycia energii przez komputery.

Współczynnik PUE równy 3 wskazuje na wysoką nieefektywność: dwie trzecie zużytej energii potrzebne jest do chłodzenia, natomiast tylko jedna trzecia mocy jest zużywana przez komputery. Gdy ten iloraz zbliża się do liczby 1, to centrum danych pracuje bardziej efektywnie. Współczynniki PUE rzędu 1,3 są już doskonałe i oznaczają, że 30% energii nie jest używane przez serwery i pamięci masowe. Idealny PUE wynosi 1.

PUE = całkowity pobór prądu przez centrum danych / pobór prądu przez sprzęt IT

- Obowiązuje zasada: im mniej efektywne są poszczególne komponenty, tym gorsza jest efektywność energetyczna całego centrum danych.
- Na efektywność centrum danych wpływa głównie aktywna moc chłodnicza serwerów i odprowadzanie ciepła z centrum danych.
- Istotna dla ekonomicznego użytkowania klimatyzacji IT jest m.in. różnica między temperaturą powietrza wlotowego a wylotowego z serwera lub z centrum danych.



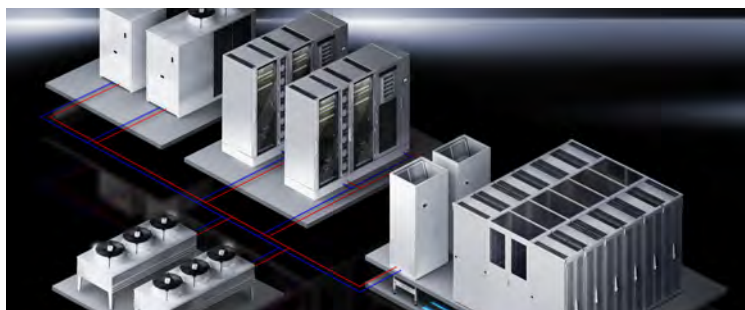
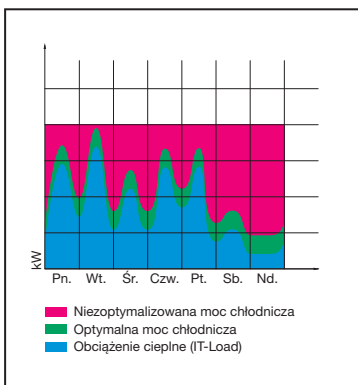
W ekonomicznym centrum danych wszystkie odbiorniki poddaje się optymalizacji pod kątem efektywności.

Drogi zwiększania efektywności centrum danych

- Zastąpienie starych serwerów nowymi serwerami typu blade, wirtualizacja i Server Load Management
- Optymalizacja klimatyzacji przez zarządzanie temperaturą i wolumenem powietrza
- Zastosowanie freecoolerów (wykorzystanie w chłodzeniu powietrza otoczenia)
- Separacja stref, czyli oddzielenie strony zimnej od ciepłej w infrastrukturze IT
- Dopasowane do potrzeb sterowanie wytwarzaniem i rozdział chłodu
- Chłodzenie na bazie wody gruntowej lub geotermii
- Alternatywne wytwarzanie prądu, np. za pomocą instalacji fotowoltaicznej, na własne potrzeby centrum danych
- Kompleksowa analiza procesów za pomocą oprogramowania DCIM (Data Center Infrastructure Management)
- Wybór lokalizacji w celu wykorzystania lepszej średniej temperatury rocznej
- Łączenie centrów danych: rozłożenie obciążenia zgodnie z kryteriami efektywności, m.in. dla klimatyzacji, kosztów energii, mocy

Przykład efektywności

Analogicznie do poboru mocy przez centrum danych, moc chłodnicza musi być zaprojektowana dla mocy maksymalnej przy niekorzystnych temperaturach otoczenia. Wykres tygodniowy pokazuje, że w związku z tym chłodzenie bez kompleksowego zarządzania jest przeważnie przewymiarowane.



Czy to chłodzenie free cooling, separacja stref, czy też optymalizacja klimatyzacji – efektywność infrastruktury IT można wyraźnie zwiększyć.

Monitoring

Mając za podstawę informacje z centralizowanego monitoringu, można wykonać trzy decydujące kroki w celu określenia faktycznego zapotrzebowania energetycznego:

- Analiza
- Optymalizacja
- Sterowanie

Już sam pomiar całkowitego zapotrzebowania centrum danych na energię często prowadzi do ujawnienia potencjałów obniżenia zużycia energii i kosztów. Jeżeli zapotrzebowanie energetyczne jest adekwatnie uwzględnione przy wyposażaniu centrum danych, często podejmowane są inne decyzje dotyczące kosztów inwestycji.

Przykładowo nieco większa inwestycja w efektywne energetycznie chłodzenie może się opłacić już po kilku miesiącach.¹⁾

Monitorowanie, sterowanie i dokumentowanie za pomocą kompleksowego oprogramowania

Niezbędne do zagwarantowania bezpieczeństwa i dostępności jest monitorowanie wszystkich systemów w centrum danych. Z tego wynika, że bezpieczne w eksploatacji centrum danych musi być wyposażone w Data Center Management System (DCIM). Odpowiednie wytyczne zostały opublikowane w bibliotece ITIL. Ten zbiór reguł można przenieść na wszystkie organizacje IT.



¹⁾ BITKOM, *Energieeffizienz im Rechenzentrum*
(Efektywność energetyczna w centrum danych)

Data Center Infrastructure Management System (DCIM)

Dla kompleksowego bezpieczeństwa centrum danych niezbędny jest ogólnosystemowy monitoring całej infrastruktury, czyli od serwera, przez klimatyzację, zasilanie elektryczne, okablowanie, zabezpieczenie przed pożarem, aż po ochronę przed nieupoważnionym dostępem. Do tego potrzebne są inteligentne systemy monitorowania. Czujniki w szafach

serwerowych i w pomieszczeniu centrum danych zbierają takie informacje, jak temperatura, wilgotność i prędkość powietrza, a także moc komputerów i przekazują dane przez system DCIM do administratora IT. W celu zwiększenia efektywności, część pracy centrum jest optymalizowana automatycznie na podstawie danych pomiarowych.



Administrator może nadzorować swoje centrum danych bezpośrednio przy szufladzie monitoringu (na zdjęciu: jednostka monitor-klawiatura 1 U Rittal)



Kontrola dostępu jest elementem bezpieczeństwa fizycznego.

- Zasilanie i zabezpieczanie energii
- Wytwarzanie i rozdzielanie chłodu do szaf serwerowych i wymienników ciepła
- Temperatura oraz wilgotność w pomieszczeniu i przy serwerach
- Monitorowanie centrum danych i szaf serwerowych
- Bezpieczeństwo z kontrolą dostępu
- Sprawność, zużycie energii, bilans energetyczny i wydajność wytwarzania chłodu

Integracja danych z centralnym systemem zarządzania budynkiem oraz monitorowanie tych danych są niezbędne dla zapewnienia optymalnej i efektywnej energetycznie pracy centrum danych.

Ważne dla administratora IT jest, aby w określonych odstępach czasu były generowane automatyczne raporty. Na ich podstawie można nadzorować obciążenie, koszty eksploatacji i efektywność centrum danych. Dzięki tym danym można określić tendencję aktualnego, miesięcznego oraz rocznego zużycia energii i zwiększyć wydajność oraz zoptymalizować efektywność.

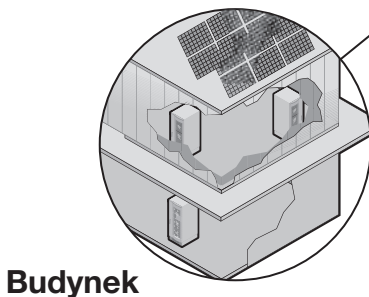
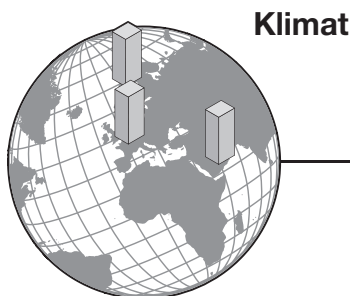
■ Lokalizacja

Czynniki lokalizacji

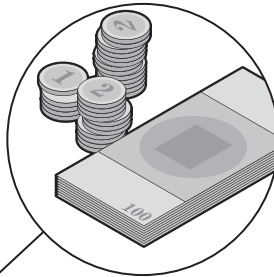
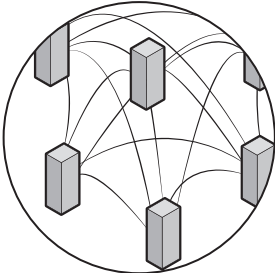
Ocena lokalizacji pod względem infrastruktury

Analiza lokalizacji w aspekcie bezpieczeństwa, dostępności i efektywności energetycznej odgrywa decydującą rolę w przypadku planowania lub opracowywania koncepcji nowego centrum danych.

- Jakie warunki klimatyczne panują w danym miejscu, np. średnia temperatura otoczenia (porównanie Dubaju, Niemiec i Norwegii)?
- Jaka infrastruktura jest do dyspozycji, np. budynek, kontener, zasilanie elektryczne lub alternatywne (instalacja fotowoltaiczna)?
- Jakie są koszty energii w danym miejscu i jakie istnieją alternatywy chłodzenia?
- Jaka jest dostępność lokalizacji (koszty niezbędnej infrastruktury, dojazdu itd.)?
- Jaki poziom wykształcenia reprezentują dostępni specjaliści?

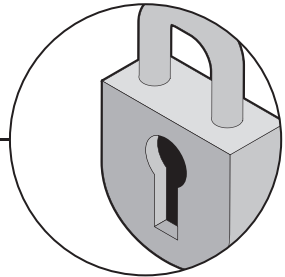


Połączenie z siecią

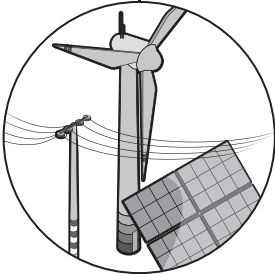


Podatki

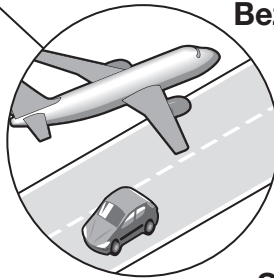
Decyzja o lokalizacji IT



Bezpieczeństwo



Koszty energii



Specjaliści, dojazd

IT INFRASTRUCTURE

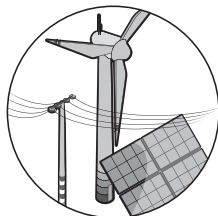
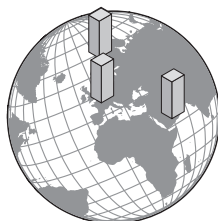
SOFTWARE & SERVICES



Czynniki lokalizacji: klimat i koszty energii

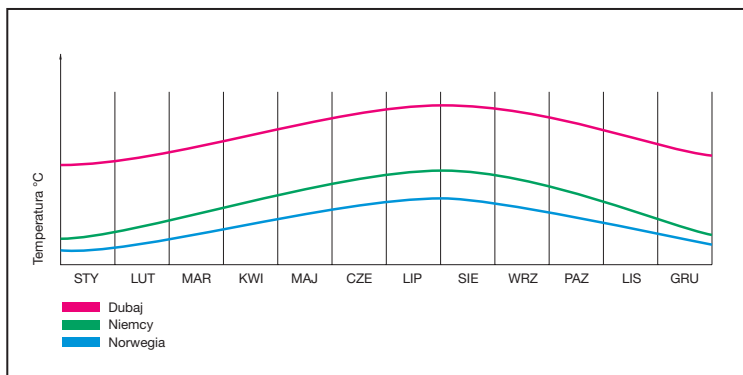
Decydującym czynnikiem przy wyborze lokalizacji nowego centrum danych są koszty energii do zasilania systemów i klimatyzacji.

Średnia temperatura otoczenia w ciągu roku (Niemcy 9,2°C lub Norwegia 5,8°C) może być decydującym czynnikiem przy wyborze lokalizacji. W przypadku niższej średniej rocznej temperatury, niezbędna klimatyzacja może być alternatywnie obsługiwana przez dłuższy czas chłodzeniem swobodnym (free cooling), czyli bez użycia chłodziarek.



Przykład:

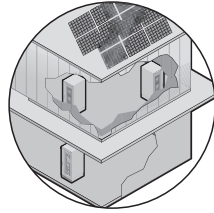
- Norwegia –
średnia roczna temperatura + 5,8°C
- Niemcy –
średnia roczna temperatura + 9,2°C
- Dubaj –
średnia roczna temperatura + 27,4°C



Porównanie średnich rocznych temperatur w Niemczech, Norwegii i Dubaju

**Czynniki lokalizacji:
budynek, dostępność,
wykwalifikowany personel**

- Położenie centrum danych w budynku
 - nasłonecznienie
 - bezpieczeństwo
 - doprowadzenie zasilania elektrycznego
- Koszty dostępności w przypadku dostosowania infrastruktury i serwerów, konserwacji, awarii systemu itd.
- Dostępność wykwalifikowanego personelu
- Możliwość rozbudowy, a przez to długoterminowe bezpieczeństwo



Coraz bardziej złożone systemy i aplikacje IT wymagają obsługi przez wykwalifikowany personel.

Czynniki lokalizacji: połączenie z siecią, podatki i bezpieczeństwo

Niezbędna jest również analiza ryzyka dla lokalizacji. Czynnikiem ryzyka mogą być:

Połączenie z siecią

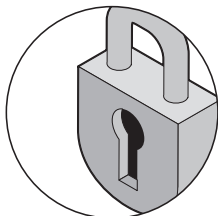
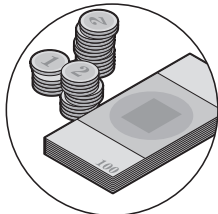
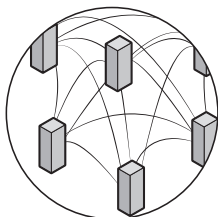
- Połączenie z węzłami internetowymi

Podatki

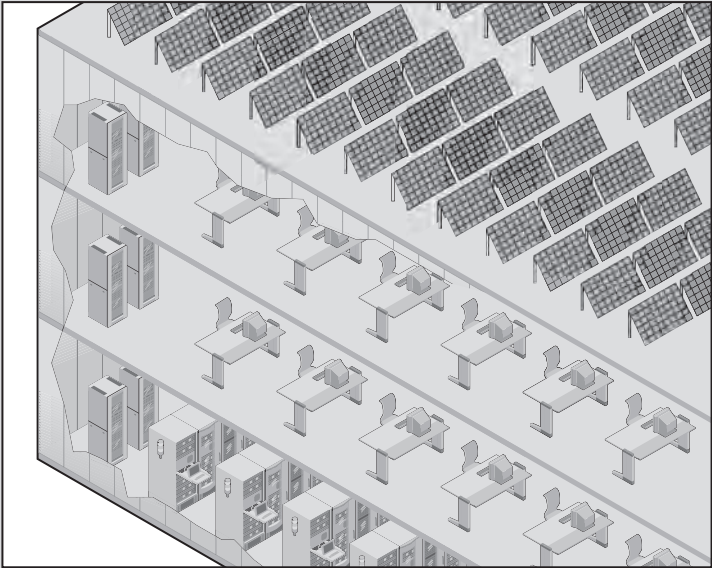
- Podatki regionalne (np. podatek od działalności gospodarczej) i opłaty

Bezpieczeństwo

- Klęski żywiołowe, np. tereny zagrożone powodzią lub trzęsieniem ziemi
- Położenie komunikacyjne, np. drogi do transportu substancji niebezpiecznych
- Odległość od lotnisk (korytarze wlotowe)
- Stabilność polityczna i sytuacja prawna
- Bliskość obiektów zagrożonych pożarem, np. elektrowni, fabryk chemicznych, rurociągów
- Źródła aktywne elektromagnetycznie, np. transformatory, stacje transformatorowe, nadajniki i trasy kolejowe
- Zabezpieczony dostęp i ochrona przed wandalizmem



Przykład znaczenia czynników lokalizacji



W przykładowej realizacji analizowana jest firma usługowa z 200 pracownikami i centrum danych o mocy 200 kW. Pracownicy firmy korzystają z procesów i narzędzi bazujących na oprogramowaniu. W związku z tym trwale zapisywane i zabezpieczane są dane cyfrowe. Niektórzy klienci wymagają archiwizacji danych do 10 lat, przez co aktualna ilość danych opiewa na 40 terabajtów. Pracownicy pracują od poniedziałku do piątku, od 6:00 rano do godz. 20:00 wieczorem, co sprzyja wykorzystaniu energii odnawialnej.

Klimat i koszty energii

Serwery w chłodnej piwnicy, klimatyzacja od strony północnej, zużycie energii przez klimatyzację i komputery koreluje z mocą instalacji fotowoltaicznej w ciągu dnia, zakup energii został zredukowany o 90%.

Budynek i dostępność

Centralne położenie, zabezpieczony dostęp na poziomie piwnicy. Dobry dojazd.

Połączenie z siecią, podatki i bezpieczeństwo

Wysokie koszty stałych łączy sieciowych, niskie podatki od działalności gospodarczej. Bezpieczne otoczenie naturalne.

■ Przyszłość

Opcje przyszłej infrastruktury IT

Nowe modele wykorzystania centrów danych, rozwój technologii i zmiana w rozumieniu sposobu udostępniania usług użytkownikom, wpłyną na rozwój i infrastrukturę centrów danych. Źle podjęta decyzja inwestycyjna może mieć kosztowne skutki w przyszłości.



Idea bezpiecznego i chronionego centrum danych będzie się w przyszłości rozwijała.

Bezpieczeństwo eksploatacji i efektywność energetyczna znajdują się na samym początku listy priorytetów i obejmują wiele aspektów. Sięgają od zoptymalizowanych modeli eksploatacyjnych, poprzez energooszczędne warianty chłodzenia, aż po zastosowanie efektywnych komponentów w zasilaczach serwerów. Ulepszenia wprowadza się na wszystkich poziomach, od mikroarchitektury serwerów, aż po wybór lokalizacji centrów danych.

Zasilanie prądem stałym

Aktualne opracowania wykazują wyraźną tendencję w kierunku zasilania serwerów prądem stałym w celu obniżenia zużycia prądu. Producent serwerów, firma Hewlett-Packard szacuje, że sprawność w przypadku scentralizowanego rozdziału prądu stałego wynosi do 10% więcej niż dla prądu przemiennego. Uważa się także, że zasilając serwery bezpośrednio napięciem stałym można by zredukować koszty zakupu nawet o 15%, a zapotrzebowanie na fizyczną powierzchnię o 25%.

Nowe komponenty elektroniczne

Należy również spodziewać się dalszego rozwoju serwerów poza formatem 19". Drogą w tym kierunku jest całkowite uszczelnienie płyt głównych i przepuszczanie nieprzewodzącego czynnika chłodniczego. Nowe procesory, np. z trójwymiarowymi tranzystorami, wykazują zawsze mniejszy TDP (Thermal Design Power) niż pobór prądu.

Gęstość mocy

Intensywne obliczeniowo aplikacje, jak np. aplikacje chmurowe, korzystanie z tzw. big data, trendy w kierunku obrazów i filmów w wysokiej rozdzielczości (High Definition, Ultra High Definition), będą wymagać efektywnych rozwiązań. Sprzecznosc między wydajnością, dostępnością i efektywnością w przypadku infrastruktury IT musi zostać inteligentnie usunięta.

Rozwiązaniem są klastry IT w szczególnych środowiskach, np. w nieczynnych sztolniach w Skandynawii – z wodą morską do chłodzenia i z wykorzystaniem energii odnawialnych.

Budowa modułowa

W wyniku standaryzacji, w przyszłości będzie się budować jeszcze więcej centrów danych o konstrukcji modułowej. Zgodnie z zasadą systemu modułowego, centrum danych można ciągle rozbudowywać o prefabrykowane moduły z szafami serwerowymi i sieciowymi, klimatyzacją i zasilaniem elektrycznym, odpowiednio do wymaganego zapotrzebowania na moc komputerów – skalownie od 20 kW do 450 kW. Konstrukcja modułowa aktywnie przyczynia się do obniżenia kosztów inwestycji i konserwacji.

Warunki klimatyczne

Zmiany widać też w przypadku warunków klimatycznych w centrum danych. Organizacja ASHRAE poluzowała dopuszczalne parametry brzegowe użytkowania centrów danych. Obecnie w centrum danych dopuszczalne są temperatury otoczenia do 40°C. Dzięki takiemu przedziałowi temperatur i wilgotności możliwe jest wykorzystanie do chłodzenia także powietrza zewnętrznego, czyli chłodzenia swobodnego (free cooling) – albo pośrednio z wodą chłodzącą, albo bezpośrednio przez filtrowane powietrze zewnętrzne. Dzięki temu centra danych na północy Europy mogą być chłodzone powietrzem zewnętrznym przez cały rok, z wyjątkiem kilku dni. Przy wyborze lokalizacji wskazane jest przeprowadzenie analizy, czy istniejące warunki temperatur zewnętrznych są odpowiednie dla chłodzenia swobodnego, a tym samym dla efektywnej energetycznie eksploatacji.



Trwale zdefiniowane infrastruktury IT umożliwiają budowę przyszłościowych centrów danych o zapotrzebowaniu mocy do 450 kW.

