Rittal – The System.

Faster – better – everywhere.

Whitepaper
Bezpieczeństwo fizyczne w technologiach IT i centrach danych

Bernd Hanstein

Spis treści

Autor: Bernd Hanstein

Po ukończeniu studiów dyplomowych z fizyki na Uniwersytecie Justusa Liebiga w Gießen w roku 1987, Bernd Hanstein pracował w centralnym dziale badawczym Siemens AG w zakresie metod testowania układów zintegrowanych. Następnie z różnych stanowisk odpowiadał w Siemens AG w obszarze sieci publicznych za implementację dużych projektów ICT. Po przejściu do Siemens VDO Automotive w roku 2002, Bernd Hanstein jako główny szef działu był odpowiedzialny za globalne testy systemu urządzeń multimedialnych do samochodów. Od 2007 roku jest szefem działu zarządzania produktami IT w Rittal w Herborn. Do głównych obszarów jego działalności należą: komponenty IT, rozwiązania systemowe RiMatrix i technologia centrów danych.

Wykaz ilustracji

Wykaz tabel

Streszczenie

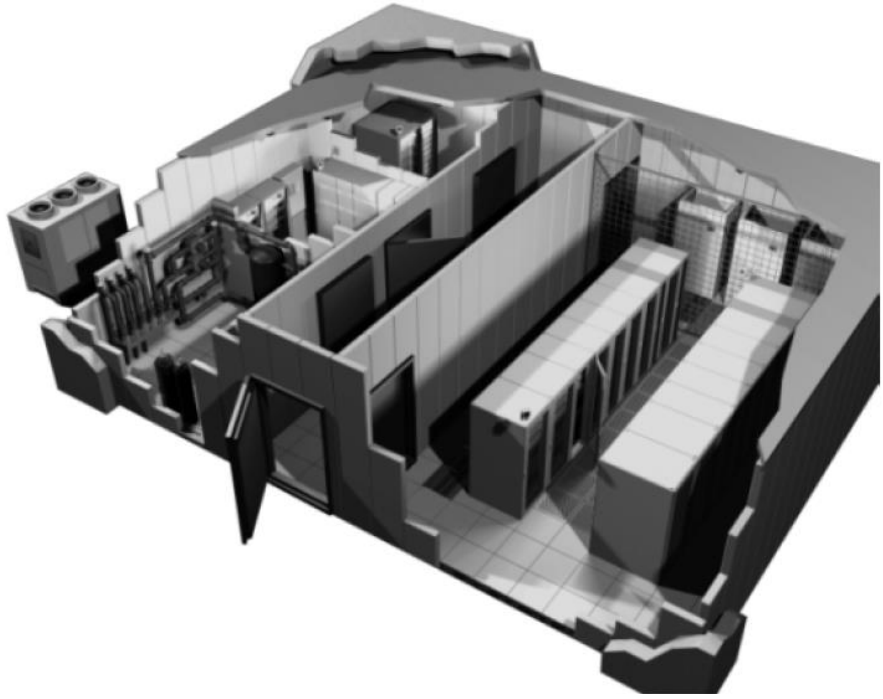
Centra danych stanowią kluczową technologię w coraz bardziej zdigitalizowanym świecie. Zawierają one systemy serwerowe, systemy pamięci masowej oraz komponenty sieciowe, których zadaniem jest udostępnienie aplikacji z gwarantowaną dostępnością i wymaganą wydajnością. Podobne znaczenie ma również fizyczna infrastruktura, która dostarcza do tych komponentów zasilanie elektryczne i chłodzenie oraz zapewnia kontrolę wszystkich parametrów eksploatacji.

Coraz większe znaczenie mają wszystkie aspekty dotyczące tematu bezpieczeństwa. Na początku są to znane rozwiązania na obszarze systemów antywirusowych czy firewalli, lecz również ochrona przed zagrożeniem fizycznym wymaga coraz większej uwagi. Chodzi tu nie tylko o zapobieganie konkretnym zagrożeniom, takim jak włamanie czy kradzież, ale również o zabezpieczenie przed podsłuchem urządzeń komputerowych z wykorzystaniem ich sygnału elektromagnetycznego i „tradycyjne“ zagrożenia ze strony ognia, dymu, wody oraz pyłu, wymieniając tylko te najważniejsze.

Niniejszy raport naświetla poszczególne scenariusze zagrożeń i pokazuje, jakie środki i działania mogą zapobiegać zagrożeniom fizycznym.

Wprowadzenie

Technologia komputerowa stanowi jeden z fundamentów nowoczesnego społeczeństwa. Nie ma takiego obszaru, który nie wykorzystywałby komputerów oraz komunikacji poprzez sieć. Usługi te bez względu na to, czy są widoczne dla użytkownika, czy pracują niezauważalnie w tle, wymagają mocy obliczeniowej i infrastruktury sieciowej. Zasoby te są udostępniane fizycznie z centrów przetwarzania danych z zastosowaniem sprzętu i jego oprogramowania w odpowiednim środowisku, wyposażonym w klimatyzację, zasilanie napięciem elektrycznym oraz łącza sieciowe – pomimo wirtualizacji. Centra danych powinny ponadto zapewniać bezpieczeństwo przed zagrożeniami takimi jak ogień, woda, włamanie czy kradzież. Ochrona ta staje się coraz ważniejsza wraz z postępującą cyfryzacją.



Rysunek 1. Prezentacja fizycznej infrastruktury centrów danych

Zabezpieczenie serwerowni przed zagrożeniem fizycznym należy rozpocząć na wielu płaszczyznach, ponieważ zagrożenia przychodzą z różnych stron. Podstawowy katalog bezpieczeństwa Federalnego Urzędu Bezpieczeństwa i Techniki Informacji (BSI) wyszczególnia 27 zagrożeń dla centrów danych [ref. 1], od siły wyższej poprzez nieprawidłowości organizacyjne, awarie techniczne aż po umyślne działanie człowieka.

Przeciwdziałają temu sprawdzone koncepcje z obszaru bezpieczeństwa IT, które dopasowano do określonych zagrożeń. Przed ogniem chronią np.: ściany ognioodporne, a zastosowane w nich przepusty kablowe również są w stanie wystarczająco długo powstrzymywać ogień. O wiele większy problem stanowi para wodna, którą w wyższych temperaturach oddaje beton na skutek pozostałej wilgoci w sieci krystalicznej. W tym przypadku stosuje się grodzie parowe i okładziny termiczne. W celu zapewnienia niezawodnej ochrony zasobów serwerowni należy podczas jej planowania, wyposażania i budowy uwzględnić szereg ważnych aspektów. Oczywiście dotyczy to nie tylko pomieszczeń murowanych, lecz modułowych rozwiązań serwerowni, które oferuje firma Rittal, poprzez zastosowanie pomieszczeń z podstawowym

stopniem ochrony oraz pomieszczeń o wysokiej dostępności i bezpiecznych rozwiązań typu Micro Data Center.

O ile kiedyś kilka dni przestoju z powodu awarii były w zupełności do zaakceptowania, to coraz większa zależność gospodarki od systemów komputerowych doprowadziła do znacznie surowszych wymagań. Uzasadnienie jest proste: awarie systemów IT wiążą się z wysokimi kosztami w przypadku każdej branży. Tylko w średniej wielkości przedsiębiorstwach awarie w obszarze krytycznych procesów IT generują koszty dochodzące do 380 000 euro rocznie. Wynika to z badań rynkowych przedsiębiorstwa Techconsult [ref.2], które przeprowadziło w roku 2013 ankietę w 300 przedsiębiorstwach zatrudniających od 200 do 4 999 pracowników. Ankieta przeprowadzona przez EMC [ref. 3] pokazuje straty danych lub awarie w ciągu ostatnich dwunastu miesięcy w 56 procentach przedsiębiorstw na terenie Niemiec.

