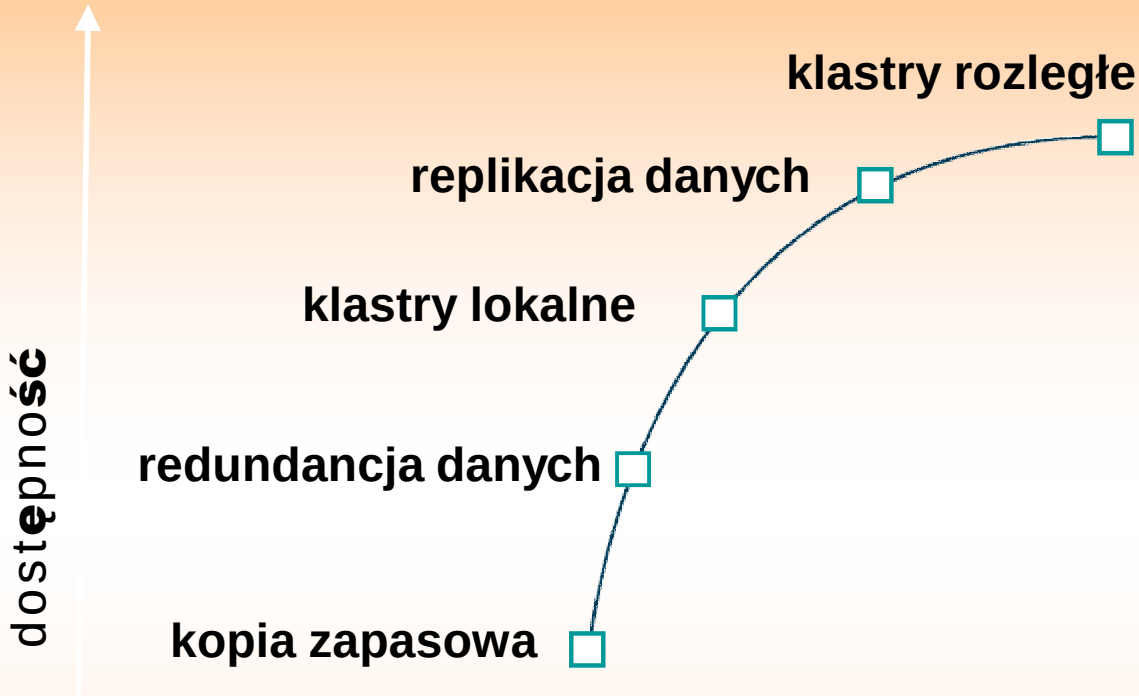
# Bezpieczeństwo i niezawodność systemów IT