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Komponenty systemowe dla infrastruktury IT

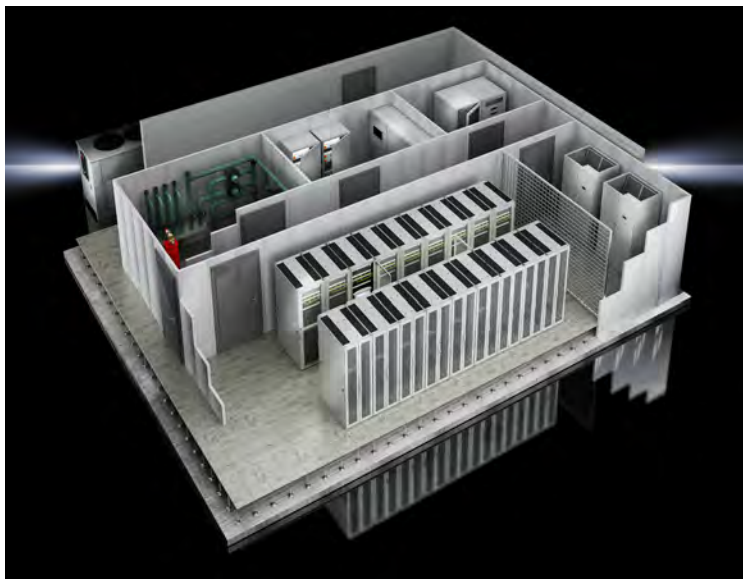
	Strona
Szafa IT	66
Konstrukcja i rama	68
Zastosowanie w środowisku przemysłowym	69
Wentylacja i zarządzanie ciepłem	70
Bezpieczeństwo dostępu	71
Zarządzanie okablowaniem	71
Elementy osłonowe	72
Bezpieczeństwo eksploatacji	72
Akcesoria ogólne	73
 IT Power	 74
Komponenty rozdziálu mocy	74
Komponenty systemu UPS	77
Komponenty systemu zarządzania energią	79
 IT Cooling	 80
Kryteria decyzyjne i warianty chłodzenia	81
Przegląd systemów	82
Rozwiązania klimatyzacji IT	83
Wytwarzanie chłodu	86
 Monitoring IT	 88
Komponenty systemu monitorowania	88
 Bezpieczeństwo IT	 90
Komponenty bezpieczeństwa do szaf i pomieszczeń	90
Ochrona przeciwpożarowa	92

■ Szafa IT

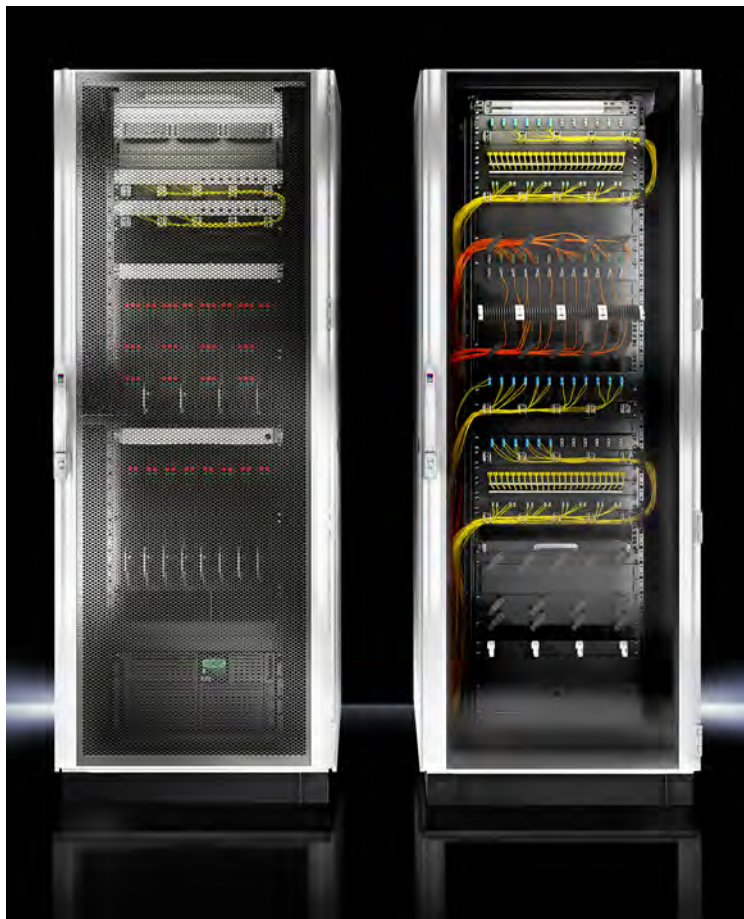
Wydajność infrastruktury IT zależy od współpracy poszczególnych komponentów. Systemy szaf IT odgrywają dzisiaj kluczową rolę pod względem dostępności, niezawodności i kosztów całkowitych (TCO) infrastruktury IT. Odpowiednie szafy serwerowe dysponują platformą systemową, w której dopasowano do siebie perfekcyjnie rozwiązania klimatyzacyjne, systemy zasilania oraz bezpieczeństwa, a dostępna przestrzeń została wykorzystana optymalnie. Główne kryteria w skrócie:

- Najwyższa z możliwych gęstość upakowania
- Efektywne wykorzystanie przestrzeni
- Zdolność do dopasowania się

Nowoczesne szafy IT są łatwe w rozmieszczeniu, wpływają pozytywnie na TCO oraz obniżają bieżące koszty eksploatacji.



Schematyczny zarys modelu centrum danych



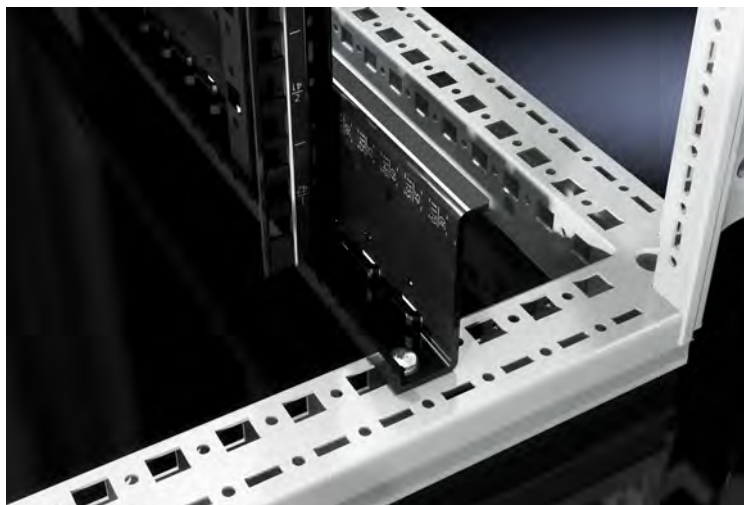
Sercem zoptymalizowanej konstrukcji szafy jest np. przetestowana miliony razy platforma szaf serwerowych i sieciowych TS 8, poddana przez Rittal dalszym ulepszeniom w nowoczesnych szafach TS IT.

Konstrukcja i rama

Współczesne generacje serwerów i sprzętu sieciowego są projektowane tak, by gęstość wewnątrz jednostki szafy stale się zwiększała. Typowa gęstość mocy jest obecnie rzędu 3-5 kW, w zastosowaniach wysokowydajnych 12-40 kW na szafę. Bezpieczna szafa serwerowa może skalowalnie pomieścić komponenty 19". Dla optymalnego wykorzystania przestrzeni oferowane są szafy o zwiększonej wysokości jak np. 47 U (2200 mm). Profile 19" ze zmienną głębokością gwarantują indywidualną rozbudowę również niejednorodnych typów architektury serwerów. Poza wysokością zwiększa się też głębokość. Szafy o głębokościach od 1000 do 1200 mm są dziś niezbędne do pomieszczenia dużych serwerów.

Ze względu na urządzenia z wentylacją boczną, jak np. core switches, zyskują popularność szafy o szerokości 800 mm i więcej. W ten sposób spełniane są specyfikacje producentów dotyczące wolnych przestrzeni dla cyrkulacji powietrza i układania kabli.

Duża nośność (do 1500 kg) jest niezbędna dla znacznej liczby serwerów, kabli, jednostek rozdziału prądu i punktów przyłożenia dla zabudowań albo do zastosowania ciężkich serwerów typu blade. Szafy serwerowe i sieciowe znajdują zastosowanie zarówno w rozwiązaniach stand alone, jak też w układzie szeregowym. Dlatego szafy powinny umożliwiać łatwe, elastyczne i skalowalne szeregowanie.



Zabudowa wnętrza

Symetryczna konstrukcja ramy zapewnia maksymalną użyteczną pojemność wewnętrzną szafy oraz umożliwia skalowalne szeregowanie w celu optymalnego wykorzystania przestrzeni we wszystkich płaszczyznach. Inteligentny system modułowy, w którego skład

wchodzi program szaf i akcesoriów, zapewnia prosty montaż, redukuje złożoność akcesoriów, co ostatecznie prowadzi do obniżenia kosztów. Ważne jest przy tym, aby szafa IT miała możliwość elastycznej modyfikacji pod przyszłe wymagania sprzętu IT.

Zastosowanie w środowisku przemysłowym

Zwykle klasa ochrony (Ingress Protection – w skrócie IP) w centrum danych nie należy do kryteriów decyzyjnych. W wyniku wspólnego rozwoju przemysłu i IT coraz więcej aplikacji IT jest integrowanych bezpośrednio w środowisku przemysłowym. W celu optymalnej ochrony powierzchniowej

oraz zwiększonej ochrony przeciwkorozyjnej stosuje się np. opracowane dla przemysłu samochodowego elektroforezowe gruntowanie zanurzeniowe. Jednocześnie istnieją szafy IT z klasą ochrony IP 55 stosowaną w przemyśle.



Wentylacja i zarządzanie ciepłem



Kolejną podstawową funkcjonalnością szafy serwerowej jest elastyczne rozwiązanie w kwestii odprowadzania ciepła i klimatyzacji precyzyjnej. Bez wystarczającego (aktywnego lub pasywnego) zarządzania ciepłem zagrożona jest niezawodność pracy. Wraz ze wzrostem gęstości upakowania rośnie wprawdzie efektywność energetyczna, jednak jednocześnie zwiększają się wymagania dotyczące rozdzielenia mocy i zarządzania ciepłem. Większa ilość przewodów zasilania i danych utrudnia odprowadzanie ciepła oraz dostęp do urządzeń.

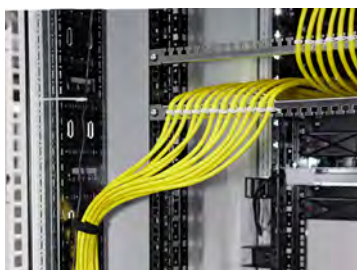
W celu zapewnienia prawidłowej cyrkulacji powietrza, drzwi powinny cechować się wysokim stopniem perforacji. Zwykle jest dostępna perforacja od 60 do 80%. W przypadku ścisłego odseparowania stref ciepłych i zimnych, potrzebne są dodatkowe osłony i przewodnice powietrza.

Bezpieczeństwo dostępu



Dodatkowo do właściwości mechanicznych i cieplnych, w szafie IT musi zostać także zabezpieczony dostęp w postaci inteligentnych systemów zamków i zabezpieczeń. Najwyższe bezpieczeństwo dostępu oferują np. systemy 4-punktowej blokady, które można rozszerzyć o elektroniczną kontrolę dostępu.

Zarządzanie okablowaniem



Perfekcyjnie przemyślane zarządzanie okablowaniem – zewnętrznym i wewnętrznym – pomaga w prowadzeniu okablowania typu sandwich, poprzez prowadzenie kabli światłowodowych z zabezpieczeniem kątów zginania, aż do wieszaków nadmiaru kabla w szafie. Kable powinny dawać się sensownie rozmieścić i ułożyć wewnątrz szafy. Urządzenia i kable powinny być przy tym łatwo i szybko dostępne. Odpowiednie systemy prowadzenia kabli zmniejszają przesłuchy w transmisji sygnałów i chronią kable przed uszkodzeniami. Kable są wprowadzane coraz częściej od góry, przez perforowaną płytę dachową lub częściowo również przez cokół lub podłogę techniczną.

Elementy osłonowe



Wysoką elastyczność w przypadku indywidualnych zastosowań zapewnia szeroki wybór np. drzwi przeszklonych, płyt dachowych z wprowadzaniem kabli i dzielonych ścian bocznych. Np. ściany boczne nie są już ze sobą skręcane, ich montaż odbywa się bez użycia narzędzi, za pomocą systemu szybkiego mocowania. Zamykane drzwi oraz ściany boczne szafy chronią serwery i dane przed nieupoważnionym dostępem. W zależności od poziomu bezpieczeństwa, dostępne są różne rodzaje zamknięć, np. z zamkiem na klucz, zamkiem szyfrowym, z blokadą elektroniczną lub biometryczną.

Bezpieczeństwo eksploatacji



Normy międzynarodowe, patenty oraz certyfikaty dają możliwość zastosowania szaf serwerowych na całym świecie. Najnowocześniejsze koncepcje uziemienia i wyrównania potencjałów, jak również opcjonalne wersje EMC zapewniają wysokie bezpieczeństwo eksploatacji. Automatyczne wyrównanie potencjałów w nowoczesnych szafach jest realizowane bezpośrednio przez zamocowanie płaszczyzny 19" (na zdjęciu Rittal TS IT).

Akcesoria ogólne

Rozbudowa indywidualna jest dodatkowo uproszczona przez wyjątkowe akcesoria.

Kilka przykładów:

- **Cokoły, ramy podpodłogowe, mocowanie do podłoża, rolki transportowe oraz ochrona przed przewróceniem**

Dostępne są różne komponenty do elastycznego mocowania do podłoża oraz do wprowadzania kabli i montażu na podłodze technicznej. W ten sposób można szybko i bez żadnych trudności zrealizować indywidualne wymagania systemu. Inteligentna ochrona przed przewróceniem zwiększa bezpieczeństwo. Rolki do dużych obciążeń zapewniają mobilność i elastyczność także maksymalnie zabudowanych szaf.

- **Półki urządzeniowe 19"**

Półki ze zmienną głębokością, do montażu na stałe lub do obciążeń maks. 150 kg – obszerny wybór ułatwia integrację sprzętową. Rowki w półkach urządzeniowych zapewniają dodatkowo optymalny pionowy przepływ powietrza.

- **Szuflady**

Do prawidłowego umiejscowienia klawiatur i dokumentów lub kabli zaprojektowano zintegrowane, wielofunkcyjne szuflady – również zamykane.

- **Integracja serwerów**

Elastyczność również w różnych rozwiązaniach architektonicznych serwerów wewnątrz szafy: szyny ślizgowe i szyny do obciążeń maks. 150 kg, z regulowaną głębokością oraz szyny do uniwersalnego montażu serwerów o zróżnicowanej architekturze z użyciem wymaganych przez producenta materiałów montażowych.

Podsumowując, kryteria bezpiecznej szafy serwerowej lub sieciowej są następujące:

- Stabilność i nośność
- Łatwy montaż i szeroki wybór akcesoriów
- Elastyczność rozbudowy i przebudowy
- Integracja odprowadzania ciepła
- Możliwości okablowania wewnątrz szafy
- Miejsce na zasilanie elektryczne
- Zabezpieczenia, np. przed nieupoważnionym dostępem
- Ochrona przeciwpożarowa
- Certyfikaty i dostępność



■ IT Power

Komponenty rozdziału mocy

Rozdział mocy wymaga maksymalnego bezpieczeństwa zasilania i pełnej, wysokiej przejrzystości. Ponadto do niezawodnej pracy IT niezbędne są również niewielkie obciążenie ogniowe oraz niskie oddziaływanie pól elektromagnetycznych.

Do obszarów zasilania i zabezpieczenia energii należą:

- Jedno lub kilka niezależnych źródeł zasilania, w zależności od wymaganej dostępności
- Przejrzysty, mający jasną strukturę energetyczną podział pomiędzy rozdzielnią główną a podrozdzielnią
- Zabezpieczenie zasilania poprzez zasilanie bezprzerwowe (systemy UPS)
- Zabezpieczenie obwodu prądu stałego za pomocą baterii i alternatywnych źródeł prądu, jak system fotowoltaiczny lub energia wiatrowa
- Włączanie i odłączanie obciążenia IT przez inteligentne systemy gniazdek zasilających



Rozdział mocy od źródła, aż do wszystkich odbiorników IT oraz zabezpieczenie energii przez UPS

¹⁾ Rittal Energy Management, strona 22/23

Przykład rozwiązania Rittal i Siemens:

- System rozdzielnic szynowych LD jako szkielet energetyczny, możliwy także w konfiguracji redundantnej
- System rozdzielnic szynowych BD2 jako odgałęzienie promieniowe w podłodze technicznej lub nad szafami do bezpośredniego zasilania
- Sieć połączeń nad skrzynkami urządzeniowymi i równoległe położony system standardowej magistrali

Główna rozdzielnia niskiego napięcia



- Strukturalne rozwiązanie systemowe dla szybkiej i bezpiecznej budowy rozdzielni niskiego napięcia
- Sprawdzona integracja systemów rozdzielnic szynowych Sivacon 8PS (system LD) z Ri4Power
- Skalowalne zastosowania w centrach danych, z możliwością modułowej rozbudowy, na przykład z systemem LD

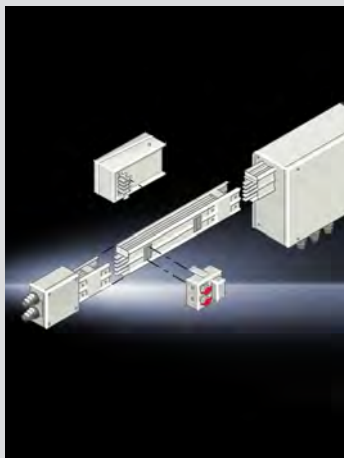
Data centre backbone



- Bezpieczne i szybkie projektowanie oraz montaż
- Jasna struktura energetyczna pomiędzy rozdzielnią główną a podrozdzielnią w centrach danych
- Kompaktowy design do wielu zastosowań w centrach danych, warianty 1000 A, 1600 A i 2000 A
- Wysoka dostępność dzięki łatwej integracji z podrozdzielnią (system BD2)

Przykład rozwiązania Rittal i Siemens:

Podrozdzielnia



- Przykład z systemem BD2
- Precyzyjny obraz rozdziału mocy w szeregach szaf
- Wysokie bezpieczeństwo zasilania i automatyczna rejestracja odbiorników
- Wysoki stopień skalowalności
- Wysoki poziom zabezpieczenia przed nieuprawnionym dostępem dzięki rozgałęzieniom z możliwością plombowania
- Elastyczne dopasowanie do struktur centrum danych poprzez zmianę kierunku w trzech wymiarach (250 A, 400 A, 630 A)

Systemy gniazdek zasilających

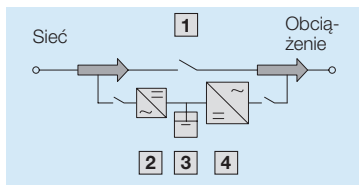


- Przykład z systemami PDU (Power Distribution Unit)
- Łatwe podłączenie PDU do skrzynek odgałęzień systemu BD2 (wtyki CE)
- Pasywne PDU bez funkcji monitorowania lub zarządzania
- PDU Metered z pomiarem prądu i mocy każdej fazy (zasilania)
- PDU Switched z dodatkowym załączaniem gniazdek
- PDU Managed z pomiarem prądu dla każdego gniazdka

Komponenty systemu UPS

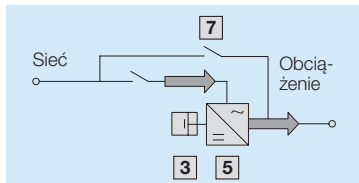
- **Prostownik** – konwertuje prąd z sieci zasilania (prąd przemienny lub trójfazowy) na prąd stały
- **Pośredni obwód prądu stałego** – ładujący baterie UPS. W przypadku awarii zasilania, obwód pośredni prądu stałego jest zasilany energią z baterii
- **Zasobnik energii** – np. baterie lub ogniwo paliwowe
- **Falownik** – przekształca energię z pośredniego obwodu prądu stałego na napięcie przemienne
- **Obejście statyczne** – zostaje aktywowane, gdy nie działa falownik, np. w przypadku przeciążenia lub uszkodzenia falownika, prostownika lub baterii

Ze względu na różne potrzeby poszczególnych urządzeń, w branży UPS przyjęły się trzy klasy określone przez Międzynarodowe Konsorcjum Inżynieryjne (IEC) w normie produktowej IEC 62 040-3 oraz przez Unię Europejską w EN 50 091-3. Są to (przedstawione w kolejności wzrostu bezpieczeństwa):



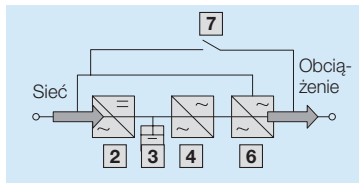
System UPS offline

Tryb normalny bez oddziaływania



System UPS line-interactive

Tryb normalny przez falownik czterokwadrantowy [5]



System UPS online

Tryb normalny przez prostownik [2] i falownik [4]

- [1] Przełącznik
- [2] Prostownik/ładowarka
- [3] Baterie
- [4] Falownik

- [5] Falownik czterokwadrantowy
- [6] Statyczny przełącznik obejściowy
- [7] Przełącznik obejścia ręcznego

UPS offline

- UPS klasy 3 wg IEC 62 040-3.2.20
- Zasilane urządzenia IT podłącza się bezpośrednio do dostępnego zasilania elektrycznego
- Zbyt wysokie lub zbyt niskie napięcie jest wykrywane przez UPS offline, po czym następuje przełączenie na tryb bateryjny
- Czas przełączenia z trybu sieciowego na bateryjny od 4 do 10 ms
- Zbyt niskie i zbyt wysokie napięcia nie są wyrównywane
- Sprawność ok. 95%

UPS net-interactive lub

UPS line-interactive

- Klasa 2 wg IEC 62 040-3.2.18
- System UPS jest podłączany między przyłączem sieciowym a zasilanym urządzeniem IT
- Elektroniczne filtry wyrównują wahania napięcia
- Jednostka baterii jest podłączana bezpośrednio
- Czas przełączenia z trybu sieciowego na bateryjny od 2 do 4 ms, przełączenie w drugą stronę bez opóźnień
- Sprawność między 95% a 98%

UPS online lub UPS w trybie pracy ciągłej

- Klasa 1 wg IEC 62 040-3.2.16
- Generują własne napięcie sieciowe
- Podłączone odbiorniki są stale zasilane napięciem sieciowym
- Jednocześnie niezależnie od wahań napięcia ładowane są baterie
- Wysokiej jakości sinusoidalne napięcie na wyjściu
- W przypadku separacji galwanicznej lub transformatora separacyjnego zakłócenia są filtrowane przez przewód neutralny
- Sprawność ok. 90%, gdyż napięcie jest konwertowane przez obejście statyczne i powstaje moc stratna oraz ciepło

Można dodatkowo zwiększyć bezpieczeństwo, realizując podwójne systemy UPS z dodatkową redundancją. Równoległe zastosowanie kilku systemów UPS jest wskazane, gdy po stronie obciążenia użytkowane są duże instalacje. Wówczas zarządzanie obciążeniem włącza lub wyłącza poszczególne systemy UPS.

Komponenty systemu zarządzania energią

System zarządzania energią dba o precyzyjny obraz zużycia i wysoką jakość energii w centrum danych, a także o dostępność rozdziału mocy. Zarządzanie energią może wchodzić w skład systemu DCIM (patrz też strona 54). Jednocześnie stanowi podstawę dla optymalizacji kosztów energii i zużycia.

Funkcje

- Wizualizacja i analiza parametrów oraz przepływu energii
- Wizualizacja zależności
- Określanie możliwych oszczędności – interpretacja wartości minimalnych i maksymalnych
- Pomiar energii do celów rozliczeniowych
- Porównywanie wewnętrzne (linia szaf / część budynkowa) lub zewnętrzne (pomieszczenia / systemy)
- Przygotowanie decyzji np. dotyczących rozbudowy zasilania elektrycznego
- Weryfikowalne zwiększanie sprawności
- Ukierunkowane usuwanie błędów dzięki szybkim i szczegółowym informacjom o zdarzeniach i usterekach
- Protokolowanie komunikatów błędów i zdarzeń
- Przestrzeganie umów o dostarczenie energii dzięki ukierunkowanemu sterowaniu odbiornikami
- Automatyczne powiadomianie personelu serwisu



■ IT Cooling

Bezpieczeństwo eksploatacji i dostępność IT w dużym stopniu zależy od odprowadzania ciepła z szafy serwerowej, względnie z centrum danych. Aby zapobiec problemom termicznym w centrach danych stosuje się modułowe koncepcje klimatyzacji, które uwzględniają temperaturę, wilgotność, prędkość i ciśnienie powietrza, jak również jego kierunek oraz straty mocy. Efektywna energetycznie, dobra koncepcja klimatyzacji i chłodzenia dla centrów danych w sposób optymalny uwzględnia potrzeby oraz warunki brzegowe.