Jeżeli chodzi o ochronę złożonych systemów, to wymagane jest podejście całościowe. Centrum przetwarzania danych składa się z wielu aktywnych obszarów: klimatyzacja, zasilanie energią elektryczną i jej rozdział, połączenia sieciowe, kontrola dostępu oraz powłoka fizyczna zaprojektowana jako konwencjonalne pomieszczenie lub modułowy system „pomieszczenie w pomieszczeniu”. Nie chodzi tu tylko o ognioodporność czy wodoszczelność poszczególnych komponentów, lecz o to, żeby cały system spełniał te wymagania. To użytkownicy są odpowiedzialni za dokładne sprawdzenie certyfikacji i gwarancji. Tylko w ten sposób można stwierdzić, że działanie ochronne funkcjonuje w odniesieniu do całości, a nie wyłącznie w przypadku poszczególnych elementów. Dlatego zatwierdzona kontrola całego systemu ma większe znaczenie dla bezpieczeństwa niż szereg pojedynczych kontroli poszczególnych komponentów.

Klimatyzacja, zasilanie elektryczne, łącza danych – wszystkie te komponenty należy optymalnie zintegrować z koncepcją serwerowni oraz uwzględnić administrowanie nimi za pomocą systemu zarządzania centrum danych. Firma Rittal, na takich obszarach jak klimatyzacja, technologia szaf 19” czy rozwiązania data center, oferuje odrębne raporty „Whitepaper”, które obszernie opisują te tematy.

Metody testowania i instytucje kontroli

Nawet jeżeli pojawi się kompletna oferta certyfikacji serwerowni, to i tak należy poddać kontroli jej poszczególne obszary funkcjonalne. Ochrona przeciwpożarowa, zabezpieczenie przed wodą oraz pyłem i dymem należy potwierdzić poszczególnymi weryfikacjami dla każdego obszaru. Zastosowanie znajdują tu międzynarodowe standardy, na straży których stoją instytucje, jak np. Niemiecki Instytut Norm (DIN), Normy Europejskie (EN), Europejska Komisja Certyfikacyjna European Certification Body GmbH (ECB) oraz Międzynarodowa Organizacja Standaryzacji (ISO).

Zaleta zastosowania wielu norm w ramach indywidualnej umowy polega na tym, że z góry można zapobiec sporom prawnym, ponieważ normy wyrażają jednoznaczne stanowisko. Zgodnie z prawem konsumenta i umowami o świadczeniu usług, jeżeli pojawiają się wady rzeczowe, to dowód przemawia wedle wszelkiego prawdopodobieństwa za użytkownikiem normy w tym sensie, że dołożył on wszelkich wymaganych starań. Może on również na tej podstawie odrzucić zarzut o niedbalstwo.

Również sami producenci mogą, o ile posiadają akredytację na danym obszarze, przeprowadzać testy np.: stopnia ochrony.

Wielu użytkowników uważa dzisiaj w szczególności European Certification Body GmbH (ECB) za znaczącą jednostkę w zakresie certyfikacji dla centrów przetwarzania danych. Jest to neutralna, akredytowana instytucja certyfikująca zgodnie z ISO/IEC 17065 [ref. 4]. Wydaje ona certyfikaty ECB•S dla produktów dotyczących bezpieczeństwa. Certyfikacja ECB•S przez European Security Systems Association (ESSA) e.V opiera się wyłącznie na wymaganiach norm europejskich i jest uznana na całym świecie. Każdy produkt zostaje odrębnie zarejestrowany i może podlegać w każdej chwili niezapowiedzianej, produkcyjno-technicznej kontroli jakości. W branży ubezpieczeniowej certyfikacja jest niezawodną i obiektywną podstawą do kalkulacji ryzyka oraz związanej z tym klasyfikacji w zakresie bezpieczeństwa technicznego. Pomieszczenie wysokiej dostępności firmy Rittal dysponuje np.: certyfikacją ECB•S.


CERTIFICATE

ECB·S

Rittal GmbH & Co. KG

E C B • S

Rysunek 2. Certyfikat ECB•S dla Rittal

Największe fizyczne zagrożenia dla serwerowni stanowią ogień, woda, pył oraz gazy pożarowe i obciążenie gruzem, zakłócenia elektromagnetyczne (kompatybilność elektromagnetyczna), a także dostęp osób nieupoważnionych. Dla każdego z tych zagrożeń istnieje jedna lub wiele norm, których należy przestrzegać. Jednym z wymagań jest określona ognioodporność ścian, np.: F90 czy F120 zgodnie z normą DIN 4102 lub EI 90 czy EI 120 zgodnie z normą EN 1363 [ref. 8]. Ściana taka spełnia swoją funkcję w przypadku pożaru

przez 90 czy 120 minut. Celem tej klasyfikacji jest ochrona ludzkiego życia, a nie serwerowni. Jeżeli wyposażenie IT ma znaleźć się w centrum zainteresowania kwestii bezpieczeństwa, to nie tylko ściana, lecz również serwerownia jako całość powinna wytrzymać napór ognia.

BSI wymaga również kontroli całego systemu w przypadku pomieszczeń IT. Tak więc, działanie 1.6 „Przestrzeganie przepisów przeciwpożarowych" [ref. 5] wymaga bezwzględnego przestrzegania obowiązujących przepisów przeciwpożarowych zgodnie z DIN 4102 „Łatwopalność materiałów i elementów budowlanych" [ref. 6] i MBO, LBO, MLAR oraz wytycznych Inspekcji Budowlanej. W przypadku pomieszczeń, w których przechowuje się ważne urządzenia IT oraz nośniki danych (serwery, archiwizacja danych itp.) należy oprócz tego zastosować część 2. normy EN 1047 [ref. 7].

Szczegółowe rozważania dotyczące zagrożeń fizycznych

Ogień

Ogień jest uznany przez administratorów za największe zagrożenie dla serwerowni. Niewielki pożar może wskutek wydzielania gazów agresywnych wyrządzić wielkie szkody w wyposażeniu IT oraz infrastrukturze. Dlatego kontrola ognioodporności jest bardzo szczegółowa. Już na potrzeby samej kontroli elementów budowalnych F 90/EL90 zgodnie z normą DIN 4102 / EN1363 [ref. 6, ref. 8] poszczególne elementy, takie jak ściany, drzwi czy materiały budowlane, poddawane są działaniu płomieni zgodnie z jednolitą krzywą temperatury. Czas kontroli wynosi 90 minut w temperaturze powyżej 1 100°C. W tym przypadku temperatura po stronie przeciwnej do pożaru może wzrosnąć jedynie o 140 kelwinów (K) (punktowo 180 K). Podczas tego testu nie mierzy się względnej wilgotności powietrza. Jednak może ona w zależności od materiału już po krótkim czasie wzrosnąć do 100%, co spowodowałoby zagrożenie dla serwerów i infrastruktury.