## Disaster Recovery

BiG Vent

BiG Vent

# Ochrona dostępności na wszystkich poziomach

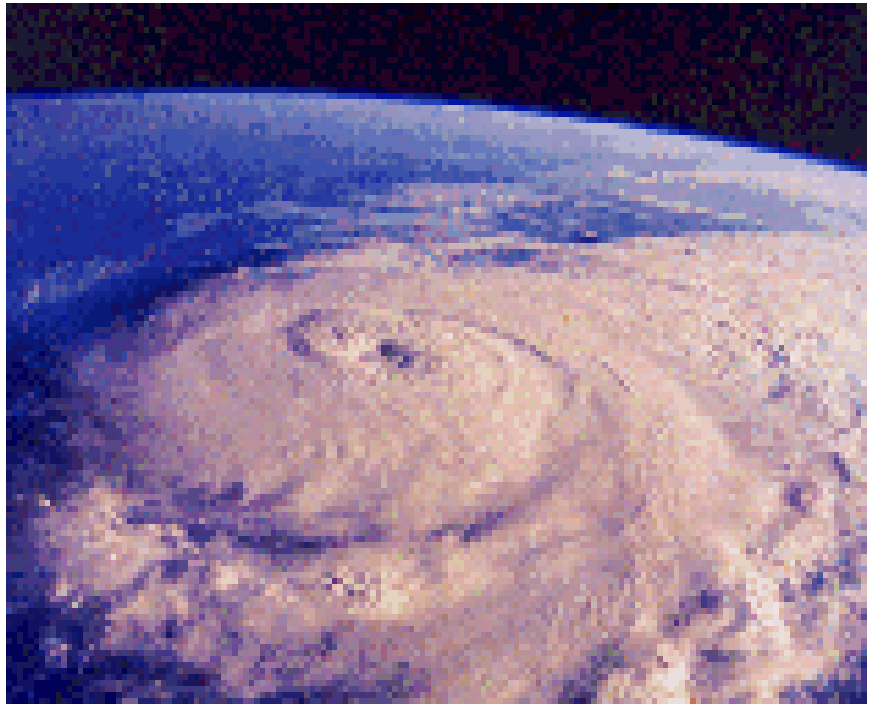



# „Mnie to się nie przydarzy.” A jeśli ?

- Dane tych ludzi były „dobrze” zabezpieczone, ale nikt nie przewidział takiego rozmiaru katastrofy !
- Opieramy działalność na infrastrukturze IT, ale pamiętajmy że komputery to nie wszystko !!!

# Czym jest DISASTER ?

- DISASTER = nieszczęście, katastrofa, chaos.
  - Kto myśli o katastrofie ? ... o 7:35 rano ??
  - Kto myślał o niej 11 września ?



# Evil stars ? Poszukajmy Powodów ...

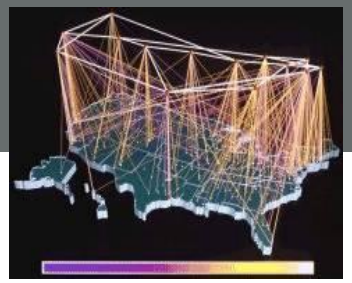
- Dziwne, żyjemy w erze informacji/technologii, ale wciąż niewielu myśli o katastrofach...
  - Disaster = evil star.
  - Pozytywne społeczeństwo.
  - Dominacja człowieka.

# Planowanie Disaster Recovery w jednym slajdzie

- **Próba racjonalnego podejścia do irracjonalnego charakteru katastrof.**
- Zasada „no GURUs”.
- Sukces warunkowany cyklicznymi testami, rozwijaniem świadomości pracowników i rozważnym podejściem do problemu.
- **Ważniejsze dzisiaj niż kiedykolwiek.**

# Dlaczego ?

- Katastrofy nie występują teraz częściej, ale my jesteśmy bardziej na nie podatni.
  - Nowoczesny biznes jest bardziej uzależniony od infrastruktury technologicznej niż kiedykolwiek.
  - Pojedynczy incydent może mieć szeroko zakrojone konsekwencje.
  - Rozwój technologii stworzył możliwości zaistnienia nowego rodzaju katastrof.



Mapa szkieletu sieci Internet

Burza śnieżna (1998)