Rozróżnia się:

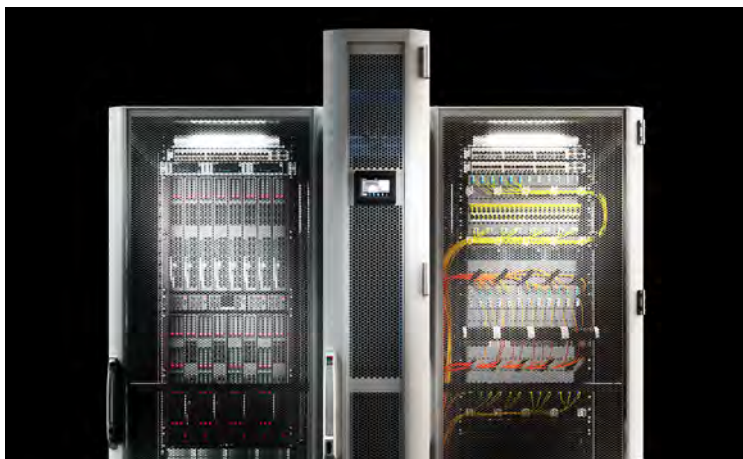
- System wentylacji (pomieszczeń)
- System klimatyzacji do odprowadzania ciepła (IT Cooling)

Obciążenie termiczne w centrum danych powstaje przez:

- **Oświetlenie, nasłonecznienie i inne źródła ciepła.**
Obciążenie to jest odprowadzane na zewnątrz przez system klimatyzacji pomieszczenia.
- **Sprzęt IT, np. serwery.**
Obciążenie to jest odprowadzane przez klimatyzację IT.

Chłodzenie aktywnych komponentów IT dzieli się na:

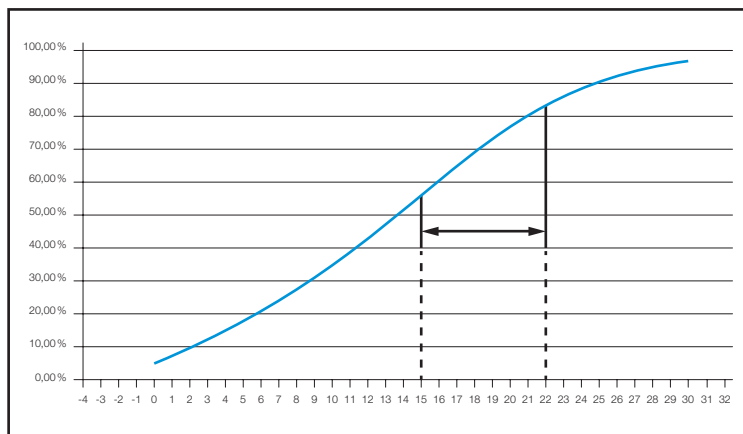
- pasywne (wykorzystujące powietrze z pomieszczenia)
- aktywne (ukierunkowane na szafę)
- chłodzenie wysokowydajne do neutralnej temperatury rozbudowy centrum danych.



Kryteria decyzyjne i warianty chłodzenia

Przygotowanie koncepcji klimatyzacji odpowiedniej do potrzeb i zakresu zastosowań, z uwzględnieniem wszystkich warunków otoczenia, wymaga wyjaśnienia zasadniczych kwestii. W planowaniu pomagają oprogramowanie narzędziowe:

- Jaki wariant chłodzenia ma zostać zainstalowany – rozwiązanie hybrydowe, chłodzenie pasywne, zintegrowana strefa ciepła?
- Jak zorganizować ustawienie z uwzględnieniem strefy zimnej i ciepłej?
- Jaka średnia temperatura powinna panować wewnątrz szafy?
- Jak duża jest różnica temperatur – temperatury dopływu, temperatury odpływu, ΔT ?
- Jaki strumień objętości jest potrzebny?
- Jakie są warunki otoczenia?
- Jaki kierunek przepływu wybrać i jaką sytuację zabudowy uwzględnić?
- Jakie są wahania obciążenia i jak oddziałują na czasy reakcji chłodzenia?
- Jakie wymiarowanie uwzględnić na przyszłość?



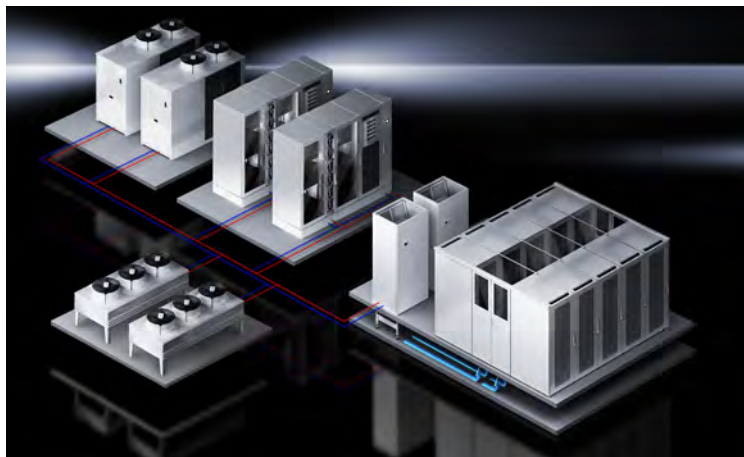
Zgodnie z „2008 ASHRAE Environmental Guidelines for Datacom Equipment“ temperatura wlotu powietrza dla urządzeń powinna wynosić od 18°C do 27°C. Dzięki właściwemu zwymiarowaniu wymiennika ciepła może być przybliżona do ok. 1,5 K do dozwolonych warunków ASHRAE.

Przegląd systemów

- **Klimatyzacja pomieszczeń**
Doprowadzanie zimnego powietrza i odprowadzanie ciepłego.
- **Klimatyzacja powietrza obiegowego**
Powietrze dopływające do centrum danych jest schładzane w wymienniku ciepła. Wymiennik ciepła jest chłodzony czynnikiem chłodniczym lub wodą.
- **Klimatyzacja szaf serwerowych**
Przy wysokich obciążeniach >20 kW mocy stratnej stosuje się wymienniki ciepła w szafie chłodzone bezpośrednio wodą lub czynnikiem chłodniczym.
- Oddzielenie chłodzenia szaf serwerowych od klimatyzacji pomieszczeń za pomocą separacji stref
- Zastosowanie efektywnych energetycznie komponentów, np. wentylatorów z elektroniczną komutacją, z regulacją mocy kompresorów chłodniczych
- Użycie tzw. swobodnego chodzenia (free cooling) lub adsorpcyjnych systemów chłodzenia w połączeniu z energią słoneczną
- Możliwie wysokie temperatury wody chłodzącej i temperatury pomieszczenia
- Regulację wszystkich podsystemów i ciągle dopasowywanie do faktycznego zapotrzebowania mocy

Efektywna energetycznie klimatyzacja IT uwzględnia:

- Wymiarowanie systemów klimatyzacji zgodnie z faktycznym zapotrzebowaniem mocy



Rozwiązania klimatyzacji IT

W zależności od mocy cieplnej w centrum danych stosuje się różne rozwiązania klimatyzacji.

Klimatyzacja przez podłogę techniczną

Przy mocy traconej w szafie do ok. 8 kW często stosuje się klasyczną klimatyzację podłogową. Zimne powietrze jest doprowadzane przez perforowaną podłogę techniczną przed szafy serwerowe centrum danych. Ciepłe powietrze wylotowe z reguły jest zasysane przez kanały wylotowe w suficie pomieszczenia

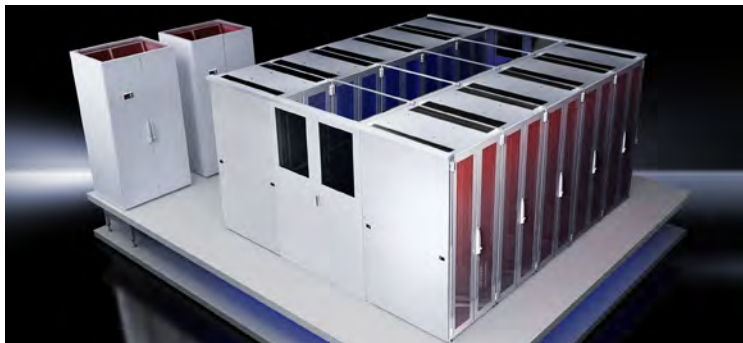
i schładzane w urządzeniu powietrza obiegowego przez wymiennik ciepła za pomocą wody lub czynnika chłodniczego. Jednocześnie dla podniesienia jakości powietrza dodaje się ok. 10% powietrza zewnętrznego. Wadą klimatyzacji podłogowej jest mieszanie się powietrza wlotowego i wylotowego, przez co zmniejsza się efektywność chłodzenia.



Klimatyzacja podłogowa z separacją stref

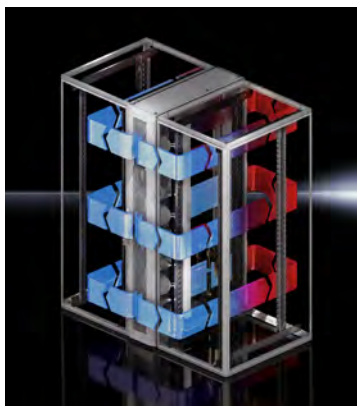
W celu zwiększenia efektywności klimatyzacji podłogowej można zabudować strefy ciepłe lub zimne.

Dzięki temu powietrze wlotowe i wylotowe przestają się mieszać. Szafy serwerowe są dokładniej zasilane zimnym powietrzem, dzięki czemu zwiększa się efektywność chłodzenia.



Chłodzenie szeregowe

Przy wymaganej mocy chłodniczej od ok. 10 kW, w większości przypadków klimatyzacja podłogowa nie wystarcza. Wówczas rozwiązania klimatyzacji są integrowane bezpośrednio w szeregach szaf, a strumienie zimnego powietrza zostają dostarczone przez podłogę techniczną. W ten sposób zostaje odciążona klimatyzacja podłogowa z separacją stref. Przy bardzo wysokim zapotrzebowaniu na moc chłodniczą przejmują one całkowicie odprowadzanie ciepła z szaf. W tym rozwiązaniu ciepło w wymienniku powietrze/woda lub powietrze/chłodziwo jest przenoszone do ciepłego medium (woda lub czynnik chłodniczy), a następnie odprowadzane.

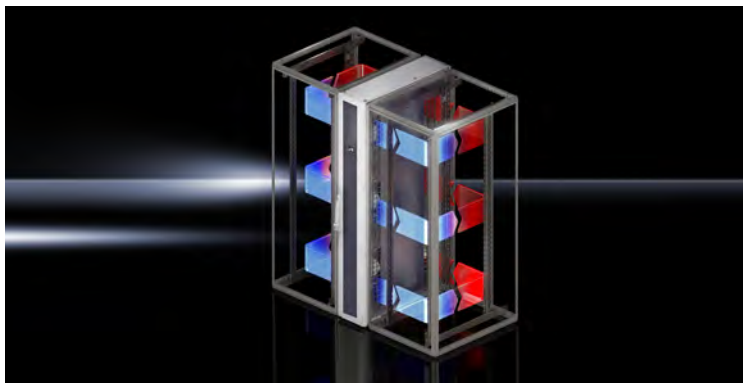


Chłodzenie szaf

Przy obciążeniach cieplnych np. w wysokowydajnych systemach obciążeniowych > 20 kW na szafę, sensowne pod względem technicznym i ekonomicznym są rozwiązania oparte na chłodzeniu szaf. Rozróżnia się przy tym aktywne i pasywne chłodzenie szaf. Decydujące znaczenie ma to, aby system chłodzenia umieścić możliwie jak najbliżej miejsca wytwarzania ciepła. Klimatyzacje High-Performance odprowadzają do 60 kW obciążenia termicznego na szafę. Cały system jest wyposażony w grodzie, dzięki którym ciepłe powietrze nie trafia do normalnego obiegu powietrza, ale jest zasysane bezpośrednio z tyłu serwerów, schładzane w wodnych wymiennikach ciepła i ponownie wdmuchiwane z przodu.

Aktywne chłodzenie szaf wymaga zainstalowania w pobliżu szaf infrastruktury wodnej. Woda dla wymienników ciepła w szafowych systemach chłodzenia najczęściej jest przygotowywana i schładzana centralnie. Efektywna energetycznie i wysokowydajna klimatyzacja może funkcjonować

także bez wentylatorów. Tymczasem doprowadzanie powietrza do systemów serwerowych ze zintegrowanymi wentylatorami dużej wydajności jest realizowane bardzo efektywnie. Do ok. 20 kW (np. Rittal LCP Hybrid) wystarczą pasywne drzwi tylne w szafach, ponieważ wysokowydajne wentylatory serwerów typu Blade wciągają powietrze do wymienników ciepła w wystarczającym stopniu. Jednak w przypadku najwyższych wymagań odnośnie wydajności, nie ma lepszego rozwiązania niż systemy oparte na zabudowie szafowej. Jeżeli aplikacja wymaga jeszcze większej mocy lub redundancji, szafowe systemy chłodzenia mogą również wzajemnie się wspierać. Jeżeli moduły są zainstalowane naprzemiennie z szafami serwerowymi, wówczas wdmuchują zimne powietrze przed front w obu kierunkach, zapewniając chłodzenie szafom serwerowym z obu stron. Jeżeli dużą rolę odgrywa redundancja, to moduły chłodzenia powinny być podłączone naprzemiennie do dwóch różnych obiegu wody.



Wytwarzanie chłodu

Niezależnie od tego, czy jest to powietrze, woda, czy czynnik chłodniczy – wszystkie te nośniki ciepła są mediami, które muszą być schładzane. Nośnik ciepła jest schładzany bezpośrednio lub pośrednio w agregatach chłodzenia lub chillerach. Coraz częściej do przygotowania wody zastosowanie znajduje chłodzenie swobodne. W dzisiejszych systemach wartość graniczna temperatury chł-

dzenia swobodnego może jak najbardziej sięgać 1,5 K żądanej temperatury dopływu wody. Poza tym stosuje się kosztowniejsze systemy chillerów. Ponieważ dopuszczalne temperatury powietrza dolotowego do serwerów zostały podniesione przez ASHRAE do 27°C, możliwe są temperatury doprowadzanej wody 20°C. Rozróżnia się trzy różne metody chłodzenia swobodnego:

Pośrednie chłodzenie swobodne

Obciążenie cieplne z centrum danych jest przenoszone przez strumień powietrza z wymiennika ciepła powietrze/woda w klimatyzatorze obiegowym do medium w postaci wody i glikolu. Medium to jest następnie schładzane powietrzem otoczenia w agregacie na zewnątrz budynku.

Bezpośrednie chłodzenie swobodne

W tej metodzie bezpośredniego chłodzenia swobodnego obciążenie cieplne z centrum danych jest kierowane bezpośrednio na zewnątrz, do powietrza otoczenia. Dopływ powietrza miesza się z powietrzem wylotowym w proporcji zależnej od temperatury zewnętrznej, dzięki czemu uzyskuje się wymaganą temperaturę powietrza wlotowego. Tylko przy wysokich temperaturach zewnętrznych chłodzenie odbywa się w trybie obiegowym ze wsparciem obiegów chłodniczych.



Inne metody chłodzenia swobodnego

Inną metodą jest chłodzenie adiabaticzne. Strumień powietrza w systemie wentylacji pomieszczeń jest nawilżany i przez to schładzany. Chłodzenie bez chłodzenia swobodnego, np. przez otwarte okna, bywa wprawdzie stosowane obecnie, jednak jest nieefektywne. Łączna ilość powietrza zewnętrznego w czasie całego roku wymaga latem chłodzenia, a zimą ogrzania. W ten sposób znacznie rosną koszty energii.

Wnioski

Efektywna energetycznie klimatyzacja centrum danych jest rozwiązana optymalnie pod względem technicznym z uwzględnieniem indywidualnych warunków budowlanych, czynników ekonomicznych i wymagań dotyczących dostępności.

Odpowiednie rozwiązanie klimatyzacji zależy od dopuszczalnych czasów awarii w roku. Zalecenia dla bezpiecznego w eksploatacji centrum danych podaje tabela BITKOM.

Kategoria centrum danych	Klimatyzacja ¹⁾			Dopuszczalny czas awarii centrum danych
	Szafa serwerowa	Szafa serwerowa	Centrum danych / serwerownia	
	do 7 kW	od 7 kW do 40 kW	500 do 2500 W/m ²	
A	Klimatyzacja niezbędna, redundancja opcjonalna	Klimatyzacja niezbędna, redundancja niezbędna, wsparcie UPS	Chłodzenie precyzyjne, redundancja, separacja stref, ew. wsparcie UPS	12 h
B	Klimatyzacja niezbędna, redundancja niezbędna	Klimatyzacja niezbędna, redundancja niezbędna, wsparcie UPS	Chłodzenie precyzyjne, redundancja, separacja stref, wsparcie UPS	1 h
C	Klimatyzacja niezbędna, redundancja niezbędna, wsparcie UPS	Klimatyzacja niezbędna, redundancja niezbędna, wsparcie UPS	Chłodzenie precyzyjne, redundancja urządzeń i rurociągów, separacja stref, wsparcie UPS	10 min
D	Klimatyzacja niezbędna, kompletna redundancja niezbędna, wsparcie UPS	Klimatyzacja niezbędna, kompletna redundancja niezbędna, wsparcie UPS	Chłodzenie precyzyjne, redundancja urządzeń i rurociągów, separacja stref, wsparcie UPS, funkcje chłodzenia awaryjnego przez dodatkowy system klimatyzacji	< 1 min

Z tego można wywnioskować, że im wyższe są wymagania odnośnie dostępności klimatyzacji IT, tym większe są inwestycje konieczne przy realizacji.

¹⁾ BITKOM, *Betriebssicheres Rechenzentrum*
(Bezpieczne w eksploatacji centrum danych)



■ Monitoring IT

Komponenty systemu monitorowania

Zdefiniowana dostępność technologii informacyjnej jest dla większości przedsiębiorstw decydującym warunkiem podstawowym bezpiecznego i optymalnego przebiegu wszystkich procesów roboczych. Bezpieczeństwo fizycznej infrastruktury IT zaczyna się od pojedynczej szafy. Konceptcja monitorowania stanowi zabezpieczenie przed kosztami wynikającymi z powstania awarii. Jednocześnie jest centralną jednostką organizacyjną służącą do integracji z systemami Facility-Management.

Komunikaty o zakłóceniach i alarmy przesyłane są do określonych systemów serwisu lub zarządzania bezpieczeństwem. Wymiana danych przez

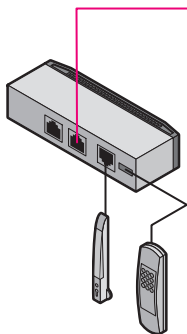
systemy magistral i integracja z systemami LAN lub systemami zarządzania budynkiem, zapewnia precyzyjny obraz wszystkich elementów ważnych dla bezpieczeństwa danych.

Zasada modułowości komponentów pozwala na indywidualne dopasowanie do określonych wymagań i rozbudowę o rozmaite czujniki i elementy wykonawcze. Dzięki integracji różnych obszarów, jak również włączeniu do systemów Facility-Management, monitoring staje się głównym punktem informacji (Central Point of Information) w centrum danych.

CMC III Processing Unit Compact

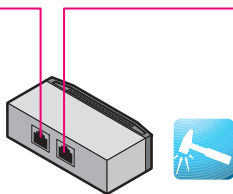
CMC III CAN-Bus Access

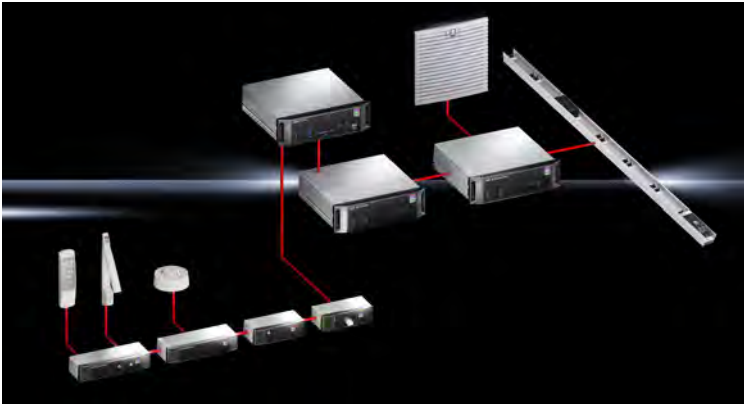
ze zintegrowanym czujnikiem dostępu IR



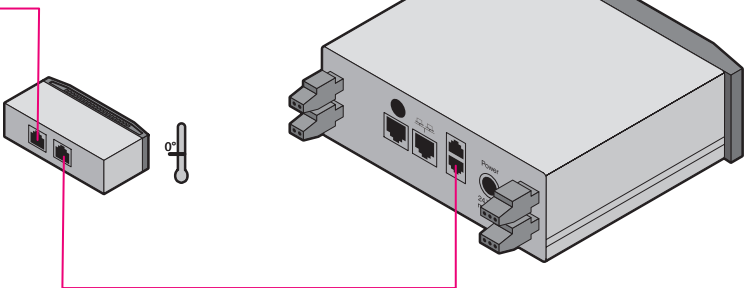
Czujniki CMC III

do bezpośredniego podłączenia





Czujniki CMC III
do bezpośredniego podłączenia



CAN-Bus

■ Bezpieczeństwo IT

Komponenty bezpieczeństwa do szaf i pomieszczeń

Optymalne fizyczne nadzorowanie przez 365 dni w roku wymaga dużych zasobów ludzkich i nie jest opłacalne w normalnej eksploatacji szafy serwerowej lub centrum danych. Jednocześnie niezbędna staje się ochrona przed nieupoważnionym dostępem. Optymalna koncepcja bezpieczeństwa uwzględnia wieloaspektowe rozwiązanie, obejmujące zarówno dostęp do szafy serwerowej, jak i do centrum danych.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Wymagania w ramach koncepcji bezpieczeństwa centrum danych

- Kontrola dostępu przez:
 - zainstalowanie w szafach i w centrum danych cyfrowego systemu zamykania
 - koncepcję uprawnień dostępu do centrum danych
 - zainstalowanie w centrum danych systemu sygnalizacji włamania połączonego z ochroną lub policją
- Kontrola infrastruktury IT przez:
 - montaż czujników monitorujących oraz rozwiązań wideo w szafach i w centrum danych
 - czujniki i technologię wczesnego wykrywania oraz gaszenia pożaru

- Kontrola klimatu przez:
 - czujniki temperatury i czujniki warunków otoczenia
- Kontrola administracji przez:
 - podział szaf i topologii sieci na segmenty
 - zainstalowanie funkcji i przełączników KVM (Keyboard-Video-Mouse)
 - integrację z jednostką monitora (szuflada monitor-klawiatura)

Jednocześnie wszystkie drogi zasilania elektrycznego, wytwarzania i rozdzielu chłodu oraz parametry bezpieczeństwa są centralnie rejestrowane i wizualizowane.