Certyfikowaną ochronę zapewnia wyłącznie kontrola systemu, podczas której kompletna serwerownia wraz ze wszystkimi komponentami, włącznie z drzwiami oraz grodzami kablowymi i rurowymi jest testowana w warunkach podobnych do rzeczywistego przypadku zagrożenia. Kontrola systemu zgodnie z EN 1047-2 [ref. 7] wymaga na przykład 60 minut działania płomienia. Następnie stosuje się 24-godzinny okres schładzania w zamkniętym piecu. Czas ten określa się jako czas dogrzewania. Obiekt kontroli pozostaje w komorze pieca do momentu gdy po kilku godzinach osiągnie najwyższą temperaturę wewnętrzną. Szczególną uwagę należy zwrócić na słabe punkty konstrukcji budowlanej, takie jak drzwi, elementy nośne drzwi oraz systemy przepustowe rur i okablowania. Żeby zdać egzamin, temperatura wewnątrz nie może wzrosnąć o więcej niż 50 K ponad temperaturę zewnętrzną i – tak samo ważne – względna wilgotność powietrza nie może przekroczyć 85%. Produkty, które przeszły pozytywnie ten i inne testy zgodnie z wymaganiami normy EN 1047-2 zostaną zarejestrowane w bazie danych ECB•S. Nawet jeżeli w normie 4102 [ref. 6] i EN 1363 [ref. 8] opisano głównie testy materiałów, to na podstawie tych norm można sprawdzać kompletne rozwiązania, takie jak sejfy i pomieszczenia bezpieczeństwa.

Gazy korozyjne i dym

Szczelność gazowa i dymowa jest kluczowym wymaganiem, które muszą spełnić serwerownie. Współczynnik szczelności jest bardzo ważny, jeżeli nie chcemy dopuścić do rozprzestrzenienia się pożaru na inne części budynku. Pożarów w środowisku IT nie gasi się wodą, lecz np.: za pomocą gazów obojętnych lub poprzez zastosowanie redukcji tlenu w otoczeniu. Rozwiązania te funkcjonują niezawodnie pod warunkiem, że gazy pozostają w pomieszczeniu i nie wychodzą przez nieszczelności na zewnątrz – do pozostałej części budynku. Również gaszenie pożaru przez redukcję tlenu nie powiedzie się, jeżeli przez drzwi, okna lub na skutek wad budowlanych do pomieszczenia zostanie zassane świeże powietrze. Jeżeli pożar wybuchnie poza serwerownią, to dobre uszczelnienie również spełni swoje zadanie. Ponadto należy chronić komponenty IT w serwerowni przed działaniem gazów agresywnych, ponieważ na skutek ich działania płyty serwerów, przełączników oraz innego sprzętu mogą korodować.

Właściwe normy dotyczące certyfikacji to DIN 18095 [ref. 9] oraz EN 1634 [ref. 10]. Część trzecia normy EN 1634 ustala metodę kontroli i związane z nią warunki kontroli w celu określenia wycieków zimnego i gorącego dymu z jednej strony zamknięcia na drugą. Mierzy się tak zwany stopnień przecieku dla każdego badanego warunku testu. W związku z serwerowniami testuje się z reguły drzwi oraz odciążające przepusty ciśnieniowe, ponieważ stanowią one zazwyczaj jedyne ruchome przepusty do wnętrza pomieszczenia. Ogień powoduje wzrost ciśnienia po stronie zadymienia do 50 paskali (Pa). Różnica ciśnienia po obu stronach powoduje wydostawanie się gazu przez wszystkie istniejące szczeliny oraz otwory. Drzwi, które spełniają swoje zadanie jako część systemu przeciwpożarowego muszą zatrzymać skutecznie strumień dymu, żeby zapewnić właściwe warunki po drugiej stronie.

Test odbywa się w komorze kontrolnej, w której z przodu montuje się obiekt kontroli. Właściwe ciśnienie zapewniają dmuchawy. System nagrzewania wytwarza temperaturę około 200°C, zbliżoną do temperatury dymu. Szczeliny uwarunkowane konstrukcją, na przykład przy progach lub pomiędzy skrzydłami drzwi, zostają zmierzone i zarejestrowane. Również automatyczne mechanizmy zamykania są sprawdzone przed testem i użyte kilka razy. Ten krótki test nie zastępuje jednak testów ciągłych mechanizmów. Jego zadaniem jest jedynie ustalenie, czy drzwi zamykają się prawidłowo.

Właściwą kontrolę dymoszczelności przeprowadza się z wykorzystaniem różnych poziomów ciśnienia do 50 Pa oraz w temperaturze otoczenia 20°C i 200°C. Obiekty kontroli, które pozytywnie przejdą test nie mogą przekroczyć zdefiniowanego w normie stopnia wymiany powietrza pomiędzy obszarem wewnętrznym i zewnętrznym. Ważne jest również sprawdzenie w trakcie testu, czy (i które) elementy drzwi zostały zniekształcone wskutek działania wysokiej temperatury i czy drzwi można otworzyć po zakończeniu testu.

Obciążenie gruzem

Należy również rozważyć zagrożenia spowodowane zawaleniem stropu. Siły związane z uderzeniem stropu mogą spowodować znaczne zniszczenia sprzętu i infrastruktury. Oprócz testów pożarowych pomieszczeń bezpieczeństwa oraz sejfów bezpieczeństwa, normy definiują testy mechaniczne i udarowe.

Norma EN 1047-2 [ref. 7.] opisuje testy mechaniczne dla pomieszczeń o wysokiej dostępności. Kontrolę tę przeprowadza się po 45 minutach oddziaływania płomieni. Również norma DIN 4102 zawiera wytyczne dotyczące testów mechanicznych. W tym przypadku ściana ognioodporna po obciążeniu płomieniem (test ognioodporności zgodnie z normą DIN 4102 ETK [ref. 6]) musi wytrzymać określone obciążenie udarowe. Jeżeli dana ściana jest ścianą nośną, to przedmiot kontrolowany musi przenieść dodatkowe obciążenie.

Wytrzymałość mechaniczną definiuje niezależnie norma EN 50 102 [ref. 11]. Zastosowanie znajduje tu więc klasyfikacja wytrzymałości mechanicznej IK, która określa ochronę na skutek obciążenia mechanicznego. Właściwa norma produktu reguluje sposób przeprowadzenia testu. Dla każdej powierzchni wykonuje się pięć obciążeń (rozmieszczonych równomiernie, wahadłowo lub na zasadzie swobodnego spadku). Przedmiot kontrolowany należy w tym przypadku zamontować na sztywnej ramie, tak żeby stawiał opór. Dotyczy to również wyeksponowanych miejsc, takich jak zawiasy i zamki. Po przeprowadzonej kontroli element kontrolowany musi być w pełni sprawny i nie może powodować zmniejszenia stopnia ochrony.

Stopnie ochrony IP: ochrona przed pyłem, wodą, cząstkami stałymi

Pył rzadko uznaje się za zagrożenie fizyczne i w typowym otoczeniu biurowym w Niemczech praktycznie nigdy nie powoduje on problemów dla IT. Inaczej wygląda to w halach produkcyjnych, w których zapylenie występuje w znacznym stopniu i nie można go usunąć całkowicie przez odciągi. Również i w tym środowisku muszą funkcjonować systemy IT i nie mogą być wystawione na działanie pyłu bez zabezpieczeń. Natomiast woda jest całkowicie oczywistym zagrożeniem dla urządzeń IT, które każdy może wskazać. W przypadku zastosowań outdoor wyposażenie IT nie może być ani narażone na zalanie, ani też być w wilgotnym otoczeniu. Awarie spowodowane wodą na skutek pęknięcia rury czy podobnych zdarzeń nie mogą pozostawić uszczerbku. W zależności od celu zastosowania oraz obiektu, ochrona jest zróżnicowana i definiuje się ją za pomocą tak zwanych stopni ochrony IP zgodnie z normą EN 60 529 [ref. 12]. Testy zgodnie z EN 60 529 klasyfikują ochronę elektrycznych środków eksploatacji do napięcia zasilania 72,5 kV za pomocą obudowy, osłony lub podobnych rozwiązań.