Budynek Federalny w Oklahoma City

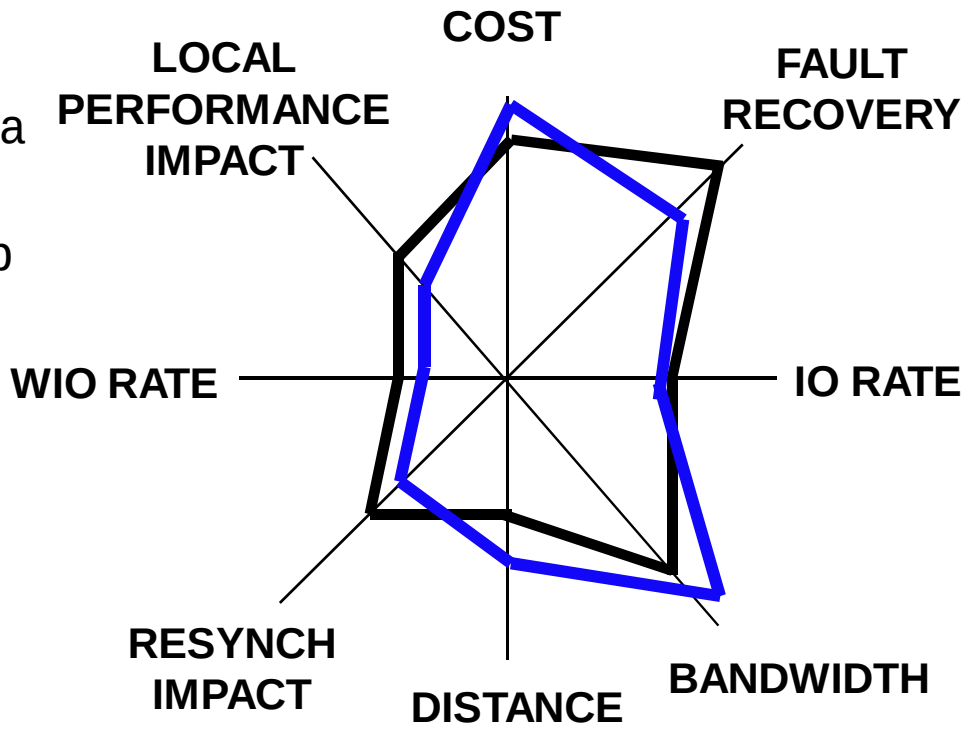
Powódź na Three Mile Island

# Szacujemy ryzyko awarii centrum danych

- Przyrost danych będzie rósł około 80% na rok (IDC)
- Największe firmy szacują wartość 100MB czystych danych powyżej $1mln (Jan William Togo)
- Przyczyny przerw w pracy firm w ostatnich 5 latach
  - Błąd operatora 40%
  - Awaria aplikacji 40%
  - Katastrofy 20%
- Co rok, na każde 500 centrów danych, 1 doświadczy poważnej awarii. (McGladrey and Pullen)

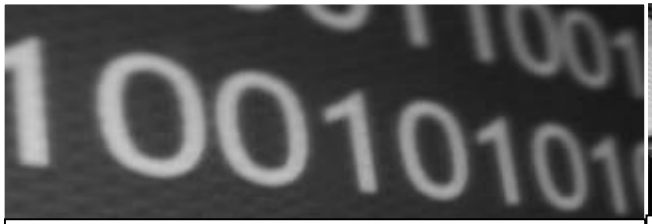
# Dla każdego coś dobrego …

- Każda organizacja ma unikalne potrzeby Disaster Recovery, i tylko ona może je sprecyzować !
- Poprawne sformułowanie tych potrzeb jest kluczem do sukcesu.
- Najpierw należy sformułować wymagania, a następnie dopasować technologię – nie na odwrót !
- Nie można zapominać o szczegółach, aby tego uniknąć podzielmy potrzeby firmy na potrzeby departamentów, działów, pionów …