Ochrona przeciwpożarowa

Konstrukcyjne środki ochrony przeciwpożarowej

Kolejnym warunkiem bezpiecznej eksploatacji centrum danych jest niezawodna ochrona przeciwpożarowa. W trakcie projektowania lub rozbudowy centrum danych należy przewidzieć odpowiednią technologię gaszenia. Poza funkcjami ochrony, jej celem jest również wczesne wykrywanie i zwalczanie pożaru wewnątrz szafy serwerowej i centrum danych za pomocą rejestracji różnych pomiarów. Pożar, dym i agresywne gazy zawsze stanowią zagrożenie dla IT, dlatego uznanymi rozwiązaniami są systemy automatycznego gaszenia lub redukcji tlenu za pomocą gazu.

Środki ochrony przeciwpożarowej wymagają uwzględnienia wszystkich niezbędnych przepisów, wytycznych i celów ochrony, aby centrum danych mogło następnie uzyskać certyfikat systemu wg EN 1047-2.

Kategoria centrum danych	Techniczna ochrona przeciwpożarowa ¹⁾			Dopuszczalny czas awarii centrum danych
	Szafa serwerowa		Centrum danych / serwerownia	
	do 7 kW	od 7 kW do 40 kW	500 do 2500 W/m ²	
A	Jednostka monitorująca z wczesnym wykrywaniem pożaru i techniką gaszenia (z pasywną rezerwą środka gaśniczego)	System sygnalizacji pożaru, jednostka monitorująca z wczesnym wykrywaniem pożaru i samodzielną techniką gaszenia (z pasywną rezerwą środka gaśniczego) lub z systemem redukcji tlenu (systemem unikania pożaru)		12 h
B	Jednostka monitorująca z wczesnym wykrywaniem pożaru i techniką gaszenia (z pasywną rezerwą środka gaśniczego)	System sygnalizacji pożaru, jednostka monitorująca z wczesnym wykrywaniem pożaru i samodzielną techniką gaszenia (z pasywną rezerwą środka gaśniczego) lub z systemem redukcji tlenu (systemem unikania pożaru)		1 h
C	System sygnalizacji pożaru, jednostka monitorująca z wczesnym wykrywaniem pożaru i samodzielną techniką gaszenia (systemem gaszenia pożaru) lub z systemem redukcji tlenu (systemem unikania pożaru) w wykonaniu redundantnym			10 min
D	System sygnalizacji pożaru, jednostka monitorująca z wczesnym wykrywaniem pożaru i samodzielną techniką gaszenia (systemem gaszenia pożaru) lub z systemem redukcji tlenu (systemem unikania pożaru) w wykonaniu redundantnym			< 1 min

¹⁾ BITKOM, *Betriebssicheres Rechenzentrum* (Bezpieczne w eksploatacji centrum danych)

Norma ta określa zarówno parametry konstrukcyjne, jak też czas trwania dokładnie zdefiniowanych obciążeń w przypadku pożaru. W uzupełnieniu do technicznej ochrony przeciwpożarowej muszą być również uwzględnione zabezpieczenia konstrukcyjne.

Organizacyjne środki ochrony przeciwpożarowej

Poza ochroną techniczną i konstrukcyjną, musi zostać uwzględniona również organizacyjna ochrona przeciwpożarowa. Znaczenie mają przy tym aktualne warunki oraz przyszły rozwój.

Do organizacyjnej ochrony przeciwpożarowej należą: plan awaryjnego wyłączenia, plan ponownego rozruchu IT, regulamin ochrony przeciwpożarowej, operacyjny plan obrony przeciwpożarowej, plan dróg ewakuacyjnych, oznakowanie tabliczkami, zakaz palenia tytoniu, zakaz spożywania żywności, szkolenie firm i pracowników, ochrona zakładowa, regulamin dla gości oraz przeszkolenie personelu.

Kategoria centrum danych	Konstrukcyjna ochrona przeciwpożarowa ¹⁾			Dopuszczalny czas awarii centrum danych
	Szafa serwerowa		Centrum danych / serwerownia	
	do 7 kW	od 7 kW do 40 kW	500 do 2500 W/m ²	
A	Ściany, podłoga, sufit: klasa oporności ogniowej co najmniej F90, ochrona przed gazem pożarowym, strugami wody, drzwi min. T90, przepusty kablowe w tej samej klasie ochrony		Ściany, podłoga, sufit: klasa oporności ogniowej co najmniej F90, ochrona przed gazem pożarowym i wodą przez 30 min, drzwi min. T90, przepusty kablowe w tej samej klasie ochrony	12 h
B	Kontrola systemu konstrukcyjnej ochrony przeciwpożarowej ściany, podłoga, sufit: zgodnie z euronormą EN 1047-2, przepusty kablowe w tej samej klasie ochrony, ochrona przed gazem pożarowym, strugami wody przez 60 min		Kontrola systemu konstrukcyjnej ochrony przeciwpożarowej ściany, podłoga, sufit: zgodnie z euronormą EN 1047-2, przepusty kablowe w tej samej klasie ochrony, ochrona przed gazem pożarowym, strugami wody przez 60 min	1 h
C	Kontrola systemu konstrukcyjnej ochrony przeciwpożarowej ściany, podłoga, sufit: zgodnie z euronormą EN 1047-2, przepusty kablowe w tej samej klasie ochrony, ochrona przed gazem pożarowym, strugami wody przez 60 min		Kontrola systemu konstrukcyjnej ochrony przeciwpożarowej ściany, podłoga, sufit: zgodnie z euronormą EN 1047-2, przepusty kablowe w tej samej klasie ochrony, ochrona przed gazem pożarowym, strugami wody przez 60 min	10 min
D	Kontrola systemu konstrukcyjnej ochrony przeciwpożarowej ściany, podłoga, sufit: zgodnie z euronormą EN 1047-2, przepusty kablowe w tej samej klasie ochrony, ochrona przed gazem pożarowym, strugami wody przez 60 min			< 1 min

¹⁾ BITKOM, *Betriebssicheres Rechenzentrum* (Bezpieczne w eksploatacji centrum danych)

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Rozwiązania dla infrastruktury IT

	Strona
RiMatrix S, RiMatrix	96
Engineering & Consulting	98
Uruchomienie, serwis i wsparcie	99
RiMatrix S	100
Pierwsze „gotowe“ centrum danych	100
Skalowalność do 450 kW	101
Rozbudowa systemu	
Rack/Cooling	102
Power	103
Cooling	104
Monitoring	105
Bezpieczeństwo z RiMatrix S	106
Elastyczność z RiMatrix S	107
RiMatrix	108
Modułowy system standardowych komponentów	108
Rozbudowa systemu	
Rack	108
Power	108
Cooling	109
Monitoring	109

Rittal – The System.

Faster – better – everywhere.

Infrastruktura IT

Budowa lub modernizacja centrum danych szybko staje się gigantycznym projektem. Na bezpiecznej, umożliwiającej nieprzerwany dostęp i efektywnej energetycznie infrastrukturze IT zyskuje całe przedsiębiorstwo. Już w fazie przygotowania i analizy można zidentyfikować potencjalne rozwiązania i inteligentnie wykorzystać różne wyzwania. Wynik: szybszy zwrot inwestycji (ROI) dzięki indywidualnym, opartym na sprawdzonych standardach rozwiązaniom.

Doradztwo

W technicznej realizacji centrum danych doradcy IT opierają się na oczekiwaniach klientów. Uwzględnia się przy tym cały łańcuch procesów:

- Doradztwo
- Sporządzanie oferty, kalkulacja ROI
- Realizacja zamówienia
- Logistyka, dostawa, uruchomienie
- Pełna dokumentacja
- Odbiór, certyfikacja
- Administracja
- Zmiany, rozbudowa
- Konserwacja, części zamienne
- Serwis, infolinia

Funkcjonujący, wzajemnie dopasowany łańcuch procesów jest dla klienta decydującym warunkiem sukcesu danego rozwiązania.

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Standardowe centrum danych RiMatrix S

RiMatrix S (S = standardowy) to **standardowa konstrukcja centrum danych** w istniejącym budynku, w pomieszczeniu bezpieczeństwa oraz jako rozwiązanie kontenerowe. Rittal oferuje **predefiniowane moduły dla centrów danych** o mocy chłodniczej 450 kW.



Zalety:

- Niskie koszty inwestycji
- Szybka dostawa i uruchomienie
- PUE (Power Usage Effectiveness) od 1,5 do 1,15
- Pełna dokumentacja wraz ze sprawdzonymi charakterystykami i kartami produktów
- Uproszczona certyfikacja końcowa gotowego do pracy centrum danych
- Możliwość łatwej rozbudowy w przyszłości oraz wysoki poziom bezpieczeństwa

Indywidualne centrum danych RiMatrix

Już w roku 2005 Rittal zaprezentował kompletne rozwiązanie **budowy indywidualnego centrum danych** RiMatrix. RiMatrix składa się z szerokiej gamy gotowych rozwiązań dotyczących: szaf, zasilania, klimatyzacji, monitoringu, zdalnego zarządzania oraz bezpieczeństwa.



Zalety:

- Indywidualne rozwiązania przeznaczone dla centrów danych opartych na standardowej bazie (Customized Data Centre)
- Elastyczność przy wyborze komponentów i technologii
- Ciągłe doskonalenie produktów
- Efektywne energetycznie rozwiązania również dla infrastruktury IT o łącznej mocy powyżej 450 kW
- Rozwiązania dopasowane do potrzeb (Pay as you grow)
- Możliwość łatwej rozbudowy na poziomie komponentów

■ RiMatrix S, RiMatrix

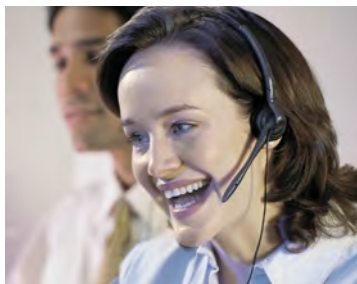
Engineering & Consulting

To siła innowacji plus IT-know-how zbudowane dzięki wieloletniemu doświadczeniu; wszystko pochodzi od jednego dostawcy.

Poprzez nasze inteligentnie dobrane schematy rozwiązań dostarczamy Państwu idealnie dopasowane do potrzeb firmy pomysły, koncepcje i innowacje dla rozwiązań IT. Warto postawić z Rittal na wysokiej klasy rozwiązania: Engineering & Consulting, budowa centrów danych, infrastruktura IT i międzynarodowy serwis Rittal. Skorzystaj z wiedzy, doświadczenia i produktów firmy odnoszącej sukcesy na całym świecie – zrób to dla siebie i dla własnego IT.

Rittal opracowuje i optymalizuje indywidualne rozwiązania IT. Od małych jednostek IT do kompleksowych centrów danych. Nasi specjaliści dokładnie analizują aktualny stan, przyszłe zapotrzebowanie, warunki budowlane i fizyczne, istniejącą strukturę IT i na tej podstawie wyciągają wnioski co do możliwych sposobów optymalizacji.

Pozwala to na zaplanowanie i wdrożenie systemów IT z maksymalną wydajnością mocy, kosztów, procesów, energii, kompatybilności, dostępności i bezpieczeństwa. W projektowaniu specjalistycznym i szczegółowym Rittal przeprowadza niezbędne analizy i obliczenia, sporządza wszystkie schematy i dokumentację oraz wybiera optymalne dla środowiska IT rozwiązania i komponenty.



Uruchomienie, serwis i wsparcie

Rittal International Services

- Prace montażowe są wykonywane przez wykwalifikowany, międzynarodowy personel (centrum szkoleniowe w Haiger, Super-Visor System)
- Do Państwa dyspozycji na całym świecie jest personel z wieloletnim doświadczeniem
- Zarządzanie jakością (niezależne badania przeprowadzane przez ekspertów zewnętrznych, a także wewnętrzne badania jakości w laboratorium, kontrole produkcji i ponadbranżowe odbiory systemu)
- Wysokie kompetencje we wszystkich dziedzinach (badania i rozwój, zaopatrzenie, sprzedaż, projektowanie, kierowanie projektem, serwis)

Przed sprzedażą

- Analiza potrzeb
- + test obciążenia
- + termografia
- + symulacja i kalkulacja

Implementacja

- Instalacja / integracja
- + uruchomienie
- + szkolenie
- + certyfikacja

Obsługa posprzedażowa

- Konserwacja/instalacja + naprawa
- + zarządzanie częściami zamiennymi
- + szkolenie
- + umowy serwisowe



■ RiMatrix S

Pierwsze „gotowe” centrum danych – RiMatrix S

Alternatywą dla budowy indywidualnych centrów danych jest RiMatrix S w trzech wersjach.

- Gotowe rozwiązanie od jednego dostawcy, tzn. mniej punktów przejścia i mniejsze koszty projektowania
- Wysokie bezpieczeństwo planowania z obliczanym z góry PUE
- Standaryzowane moduły centrum danych w produkcji seryjnej
- Jeden numer katalogowy. Pełna funkcjonalność, wraz z szafami serwerowymi i sieciowymi, klimatyzacją, rozdzieleniem i zabezpieczeniem zasilania oraz monitoringiem i DCIM (Data Center Infrastructure Management)
- Natychmiastowa dostawa



ENCLOSURES

POWER DISTRIBUTION

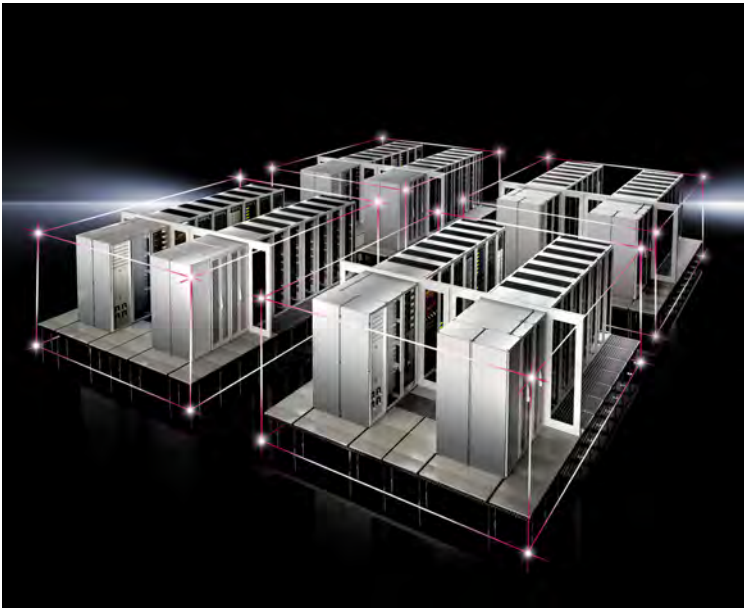
CLIMATE CONTROL

Skalowalność do 450 kW

Wszystkie moduły Rimatrix S można dowolnie skalować w zakresie mocy do 450 kW. Dostępne są różne moduły, znajdujące zastosowanie zgodnie z warunkami przestrzennymi.

Przykłady:

- Łatwy montaż struktur w układzie typu szachownica
- Układ równoległy lub szeregowy
- Wspólna strefa zimna i/lub ciepła
- Łatwa integracja z infrastrukturą zasilającą



Rozbudowa systemu – Rack/Cooling

- Klimatyzacja oszczędnie umieszczona w podłodze technicznej
- Redundancja n+1 w klimatyzacji
- Łatwe prowadzenie powietrza i wysoka efektywność energetyczna
- Stelaże TS IT z ramą 19", z separacją dla konsekwentnego odgródnienia stref ciepłych od zimnych
- Beznarzędziowy montaż akcesoriów TS IT
- Głębokość szafy 1200 mm, wysokość montażowa 42 U



Rozbudowa systemu – Power

Zabezpieczenie zasilania stanowi modułowy system UPS. Wysoką dostępność zapewnia pełna redundancja n+1 z kompleksową architekturą równoległą. Baterie umożliwiają bezpieczne wyłączenie serwerów lub uruchomienie generatora.

Maksymalne obciążenie wynosi 60 kW dla modułu Single 6 i 90 kW dla Double 9. Wszystkie komponenty mogą być nadzorowane przez system monitorowania CMC III oraz zintegrowane z DCIM RiZone.



Rozbudowa systemu – Cooling

Do klimatyzacji przewidziano systemy Zero U-Space Cooling (ZUCS), dzięki czemu nie traci się miejsca do montażu serwerów.

- Wymienniki ciepła znajdują się pod szafami
- Przyłącza wymienników ciepła są łatwo dostępne przez podłogę techniczną z tyłu szaf
- Redundancja n+1 umożliwia wysoką dostępność. Niezbędna moc chłodnicza jest dostarczana nawet w przypadku awarii jednego z ZUCS
- Wentylatory EC gwarantują niskie zużycie energii, a ich parametry pozwalają na pracę w energooszczędnym obszarze obciążenia częściowego
- Aby ułatwić serwisowanie, wentylatory umieszczono w podłodze technicznej przed stelażami serwerowymi
- Inteligentne prowadzenie powietrza przez podłogę techniczną zapewnia optymalną eksploatację



Rozbudowa systemu – Monitoring

- System monitorowania CMC nadzoruje wszystkie istotne parametry, jak np. temperatura, wilgotność powietrza, wycieki itp.
- Połączenie z produktami security, jak np. systemy RAS
- Ciągłe monitorowanie i analizowanie stanów pracy przez oprogramowanie DCIM RiZone
- Wizualizacja wartości zużycia i efektywności aktywnych systemów
- Inteligentne procedury optymalizacji i zabezpieczenia w zarządzaniu alarmem
- Predefiniowane projekty, monitoring i zarządzanie plug & play



Bezpieczeństwo z RiMatrix S

RiMatrix S zapewnia bezpieczeństwo poprzez:

- zmniejszoną złożoność
- wypróbowane i sprawdzone pod względem jakości komponenty
- zdefiniowane i nadzorowane procesy produkcji
- udokumentowany test systemu kompletnego modułu centrum danych.

Dla użytkownika oznacza to:

- niskie koszty inwestycji
- PUE (Power Usage Effectiveness) do 1,15
- sprawdzone charakterystyki i karty produktu.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Elastyczność z RiMatrix S

Moduły mają elastyczne zastosowanie dzięki oddzieleniu modułów RiMatrix S od powłoki fizycznej oraz zdefiniowanym punktom połączenia z infrastrukturą.

Dla użytkownika oznacza to:

- łatwą integrację z nowymi lub już istniejącymi pomieszczeniami z separacją strefy zimnej lub ciepłej
- montaż w atestowanych pomieszczeniach bezpieczeństwa ...
- ... lub jako elastyczne rozwiązanie kontenerowe
- uproszczoną dostawę na całym świecie dzięki standardowym modułom
- możliwość uruchomienia przez ponad 150 partnerów serwisowych oraz 1 000 techników serwisu.



■ RiMatrix

Modułowy system ze standardowych komponentów

Rack



Szafy sieciowe/serwerowe

- Indywidualne zastosowanie do ustawienia wolnostojącego i dla centrów danych
- Kompletnie rozwiązania systemowe dla małych i dużych sieci
- Maksymalne możliwości rozbudowy i bezpieczeństwo urządzeń
- Bezpieczeństwo inwestycji i elastyczność dzięki łatwej przebudowie oraz zastosowaniu obszernego systemu modułowego

Obudowa naścienna

- Duży wybór – dla każdego zastosowania odpowiednia obudowa – do klasy ochrony IP 66
- Dostępne różne rozmiary od 3 U do 21 U
- Duży wybór akcesoriów w ramach „Rittal – The System.“
- Szybka instalacja i przebudowa oraz łatwy montaż dzięki koncepcji modułowej

Power



Systemowe zarządzanie energią

- Kompleksowe rozwiązania dla rozdziału i zabezpieczenia energii, całkowicie modułowe i umożliwiające elastyczną rozbudowę w każdej chwili
- Największa wydajność energii i optymalizacja kosztów przy maksymalnej dostępności całego systemu
- Redukcja kosztów
- Wysokie bezpieczeństwo inwestycji
- Wszystko od jednego dostawcy

Cooling



- Najnowocześniejsza technologia klimatyzacji od chłodzenia pojedynczych szaf, aż po kompletne centrum danych
- Indywidualne koncepcje klimatyzacji szaf, szeregów i pomieszczeń
- Większe bezpieczeństwo i wyższa efektywność energetyczna oraz redukcja kosztów
- Optymalizacja przez separację stref i ogólnosystemowe koncepcje regulacji
- Energooszczędne chłodzenie za pomocą chillerów IT
- Zminimalizowanie kosztów eksploatacji przez Free Cooling
- Rozwiązania przyjazne dla środowiska dzięki oszczędności zasobów i emisji CO₂
- Projektowanie, montaż, uruchomienie i serwis – wszystko od jednego dostawcy!