Stopnie ochrony IP (IP = International Protection) zawierają prostą kombinację liczb, określającą czynniki, przed którymi obudowa ma chronić swoją zawartość. Generalnie należy chronić osoby przed dostępem do części niebezpiecznych, znajdujących się w obudowie. Należy również zabezpieczyć środek eksploatacji wewnątrz obudowy przed możliwością przedostania się stałych ciał obcych oraz wody. Niebezpieczne są w tym przypadku części aktywne, które mogą spowodować porażenie elektryczne oraz części mechaniczne, których dotknięcie również może okazać się niebezpieczne.

Stopień ochrony podaje się za pomocą zapisu w formie IP XY. Pierwsza cyfra charakterystyczna zaczyna się od zera i kończy na 6, przy czym wyższa cyfra charakterystyczna obejmuje w każdym przypadku wszystkie cechy niższych cyfr. Definiują one ochronę przed ciałami stałymi oraz pyłem.

Kod	**Cecha ochrony**
IP 1x	Ochrona przed stałymi ciałami obcymi o średnicy 50 mm i większej
IP 2x	Ochrona przed stałymi ciałami obcymi o średnicy 12,5 mm i większej
IP 3x	Ochrona przed stałymi ciałami obcymi o średnicy 2,5 mm i większej
IP 4x	Ochrona przed stałymi ciałami obcymi o średnicy 1,0 mm i większej
IP 5x	Ochrona przed pyłem
IP 6x	Pyłoszczelność

Tabela 1: Systematyka IP – ochrona przed pyłem i ciałami stałymi

Cyfra druga oznacza ochronę przed wodą. Występują tu cyfry od 0 do 8, do cyfry 6 obowiązuje taki mechanizm, jak w przypadku pierwszych cyfr.

Kod	Cecha ochrony
IP x1	Ochrona przed pionowo padającymi kroplami wody
IP x2	Ochrona przed pionowo padającymi kroplami wody, obudowa pochylona o 15°
IP x3	Ochrona przed natryskiwaniem wodą pod dowolnym kątem od 60° do pionu z każdej strony
IP x4	Ochrona przed bryzgami wody z dowolnego kierunku
IP x5	Ochrona przed strumieniem wody z dowolnej strony
IP x6	Ochrona przed silnym strumieniem wody z dowolnej strony
IP x7	Ochrona przed skutkami krótkotrwałego zanurzenia w wodzie przy ciśnieniu rozpatrywanym oraz warunkach określonego czasu
IP x8	Trwałe zanurzenie w wodzie

Tabela 2: Systematyka IP – ochrona przed wodą

W Niemczech w większości przypadków kontrole przeprowadza TÜV i VDE. Ponadto testami stopnia ochrony zajmują się laboratoria kontroli producentów różnych produktów. Laboratorium kontroli jakości firmy Rittal jest akredytowane przez DAKKS oraz UL również w zakresie stopni ochrony. Oprócz testów stopnia ochrony IP zgodnie z normą EN, firma Rittal przeprowadza również kontrole stopni ochrony zgodnie z przepisami UL i NEMA, które mają duże znaczenie na rynku amerykańskim.

Rysunek 3. Kontrola stopnia ochrony IP

Sprawdza się krótkotrwałe, a nie ciągłe obciążenie, tak jak to bywa w przypadku godzinnych lub trwających wiele dni opadów. Dlatego wysoki stopień ochrony nie oznacza możliwości zastosowania urządzenia na wolnym powietrzu. W przypadku testów dotyczących przenikania ciał obcych lub pyłu sprawdza się najpierw za pomocą obiektów o zdefiniowanej wielkości możliwość ich przeniknięcia do wnętrza przedmiotu. Dla testów powyżej IP 5x stosuje się komorę pyłową z możliwością wytwarzania podciśnienia lub bez niej. Środkiem testowym jest puder talku, który można łatwo wykryć na powierzchniach. W przypadku stopnia ochrony IP 5x pył może przedostać się do urządzenia wyłącznie w takich ilościach, które umożliwią prawidłowe funkcjonowanie urządzenia i nie wpłynie to na jego bezpieczeństwo. Wartość maksymalna zgodnie z DIN EN 62208 [Ref. 13] wynosi gram na metr kwadratowy powierzchni. Dla stopnia ochrony IP 6x do wnętrza nie może przedostać się żadna ilość pyłu.

Do testów z cieczą stosuje się skraplacze, rury wychyłowe oraz natryski o różnych średnicach dysz. Dla IP x7 używa się zbiorników zanurzeniowych. Wszystkie testy mają ten sam cel: woda nie może spowodować uszkodzeń.

Ochrona przed niepowołanym dostępem

W normalnym przypadku serwerownie powinny być chronione wewnątrz budynków przed możliwością przedostania się do nich osób nieupoważnionych, pomimo że osoby te muszą pokonać wszystkie inne trudności, takie jak bramki, recepcja, kamery oraz czujność pracowników. Mimo wszystko istotne jest zabezpieczenie przed możliwością włamania do pomieszczenia, które zawiera drogi sprzęt komputerowy oraz ważne dane. Jak dobre jest to zabezpieczenie, podaje norma Resistance Class (RC). Normę RC definiuje DIN V ENV 16 27 ff [ref. 14]. Ingerencja przy użyciu narzędzi odbywa się analogicznie do normy DIN EN 1630/ 2011-09 [ref. 15] i wykorzystuje sześciostopniowy system klasyfikacji.

Rozróżnienia dokonano na podstawie zdolności sprawcy oraz jego wyposażenia w środki pomocy. Zakres kształtuje się od niedoświadczonego sprawcy/wandalizmu bez narzędzi po doświadczonego, bardzo zmotywowanego sprawcę, który dysponuje całym zbiorem przydatnych narzędzi elektrycznych. Występuje przy tym wytyczna czasu, w którym element kontrolowany musi wytrzymać próbę włamania, żeby zaliczyć test.

Dla kategorii RC 1 komponenty wykazują ograniczoną lub niską ochronę podstawową przed próbami włamania z użyciem siły fizycznej z zastosowaniem takich czynności jak: nacisk, naskok, uderzenie ramieniem, podniesienie i wyrwanie. Ponadto przeprowadza się trzyminutowy, nieniszczący test manipulacji za pomocą małych narzędzi w celu demontażu komponentów, które umożliwiają odkręcenie z zewnątrz. Czas trwania ingerencji odnosi się do każdego punktu ingerencji. Jeżeli na przykład sprawdza się kompletny sejf bezpieczeństwa, to występuje tu wiele punktów ingerencji, takich jak drzwi od strony zawiasów, drzwi od strony zamka oraz prowadnice kablowe. Czas całkowity wynika z sumy wszystkich punktów ingerencji. Pozostałe kategorie przedstawia poniższa tabela.