BiG Vent

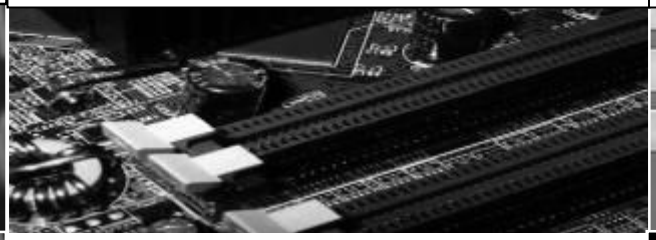
# Zagrożenia dla dostępności informacji



USZKODZENIE DANYCH

DEFEKT PODZESPOŁU

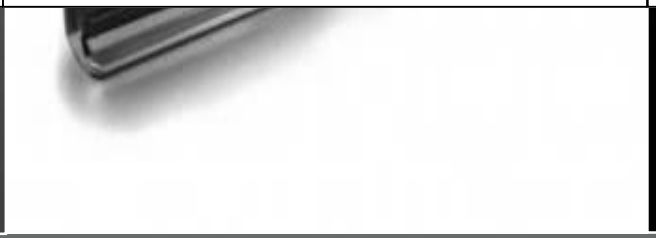

USTERKA APLIKACJI




BŁĄD OPERATORA

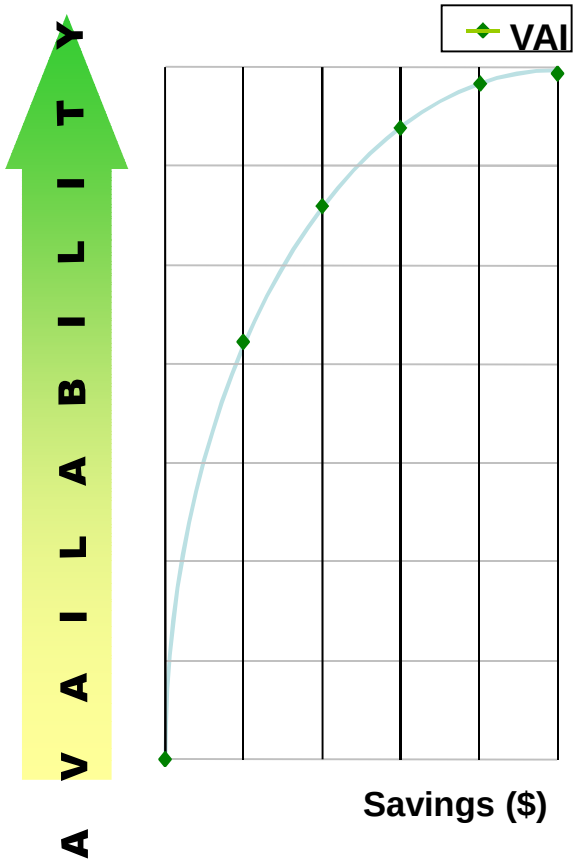
KONSERWACJA

KATASTROFA



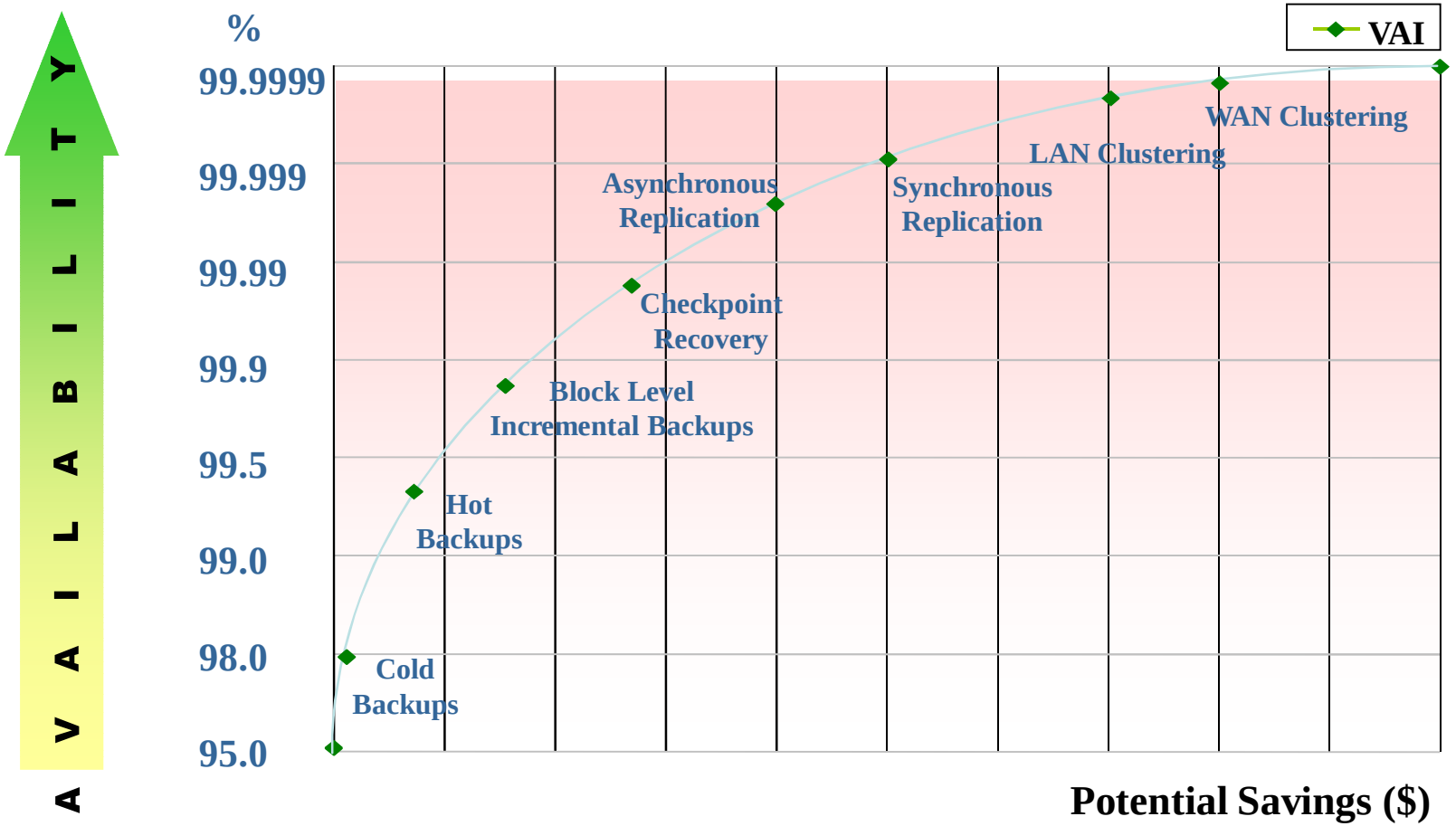