Monitoring



- Lepszy przegląd infrastruktury IT
- Zwiększone bezpieczeństwo
- Automatyczne procesy
- Wysoka efektywność kosztów
- Znaczna oszczędność energii
- Łatwe projektowanie
- Szybka instalacja
- Elastyczne i indywidualne rozwiązania dzięki produktom seryjnym Rittal
- Wysoki standard jakości dzięki wzajemnie dopasowanym produktom seryjnym

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Wiedza ekspertów

	Strona
Normy i przepisy	112
Kompatybilność elektromagnetyczna.....	121
Kable miedziane	128
Światłowody	131
Okablowanie sieciowe	134
Złącza wtykowe	138
Ważne urządzenia technologii sieciowej	140
Procedury dostępu do sieci	144
Terminologia internetowa	150

■ Normy i przepisy

Ważne normy w branży telekomunikacyjnej i przesyłu danych

Przegląd norm, ogólnie	
PN-EN 61 000-6-3 (VDE 0839 część 6-3)	Kompatybilność elektromagnetyczna (EMC) – Odporność w środowiskach mieszkalnych itp.
PN-EN 61 000-6-1 (VDE 0839 część 6-1)	Kompatybilność elektromagnetyczna (EMC) – Normy ogólne – Odporność w środowiskach mieszkalnych itp.
PN-EN 50 098-1	Okablowanie informatyczne na terenie użytkownika – Część 1: Podstawowy dostęp do sieci ISDN
PN-EN 60 794 (VDE 0888)	Kable światłowodowe
PN-EN 60 825-2 (VDE 0837 część 2)	Bezpieczeństwo urządzeń laserowych – Część 2: Bezpieczeństwo światłowodowych systemów telekomunikacyjnych
PN-EN 55 022 (VDE 0878 część 22)	Urządzenia informatyczne – Charakterystyki zaburzeń radioelektrycznych – Poziomy dopuszczalne i metody pomiarów
PN-EN 50 288-5-1 (VDE 0819-5-1:2014-03)	Przewody wielożyłowe stosowane w cyfrowej i analogowej technologii przesyłu danych Część 5-1: Wymagania grupowe dotyczące przewodów ekranowanych, testowanych do częstotliwości 250 MHz – Przewody przeznaczone do poziomego i pionowego układania w budynkach
PN-EN 60 603-7-1 (VDE 0687-603-7-1:2012-01)	Złącza do urządzeń elektronicznych Część 7-1: Specyfikacja szczegółowa dotycząca złączy 8-torowych, ekranowanych, swobodnych i stałych

Instalacja urządzeń końcowych

Przegląd norm dla instalacji urządzeń końcowych	
PN-EN 50 310 (VDE 0800-2-310:2011-5)	Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym
PN-EN 61 918 (VDE 0800-500:2009-01)	Przemysłowe sieci komunikacyjne – Instalowanie sieci komunikacyjnych w obiektach przemysłowych
DIN VDE 0845 VDE 0845 Załącznik 1:2010-11	Ochrona przepięciowa urządzeń informatycznych (instalacji IT)

Rodzaj i zastosowanie kabli komunikacyjnych	
DIN VDE 0891	Zastosowanie kabli i przewodów izolowanych do urządzeń telekomunikacyjnych oraz urządzeń służących do przetwarzania informacji
PN-EN 60 794 (VDE 0888)	Kable światłowodowe
PN-EN 50 174-2 (VDE 0800 część 174-2)	Technologia informacyjna – Instalacja okablowania, planowanie i wykonywanie instalacji wewnątrz budynków



Instalacja sieci

Krótka informacja o serii norm PN-EN 50 173 Technika informatyczna – Systemy okablowania strukturalnego

Koncepcja niezależnego systemu okablowania strukturalnego jest dzisiaj nieodzownym składnikiem infrastruktury IT budynków, gdyż w porównaniu z metodami ukierunkowanymi na konkretne potrzeby oferuje ona znaczne korzyści techniczne i ekonomiczne. Rozwiązanie to zostało pierwotnie opracowane jako niezależne od usług, uniwersalne okablowanie do obsługi informacyjnych i komunikacyjnych aplikacji sieciowych w budynkach biurowych. Podstawowe właściwości niezależnych systemów okablowania strukturalnego: jednolita topologia, klasyfikacja kanałów transmisji o zdefiniowanych parametrach, jednolity interfejs do podłączania urządzeń końcowych. Po wprowadzeniu pewnych modyfikacji, właściwości te dają się również zastosować do innych dziedzin. Przykładem takich zastosowań są obiekty przemysłowe, budynki mieszkalne i centra danych.

Seria norm EN 50 173 została opracowana przez CENELEC/TC 215 w odpowiedzi na potrzebę uregulowania tych obszarów zastosowania zgłaszaną przez użytkowników. W dalszym rozwoju tej serii zwrócono uwagę na to, aby te wymagania i właściwości, które dotyczą większej liczby lub wszystkich rodzajów budynków, były określone tylko jeden raz – w części 1.

Dlatego przy realizacji niezależnego systemu okablowania strukturalnego w określonym otoczeniu (rodzaj budynku, lokalizacja) razem z PN-EN 50 173-1 zawsze znajduje zastosowanie odpowiednia część – 2, 3, 4, 5, ...

PN-EN 50 173-1 zawiera ogólnie obowiązujące ustalenia dotyczące pierwotnych i wtórnych podsystemów okablowania, a także istotne pod względem techniki transmisji specyfikacje klas kanałów transmisji i odpowiednich komponentów przewodów, złączy wtykowych i kabli przyłączeniowych urządzeń końcowych.

W aktualnym wydaniu **EN 50 173-1: 2011-09, Technika informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne**

Jedną z istotnych nowości było wprowadzenie wymagań dla kategorii komponentów 6A i 7A. Inne zmiany w porównaniu z poprzednim wydaniem dotyczą modyfikacji wymagań tłumienności dla koncentrycznych kanałów transmisji, modyfikacji kanału transmisji klasy OF-100 dla okablowania światłowodowego i zdefiniowania nowej kategorii światłowodów OM4, uzupełnienia i modyfikacji wymagań dotyczących techniki łączeniowej. Aktualne są również definicje nowego typu wtyku dla 2 światłowodów oraz dla 12 i 24 włókien, zmiana wymagań badawczych dla mechanicznych i środowiskowych parametrów techniki łączeniowej, aktualizacja załącznika F „Obsługiwane aplikacje” i wprowadzenie nowego załącznika normatywnego 1 „Metody pomiarów w celu określenia zgodności z normami serii EN 50 173”.

PN-EN 50 173-2, Część 2: Pomieszczenia biurowe

Zawiera uregulowania dotyczące trzeciego (horyzontalnego) podsystemu okablowania, a także wymagania dla przyłącza IT przy stanowisku roboczym, stosowanego w pomieszczeniach biurowych. Wymagania te w tym samym stopniu dotyczą pomieszczeń w budynkach o mieszanym przeznaczeniu (mieszkania, gabinety lekarskie, kancelarie i podobne), które mają być używane jako biuro. Poza uwzględnieniem nowych kanałów transmisji EA i FA oraz odpowiedniej kategorii komponentów 6A i 7A, norma zawiera wymagania dla światłowodów wielomodowych kategorii OM4 i światłowodów jednomodowych kategorii OS2, a także zmienione uregulowania dla techniki połączeniowej.

PN-EN 50 173-3, Część 3: Zabudowania przemysłowe

Zawiera szczególne uregulowania dla systemów okablowania strukturalnego stosowanych w lokalizacjach o charakterze przemysłowym. Tym samym jest wsparciem dla użytkowników systemów automatyki przemysłowej, którzy w coraz większym stopniu są zainteresowani zastosowaniem niezależnej infrastruktury w miejsce własnych rozwiązań. Ma to zastosowanie zwłaszcza w kompleksowej integracji tych rozwiązań z istniejącymi sieciami firmowymi w części biurowej, które z reguły już od wielu lat są wykonane strukturalnie i najczęściej używają protokołów bazujących na sieci Ethernet. Obsługiwane aplikacje do nadzorowania i sterowania procesami są podane w PN-EN 50 173-1.

Topologiczną specyfikę używanych w przemyśle systemów okablowania strukturalnego uwzględniono

przez wprowadzenie dodatkowych podsystemów okablowania piętrowego i pośredniego, poza tym podane zostały przykłady typowych realizacji i maksymalne możliwe długości kanałów transmisji. Norma zawiera także odpowiednie wymagania dotyczące stosowania włókien z tworzyw sztucznych i włókien kwarcowych w powłokach z tworzyw sztucznych oraz kanałów transmisji z symetrycznymi kablami miedzianymi i kablami światłowodowymi z włókien kwarcowych. Często spotykane w systemach przemysłowych surowe warunki otoczenia są uwzględnione w uregulowaniach dotyczących stosowanej techniki połączeniowej. Poza tym opracowano nowe klasy transmisji EA i FA oraz odpowiednie kategorie komponentów 6A i 7A, a także zawarto zmienione uregulowania dotyczące techniki połączeniowej dla światłowodów.

PN-EN 50 173-4, Część 4: Zabudowania mieszkalne

Zawiera uregulowania dla systemów okablowania strukturalnego stosowanych w budynkach mieszkalnych (domach jedno- i wielorodzinnych). Wymagania te w tym samym stopniu dotyczą pomieszczeń w budynkach o mieszanym przeznaczeniu (mieszkania, gabinety lekarskie, kancelarie itd.), które mają być używane do celów mieszkaniowych. Jednocześnie uwzględniono, że w mieszkaniach muszą być obsługiwane różnorodne aplikacje sieciowe z jednej lub kilku następujących grup: technologia informacyjna i komunikacyjna (ICT), technologia radiowo-komunikacyjna (BCT), a także sterowanie, regulacja i komunikacja w budynkach (CCCB).

Do obsługi aplikacji ICT i BCT norma wprowadza podsystem okablowania mieszkaniowego, który w razie potrzeby może być uzupełniony o drugi podsystem. W przeciwieństwie do gwiazdzystej struktury w aplikacjach ICT i BCT, topologia aplikacji CCCB może przyjmować różne formy (np. magistrala, odgałęzienie, zamknięta pętla).

W związku z tym rozdział 5. normy definiuje dla tych aplikacji własną strukturę okablowania, która może być zrealizowana w podsystemie okablowania zasilania stref. Odpowiednie aplikacje CCCB są na przykład określone w normach serii PN-EN 50 090. Poza uwzględnieniem nowych kanałów transmisji EA i FA oraz odpowiedniej kategorii komponentów 6A i 7A, norma zawiera skorygowany poziom kanałów transmisji BCT z kablami koncentrycznymi, zaktualizowane równania na długość kanałów transmisji BCT, a także zmienione uregulowania dla techniki połączeniowej.

PN-EN 50 173-5, Część 5: Centra danych

Po raz pierwszy daje do dyspozycji operatorom i projektantom centrów danych narzędzie umożliwiające okablowanie strukturalne i jednocześnie uwzględniające szczególne potrzeby i właściwości tych placówek. Centra danych wyróżniają się m.in. bardzo

dużym udziałem kabli do transmisji danych, służących do udostępniania centralnych usług serwerowych (np. dla webhostingu) dużej liczbie użytkowników, zarówno wewnętrznych, jak zewnętrznych. Norma definiuje topologię okablowania o elastycznej strukturze – umożliwiającej szybkie i ekonomiczne wprowadzanie zmian oraz rozbudowę okablowania przy minimalnym przerywaniu bieżącej eksploatacji, a jednocześnie uwzględniającej konieczność redundantnych rozwiązań sieciowych.

Infrastruktura okablowania przyszłościowa pod kątem technicznym i atrakcyjna pod względem ekonomicznym jest oferowana przez klasy wysokowydajnych kanałów transmisji, które uwzględniają także błyskawiczny wzrost prędkości transferu danych urządzeń transmitujących w centrach danych. Także w tej części uwzględniono nowe klasy kanałów transmisji EA i FA oraz odpowiednie kategorie komponentów 6A i 7A. Ponadto norma ta zawiera sprecyzowane uregulowania dla okablowania światłowodowego i wielomodowych kabli światłowodowych, nowe uregulowania dotyczące techniki połączeniowej i normatywny załącznik B „Zastosowanie techniki połączeniowej dużej gęstości upakowania w okablowaniu światłowodowym“.

Obsługiwane zastosowania sieciowe (załącznik E)

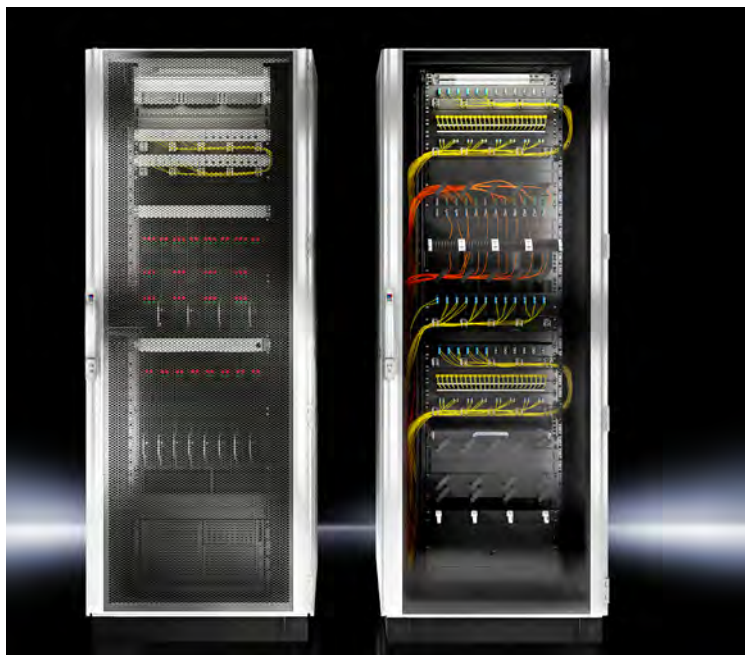
Kl.	Zastosowanie sieciowe	Źródło	Dalsza nazwa
A	PBX X.21 V.11	Wymaganie krajowe Zalecenie ITU-T X.21 Zalecenie ITU-T X.21	
B	S0 Bus (rozszerzone) S0 point-to-point S1/ S2 CSMA/CD 1Base5	Zalecenie ITU-T 1.430 Zalecenie ITU-T 1.430 Zalecenie ITU-T 1.431 ISO/IEC 8802-3	Podstawowe przyłącze ISDN Podstawowe przyłącze ISDN Pierwotne przyłącze multipleksowe ISDN Star LAN
C	CSMA/CD 10Base-T CSMA/CD 100Base-T4 Token Ring 4 Mbit/s	ISO/IEC 8802-3 ISO/IEC 8802-3 ISO/IEC 8802-5	Ethernet Fast Ethernet
D	TP-PMD CSMA/CD 100Base-TX Token Ring 100 Mbit/s CSMA/CD 1000Base-T	ISO/IEC FCD 9314-10 ISO/IEC 8802-3 ISO/IEC 8802-5t ISO/IEC 8802-3	Warstwa fizyczna nieza- leżna od nośnika, jakim jest skrętka Fast Ethernet High Speed Token Ring Gigabit Ethernet
E	ATM LAN 1.2 Gbit/s	ATM Forum af-phy-0162.000	ATM-1200/kategoria 6
F	FC-100-TP	ISO/IEC 14 165-114	
Kanały okablowania klasy światłowodów			
	CSMA/CD 10Base-F Token Ring FDDI SM-FDDI LCF-FDDI FC-PH ATM	ISO/IEC 8802 AM ISO/IEC TR 11802-4 EN ISO/IEC 9314-3 ISO/IEC 9314-4 ISO/IEC C 9314-9 ISO/IEC CD 14165-1 Zalecenie ITU-T 1.432	Przyłączenie stacji do kabli światłowodowych Podzielony interfejs danych z przewodami światłowo- dowymi Modem wejściowy FDDI FDDI z tanim światłowodem Fibre Channel B-ISDN

Ważne przepisy dla szaf i obudów do transmisji danych i telekomunikacji

„Rittal – The System.“ to efektywne rozwiązania systemowe dla branży IT dzięki modułowej i skalowalnej infrastrukturze.

Stale rosnące wymagania dotyczące ciągłej dostępności systemów IT wymagają dopasowanych rozwiązań centrów przetwarzania danych z jednego źródła. Rittal, jako mający wieloletnie doświadczenie partner systemowy branży IT, dysponuje wiedzą w zakresie panujących w niej wymagań i bardzo specyficznej tematyki.

Niezależnie od tego, czy chodzi o technologię serwerową i sieciową, czy o budowę centrów danych – innowacyjne rozwiązania Rittal dla środowiska IT zapewniają bezpieczeństwo, dostępność i optymalizację kosztów. Rozwiązania te są zgodne z międzynarodowymi normami oraz przepisami i wyznaczają najnowsze standardy. Odpowiednie normy, przepisy i przydatne wskazówki są podane w następnym rozdziale.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

DIN 41 488 Arkusze 1 – 3	Wymiary podziału dla szaf sterowniczych
DIN 41 494 Część 7	Budowa urządzeń elektronicznych, wymiary dla szaf i stelaży szeregowych (wymiary dla systemu 19")
DIN 43 668	Kluczyki do komórek lub do drzwi szafy dla elektrycznych instalacji rozdzielczych (wkładka dwupiorkowa) Rozmiar 3: Instalacje niskonapięciowe
ETS 300 119-3	Inżynieria środowiska (EE) – Europejskie normy telekomunikacyjne dotyczące urządzeń, część 3: Wymagania inżynierskie dla różnorodnych stojaków i obudów
IEC 60 297-3-100	Wymiary struktur mechanicznych serii 482,6 mm (19 cali), część 3-100: Podstawowe wymiary paneli frontowych, kaset „subrack”, szyn oraz szaf, Osłony i stojaki, część 2: Szafy i wymiary stojaków
DIN 43 656	Kolory stosowane do elektrycznych wewnętrznych instalacji rozdzielczych

Niemiecka ustawa o przemyśle energetycznym określa: „Elektryczne instalacje energetyczne i urządzenia zużywające energię elektryczną należy ustawiać i eksploatować zgodnie z przepisami, czyli według uznanych zasad techniki. Zalicza się do nich przepisy Niemieckiego Związku Elektrotechników (VDE)“.

Przy powszechności i różnorodności instalacji poniżej 1000 V, szczególne znaczenie ma VDE 0100 „Przepisy dotyczące wykonywania instalacji energetycznych o napięciach znamionowych do 1000 V“.

W przypadku instalacji elektroenergetycznych należy dodatkowo uwzględnić techniczne warunki ich podłączania (**TAB**) określone przez przedsiębiorstwo energetyczne (**EVU**), natomiast dla instalacji telefonicznych i antenowych – przepisy dotyczące urządzeń telekomunikacyjnych VDE 0800 i ustalenia dotyczące instalacji antenowych VDE 0855.

Nowo budowane instalacje powinny gwarantować niezawodność oraz ekonomiczność. Istotne wskazówki dotyczące tych zagadnień określają warunki przyłączeniowe przedstawione w wydanym przez Niemiecki Komitet Normalizacyjny (**DNA**) katalogu norm (**DIN**).

Znak CE: Sytuacja prawna, normalizacja

Dyrektywy UE

Dyrektywy określają dla krajów członkowskich UE podstawy ujednoczenia (prawnych) przepisów i norm w celu ułatwienia ruchu towarowego w obrębie Unii Europejskiej.

Produkty, które są zgodne z opisanymi w dyrektywach wymaganiami, muszą być oznakowane symbolem CE.

Dyrektywy mające znaczenie dla produktów Rittal:

- Dyrektywa EMC 2004/108/WE
- Dyrektywa niskonapięciowa 2006/95/WE

Producent umieszczający symbol CE potwierdza na własną odpowiedzialność zgodność ze wszystkimi dyrektywami UE dotyczącymi danego produktu. To oznacza, że musi wiedzieć jakimi dyrektywami są objęte jego produkty.

Urządzenia przewidziane i stosowane do rozdzielnic i sterownic niskonapięciowych wg PN-EN 61439 podlegają dyrektywie niskonapięciowej, są oceniane wg PN-EN 62208 i oznaczane symbolem CE.

Puste obudowy do zastosowań ogólnych i IT oraz mechaniczne komponenty akcesoriów nie podlegają żadnej obecnie obowiązującej dyrektywie UE.

■ Kompatybilność elektromagnetyczna

Co oznacza określenie EMC?

Kompatybilność elektromagnetyczna (EMC) to zdolność urządzenia elektrycznego do zadowalającego funkcjonowania w swoim otoczeniu elektromagnetycznym, bez większego niż to konieczne wpływu na to otoczenie, w skład którego wchodzi również inne urządzenia.

Wysokie gęstości upakowania w podzespołach elektronicznych i coraz większe prędkości przetwarzania sygnału w złożonych elektronicznych urządzeniach oraz systemach sterowania, pomiaru, regulacji, przetwarzania, transmisji danych i komunikacji, często powodują błędy, które są wywołane oddziaływaniem elektromagnetycznym.

Istnieją zasadnicze wymagania odnośnie:

- utrudnienia / zmniejszenia emitowania zakłóceń
- zdefiniowanej odporności na zakłócenia.

Dla odporności na zakłócenia obowiązują następujące definicje:

Odporność na zakłócenia istnieje wówczas, gdy wartości zakłóceń (do określonej wysokości) nie powodują niepoprawnego funkcjonowania.

■ Ograniczenie funkcjonowania

Zmniejszenie normalnego funkcjonowania, które jest jeszcze dopuszczalne.

■ Niepoprawne działanie

Zmniejszenie normalnego funkcjonowania, które nie jest dopuszczalne. Niepoprawne działanie kończy się wraz z zaniknięciem zakłóceń.

■ Zanik działania

Ograniczenie normalnego funkcjonowania, które nie jest dopuszczalne i może zostać usunięte np. tylko poprzez naprawę.



Podstawowe pojęcia tematyki EMC

- Oddziaływanie elektromagnetyczne to oddziaływanie wielkości elektromagnetycznych na obwody elektryczne, urządzenia, systemy lub żywe istoty.
- Źródło zakłócenia to źródło, z którego pochodzą zakłócenia.
- Obiekt zakłócany to urządzenie elektryczne, którego działanie może zostać zakłócone przez wartości zakłóceń.
- Sprzężenie to wzajemny stosunek pomiędzy obwodami elektrycznymi, w którym energia z jednego obwodu elektrycznego może zostać przeniesiona do drugiego.
- Wartość zakłócenia to wielkość elektromagnetyczna, która w urządzeniu elektrycznym może wywołać niepożądane oddziaływanie (napiecie zakłócenia, prąd zakłócenia, natężenie pola zakłócenia).

Źródła zakłóceń i wartości zakłóceń

Można rozróżnić następujące źródła zakłóceń:

- Wewnętrzne źródła zakłóceń – sztuczne, tj. uwarunkowane technicznie
- Zewnętrzne źródła zakłóceń – naturalne, np. piorun, wyładowania elektrostatyczne – sztuczne, tj. uwarunkowane technicznie

W przypadku technicznie uwarunkowanych źródeł zakłóceń należy rozróżnić oddziaływania powstałe podczas eksploatacji, wykorzystujące wielkości elektromagnetyczne (np. urządzenia radiokomunikacyjne, radar itd.) oraz wielkości elektromagnetyczne występujące podczas eksploatacji lub w przypadku awarii, które nie są wytwarzane do użytkowania (np. łuk elektryczny przy zestyku rozdzielczym, pola magnetyczne dużego natężenia prądu itd.).

Wartościami zakłóceń mogą być napięcia, prądy, pola elektryczne, magnetyczne i elektromagnetyczne, które występują okresowo w sposób ciągły lub czasowo w sposób przypadkowy w postaci impulsu.

W sieciach niskiego napięcia obowiązują poniższe zasady:

- Przejściowe procesy powodujące największe zakłócenia w sieciach niskiego napięcia wywoływane są przez przełączanie ciężarów indukcyjnych, np. narzędzi ręcznych z napędem elektrycznym, elektrycznych urządzeń gospodarstwa domowego, świetlówek.
- Najniebezpieczniejsze przepięcia (według wielkości, czasu trwania i zawartości energii) wywoływane są przez bezpieczniki odłączane w przypadku zwarcia (czas trwania w milisekundach).

Wyładowania elektrostatyczne

Podczas tarcia ciał stałych może dojść do wyładowań elektrostatycznych, które w przypadku powierzchni przewodzących są wprawdzie ponownie szybko odprowadzane, jednak na niektórych dobrze przewodzących powierzchniach mogą one pozostać. Napięcia elektrostatyczne związane z wyładowaniami na materiałach nieprzewodzących mogą powodować zakłócenia w działaniu elementów elektronicznych podczas zetknięcia z elementami przewodzącymi lub doprowadzić do ich zniszczenia.