Kod	**Czas trwania**	**Doświadczenie**	**Opis / środek pomocniczy**
RC 2	3 min	Sprawca przypadkowy	Proste narzędzia: śrubokręt, obcęgi i klin
RC 3	5 min	Sprawca rutynowy	Dodatkowo: dwa śrubokręty i dłuto
RC 4	10 min	Sprawca doświadczony	Dodatkowo: narzędzia do cięcia i narzędzia udarowe, np.: siekiera, dłuto, młotek i łyżka ślusarska oraz wiertarka akumulatorowa.
RC 5/ RC6	10 min	Sprawca doświadczony	Dodatkowo: dodatkowe narzędzia pod ręką wraz z wiertarką, piła wzdłużna lub szablowa, szlifierka kątowa o średnicy tarczy 250 mm.

Tabela 3: Systematyka RC – Ochrona przed dostępem osób nieupoważnionych

Ochrona EMC

Pola elektromagnetyczne stanowią nieunikniony skutek przepływu prądu. Emitowana energia, nazywana promieniowaniem elektromagnetycznym, jest niepożądana, a nawet szkodliwa. Silne pola elektromagnetyczne mogą mieć negatywny wpływ na inne urządzenia elektryczne i umożliwiać uzyskiwanie informacji przez osoby nieupoważnione.

Pomieszczenia bezpieczeństwa IT chronią – o ile zostały właściwie zaplanowane i zbudowane – sprzęt oraz informacje przed negatywnymi skutkami promieniowania elektromagnetycznego. Kompatybilność elektromagnetyczna opisuje, w jaki sposób można chronić urządzenia przed zakłóceniami z innych urządzeń. W tym celu należy zastosować odpowiednie środki.

Pomieszczenie bezpieczeństwa w podstawowym zakresie nie zapewnia całościowo zdefiniowanej ochrony. W przypadku kompatybilności elektromagnetycznej chodzi również o to, żeby zatrzymać promieniowanie elektromagnetyczne, z wykorzystaniem którego osoby nieupoważnione mogłyby uzyskać wartościowe i poufne informacje. Pomieszczenia bezpieczeństwa firmy Rittal mają podstawowy zakres kompatybilności elektromagnetycznej (EMC), który można zwiększyć za pomocą dalszych środków konstrukcyjnych. Poniższa tabela zawiera przegląd istotnych norm.

Obszar zastosowania	**Emisja zakłóceń**	**Odporność na zakłócenia**
Urządzenia informatyczne	EN 55022 (P)	EN 55024 (P)
Obszar mieszkalny	EN 61000-6-3 (FG)	EN 61000-6-1 (FG)
Instalacje przemysłowe	EN 61000-6-4 (FG)	EN 61000-6-2 (FG)
Transmisja sygnału na sieci niskiego napięcia	EN 50065-1 (P)	EN 61000-6-2 (FG)
Urządzenia oświetlenia	EN 55015 (P)	EN 61000-6-2 (FG)

Tabela 4: Podstawowe normy techniczne kompatybilności elektromagnetycznej dla produktów, rodzin produktów

Normy kompatybilności elektromagnetycznej dla produktów oraz obszarów otoczenia zawierają wartości graniczne emisji zakłóceń w zdefiniowanych zakresach częstotliwości i natężenia pól, np.: w normie DIN EN 55022 (VDE 0878-22):2011-12 [ref. 16].

System utworzony na podstawie tych wartości granicznych oraz opisana klasyfikacja wymagań w normie DIN EN 55024 (VDE 0878-24):2011-09 [ref. 17] dotyczą odporności urządzeń informatycznych na zakłócenia oraz zapewniają odporność na zakłócenia elektromagnetyczne pomiędzy urządzeniami wszelkiego typu i urządzeniami IT podczas codziennej eksploatacji.

Zakres zastosowania / kontrola	**Norma**
Pomieszczenia absorpcyjne, część 1: Pomiar tłumienności ekranu	EN 50147-1 : 1996
Norma IEEE dotycząca metod pomiaru skuteczności ekranowania obudów	IEEE Std 299-1997

Tabela 5: Normy kontroli kompatybilności elektromagnetycznej EMC (dla osłon pomieszczeń)

Właściwości odporności elektromagnetycznej dla pomieszczeń bezpieczeństwa IT muszą spełnić dwa zadania. Po pierwsze muszą zapobiec ingerencji zamierzonego lub niezamierzonego promieniowania elektromagnetycznego w urządzenia IT. Po drugie muszą zapobiec wypłynięciu poufnych informacji z urządzeń IT. Działanie osłaniające obudów urządzeń oraz szaf, w których zostały umieszczone urządzenia, można istotnie zwiększyć poprzez zastosowanie dodatkowego ekranowania pomieszczenia. W tym zakresie nie istnieją jednak żadne normatywne wytyczne.

Rysunek 4. Kontrola kompatybilności elektromagnetycznej (EMC)

Również i tu idealna byłaby bezszczelinowa, elektrycznie przewodząca powłoka, która nie wpuszcza i nie wypuszcza sygnałów elektromagnetycznych. W praktyce jest to niemożliwe, ponieważ zabezpieczone pomieszczenia IT oraz rozwiązania sejfowe składają się z segmentów ścian wykonanych z blachy stalowej, które poprzez płaskie, przewodzące połączenia tworzą bezszczelinową, przewodzącą powłokę. Otwory oraz fugi należy ekranować za pomocą odpowiednich środków, co w szczególności w przypadku drzwi wejściowych powoduje znaczny nakład konstrukcyjny. Jakość ekranu określa wielkość wymaganych otworów oraz jakość zastosowanych elementów ekranujących, jak również ich połącznie z powłoką podstawową. Zasada jest następująca: czym większy otwór (prostokątne otwory/fugi: najdłuższa strona; okrągłe otwory: średnica), tym słabsze działanie ekranujące w rozważanym zakresie częstotliwości.

Czym wyższa jest częstotliwość występujących pól elektromagnetycznych, tym gorszy wpływ mają otwory w powłoce. Dlatego należy rozważyć zastosowanie specjalnych uszczelniaczy oraz przepustów kablowych lub też użycie złączy filtrowanych. Zasadniczo konstrukcyjne rozwiązanie systemu uszczelnienia określa w znacznym stopniu stopień tłumienia. Czym więcej punktów mocujących w ścianie dla zawiasów i mocowań drzwi oraz czym bardziej równomierna jest siła docisku i styk (niższa impedancja) powłoki do drzwi/sufitu wzdłuż uszczelnień, tym bliżej ideału. Przewodzące uszczelniacze specjalne z włókna metalowego na tworzywie piankowym jako uszczelnienie kombinowane dla zachowania kompatybilności elektromagnetycznej oraz stopnia ochrony osiągają wyższe wartości tłumienia w zakresie częstotliwości do 1 GHz lub powyżej. Łączą one metalowe, gładkie powierzchnie wewnętrzne drzwi oraz demontowalne ściany, blachy denne lub sufitowe z metalowymi krawędziami uszczelniającymi obudowy lub struktury.

Za pomocą dopuszczalnych środków można osiągnąć wartości tłumienia ekranu dla pomieszczeń bezpieczeństwa do 60 dB w zakresie częstotliwości od 30 MHz do 3 (10) GHz. Wartości tłumienia ekranu powyżej 60 dB wymagają w istotnym zakresie częstotliwości nadzwyczajnego nakładu konstrukcyjnego. Tego typu wysokie działanie ekranujące można znaleźć z reguły wyłącznie w zabezpieczonych pomieszczeniach IT administracji państwowej (wojsko, policja, służby informacyjne, ministerstwa itp.). Zabezpieczone pomieszczenia firmy Rittal spełniają podstawowe wymagania kompatybilności elektromagnetycznej oraz umożliwiają podniesienie do wyższego zakresu ochrony elektromagnetycznej z zastosowaniem dopuszczalnego nakładu.