BiG Vent

# W pogoni za 9-tkami, czyli „Kto potrzebuje zapasowego centrum danych?”

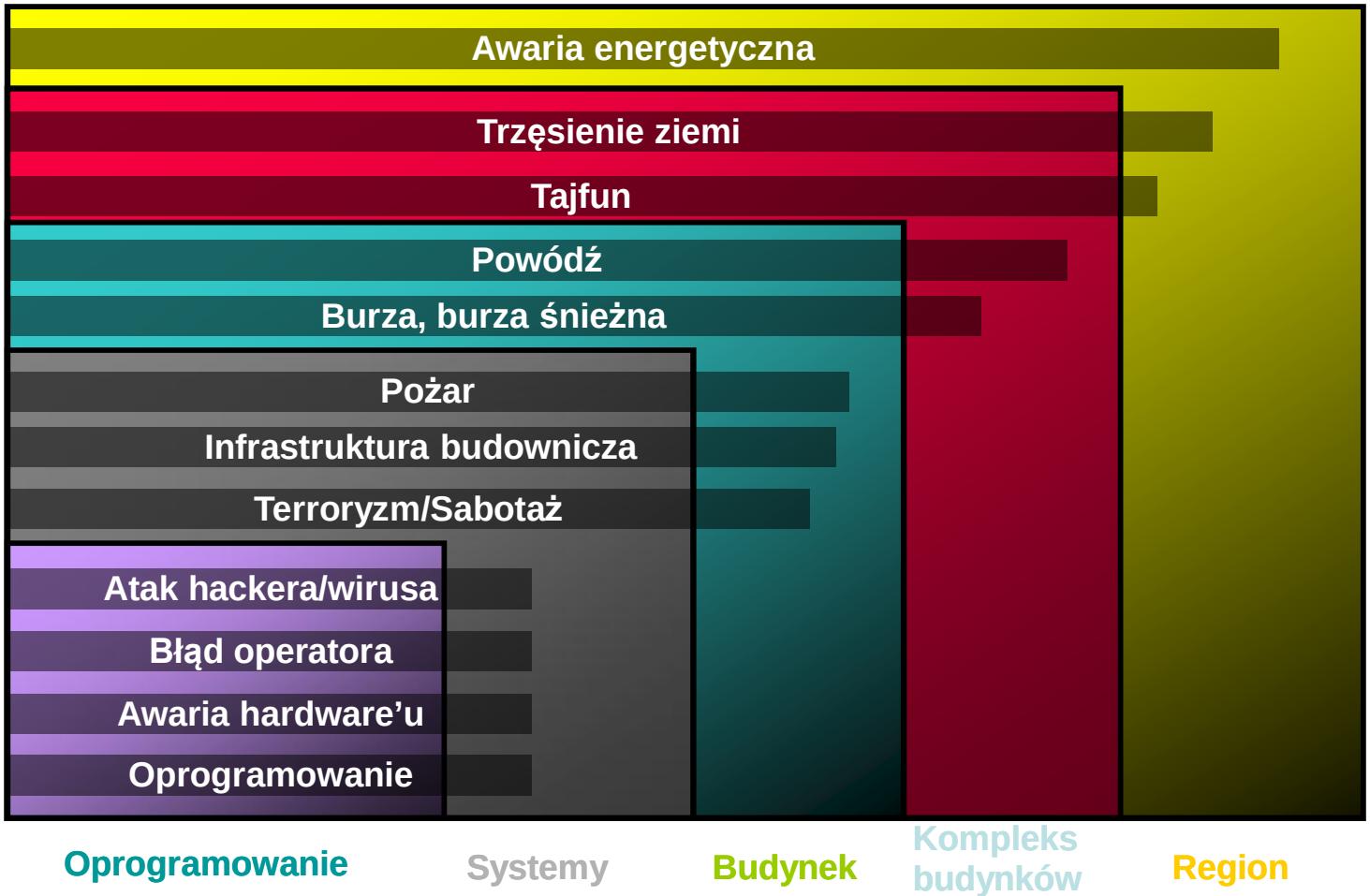



| % uptime | Annual downtime | Annual Home Shopping Cost | Annual Brokerage System Cost |
|---|---|---|---|
| 99.9999 | 30 seconds | $950 | $53,750 |
| 99.999 | 5 minutes | $9,417 | $537,500 |
| 99.99 | 52 minutes | $98,000 | $5,590,000 |
| 99.9 | 8.75 hours | $988,750 | $56 million |
| 99.5 | 43.7 hours | $5 million | $280 million |
| 99.0 | 87.6 hours | $10 million | $560 million |
| 98.0 | 180+ hours | $20+ million | $1+ billion |
| 95.0 | 450+ hours | $50+ million | $3+ billion |