Nie bez znaczenia są również wyładowania elektrostatyczne z ciała człowieka na elementy obsługi oraz obudowy urządzeń. Powstające w tym przypadku napięcia mogą wynosić do 15.000 V, mogą płynąć ładunki wyładowania do 5 A, przy nachyleniu charakterystyki prądu do 5 kA/μs. Ryzyko zakłóceń działania lub powstania uszkodzeń zwiększa się w przypadku słabiej przewodzących wykładzin podłogowych i mniejszej wilgotności powietrza.

Przykłady wrażliwości elementów półprzewodnikowych

Zagrożone podzespoły	Napięcie
Układy scalone (IC, Integrated Circuit) P-FP (Plastic Flat Pack) i P-LCC (Plastic Leaded Chip Carrier)	od 20 V
Diody Schottky'ego	od 30 V
Tranzystory polowe i EPROMy	od 100 V
Wzmacniacze operacyjne	od 180 V
Rezystory stałe	od 350 V
TTL Schottky'ego	od 1000 V
IC C-LCC (Ceramic Leaded Chip Carrier)	od 2000 V

Środki ochrony podzespołów zagrożonych elektrostatycznie

- Zagrożone podzespoły powinny pozostawać w oryginalnym opakowaniu aż do momentu ich obróbki.
- Zagrożone podzespoły mogą być przechowywane i transportowane tylko w wysokoomowych lub antystatycznych pojemnikach.
- Podczas wyjmowania podzespołu z opakowania najpierw należy dotykaniem rozładować opakowanie. Dopiero potem można wyjąć podzespół.
- W przypadku montażu na płycie najpierw należy dotykaniem rozładować płytkę. Dopiero potem można zamontować podzespół.
- Obróbka podzespołów może odbywać się tylko na specjalnie wyposażonych stanowiskach roboczych:
 - końcówki lutownic muszą być uziemione
 - stoły robocze i podłogi muszą być antystatyczne i uziemione
 - obróbka powinna się odbywać na matach roboczych, które są połączone ze skórą poprzez opaskę uziemiającą
 - odzież robocza powinna być wykonana z bawełny, a nie z elektryzujących się włókien sztucznych
 - buty powinny być otoczone materiałem przewodzącym prąd.
- Należy zachowywać minimalną odległość 10 cm od monitorów ekranowych.

Mechanizmy oddziaływania i środki zaradcze

Można wyróżnić następujące mechanizmy sprzężenia:

- Oddziaływanie na przewody
- Oddziaływania pól
 - oddziaływanie na pole
 - oddziaływanie przez promieniowanie

Oddziaływanie na przewody

Sprężenie galwaniczne

Do oddziaływań dochodzi na wspólnych odcinkach przewodów (przewody zasilające, uziemienie itp.). Można je wykluczyć lub ograniczyć przez:

- krótkie wspólne odcinki przewodów o niskiej rezystancji
- osobne zasilanie elektryczne
- separację potencjałów przez transformatory, transformatory separacyjne, przekładniki itp. w przypadku przewodów sygnałowych i poprzez oddzielenie zasilania elektrycznego od transmisji informacji.

Sprężenie pojemnościowe

Sprężenia pojemnościowe są powodowane przez przypadkowe pojemności należące do różnych obwodów, które tworzą się między strukturami przewodzącymi. Środki zapobiegawcze:

- krótkie, możliwie nierównoległe przewody między elementami
- zastosowanie przewodów ekranowanych.

Sprężenie indukcyjne

Zwłaszcza duże, szybko zmieniające się w czasie prądy lub wyładowania elektrostatyczne i błyskowe, mogą indukować napięcia zakłócające pomiędzy niezależnymi obwodami prądowymi. Napięcia te bywają zinterpretowane jako sygnał lub prowadzą do przebicia.

Do zminimalizowania lub wykluczenia tych problemów służą:

- zastosowanie skrętki lub przewodów ekranowanych
- duże odległości między przewodami do przesyłu energii i informacji
- możliwie małe powierzchnie między obwodami elektrycznymi.

Oddziaływanie falowe

Fale elektromagnetyczne generowane przez sprężenia pojemnościowe i indukcyjne na przewodach powodują napięcia zakłócające, gdy długość fali zakłócenia jest zbliżona do wymiarów systemu, albo gdy czasy narastania impulsów zakłócających odpowiadają czasom trwania sygnału. Środkiem zapobiegawczym jest:

- zastosowanie przewodów ekranowanych.

Poza tym jako środki redukujące stosuje się:

- filtry i / lub
- urządzenia ochrony przepięciowej.

Oddziaływanie pola (o niskiej częstotliwości)

Duże natężenia prądu niskiej częstotliwości powodują powstanie pola magnetycznego niskiej częstotliwości, które może wzbudzać napięcia zakłóceniewe lub wywoływać zakłócenia wskutek bezpośredniego działania magnetycznego (pamięć magnetyczna komputerów, wrażliwe elektromagnetyczne urządzenia pomiarowe). Pola elektryczne niskiej częstotliwości o dużej mocy mogą być wytwarzane przez wysokie napięcie o niskiej częstotliwości (linie napowietrzne wysokiego napięcia) i mogą prowadzić do napięć zakłóceniewych (sprężenie pojemnościowe).

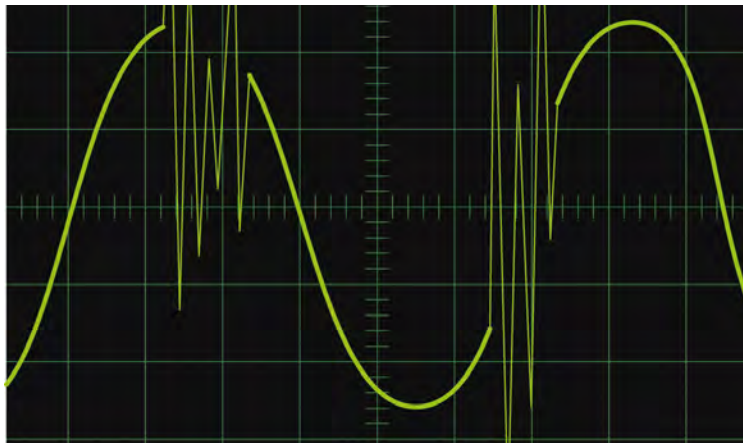
Praktyczne znaczenie mają pola magnetyczne, których oddziaływanie można zmniejszyć przez:

- przewody ekranowane
- obudowy ekranujące (decydująca jest właściwość materiału określana jako przepuszczalność magnetyczna, zbyt mała dla blachy, znacznie lepsza w przypadku np. mumetalu).

Oddziaływanie przez promieniowanie (wysoka częstotliwość)

Fale elektromagnetyczne wywołane obwodem elektrycznym na wolnej przestrzeni mogą wytwarzać zakłócenia napięcia, które należy rozważać zależnie od odległości do miejsca jego powstawania (pole bliskie lub dalekie). W polu bliskim przeważają albo komponenty elektryczne (E), albo komponenty magnetyczne (H) pola elektromagnetycznego, w zależności od tego, czy źródło zakłócenia prowadzi wysokie napięcie i mały prąd, czy wysoki prąd i małe napięcie. W polu dalekim zasadniczo nie można już rozpatrywać E i H osobno. Istnieje możliwość zmniejszenia oddziaływania za pomocą:

- ekranowanych przewodów
- ekranujących obudów (klatka Faradaya!).



Ekranowanie wysokich częstotliwości (HF) obudowy

Badanie profilu wymagań może zostać przeprowadzone zgodnie z poniższą listą kontrolną.

Lista kontrolna profilu wymagań odnośnie obudowy EMC

- Jakie wielkości zakłócające występują w danym zastosowaniu (elektryczne, magnetyczne czy pole elektromagnetyczne)?
- Jakie wartości graniczne zakłóceń mogą wystąpić w zastosowaniu (natężenie pola, zakres częstotliwości)?
- Czy wymagania mogą zostać spełnione przez standardową obudowę czy obudowę z ekranowaniem wysokich częstotliwości (porównanie z diagramami tłumienia)?
- Czy zachodzą inne wymagania EMC (odgrodzenie w obudowie, szczególne wyrównanie potencjałów w obudowie itd.)?

Każda obudowa z blachy stalowej oferuje już dobry **poziom podstawowego ekranowania** w szerokim zakresie częstotliwości, tj. tłumienie pól elektromagnetycznych. Dla dużych szaf sterowniczych można uzyskać **średnie ekranowanie** niskim kosztem, tworząc wielokrotne połączenia przewodzące pomiędzy wszystkimi częściami obudowy.

Wysokie wartości ekranowania w obszarze częstotliwości powyżej ok. 5 MHz uzyskiwane są dzięki zastosowaniu specjalnych uszczelnień, które szczelnie łączą elektrycznie odsłonięte wewnętrzne powierzchnie metalowe drzwi i zdejmowanych ścian, blach dachowych i podłogowych z nieodsłoniętymi krawędziami metalowymi korpusu lub szkieletu obudowy. Im wyższe występują częstotliwości, tym bardziej istotne stają się otwory w obudowie.



■ Kable miedziane

Kody kolorów przewodów izolowanych i nieizolowanych

System prądowy	Oznaczenie przewodu	Oznaczenie skrótowe	Kolor	Oznaczenie przewodu	Oznaczenie skrótowe	Symbol	Kolor
Prąd stały	dodatni ujemny środkowy	L+ L- M	¹⁾ ¹⁾ bi	Przewód neutralny z funkcją ochronną	PEN		gegn
Prąd przemienny	fazowe neutralny	L1; L2; L3 N	¹⁾ bi	Przewód ochrony	PE		gegn
¹⁾ Kolor nie jest określony			-	Uziemienie	E		¹⁾

Skrótowe oznaczenia typów przewodów i kabli telekomunikacyjnych

Przykład:

J- Y (St) Y 20 x 2 x 0,6 Lg

Pozycja oznaczenia:

J-	Y	(St)	Y	20	x 2	x 0,6	Lg			
1	2	3	4	5	6	7	8	9	10	11

= kabel instalacyjny, izolacja żył z PVC, ekran elektrostatyczny, osłona kabla z PVC, 20 par żył, średnica przewodu 0,6 mm, o konstrukcji warstwowej

1 Typ kabla

A-: kabel zewnętrzny
FL-: przewód płaski
J-: kabel instalacyjny i wtykowy
Li-: żyła wielodrutowa
S-: kabel instalacyjny

2 Powłoka izolacyjna

Y: polichlorek winylu (PVC)
2Y: polietylen (PE)
02Y: polietylen piankowy

3 Ekran

C: opłot miedziany
(K): ekran z taśmy miedzianej na płaszczu PE
(L): taśma aluminiowa
(mS): ekran magnetyczny z taśmy stalowej
(St): ekran elektrostatyczny

4 Powłoka

E: zatapiana taśma z tworzywa sztucznego
FE: kabel uniepalniony < 20 minut
G: powłoka gumowa
H: materiał bezhalogenowy
L: gładka powłoka aluminiowa
(L)2Y: powłoka aluminiowa laminowana tworzywem PE
M: powłoka ołowiana

5 Osłona

Y(v): powłoka PVC (wzmocniona)
2Y: powłoka PE

11 Pancerz

A: warstwa drutów Al do ochrony indukcyjnej
B: taśma stalowa do ochrony indukcyjnej

10 Układ żył

Bd: skręt pięczkowy
Lg: skręt warstwowy
rd: okrągły
se: sektorowy

9 Rodzaj / typ skrętki

DM: czwórka DM (czwórka Dieselhorst-Martin)
Kx: przewód koncentryczny
P: skrętka parowa
PiMF: pary w folii metalowej
St: czwórka gwiazdowa ze szczeg. wł.
St I: czwórka gwiazdowa bez toru pochodnego
St II: czwórka gwiazdowa do kabli miejscowych
St III: czwórka gwiazdowa, przy 800 Hz
St IV: czwórka gwiazdowa, przy 120 kHz
St V: czwórka gwiazdowa, przy 550 kHz
St VI: czwórka gwiazdowa, przy 17 MHz

8 Średnica przewodu w mm

7 Element skrętki

x 1: pojedyncza żyła
x 2: para (żyła podwójna)
x 3: trójka
x 4: czwórka




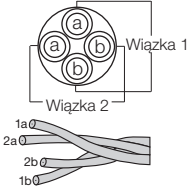
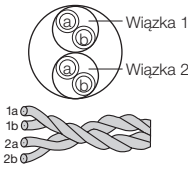

6 Liczba elementów skrętki

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Budowa kabli miedzianych, elementy skrętki

Przewód 	Żyła to przewód w powłoce izolacyjnej.
Para (żyła podwójna) 	Para (żyła podwójna) składa się z dwóch skręconych ze sobą żył, które tworzą jedną wiązkę (pętlę). Para jest najprostszym symetrycznym elementem skrętki.
Para (żyła podwójna) 	Para ekranowana to para w folii metalowej (PIMF). Składa się z dwóch skręconych ze sobą żył, które tworzą jedną wiązkę (pętlę), na którą jest nałożony ekran elektrostatyczny. Ocynkowana żyła żelazna (żyła pomocnicza) jest na całej długości połączona z ekranem elektrostatycznym.
Czwórka gwiazdowa 	Czwórka składa się z czterech skręconych ze sobą żył, z których żyły leżące naprzeciw siebie tworzą jeden tor (pętlę, wiązkę, obwód podstawowy). Wiązki nazywane są też parami żył.
Czwórka DM (czwórka Dieselhorst-Martin) 	W czwórce DM dwie żyły są skręcone w parę, a dwie pary są skręcone ze sobą. Obie pary mają różny skok skrętu w celu uzyskania lepszego tłumienia przesłuchu. Czwórka DM ma mniejsze pojemności robocze i mniejsze tłumienie niż czwórka gwiazdowa.
Pęczek 	Pęczek składa się z pięciu połączonych elementów skrętki.

Oznakowanie, numeracja kabli komunikacyjnych

Kable komunikacyjne są numerowane ZAWSZE parami:

- Skręt pęczkowy (oznakowanie kolorami i pierścieniami)
Kolorы dla czwórki: czerwony (rt), zielony (gn), szary (gr), żółty (ge), biały (ws);
Pierścienie na żyłę: [liczba/odległość w mm];
od 11 par: dodatkowe oznakowanie kolorami pęczków

Czwórka -- 1 ---- 2 ---- 3 ---- 4 ---- 5 ----

Para 1 2 3 4 5 6 7 8 9 10

Przewód

a [0/0] [2/34] [0/0] [2/34] [0/0] [2/34] [0/0] [2/34] [0/0] [2/34]

b [1/17] [2/17] [1/17] [2/17] [1/17] [2/17] [1/17] [2/17] [1/17] [2/17]

- Skręt warstwowy (oznakowanie kolorami)
Liczenie warstwami od zewnątrz do wewnątrz;
wszystkie żyły a białe, każda pierwsza żyła warstwy a czerwona (numeracyjna);
Żyły b w kolejności rosnącej:
niebieska (bl), żółta (ge), zielona (gn), brązowa (bn), czarna (sw)

Warstwa ----- zewnętrzna ----- środkowa --- wewn.

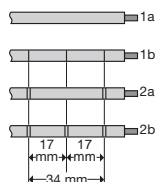
Para 1 2 3 4 5 6 7 8 9 10

Przewód

a **czerw.** biała biała biała biała biała **czerw.** biała biała **czerw.**

b bl ge gn bn sw bl ge gn bn sw

Oznakowanie pierścieniami (np. dla J-2Y(St)Y 2x2x0,6 Bd)



Kolor podstawowy czerwony, pierścienie czarne

Oznakowanie kolorami (np. dla J-Y(St)Y 2x2x0,6 Lg) nowe (stare)

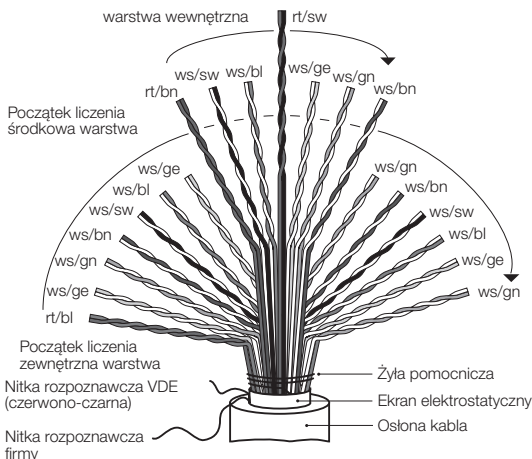
rt (ge)

sw (rt)
Para 1

ws (gn)

ge (bl)
Para 2

Przykład: J- Y (St) Y 20 x 2 x 0,6 Lg



Oznakowanie kabli światłowodowych

Skrótowe oznaczenie typu

Przykład:

A- W S F (ZN)2Y Y 12 G 50/125 3,0 B 600 Lg

= kabel zewnętrzny z wypełnioną tubą, metalowe elementy w ośrodku kabla, który jest wypełniony, powłoka PE z niemetalowymi elementami zabezpieczenia naciągu i powłoka PVC, 12 włókien gradientowych o średnicy rdzenia 50 µm i średnicy powłoki 125 µm, współczynnik tłumienia ≤ 3 dB/km i szerokość pasma 600 MHz na km przy długości fali 850 nm, skręt warstwowy.

Pozycja oznaczenia:

A-	W	S	F	(ZN)2Y	Y	12	G	50/	125	3,0	B	600	Lg
1	2	3	4	5	6	7	8	9	10	11	12	13	14

1 Typ kabla

A-: kabel zewnętrzny
AT-: kabel zewnętrzny, z możliwością podziału
J: kabel wewnętrzny

2 Budowa

F: włókno
V: włókno pełne
W: tuba, wypełniona
B: tuba z wiązką, wypełniona

3 Ośrodek kabla

S: metalowy element w ośrodku kabla

4 Wypełnienie

F: wypełnienie żelem na bazie oleju mineralnego

5 Powłoka

H: powłoka zewn. z materiału bezhalogenowego
Y: powłoka PVC
2Y: powłoka PE
(L)2Y: materiał warstwowy
(ZN)2Y: powłoka PE z niemetalowymi elementami zabezpieczenia naciągu

6 Pancerz

B: pancerz
BY: pancerz z osłony PVC
B2Y: pancerz z osłony PE
H: powłoka z materiału bezhalogenowego
Y: powłoka PVC

14

Lg: skręt warstwowy

13

xxx: szer. pasma w MHz dla L = 1 km

12 Okna transmisyjne

B: długość fali 850 nm
F: długość fali 1300 nm
H: długość fali 1550 nm

11

xxx: współczynnik tłumienia w dB/km

10

xxx: średnica powłoki w µm

9

xxx: średnica rdzenia w µm lub średnica pola µm dla włókien jednomodowych (MNM)

8 Typ włókna

E: włókno jednomodowe (MNM)
G: włókno gradientowe szkło/szkło
K: włókno skokowe z tworzywa szt.

7

xxx: liczba żył

Typowe parametry światłowodów – przykład

Typ włókna	G 50/125	E 9/125
Średnica rdzenia w μm	50 ± 3	≈ 9
Średnica pola μm	–	9 ± 1
Średnica powłoki w μm	125 ± 25	125 ± 25
Wytrzymałość na rozciąganie	5 N	5 N
Średnie naprężenie niszczące	50 N	50 N
Promień zgięcia	50 mm	50 mm
Szerokość pasma w MHz \times km dla	850 nm: 200...600; 1300 nm: 600...1200	
Tłumienie w dB/km dla	850 nm: 2,5...3,5; 1300 nm: 0,7...1,5	
Dyspersja w ps/nm \times km dla	–	1300 nm: < 5; 1550 nm: < 20

■ Okablowanie sieciowe

Szerokość pasma (bandwidth)

Szerokość pasma to ściśle biorąc, różnica między górną a dolną częstotliwością podawana w jednostkach fizycznych – hercach (Hz). Im większa szerokość pasma, tym teoretycznie można przesłać więcej informacji w jednostce czasu. Tym samym jest to parametr analogowej pojemności transmisyjnej kanału. Poza tym

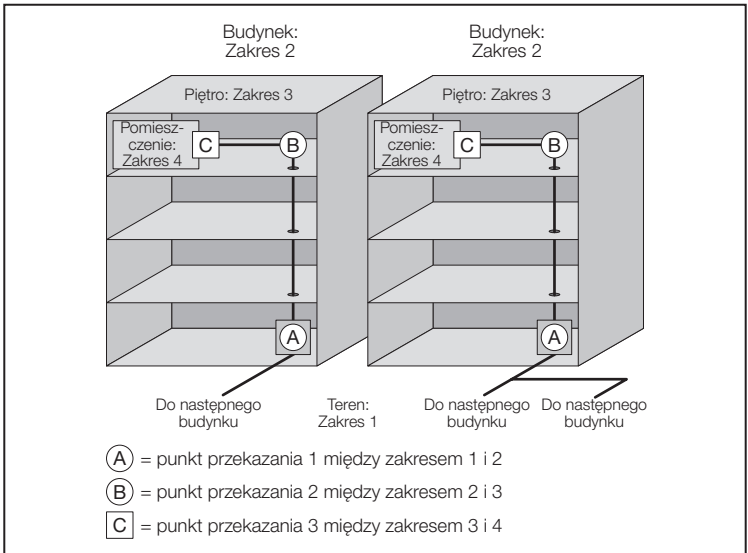
szerokość pasma jest dzisiaj także miarą pojemności transmisyjnej systemu w jednostkach bit/s, Mbit/s lub ich wielokrotności. Istnieje przy tym bezpośredni związek między szerokością pasma a prędkością transmisji: w transmisji danych maksymalna prędkość transmisji zależy bezpośrednio od szerokości pasma sieci.

Okablowanie budynkowe (building wiring)

Okablowanie budynkowe jest składnikiem okablowania strukturalnego. Mianem okablowania budynkowego określa się uniwersalne, niezależne okablowanie w budynku, przeznaczone do komunikacji IT. Standard okablowania budynkowego obejmuje:

- projektowanie okablowania
- projekt topologii i sieci
- instalację
- kompatybilność elektromagnetyczną
- klasy mocy i klasy użytkowe typów kabli.

Okablowanie budynkowe, jako tak zwane okablowanie wtórne, obejmuje zakres od rozdzielacza do budynkowego do rozdzielacza piętrowego.