Dalsze informacje dotyczące tematyki kompatybilności elektromagnetycznej znajdują się w oddzielnym raporcie dostawcy infrastruktury IT [ref. 18].

Modułowe pomieszczenia bezpieczeństwa oraz sejfy bezpieczeństwa

W zasadzie każde pomieszczenie można wykorzystywać jako serwerownię lub przebudować je na serwerownię. Należy przy tym rozważyć różne aspekty infrastruktury IT. Bez chłodzenia odprowadzenie energii cieplnej z urządzeń IT jest w okresie letnim niemożliwe, a dostępu nie można kontrolować, urządzenia stoją często na podłodze, natomiast w sytuacji zalania mogą zostać łatwo uszkodzone. Jeżeli do dyspozycji nie ma odpowiedniego pomieszczenia, zabezpieczone modułowe pomieszczenia IT lub sejfy serwerowe stanowią sensowną alternatywę. Pomieszczenia bezpieczeństwa montuje się w istniejącym pomieszczeniu, a następnie wyposaża się je we wszystkie elementy, które tworzą niezawodne data center. Rozwiązania te chronią przed zagrożeniem fizycznym oraz oferują sprawdzoną systemową ochronę dla IT.

Micro Data Center

To nieco mniejsze, ale nie mniej profesjonalnie chroniące przez zagrożeniami fizycznymi sejfy serwerowe. Są to w pełni wyposażone kompaktowe serwerownie, które należy jedynie podłączyć do wymaganych mediów. Firma Rittal oferuje oprócz sejfu serwerowego Micro Data Center (MDC), Level A dla wymagań ochrony podstawowej również sejf Micro Data Center (MDC), Level B oraz Micro Data Center (MDC), Level E.

Rysunek 5. Zakres produktów Micro Data Center Level E, Level B, Level A

Sejf MDC Level A jest kompletnym systemem z wbudowaną klimatyzacją oraz układem dwóch drzwi dla prostej instalacji i zarządzania. Jest to najmniejsze centrum danych dla małych przedsiębiorstw, które służy do ochrony systemów serwerowych i pamięci masowej oraz krytycznych danych przedsiębiorstwa i może pomieścić do 15 jednostek 19”.

Sejf MDC Level B został standardowo wyposażony w stelaż ramowy Rittal TS IT wraz z przednią i tylną płaszczyzną montażową 19” i jest dostępny w dwóch różnych wysokościach (42 lub 47 jednostek wysokości) oraz w dwóch głębokościach wewnętrznych (1 000 mm oraz 1 200 mm). Sejf zapewnia ochronę przeciwpożarową powyżej 90 minut i został sprawdzony

zgodnie z normą EN 1363. Oferuje on ochronę przeciwwłamaniową RC2, stopnień ochrony IP56 oraz został przetestowany przez instytut kontroli materiałowej budownictwa (MPA) w Braunschweig pod względem szczelności w oparciu o normę EN 1634.

Na potrzeby wymagań wysokiego bezpieczeństwa sejf MDC Level E zapewnia ochronę przeciwpożarową powyżej 90 min zgodnie z normą DIN 4102 (zachowanie wartości granicznych normy 1047-2, ΛT 50 K, wzgl. wilgotność powietrza < 85% przez 30 minut), stopnień ochrony IP 56, klasę przeciwwłamaniową RC2, opcjonalnie RC 3 lub WK 4 i chroni niezawodnie przed gazami pożarowymi.

Cechy MDC	**Level E**	**Level B**	**Level A**
Wysokość montażowa U	42 / 47	42 / 47	15
Użytkowa głębokość wewnętrzna w mm	1 000 / 1 200	1 000 / 1 200	1 000
Ochrona przeciwpożarowa	Klasa ognioodporności F 90 (DIN 4102 część 2) Zachowanie wartości granicznych ΔT < 50 K, wzgl. wilgotność powietrza < 85 % przez 30 minut	Klasa ognioodporności EI 90 / F 90 (DIN EN 1363-1: 1999/ w oparciu o normę DIN 4102-2:1997	Klasa ognioodporności F 90 (DIN 4102 część 2) Zachowanie wartości granicznych ΔT < 50 K, wzgl. wilgotność powietrza < 85 % przez 10 minut
Ochrona przeciwwłamaniowa	RC 2, opcjonalnie RC 3 przy użyciu narzędzi analogicznie do DIN EN 1630/2011-09/RC 2 Opcjonalnie WK IV przy użyciu narzędzi analogicznie do DIN V ENV 1630/1999-04	RC 2 przy użyciu narzędzi analogicznie do DIN EN 1630/ 2011-09/RC 2	WK II przy użyciu narzędzi analogicznie do DIN V ENV 1630/1999-04/WK II
Stopień ochrony	IP 56 zgodnie z EN 60 529	IP 56 zgodnie z EN 60 529	IP 55 zgodnie z EN 60 529
Dymoszczelność	W oparciu o normę DIN 18095-2: 1991-034)	W oparciu o normę DIN EN 1634-3: 2005-01	
Modułowa konstrukcja	tak	tak	nie
Zabudowa w trakcie eksploatacji	tak	nie	nie
Możliwości rozbudowy	tak	nie	nie

Tabela 6: Przegląd cech sejfów MDC

Dzięki zastosowaniu modułowych i skalowalnych komponentów wyposażenia sejfy Micro Data Center mogą utworzyć w pełni wyposażoną kompaktową serwerownię. Należą do tego również dodatkowe urządzenia z oferty produktów firmy Rittal, takie jak system monitorowania Computer Multi Control III (CMC III), system wczesnego wykrywania i gaszenia pożaru DET-AC III, inteligentny układ rozdziału zasilania za pomocą Power Distribution Unit (PDU) czy Power System Modul (PSM) oraz urządzenia do klimatyzacji.

Pomieszczenia bezpieczeństwa

Modułowe pomieszczenie bezpieczeństwa IT można zainstalować zarówno w nowym pomieszczeniu, jak również w pomieszczeniu już używanym. Pomieszczenie można zamontować praktycznie bez emisji pyłu i hałasu. Umożliwia ono łatwą rozbudowę lub przeniesienie w inne miejsce. Pomieszczenie to zapewnia lepszą ochronę przeciwpożarową, przed zalaniem wodą oraz przed zakłóceniami elektromagnetycznymi niż standardowe pomieszczenie. W zależności od wymaganej dostępności można zastosować pomieszczenia w zakresie ochrony podstawowej, jak i przeznaczone dla wymagań wysokiej dostępności. Pomieszczenie wysokiej dostępności firmy Rittal oferuje najwyższe bezpieczeństwo fizyczne dla centrum danych oraz lokalizacji systemów IT. System otrzymał certyfikację wydaną przez ECB zgodnie z zasadami ECB•S oraz spełnia wymagania normy EN 1047-2 w sposób nieograniczony.

Rysunek 6. Pomieszczenie bezpieczeństwa IT firmy Rittal

Pomieszczenia bezpieczeństwa IT wyposaża się z reguły w drzwi bezpieczeństwa. W zależności od wymagań mogą one różnić się znacznie pod względem wykonania. W celu zabezpieczenia drzwi przed wandalizmem oraz próbami włamania, system drzwi należy wyposażyć w wielowarstwowy, ognioodporny pakiet blach stalowych z dookólną ościeżnicą oraz dookólnym zawinięciem ogniowym i uszczelniającym. W obszarze zawinięcia drzwi zamocowano drążone uszczelniacze gumowe oraz rozszerzalne uszczelniacze odporne na wysoką temperaturę. Istotny element układu stanowi mechanizm zamykania. Powinien on z jednej strony niezawodnie chronić przed dostępem osób postronnych, z drugiej strony umożliwić osobom znajdującym się w pomieszczeniu szybkie opuszczenie obszaru zagrożenia w przypadku awarii. W tym celu wyposażono zamki w bezpieczne mechanizmy blokujące, sworznie ryglujące oraz układ otwierania na wypadek paniki. Bezpieczny mechanizm blokujący dysponuje mocowaniem jednostki zamka. Osoby, które podczas alarmu znajdują się jeszcze w pomieszczeniu (przy zamkniętych drzwiach), mogą je w każdej chwili opuścić przez standardowe otwarcie antypaniczne. Automatyczny układ zamykania drzwi umożliwia zmienne ustawienie opóźnienia zamykania.

Pomieszczenie ochrony podstawowej **GSR**	**Pomieszczenie ochrony podstawowej Plus** **GSR Plus**	**Pomieszczenie o wysokiej dostępności** **HVR**
		
Ochrona podstawowa Pomieszczenia infrastruktury IT, centrali sterujących	**Ochrona rozszerzona** Serwerownie o średnim zapotrzebowaniu na bezpieczeństwo, serwerownie archiwizacji danych	**Ochrona wysokiej dostępności** Serwerownie główne o wysokim zapotrzebowaniu na bezpieczeństwo, rozwiązania wysokiej dostępności

Tabela 7: Oferta produktów pomieszczeń bezpieczeństwa firmy Rittal.

Prawie w każdym przypadku wymagana jest kontrola dostępu do drzwi serwerowni. Profesjonalne pomieszczenia bezpieczeństwa są wyposażone w system kontroli dostępu, który obsługuje styki bezpotencjałowe przez rozdzielacz interfejsów VdS. Umożliwia to sprzężenie statusu drzwi z centralnym systemem zarządzania budynkiem. Jeżeli jednak wymagane jest wyłącznie sprawdzenie statusu drzwi, to wystarczy zastosowanie styku statusu. Również blokady drzwi w profesjonalnych pomieszczeniach bezpieczeństwa można kontrolować w celu przekazania informacji do systemu antywłamaniowego lub centrali bezpieczeństwa. Certyfikowane drzwi pomieszczenia bezpieczeństwa zapewniają optymalną ochronę przed ogniem, wodą, włamaniem oraz innymi zagrożeniami fizycznymi.

Idealne pomieszczenie bezpieczeństwa to takie, które nie wymaga żadnych przepustów. Nie jest to możliwe choćby z powodu konieczności zastosowania drzwi. Również infrastruktura IT w pomieszczeniu bezpieczeństwa i sejfach bezpieczeństwa wymaga podłączenia do układów chłodzenia, prądu i sieci. Do tego celu służą przepusty kablowe, których właściwości powinny zapobiec osłabieniu bezpieczeństwa całego systemu.

Rozwiązań przepustów jest wiele: stosuje się twarde systemy grodziowe, które zapewniają w obszarze wprowadzenia okablowania większe bezpieczeństwo w zakresie manipulacji, i miękki system grodziowy wypełniony elastycznym materiałem uszczelniającym, stosowany najczęściej jako rozwiązanie standardowe w pomieszczeniach bezpieczeństwa. Odmienny czynnik kształtujący stanowią grodzie okrągłe wypełnione modułami uszczelniającymi, które sprawdzają się w szczególności w przypadku istniejących kabli, rur i traktów kablowych konstrukcji budynku. Konkretne zamknięcie wypełnionej grodzi powinien zawsze wykonać specjalista autoryzowany przez producenta. Tylko w taki sposób można zagwarantować pełną ochronę pomieszczenia bezpieczeństwa.

Kryterium	Norma	GSR	HVR
Kontrola systemu	Kontrola poniższych poziomów ochrony jako całego systemu lub całej konstrukcji.	Tak	Tak
Ochrona przeciwpożarowa	Certyfikat ECB·S wg PN-EN 1047-2, wzrost temperatury 50 K i 85 % wilgotność wzgl. do 24 godzin (okres dogrzewania), wystawienie na działanie płomieni przez 60 minut	Nie	Tak
	Wzrost temperatury 50 K i 85 % wilgotności względnej, bez okresu dogrzewania, wystawienie na działanie płomieni przez 30 minut	Opcjonalnie	-
	F 120 wg DIN 4102	Nie	Tak
	F 90 wg DIN 4102	Tak	-
Korozyjne gazy pożarowe	Dymoszczelność w oparciu o DIN 18 095	Tak	Tak
Obciążenie gruzem	Odporność uderzeniowa do 200 kg	Tak	Tak
Woda	IP x6 wg EN 60 529	Tak	Tak
	Ochrona przed wodą stojącą	-	Tak
Pył	IP 5x wg EN 60 529	Tak	Tak
Dostęp osób nieupoważnionych	WK IV wg DIN V ENV 1630, tylko system drzwi	-	Tak
	WK III wg DIN V ENV 1630 lub DIN V 18 103 (ET2)	Opcjonalnie	Tak
	WK II wg DIN V ENV 1630	Tak	-
EMC	Ochrona przed emisją i odporność na zakłócenia wysokiej częstotliwości	Opcjonalnie	Opcjonalnie

Tabela 8: Przegląd cech pomieszczenia bezpieczeństwa firmy Rittal

Wyposażenie IT pomieszczenia bezpieczeństwa wymaga chłodzenia. W tym celu stosuje się odpowiednie metody, niektóre z nich wymagają doprowadzenia świeżego powietrza przez jeden lub wiele otworów w pomieszczeniu. Jeżeli w otoczeniu pomieszczenia bezpieczeństwa wybuchł pożar, to taki otwór musi zostać zamknięty, żeby do pomieszczenia z zewnątrz nie przedostała się żadna ilość dymu. Odbywa się to za pomocą klap lub suwaków z materiałów ognioodpornych, które zatrzymują gaz pożarowy.

Napęd takich suwaków klimatyzacyjnych lub klap przeciwpożarowych musi być w przypadku pożaru niezależny od zasilania. W zależności od wielkości, położenia i kształtu otworu można stosować różne typy napędów. I tak w normalnym przypadku napędu suwaka klimatycznego do napowietrzania i odpowietrzania stosuje się elektryczne systemy napędowe. W sytuacji pożaru klapa musi zamknąć otwór za mocą mechanizmu mechanicznego na przykład sprężyny lub magnesu.

Stosowane rozwiązanie to suwak nadciśnieniowy. Jeżeli włączy się system gaszenia z gazem obojętnym lub chemicznym środkiem gaśniczym, to powstałe nadciśnienie musi zostać odprowadzone. Umożliwia to odpowiedni, ognioodporny suwak wyposażony w napęd elektryczno-pneumatyczny. W przypadku alarmu następuje odprowadzenie ciśnienia przez krótkotrwałe otwieranie suwaka. Właśnie w kwestii czysto mechanicznych układów zamykających należy dopasować uszczelniacze optymalnie do przypadku zastosowania, ponadto muszą one być bardzo wydajne. Wymaga to zastosowania wysoce elastycznych i szczelnych taśm zamykających o znacznej wytrzymałości na wysokie temperatury.