Okablowanie budynkowe z zakresem pionowym i zakresem piętrowym

Źródło: *Lexikon der Datenkommunikation* (Leksykon transmisji danych)

Klasy użytkowe sieci i kategorie kabli

Klasa	Kategoria	Zakres częstotliwości	Możliwe zastosowania
A	1	do 100 kHz	Telefon analogowy
B	2	do 1 MHz	ISDN
C	3	do 16 MHz	10BaseT, Token Ring
D	5	do 100 MHz	100BaseTX
E	6	do 250 MHz	Gigabit-Ethernet, ATM
F	7	do 600 MHz	Gigabit-Ethernet, ATM

Parametry często stosowanych kabli telekomunikacyjnych

Ø żyły d mm	Parametry				Tłumiennosc jednostkowa α do 800 Hz dB/km	Impedancja falowa Z_w przy 800 Hz Ω
	R Ω /km	L mH/km	G μ S/km	C nF/km		
0,4	270	0,7	0,1	34	1,31	1260
0,6	122	0,7	0,1	37	0,91	810
0,8	67	0,7	0,1	38	0,69	590
0,9	52	0,7	0,1	34	0,58	550
1,2	29	0,7	0,1	35	0,45	430

■ Złącza wtykowe

Przyrządkowanie rodzajów wtyczek i kabli

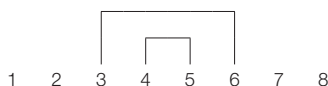
Gniazdo/złącze	Rodzaj kabla
Twinax; BNC-E; BNC-F	Kabel koncentryczny
RJ 11 – 45 48 Mod. Jacks; 32 Mod. Jacks	Ekranowane / nieekranowane kable ze skrętką parową (2- do 4-parowe)
F-SMA E 2000; LC; MTRJ; ST; ST-Duplex; Biconic; FC-PC	Światłowodowy
D-Sub 9-pinowe; D-Sub 15-pinowe; D-Sub 25-pinowe; ADO 4/8; TAE 4/6	Przewody ekranowane/nieekranowane

Konfiguracja pinów i przyrządkowanie par do okablowania twisted pair ze złączami wtykowymi RJ 45

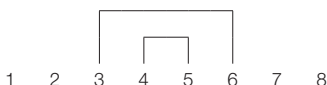
Ethernet



Token Ring



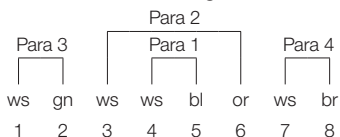
ISDN



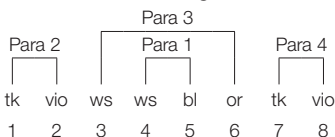
TPDDI/ATM



1000 BaseT według TIA 568 A



1000 BaseT według TIA 568 B



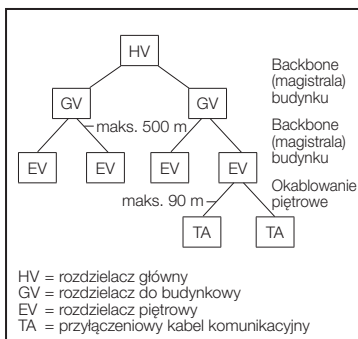
Wybór złączy wtykowych światłowodowych

Typ	Przeznaczenie	Typowa tłumienność	Zalety	Wady
F-SMA	Włókna wielomodowe	0,7...1 dB (G50/125) 0,6...0,8 dB (G62,5/125)	Wtyk nierozłączalny ręcznie, bez użycia narzędzi (przy użyciu określonego momentu dokręcania)	<ul style="list-style-type: none"> ■ Uciążliwe podłączanie w przypadku gęsto upakowanych pól krosowych ze względu na połączenie śrubowe ■ Brak zabezpieczenia przed skręceniem, przez to brak kontaktu włókna, wysokie wartości tłumienia
DIN	Włókna jedno- i wielomodowe	0,2...0,4 dB (9/125) 0,2...0,4 dB (50/125)	Dokładne centrowanie rdzenia włókna we wtyku	<ul style="list-style-type: none"> ■ Tylko norma DIN, brak szerokiego rozpo-wszecznienia (Telekom) ■ Brak możliwości bezpośredniego montażu, pigtaile muszą być spawane
FC/PC	Włókna jedno- i wielomodowe	0,2...0,5 dB (9/125) 0,2...0,5 dB (50/125)	Podobne do wtyków DIN	
ST	Włókna jedno- i wielomodowe	0,3...0,4 dB (G50/125) 0,2...0,3 dB (G62,5/125)	Odporne na przekręcanie po podłączeniu	
SC	Włókna jedno- i wielomodowe	0,3 dB	<ul style="list-style-type: none"> ■ Odporne na przekręcanie ■ Zatraskuje się po wsunięciu 	
FDDI (MIC)	Włókna jedno- i wielomodowe	0,5 dB	<ul style="list-style-type: none"> ■ Bez zamiany ścieżki nadawczej i odbiorczej ■ Jednoznaczne przyporządkowanie portów przez kodowanie 	<ul style="list-style-type: none"> ■ Skomplikowana konstrukcja, brak możliwości formowania pól ■ Wtyk i gniazdko zajmują dużo miejsca
E 2000	Włókna jedno- i wielomodowe	0,2...0,4 dB (9/125) 0,2...0,4 dB (50/125)	<ul style="list-style-type: none"> ■ Mechanizm zatraskowy ■ Osłona/klapka zabezpieczająca chroni użytkownika przed promieniem lasera ■ Kompaktowa konstrukcja do dużych gęstości upakowania 	
LC	Włókna jedno- i wielomodowe	0,2 dB	<ul style="list-style-type: none"> ■ Zamknięcie zaciskowe ■ Kompaktowa konstrukcja do dużych gęstości upakowania 	
MTRJ	Włókna jedno- i wielomodowe	0,3 – 0,5 dB	<ul style="list-style-type: none"> ■ Zamknięcie zaciskowe ■ Kompaktowa konstrukcja do dużych gęstości upakowania 	

■ Ważne urządzenia technologii sieciowej

Rozdzielacz do budynkowy (building distributor, BD)

Rozdzielacz ten stanowi punkt przejścia od okablowania terenowego do okablowania budynkowego. Zawiera wszystkie punkty podłączenia okablowania budynkowego z polami rozrządowymi i krosowymi oraz punkty podłączenia okablowania terenowego. Może przy tym zawierać medium przenoszące, np. z przewodów światłowodowych na kable twisted pair lub inne kable danych.



Rozdzielacz do budynkowy

Karta sieciowa (Network Interface Card – NIC)

do sieci Ethernet

Obejmuje:

- Interfejs sieciowy, do 10Base5, 10Base2, 10BaseT, 100BaseT..., do połączenia z okablowaniem sieciowym
- Przetwarzanie danych równoległych na dane bit po bicie
- Interfejs magistrali (bus) do połączenia z magistralą PC

NIC pracuje na warstwie OSI 1 i 2; karty sieciowe obsługujące 10 i 100 Mbit/s automatycznie przestawiają się na właściwą prędkość.

Brama (gateway)

Pod zbiorczym pojęciem **bramy** zgrupowano szereg różnych pod względem technicznym urządzeń, których zadaniem jest zapewnienie połączenia między sieciami. Zależnie od złożoności, brama może być prostym wzmacniaczem lub nawet kompletnym komputerem.

Zakresy okablowania wg standardu okablowania EIA/TIA 568

Bramy są niezbędne, gdy istniejąca sieć:

- ma być strukturalna, czyli podzielona na podsieci
- ma zostać rozszerzona, czyli fizycznie powiększona
- powiązana z innymi sieciami, czyli gdy kilka sieci LAN ma być połączonych ze sobą lub z łączem WAN, w wyniku czego powstaje sieć heterogeniczna.

Repeater

Wzmacniacz odświeżający sygnały, umożliwia zwiększenie maksymalnej długości segmentu; pracuje na warstwie OSI 1; inne formy:

- **Repeater wieloportowy**, umożliwia podział sieci na segmenty dla zwiększenia dostępności
- **Łącznik gwiazdowy (star coupler)** do połączenia licznych segmentów sieci, umożliwia zmianę medium (np. z miedzi na światłowód)

Źródło: Lexikon der Datenkommunikation (Leksykon transmisji danych)

- **Hub lub koncentrator** do budowania sieci w topologii gwiazdy, z dodatkowymi funkcjami (bridge, router), często z możliwością kaskadowania; uniwersalne, szeroko rozpowszechnione urządzenie.

Most (bridge, switch → multiport bridge)

Do dzielenia dużych sieci na mniejsze podsieci; błędne pakiety danych pozostają w podsieci, istnieje możliwość oddzielenia obciążenia, gdyż pakiety danych nie są transportowane dla adresu we własnej sieci; pracuje na warstwie OSI 2; inne formy:

- **Local bridge** do łączenia sieci tego samego rodzaju, a także – różnych sieci (np. Ethernet – Token Ring)

- **Remote bridge** do łączenia sieci przez sieci WAN

- **Multiport bridge** (często identyczny ze switchem) do łączenia kilku podsieci.

Router

Do wyszukiwania trasy w rozległych sieciach LAN i WAN różnych typów, protokołów i topologii, pracuje na warstwie OSI 3.

Brama (gateway)

Do łączenia całkowicie różnych sieci, np. sprzężenie LAN z publiczną siecią WAN lub systemami hosta, pracuje na warstwach OSI 4, 5, 6 lub 7.

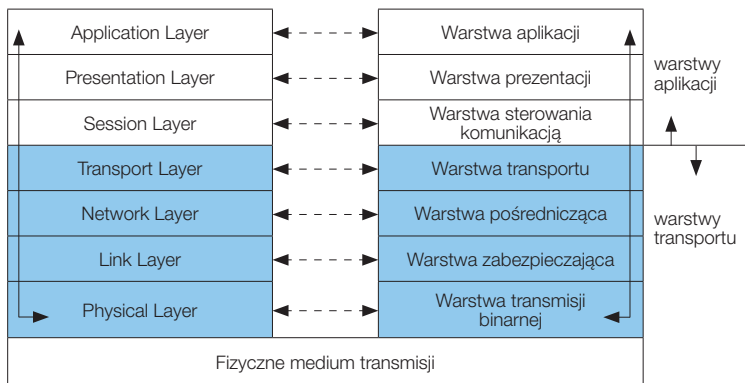
Model warstw OSI wg ISO

(OSI: Open Systems Interconnection, ISO: International Standards Organization)

Model OSI opisuje wszystkie komponenty, które są niezbędne do komunikacji pomiędzy komputerami. Łącznie zdefiniowano siedem kolejnych warstw. Programy, które znajdują się na najwyższej płaszczyźnie modelu, powinny być w stanie funkcjonować całkowicie niezależnie od modelu i sieci. Ich dostęp do medium transmisji jest realizowany poprzez wszystkie siedem warstw.

Informacje, które mają być przesłane z jednego systemu do drugiego, muszą być najpierw przekazane z naj-

wyższej warstwy poprzez wszystkie znajdujące się pod nią. Transport odbywa się przy tym przez medium fizyczne (okablowanie sieciowe). Jednocześnie na każdej warstwie do danych doczepiane są informacje sterujące i kontrolne (protokoll overhead). Komunikować się między sobą mogą tylko systemy posiadające zgodną strukturę warstw. Z siedmiu warstw modelu trzy górne (5, 6, 7) są zorientowane na aplikacje, cztery dolne (1-4) to warstwy transportujące.



Źródło: *Lexikon der Datenkommunikation* (Leksykon transmisji danych), strona 374

- faktyczny transport
- - - - - wirtualne protokoły warstw

Model referencyjny OSI z podziałem na warstwy aplikacji i transportu

Niektóre podstawowe pojęcia w modelu OSI:

Instancje: Instancją jest moduł w warstwie, który może być zrealizowany za pomocą sprzętu i oprogramowania. Komunikacja może się odbywać pionowo z instancjami w wyższych lub niższych warstwach, a także poziomo z osobnymi przestrzennie instancjami.

Usługi: Usługi to świadczenia, które warstwa oferuje wyższej warstwie.

Protokoły: Komunikacja między instancjami na tym samym poziomie odbywa się za pomocą protokołów.

Pakiety: Wiadomości między warstwami są wymieniane przez pakiety.

7. Warstwa aplikacji / płaszczyzna obróbki / Application Layer

To część oprogramowania aplikacji odpowiedzialna za komunikację,

jednocześnie jest to punkt wyjściowy i docelowy transportowanych danych użytkowych.

Podczas transmisji danych warstwa jest odpowiedzialna np. za dopasowanie pliku do obowiązujących w systemie docelowym konwencji (np. dotyczących nazwy pliku).

Przykładem usługi na tym poziomie może być mailing elektroniczny.

6. Warstwa prezentacji / płaszczyzna dopasowania / Presentation Layer

Dostarcza programowi aplikacji interfejs sieciowy i określa rodzaj dostępu programu do sieci. W tym celu udostępnia funkcje do transportu danych. Konwertuje przychodzące z góry dane do standardowego formatu obowiązującego w sieci, tak więc do jej zadań należy formatowanie, strukturyzacja, szyfrowanie i kompresowanie danych.

5. Warstwa sesji / płaszczyzna sterowania / Session Layer

Udostępnia w sieci połączenie dla usług sieciowych znajdujących się powyżej. Warstwa sesji jest odpowiedzialna za sterowanie komunikacją między dwoma aplikacjami.

4. Warstwa transportu / Transport Layer

Jest odpowiedzialna za nawiązanie połączenia między dwoma urządzeniami; to jedyna warstwa transportu utrzymująca połączenie P2P między fizycznymi punktami końcowymi. Jako najwyższa z warstw transportujących oferuje warstwom aplikacji znajdującym się nad nią ogólną i niezależną usługę transmisji. Dla warstwy transportowej nie ma znaczenia, czy warstwy od 1 do 3 są zrealizowane jako LAN, czy jako WAN.

3. Warstwa pośrednicząca / płaszczyzna sieci / Network Layer

Warstwa pośrednicząca jest dodatkową płaszczyzną, która właściwie nie jest potrzebna, gdy systemy końcowe są ze sobą połączone łączem bezpośrednim. Jednak w złożonych i heterogenicznych sieciach bezpośrednie połączenie zdarza się bardzo rzadko. Warstwa pośrednicząca umożliwia wysyłanie danych w złożonych i heterogenicznych sieciach poprzez węzły sieci, aż do celu (w systemach końcowych z bezpośrednim połączeniem nie jest potrzebna). W sieciach bazujących na pakietach (np. wszystkie LAN) steruje ona nawiązaniem połączenia oraz rozłączaniem, jest odpowiedzialna za wybór trasy (routing) i za adresowanie. Warstwa pośrednicząca realizuje połączenie P2P między urządzeniami. Urządzeniami tymi niekoniecznie muszą być

systemy końcowe, mogą to być także bramy sieciowe. Przykładem usługi na płaszczyźnie 3 jest warstwa pakietów X.25.

2. Warstwa zabezpieczająca / płaszczyzna połączenia danych / Link Layer

Odpowiada za bezbłędną transmisję danych. Przychodzący z góry strumień binarny jest rozkładany na ramki (frames), ponieważ indywidualna transmisja bloków danych nie sprawia trudności, jest bardziej przewidywalna i łatwiejsza do skorygowania. Po stronie odbiorcy warstwa zajmuje się odtworzeniem strumienia binarnego z przychodzących z dołu ramek. Poza tym w przypadku sieci opartych na łączach (np. sieci telefoniczne, ISDN) steruje ona nawiązaniem połączenia i rozłączaniem. Przykładem realizacji płaszczyzny 2 jest protokół HDLC X.25.

1. Warstwa transmisji binarnej / płaszczyzna fizyczna / Physical Layer

Jest jedyną warstwą, która wchodzi w bezpośredni kontakt z fizycznym medium transmisji, przez co odpowiada ona za definicje elektryczne i mechaniczne (jak np. konfiguracja wtyków, wartości napięć i sygnały interfejsu). Warstwa transmisji binarnej definiuje fizyczne połączenie wewnątrz sieci. Jej zadaniem jest sterowanie medium i procedurą transmisji. Jako jedyna warstwa, wysyła i odbiera nieuporządkowane bezpośrednio strumienie binarne. Przykładem jest interfejs X.21 – stosowany również w protokole X.25.

■ Procedury dostępu do sieci

CSMA/CD i Ethernet

Zalecenia IEEE **802.3** opisują procedurę dostępu **CSMA/CD** (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection) i fizyczną transmisję na magistrali danych. Wszystkie stacje są podłączone do dwukierunkowej magistrali. Dane mogą być przesyłane z prędkościami od 1 do 10 Mbit/s. Chociaż w zaleceniach przyjmuje się strukturę magistrali, dzisiejsze sieci są zbudowane raczej gwiazdźście: każda stacja utrzymuje połączenie z centralnym węzłem (hubem), który wewnętrznie przełącza wszystkie podpięte łącza. Tak fizycznie powstaje gwiazda,

która jednak przez zarządzanie węzła wpisuje się, jak wcześniej, strukturę magistrali.

Procedura dostępu do medium CSMA/CD często bywa błędnie porównywana z **Ethernetem**, który jest właściwie specjalnym produktem stosującym CSMA/CD. Została opracowana przez firmy Xerox, DEC oraz Intel i jest stosowana od około 20 lat. Rozwinięciem są Fast Ethernet (100Base...) i Gigabit Ethernet (1000Base...) dla prędkości transmisji do 100 lub 1000 Mbit/s.

Warianty okablowania Ethernet

Nazwa	Typ kabla	Długość segmentu	Segmety	Stacje we wszystkich segmentach	Min. odl. stacji	Prędkość transmisji
10Base5 ThickWire	Kabel koncentryczny	500/3000 m	5	100/492	2 m	10 Mbit/s
10Base2 ThinWire	Kabel koncentryczny	185/925 m	5	30/142	0,5 m	10 Mbit/s
10BaseT TwistedPair	Skръtka miedziana	100 m	1	1	–	10 Mbit/s
10BaseFP	Światłowód	500 m	1	1	–	10 Mbit/s
10BaseFB	Światłowód	2 km	1	1	–	10 Mbit/s
100BaseT	Skръtka miedziana	100 m	1	1	–	100 Mbit/s
100BaseVG	Skръtka miedziana	100 m	1	1	–	100 Mbit/s
1000BaseCX	Twinax kabel miedziany	25 m	1	1	–	1000 Mbit/s
1000BaseLX	Światłowód wielomodowy jednomodowy	440/550 m 3000 m	1	1	2 m	1000 Mbit/s
1000BaseSX	Światłowód wielomodowy	260/550 m	1	1	2 m	1000 Mbit/s

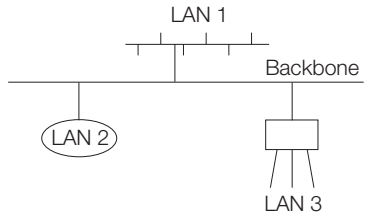
Token Ring

Token Ring w związku z rozpowszechnieniem struktur sieci LAN znajduje się na drugim miejscu. Pierwotnie opracowany przez IBM, dopiero później stał się standardem w zaleceniach IEEE 802.5 i zadomowił się głównie w środowiskach zdominowanych przez komputery IBM. Technologia LAN o topologii pierścienia jest z powodzeniem stosowana od około 10 lat. Prosta struktura pierścienia została lekko zmodyfikowana w celu zwiększenia odporności na awarię. Każda stacja jest osobno podłączona poprzez centrum okablowania (rozdzielacz pierścienia lub Ring Wiring Concentrator, RWC). W ten sposób powstaje gwiazdzista pętla, która

jest gwiazdą pod względem fizycznym, a pod względem logicznym – pierścieniem. Pierścień może być użytkowany z prędkościami 4 lub 16 Mbit/s, a jego okablowanie stanowi wielożyłowy przewód miedziany twisted pair. Wymiana danych na Token Ring odbywa się jednokierunkowo. Każda stacja odbiera dane po stronie odbiorczej i z małym opóźnieniem przekazuje po stronie nadawczej do następnej stacji. Buforowanie i krótkie opóźnienie jest niezbędne, aby uprawnienie do nadawania – tak zwany wolny token – trafił do całej sieci. Procedura dostępu nosi nazwę token passing.

Backbone (BB)

Sieć Backbone w sieciach uporządkowanych hierarchicznie tworzy specjalną infrastrukturę do wymiany informacji między sieciami i systemami. Z reguły określa się w ten sposób np. sieć Wide Area Network (WAN), która łączy większą liczbę podsieci jak Local Area Networks (LAN) poprzez mosty (bridges) i routery (router). Charakteryzuje się krótkimi czasami awarii, dużą pojemnością transmisyjną i brakiem przyłączy elementów. Rozróżnia się collapsed Backbones i rozproszone, distributed Backbones.

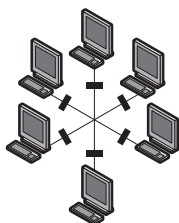


Źródło: Lexikon der Datenkommunikation (Leksykon transmisji danych)

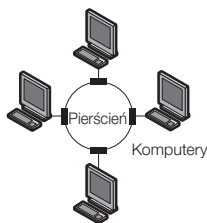
Topologie sieci

Topologia opisuje zasadniczą geometryczną strukturę okablowania. Popularność zyskały cztery podstawowe topologie: pierścienia, magistrali, gwiazdy i drzewa. W większych sieciach można znaleźć głównie mieszane formy tych topologii.

		Zalety i wady
Pierścień	W topologii pierścienia stacje sieciowe są połączone odpowiednio z następną stacją, a ostatnia z pierwszą, w wyniku czego powstaje pierścień: np. Token Ring; FDDI	+ Odporność na awarie + Gwarantowana szerokość pasma – Duże koszty – Złożoność
Magistrala	Wszystkie stacje sieciowe komunikują się przez wspólny kabel danych: np. Ethernet	+ Złożoność w małych sieciach – Problemy z awaryjnością – Analiza błędów – Szerokość pasma w dużych sieciach
Gwiazda	Z węzła centralnego sieci (hub, switch) wychodzą połączenia P2P z poszczególnymi węzłami sieci	+ Odporność na awarie + Szerokość pasma – Awaria centralnego węzła sieci
Drzewo	Topologia drzewa wyróżnia się dużą elastycznością struktury. Może być zbudowana przez kaskadowanie hubów lub switchy: np. 100Base-AnyLan.	+ Elastyczność – Złożoność

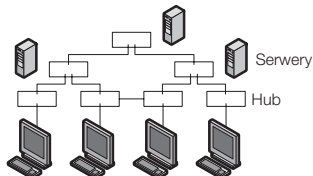


Gwiazda

Pierścień
Komputery

Magistrala

Kontroler



Stacja robocza

Drzewo

Serwery

Hub

Protokoły sieciowe

Liczne protokoły sieciowe połączono w zestawy protokołów służących do różnych zadań komunikacji w sieciach.

Przykłady zestawów protokołów

		Zalety i wady
TCP/IP	<p>(Transmission Control Protocol/Internet Protocol)</p> <p>Komputery znajdujące się w sieci są identyfikowane na podstawie adresów IP. Urządzenie z adresem IP jest nazywane hostem. Pierwotnie TCP został opracowany jako monolityczny protokół sieciowy, jednak później podzielono go na protokoły IP i TCP. Główną grupę rodziny protokołów uzupełnia User Datagram Protocol (UDP), następny protokół transportowy.</p> <p>Poza tym istnieją jeszcze liczne protokoły pomocnicze i protokoły aplikacji, jak np. DHCP i ARP.</p> <p>Opracowany przez Ministerstwo Obrony USA pod koniec lat 70. jako członek rodziny protokołów DoD (Department of Defense), jest jednym z najbardziej rozpowszechnionych zestawów protokołów. Jego implementacje znajdują zastosowanie we wszystkich ważnych platformach systemów operacyjnych, jak Unix, VMS, Windows i DOS. Szczególnie przydatny w środowisku heterogenicznym.</p>	<ul style="list-style-type: none"> + heterogeniczne środowisko + możliwość routingu + szerokie rozpowszechnienie
IP	Protokół internetowy	

Zestaw protokołów TCP/IP

Protokół transportowy TCP

TCP jest protokołem zorientowanym na połączenia, z usługami korygowania błędów i kontroli przepływu. Dostarczanie tych usług wiąże się z dodatkowym kosztem, gdyż połączenia muszą być nawiązywane i zamykane. Korygowanie błędów wymaga dodatkowych zasobów.