O bezpieczeństwie w serwerowni, jak również w pomieszczeniach bezpieczeństwa oraz w sejfach bezpieczeństwa, stanowi zastosowanie wysokiej jakości sytemu wczesnego rozpoznania zadymienia w połączeniu w wydajnym systemem gaszenia. Szybka reakcja wymaga zastosowania systemu wczesnego wykrywania zadymienia, który wyłapuje cząsteczki dymu. W tym przypadku stosuje się najczęściej detektory rozproszenia światła. Miarą gęstości dymu jest rozproszenie promienia światła na istniejących cząsteczkach dymu. Detektory rozproszenia światła funkcjonują zarówno jako czujniki punktowe zamontowane na suficie, jak również w systemach zasysania dymu.

Z powodu określonego przepływu powietrza w serwerowni, powstały dym dostaje się do czujników często zbyt późno lub wcale. W celu zapewnienia wczesnego wykrycia zadymienia nieodzowne jest zastosowanie systemu wczesnego wykrywania.

Zasterowanie aktywnego systemu gaszenia odbywa się z reguły za pomocą podwójnego czujnika lub zależności od dwóch grup, co zapobiega fałszywym alarmom. Do gaszenia używa się najczęściej gazu obojętnego lub chemicznej mieszanki. Nie można zastosować piany gaśniczej czy proszku, ponieważ uszkodziłyby to systemy IT i komponenty infrastruktury. Zastosowanie systemu redukcji tlenu również może skutecznie zapobiegać pożarom. Ogranicza on poziom tlenu w serwerowni na tyle, by powstanie pożaru stało się niemożliwe.

Literatura

Ref. 1 BSI Grundschutzkatalog (Katalog ochrony podstawowej BSI), Link: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Ref. 2 Studie „Kritische IT-Systeme im Mittelstand“ (Studium „Krytyczne systemy IT dla średnich przedsiębiorstw”), Techconsult im Auftrag von HP Deutschland, 2013, Link: http://www.softexpress.de/Media/seite_hardware/ProactiveCare/HP_Ergebnispr%C3%A4sentation_Kritische_IT_Mittelstand_Handout_2013.pdf

Ref. 3 EMC-Studie, 2014, Link: http://germany.emc.com/about/news/press/2014/20141209-01.htm

Ref. 4 ISO/IEC 17065, Link: http://www.iso.org/iso/catalogue_detail.htm?csnumber=46568

Ref. 5 BSI Maßnahme 1.6 „Einhaltung von Brandschutzvorschriften“ („Przestrzeganie przepisów przeciwpożarowych”), Link: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m01/m01006.html

Ref. 6 DIN 4102 „Brandverhalten von Baustoffen und Bauteilen“ („Proces spalania materiałów i elementów konstrukcji budowlanych.”)

Ref. 7 EN 1047-2, Link: http://www.beuth.de/langanzeige/DIN+EN+1047-2/113261910.html

Ref. 8 EN 1363 „Badania odporności ogniowej – Część 1: Wymagania ogólne”

Ref. 9 DIN 18095 „Türen; Rauchschutztüren; Begriffe und Anforderungen“ („Drzwi; drzwi przeciwdymne; pojęcia i wymagania.”)

Ref. 10 EN1634 „Badania odporności ogniowej i dymoszczelności zestawów drzwiowych i żaluzjowych, otwieralnych okien i elementów okuć budowlanych“

Ref. 11 EN 50102 „Stopnie ochrony przed zewnętrznymi uderzeniami mechanicznymi zapewnianej przez obudowy urządzeń elektrycznych (Kod IK)”

Ref. 12 EN 60529 „Stopnie ochrony zapewnianej przez obudowę (kod IP)“

Ref. 13 DIN EN 62208 „Puste obudowy do rozdzielnic i sterownic niskonapięciowych – Wymagania ogólne“

Ref. 14 DIN EN 1627 „Drzwi, okna, ściany osłonowe, kraty i żaluzje – Odporność na włamanie – Wymagania i klasyfikacja”.

Ref. 15 DIN EN 1630 „Drzwi, okna, ściany osłonowe, kraty i żaluzje – Odporność na włamanie – Metoda badania dla określenia odporności na próby włamania ręcznego”.

Ref. 16 DIN EN 55022 „Urządzenia informatyczne – Charakterystyki zaburzeń radioelektrycznych – Poziomy dopuszczalne i metody pomiarów”.

Ref. 17 DIN EN 55024 „Urządzenia informatyczne – Charakterystyki odporności – Poziomy wymagane i metody pomiarów”.

Ref. 18 Rittal – „Whitepaper – EMV-Schutz bei Sicherheitsräumen“ („Ochrona przed zakłóceniami elektromagnetycznymi dla pomieszczeń bezpieczeństwa.”).

Wykaz skrótów

BSI	Bundesamt für Sicherheit in der Informationstechnik (Federalny Urząd Bezpieczeństwa IT)
CMC	Computer Multi Control (System Rittal do monitorowania infrastruktury IT)
DAKKS	Deutsche Akkreditierungsstelle (niemiecka jednostka akredytująca)
DETA-AC	Instalacja wykrywania i gaszenia pożaru
DIN	Deutsches Institut für Normung (niemiecki instytut normalizacji)
ECB	European Certification Body GmbH
EMC	Kompatybilność elektromagnetyczna
EN	Europäische Norm (norma europejska).
ESSA	European Security Systems Association (ESSA) e.V.
GSR	Pomieszczenie ochrony podstawowej
HE	Jednostka wysokości = 44,45 mm
HVR	Pomieszczenie o wysokiej dostępności
IEC	International Electrotechnical Commission
IK-Code	Stopnie ochrony przed zewnętrznymi uderzeniami mechanicznymi zapewnianej przez obudowy urządzeń elektrycznych (Kod IK)
IP-Code	Stopnie ochrony zapewnianej przez obudowy
ISO	International Organization for Standardization
IT	Technologia informacyjna

LBO	Landesbauordnung (krajowe prawo budowlane)
MDC	Micro Data Center
MBO	Musterbauordnung (federalna ustawa budowlana)
MLAR	Muster-Leitungsanlagen-Richtlinie (wzorcowe wytyczne konferencji ministrów budownictwa odnośnie wymagań dotyczących technicznych aspektów ochrony przeciwpożarowej instalacji elektrycznych)
NEMA	National Electrical Manufacturers Association
NOAEL	NOAEL (z ang. no observable adverse effect level – poziom niewywołujący dających się zaobserwować szkodliwych skutków)
PDU	Rittal Power Distribution Unit (Jednostka dystrybucji mocy firmy Rittal)
PSM	Rittal Power System Modul (modułowe PDU)
RC	Resistance Class (klasa odporności)
TÜV	Technischer Überwachungsverein (Niemieckie stowarzyszenie dozoru technicznego)
UL	Underwriters Laboratories Inc., certyfikacja w USA
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik (Niemieckie stowarzyszenie elektrotechniki, elektroniki, techniki informacyjnej)
VDMA	Verband Deutscher Maschinen- und Anlagenbau (Niemiecki związek producentów maszyn i urządzeń przemysłowych)
VdS	VdS Schadenverhütung GmbH, http://vds.de
WK	Widerstandsklasse (klasa odporności) (zastępowany przez RC = resistance class)

Rittal – The System.

Faster – better – everywhere.

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

Rittal Sp. z o.o. • The Park Warsaw, budynek 3
ul. Krakowiaków 48 • 02-255 Warszawa
Tel.: (022) 310 06 00 • Fax: (022) 310 06 16
www.rittal.pl • e-mail: rittal@rittal.pl • Tech Info 0 801 380 320