Niektóre pojęcia dotyczące protokołów TCP/IP

ARP	(Address Resolution Protocol) przyporządkowanie adresów sprzętowych do adresów IP				
BGP	(Border Gateway Protocol) zawiera informacje o dostępności i informacje o najlepszej wybranej drodze				
BIND	(Berkeley Internet Name Domain) implementacja DNS				
BOOTP	(Boot-Protocol) węzeł sieciowy żąda informacji z sieci. Odpowiedzi są wysyłane przez serwer BOOTP				
Datagram	Jednostka informacji w warstwie 3 lub 4 modelu TCP/IP				
DNS	(Domain Name System) budowa systemu hierarchii nazw				
EGP	(Exterior Gateway Protocol) dostarcza informacji o trasach, ale nie szuka najlepszej trasy				
ftp	(file transfer protocol) protokół transmisji danych				
HELLO	Protokół HELLO określa trasę w oparciu o czas odpowiedzi				
ICMP	(Internet Control Message Protocol) dostarcza informacji o statusie i błędach w TCP/IP				
MAC	(Medium Access Control) fizyczne adresy dostępu do mediów				
SNMP	(Simple Network Management Protocol) protokół zarządzania do ustawiania i administrowania urządzeniami sieciowymi				
SOAP	Pierwotnie Simple Object Access Protocol to protokół sieciowy, za pomocą którego są wymieniane dane między systemami oraz są przeprowadzane Remote Procedure Calls. SOAP jest standardem przemysłowym należącym do World Wide Web Consortium (W3C). SOAP w stosie TCP/IP:				
	Zastosowanie	SOAP			
		HTTP	HTTPS	...	
	Transport	TCP			
	Internet	IP (IPv4, IPv6)			
Dostęp do sieci	Ethernet	Token Bus	Token Ring	FDDI	...

SMTP (Simple Mail Transfer Protocol)

Prosty protokół do przekazywania poczty elektronicznej.

Protokół pośredniczący IP

Bezpośrednio nad właściwą technologią sieciową warstw 1 i 2, jako protokół pośredniczący stosowany jest protokół internetowy. Dostarcza warstwom znajdującym się ponad zawodnej (niekontrolowanej) i niewymagającej połączenia usługi datagramów.

Dane są przekazywane w formie bloków danych (pakietów IP lub pakietów internetowych) w niewymagającej połączenia komunikacji. Poza tym protokół odpowiada za adresowanie i wybór trasy (routing) przez bramy i rutery łączące ze sobą poszczególne sieci w internecie.

W IP każdy węzeł sieci może się komunikować bezpośrednio z innym. Nie ma tutaj koncepcji hierarchicznej.

Adresowanie IP

Klasa adresu	Bit klasy	Liczba bitów sieciowych	Ważny zakres adresów	Komentarz
A	0	7	1 do 126	0 i 127 są zarezerwowane
B	10	14	128.1 do 191 254	255 zarezerwowany dla broadcastu
C	100	21	192.0.1 do 223.255.254	
D	1110	–	224.0.0.0 do 239.255.255.254	zarezerwowane dla multicastu
E	1111	–	240.0.0.0 do 255.255.255.254	zarezerwowane dla multicastu

■ Terminologia internetowa

Przeglądarka, browser	Program, za pomocą którego można odczytywać i interpretować strony HTML
CIX	(Commercial Internet Exchange) Umowa między dostawcami sieciowymi w celu przepływu danych
DNS	(Domain Name System) System budowania hierarchii komputerów
FTP	(File Transfer Protocol) Usługa internetowa do kopiowania plików
HTML	(Hypertext Markup Language) Hipertekstowy język znaczników wykorzystywany do konstruowania stron informacyjnych w plikach tekstowych, które można przeglądać za pomocą przeglądarek
HTTP	(Hypertext Transfer Protocol, „protokół przesyłania dokumentów hipertekstowych”) Protokół transmisji danych w sieci. Jest wykorzystywany głównie do ładowania w przeglądarce stron pobranych z internetu
HTTPS	Protokół HTTPS jest stosowany do szyfrowania i autoryzacji komunikacji między serwerem internetowym a przeglądarką (klientem). Litera S oznacza Secure.
InterNIC, NIC	(Network Information Center) Przydzielanie jednoznacznych na całym świecie adresów komputerów dla internetu. InterNIC to międzynarodowa organizacja. Każdy kraj ma własną jednostkę NIC. Niemieckie NIC znajduje się w Karlsruhe.
IP	(Internet Protocol) Protokół bazowy internetu
IRC chat	(Internet Relay Communication) Forum dyskusyjne „na żywo”
MIME	(MultiMedia) Przykładowo: e-mail w formacie MIME może poza tekstami ASCII zawierać także binarne pliki danych. Nadawca generuje jeden spójny plik wiadomości, który z kolei jest rozpakowywany u odbiorcy
PPP	(Point-to-Point-Protocol) Protokół TCP/IP przez łącze szeregowe (telefoniczne)
SLIP	(Serial Line Internet Protocol) Alternatywny protokół TCP/IP przez łącze szeregowe (telefoniczne)
TELNET	Połączenie terminalowe z odległym komputerem w sieci
URL	(Unified Resource Locator) Element z języka HTML. Za pomocą URL można zaadresować grafikę, program lub plik na dowolnym komputerze w internecie
WAIS	(Wide Area Information Service) Wyszukiwanie informacji w internecie w indeksowanych bazach danych
WWW	(World Wide Web) System informacyjny w internecie bazujący na języku HTML

Za pomocą URL (URL: Unified Resource Locator) można kopiować pliki różnych formatów i/lub wyświetlać je w przeglądarce. URL składa się z protokołu, nazwy komputera, katalogu i pliku. Najpopularniejsze protokoły to http, ftp, file i mailto.

Przykłady

http	http://www.rittal.pl/index.html	Zostanie wczytany i wyświetlony plik index.html.
ftp	ftp://ftp.rittal.pl/prezentacja.ppt	Plik prezentacja.ppt zostanie skopiowany na dysk twardy.
file	file://C:/EMC_INFO.htm	Zostanie wczytany plik EMC_INFO.htm z lokalnego dysku twardego.
mailto	mailto:nazwisko@rittal.pl	Za pośrednictwem przeglądarki uruchomi się program pocztowy. Zostanie przypisany adres odbiorcy.

Domain Name System (DNS)

W DNS dla wszystkich komputerów w sieci są nadane logiczne nazwy odpowiadające numerycznym adresom sieciowym. Cała przestrzeń adresowa w internecie jest podzielona na domeny (przedziały), które są obsługiwane odpowiednio przez specjalnie do tego przeznaczony komputer, Domain Name Server.

Serwerami nazw są komputery lub programy przetwarzające informacje w ramach struktury hierarchicznej przestrzeni adresowej. Każdy Name Server odpowiada tylko za przypisane

domenie i utrzymuje dodatkowe połączenia z sąsiednimi serwerami nazw. Za pomocą tych zewnętrznych kontaktów może przekazywać informacje do innych serwerów, gdy adresat wiadomości znajduje się w innej domenie.

Serwery nazw przekształcają adresy symboliczne na adresy sieciowe. Interpretacja odbywa się przy tym od prawej do lewej. Skrajnie po prawej stronie znajduje się więc identyfikator najwyższego poziomu. Najczęściej różni się dwuznakowe identyfikatory kraju lub grup użytkowników.

■ Glosariusz

ASHRAE

- Według niemieckiej Wikipedii: American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), jest amerykańskim stowarzyszeniem zawodowym inżynierów ogrzewnictwa, chłodnictwa i klimatyzacji. Siedziba stowarzyszenia mieści się w Atlancie. Założone w 1894 r. jako American Society of Heating and Ventilating Engineers (ASHVE), w 1954 r. zmieniło nazwę na American Society of Heating and Air-Conditioning Engineers (ASHAE). Dzisiejszą nazwę organizacja otrzymała w 1959 r. po połączeniu z American Society of Refrigerating Engineers (ASRE). Podręcznik ASHRAE jest czterotomowym poradnikiem techniki klimatyzacji. Co roku jest wydawany na nowo jeden tom. ASHRAE publikuje także normy i wytyczne w zakresie techniki klimatyzacji, na które powołują się budowlane regulacje prawne.

Bypass

- Według niemieckiej Wikipedii: Bypass (ang. „obejście“, „pomost“) oznacza: Bypass (systemy cyfrowe), potokowość w CPU

CRAC

(Computer Room Air Condition)

- System powietrza obiegowego w centrum danych

Customized Data Center

- Indywidualne rozwiązania centrum danych oparte na standardowej bazie

DCIE

- Data Center Infrastructure Efficiency. DCIE ocenia sprawność zużytej w centrum danych energii w procentach.

DCIM

- Według niemieckiej Wikipedii: Skrót oznaczający: Data Center Infrastructure Management – dyscyplina dotycząca planowania centrów danych Green IT częściowo wspierana przez oprogramowanie.

Dostępność

- Dostępność infrastruktury IT oblicza się w następujący sposób: $\text{Dostępność} = (1 - \text{czas awarii} / \text{czas produkcji} + \text{czas awarii}) \times 100$. System IT jest określany jako dostępny, gdy jest w stanie wykonać zadania, do których został przewidziany. Dostępność jest podawana w procentach i dzieli się na klasy dostępności.

Falownik

- Według niemieckiej Wikipedii: Falownik (także inwerter) to urządzenie elektryczne przekształcające napięcie stałe na napięcie przemienne, czyli prąd stały na prąd zmienny. Wraz z prostownikami i przetwornicami, falowniki tworzą podgrupę przekształtników.

Fotowoltaika

- Według niemieckiej Wikipedii: Dziedzina nauki i techniki zajmująca się bezpośrednim przekształcaniem energii światła, najczęściej światła słonecznego, na energię elektryczną za pomocą ogniw słonecznych (solarnych).

Jednostka wysokości

- Według niemieckiej Wikipedii: Jednostka wysokości, w skrócie U (ang. Unit, w skrócie U lub Rack Unit, w skrócie RU), jest jednostką miary opisującą wysokość urządzenia, którą stosuje się dla obudów elektroniki (ang. rack). Urządzenia o wysokości jednej jednostki są określane jako „1 U”, urządzenia o wysokości dwóch jednostek jako „2 U” itd. 1 U = 1¼ cala = 44,45 mm. Obudowy urządzeń zwymiarowane w jednostkach U są przeznaczone do montażu w tzw. rackach (stojakach montażowych) 19”. Szerokość przednich płyt 19” wynosi 482,6 mm.

IT Infrastructure Library (ITIL)

- Według niemieckiej Wikipedii: IT Infrastructure Library (ITIL) to zbiór zaleceń w formie szeregu publikacji, dotyczących realizacji IT-Service-Management (ITSM), które w międzyczasie stały się de facto standardem w zakresie procesów biznesowych IT. W publikacji opisane zostały procesy niezbędne do użytkowania infrastruktury IT, struktura organizacji i narzędzia. Podstawą koncepcji ITIL jest zdefiniowanie procesów, które powinny funkcjonować w ramach organizacji świadczącej usługi IT dla klientów. Planowanie, dostarczanie, wspieranie i optymalizacja usług informatycznych są przy tym rozpatrywane jako istotne czynniki dla osiągnięcia celów biznesowych przedsiębiorstwa. Treści te są w Niemczech rozwijane i ulepszone przez organizację itSMF Deutschland e. V. , która jednocześnie jest platformą wymiany wiedzy i doświadczeń oraz wspiera ona industrializację IT.

Katalogi ochrony podstawowej IT

- Według niemieckiej Wikipedii: Katalogi ochrony podstawowej IT, IT-Grundschutz-Kataloge (przed 2005 r.: Podręcznik ochrony podstawowej IT, IT-Grundschutzhandbuch) jest zbiorem dokumentów niemieckiego Federalnego Urzędu ds. Bezpieczeństwa Techniki Informatycznej (BSI), poświęconych określaniu i likwidowaniu słabych punktów bezpieczeństwa środowisk IT.

Klimatyzacja precyzyjna

- Funkcjonalność i bezpieczeństwo pracy w odniesieniu do odprowadzania ciepła.

Monitoring

- Tutaj: Monitorowanie, sterowanie i dokumentowanie za pomocą kompleksowego oprogramowania. Według niemieckiej Wikipedii: Słowo *monitoring* jest ogólnym pojęciem definiującym wszelkiego rodzaju bezpośrednie i systematyczne rejestrowanie (protokołowanie) oraz dozorowanie procesu lub procesów za pomocą technicznych środków pomocniczych (na przykład długookresowe EKG) lub innych systemów obserwacji. Jednocześnie regularne, cykliczne przeprowadzanie tych czynności jest centralnym elementem danego programu monitorującego, co umożliwia wyciągnięcie wniosków na drodze porównania wyników. Jedną z funkcji monitoringu polega na dokonywaniu ingerencji w obserwowany proces w przypadku, gdy przybiera on niepożądany przebieg lub gdy przekroczone są określone wartości progowe (patrz też technika regulacji). Dlatego monitoring jest szczególnym typem protokołowania.

MS

- Zasilanie / średnie napięcie

MSHV

- Główna rozdzielnia średniego napięcia

NSHV

- Główna rozdzielnia niskiego napięcia

PDU

- Power Distribution Unit

Power Management System

- System zarządzania energią zapewnia przejrzystość obrazu zużycia oraz dba o jakość energii w centrum danych, a także o dostępność rozdziału mocy. Może on wchodzić w skład systemu DCIM (Data Center Management System). Jednocześnie stanowi podstawę dla optymalizacji zużycia i kosztów energii.

Prostownik

- Według niemieckiej Wikipedii: Prostowniki są stosowane w elektrotechnice i elektronice do przekształcania napięcia przemiennego na napięcie stałe. Wraz z falownikami i przetwornicami tworzą podgrupę przekształtników. W celu stłumienia zmienności, wyprostowane napięcie zwykle poddaje się wygładzaniu.

PUE

- Power Usage Effectiveness. Całkowity pobór prądu przez centrum danych / pobór prądu przez sprzęt IT. Na współczynnik PUE składa się całkowita ilość energii zużytej w centrum danych w stosunku do zużycia energii przez komputery.

Redundancja

- Według Wikipedii: Redundancja, przym. redundantry, (łac. redundare 'przelewać się, być w nadmiarze') oznacza:
 - ogólnie stan nadwyżki w stosunku do tego, co zwykle.
 - redundancja (w technice), obecność funkcjonalnie takich samych lub porównywalnych elementów zasobów technicznych (najczęściej ze względów bezpieczeństwa), gdy nie są one potrzebne do bezzakłócenowej, normalnej pracy.

RiMatrix

- Standardowe i wzajemnie dopasowane komponenty systemowe do montażu, rozbudowy lub przebudowy nowych, istniejących lub stale rozwijających się centrów danych w przedsiębiorstwach. Składa się z prefabrykowanych modułów do montażu w posiadających atest systemu pomieszczeniach bezpieczeństwa, standardowych zamkniętych korytarzach lub kontenerach.

RiMatrix S

- Pierwsze w całości prefabrykowane, produkowane seryjnie centrum danych, wstępnie certyfikowane przez TÜV Rheinland.

Rittal – The System.

- Produkty dostępne jako modułowa, spójna platforma systemowa, która dzięki maksymalnej kompatybilności systemowej znacznie przyspiesza etapy prac, takie jak: projektowanie, montaż, przebudowa i uruchomienie. Jednocześnie zwiększona zostaje efektywność i komfort.

Selektor RiMatrix S

- Narzędzie doboru do indywidualnego projektowania kompletnego centrum danych RiMatrix S. Dostępny na stronie www.rittal.com lub do pobrania jako aplikacja.

TDP

- Thermal Device Power

Tier®

- Stopnie dostępności (Tier). Instytut US Uptime zdefiniował klasy dostępności dla centrów danych, tak zwane Industrie Standards Tier® Classification.

Platforma serwerowa TS 8

- TS 8 jest sercem zoptymalizowanej konstrukcji szaf Rittal. Platforma serwerowa TS 8 poddana została przez Rittal dalszym ulepszeniom w nowoczesnych szafach TS IT.

UPS

- Bezprzerwowe zasilanie prądem. Bezpieczeństwo zasilania elektrycznego w standardowych centrach danych Rittal RiMatrix S zapewnia zintegrowany system UPS. Modułowe zasilanie bezprzerwowe również na zasadzie redundancji n+1 z kompleksową architekturą równoległą.

UV

- Podrozdzielnia

ZUCS

- Zero U-Space Cooling System. Znajduje zastosowanie w klimatyzacji standardowych centrów danych Rittal RiMatrix S. Każdy stojak serwerowy dysponuje własnym wymiennikiem ciepła i wentylatorami w podłodze technicznej. Koncepcja ta nosi nazwę Zero U-Space Cooling System (ZUCS), ponieważ elementy chłodzenia nie zajmują miejsca w szafie. W przypadku awarii jednego ZUCS, klimatyzacja całego modułu nadal funkcjonuje dzięki redundancji n+1.

■ Źródła

Publikacje BITKOM

Bundesverband Informationswirtschaft
Telekommunikation und neue Medien e.V.
(Niemieckie Stowarzyszenie Informatyki,
Telekomunikacji i Nowych Mediów)
Albrechtstraße 10A
10117 Berlin
www.bitkom.org

- *Betriebssicheres Rechenzentrum*
(Bezpieczne w eksploatacji centrum danych)
przewodnik, wersja z grudnia 2013
- Seria publikacji Umwelt & Energie
(Środowisko i energia), tom 2:
Energieeffizienz im Rechenzentrum
(Efektywność energetyczna w centrum danych)
Przewodnik po projektowaniu,
modernizacji i eksploatacji centrów danych

Bundesamt für Sicherheit in der Informationstechnik, BSI (Federalny Urząd ds. Bezpieczeństwa Techniki Informacyjnej)

Godesberger Allee 185 – 189
53175 Bonn
www.bsi.bund.de

- Informacje z internetu
Referat B 23, Dział PR

TÜV Rheinland

TÜV Rheinland AG
Am Grauen Stein
51105 Köln
www.tuv.com
www.tuv.com/consulting

- Informacje z internetu:
Katalog kryteriów do audytu
serwerowni i centrów danych

LEXIKON DER DATENKOMMUNIKATION

(Leksykon transmisji danych)

MITP Verlag GmbH
Königswinterer Str. 418,
D-53227 Bonn

- Klaus Lipinski (wyd.)

LEXIKON DER KOMMUNIKATIONS- UND INFORMATIONSTECHNIK

(Leksykon techniki telekomunikacyjnej i informatycznej)

Hüthig GmbH
Im Weiher 10
D-69121 Heidelberg

- Niels Klaußmann

Bibliothek Microsoft TechNet

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
USA
<http://technet.microsoft.com/de-de/library/bb432646.aspx>

- *Ermitteln der Kosten für die Verfügbarkeit*
(Określanie kosztów dostępności)

Beuth Verlag GmbH

Am DIN-Platz Burggrafenstraße 6
10787 Berlin

- Cytowane normy:
IEC, VDE, DIN

Rittal GmbH & Co. KG

Postfach 1662, 35726 Herborn
Niemcy

Wykłady i publikacje specjalistyczne
(Whitepaper)

- Nowoczesne infrastruktury w centrum danych (przegląd potrzeb średnich przedsiębiorstw, Bernd Hanstein)
- Centrum danych przyszłości (Bernd Hanstein)
- Wyzwanie: centrum danych
- Efektywna energetycznie klimatyzacja IT (Daniel Luther)
- Rozdział mocy w centrum danych
- Zabezpieczenie energii w centrum danych za pomocą modułowych systemów UPS (Jörg Kreiling)
- Sieć czujników do monitorowania szaf i pomieszczeń
- RiZone – oprogramowanie zarządzające Rittal dla infrastruktury IT (Bernd Hanstein, Markus Schmidt, Thorsten Weller)
- Systemy gaszenia w centrum danych (Alexander Wickel)

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

TS IT – zintegrowana wartość dodana

1 Indywidualne zastosowanie

Podstawa dla prawie wszystkich wymagań w technologii sieciowej i serwerowej.

2 Wysoka obciążalność i elastyczna zabudowa

Obciążalność do 1500 kg przy beznarzędziowej regulacji odległości 19" płaszczyzn montażowych.

Łatwa realizacja alternatywnych wymiarów zabudowy dzięki bocznemu przesunięciu (możliwe 21", 23", 24").

3 Beznarzędziowy montaż

Montaż akcesoriów systemowych za pomocą nowej i szybkiej technologii Snap-In (m.in. półek urządzeńowych, kanałów kablowych i wielu innych).

4 Przemysłane zarządzanie okablowaniem

Wielofunkcyjny dach do bocznego wprowadzania kabli, zapewniający maksymalny komfort i swobodny dopływ powietrza do aktywnych komponentów.

5 Szybki montaż ściany bocznej

Dzielona ściana boczna z szybkim zamknięciem i zintegrowanym zamkiem z dodatkową blokadą wewnętrzną.

6 Nowa koncepcja drzwi

Drzwi przeszklone do wysokowydajnych zastosowań serwerowych z klimatyzacją LCP lub drzwi wentylowane do klimatyzowanych pomieszczeń.

7 Dzielone drzwi tylne

Dzielone drzwi tylne od wysokości 1800 mm do optymalnego ustawienia.

8 Inteligentne akcesoria

Łatwy i szybki wybór akcesoriów systemowych dzięki nowej koncepcji TS IT.

9 Zintegrowana wartość dodana w systemie 19"

Bezpośredni i oszczędzający powierzchnię, beznarzędziowy montaż zatrzaskowy nowej szyny prądowej Rittal PDU z tyłu, w przestrzeni Zero-U Beznarzędziowa integracja zarządzania okablowaniem i Dynamic Rack Control z przodu.

10 Prosty montaż

Oznakowanie jednostek wysokości i siatka wymiarowa głębokości do łatwej regulacji odległości 19" płaszczyzn.

Dotychczas ukazały się:

1

2013

Budowa rozdzielnic i sterownic zgodnie z normą

Zastosowanie EN 61 439

2

2013

Chłodzenie szaf sterowniczych i procesów

3

2013

Szafy sterownicze – wiedza ekspertów

4

2014

Świat infrastruktury IT

Informacje ogólne i podstawy podejmowania decyzji

Rittal – The System.

Faster – better – everywhere.

- Szafy sterownicze
- Rozdział mocy
- Klimatyzacja
- Infrastruktura IT
- Software & Services

Rittal Sp. z o.o.
ul. Domaniewska 49 · 02-672 Warszawa
Tel.: (0 22) 310 06 00 · Fax: (0 22) 310 06 16
rittal@rittal.pl · www.rittal.pl



FRIEDHELM LOH GROUP