# 9-tek ciąg dalszy, czyli „Co powinno znaleźć się w BDC ?”

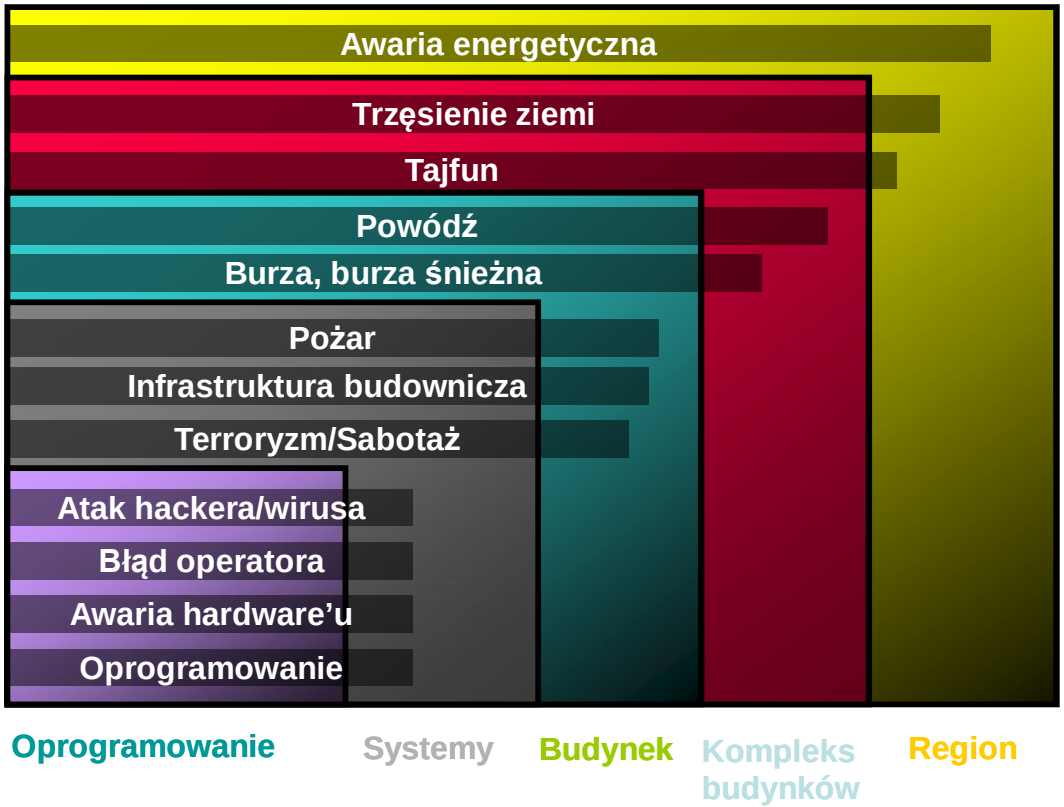


# Zagrożenia i ich zasięg



# Oprogramowanie i Systemy

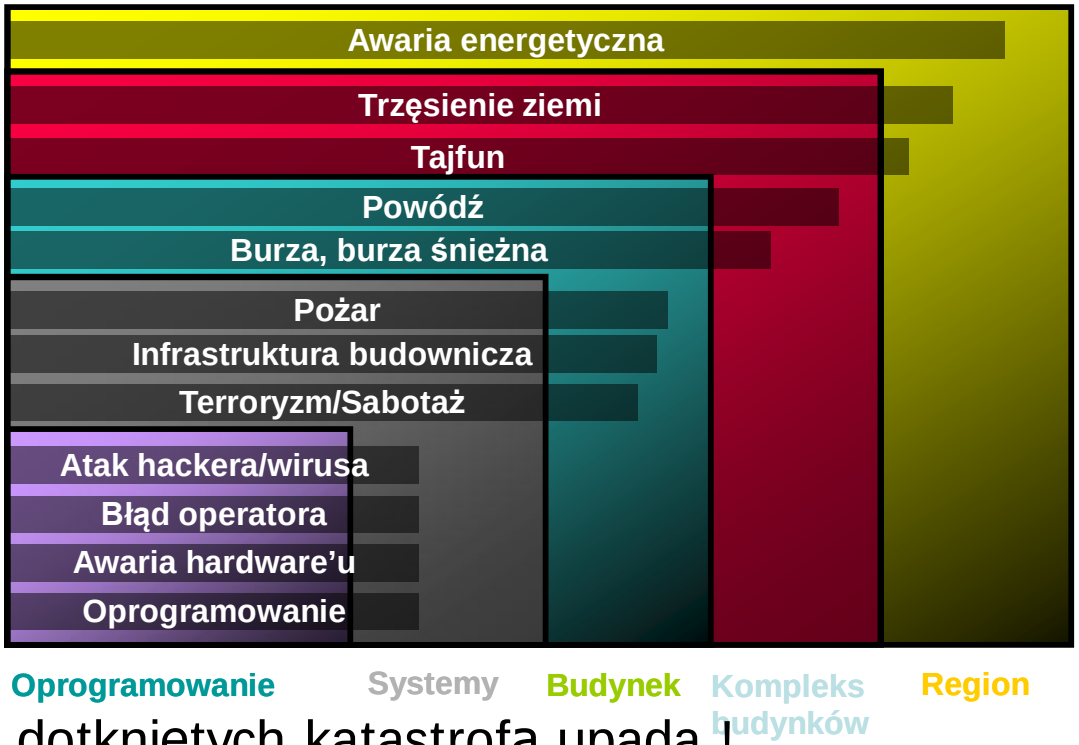
- Generalnie dobrze pojmowane
- W zasadzie są zagrożone usunięciem lub zniszczeniem danych
- Rozwiązywane za pomocą procedur backup/restore
- Zapasowe kopie danych i aplikacji przechowywane w zdalnej lokalizacji



# Budynki, kompleksy, regiony

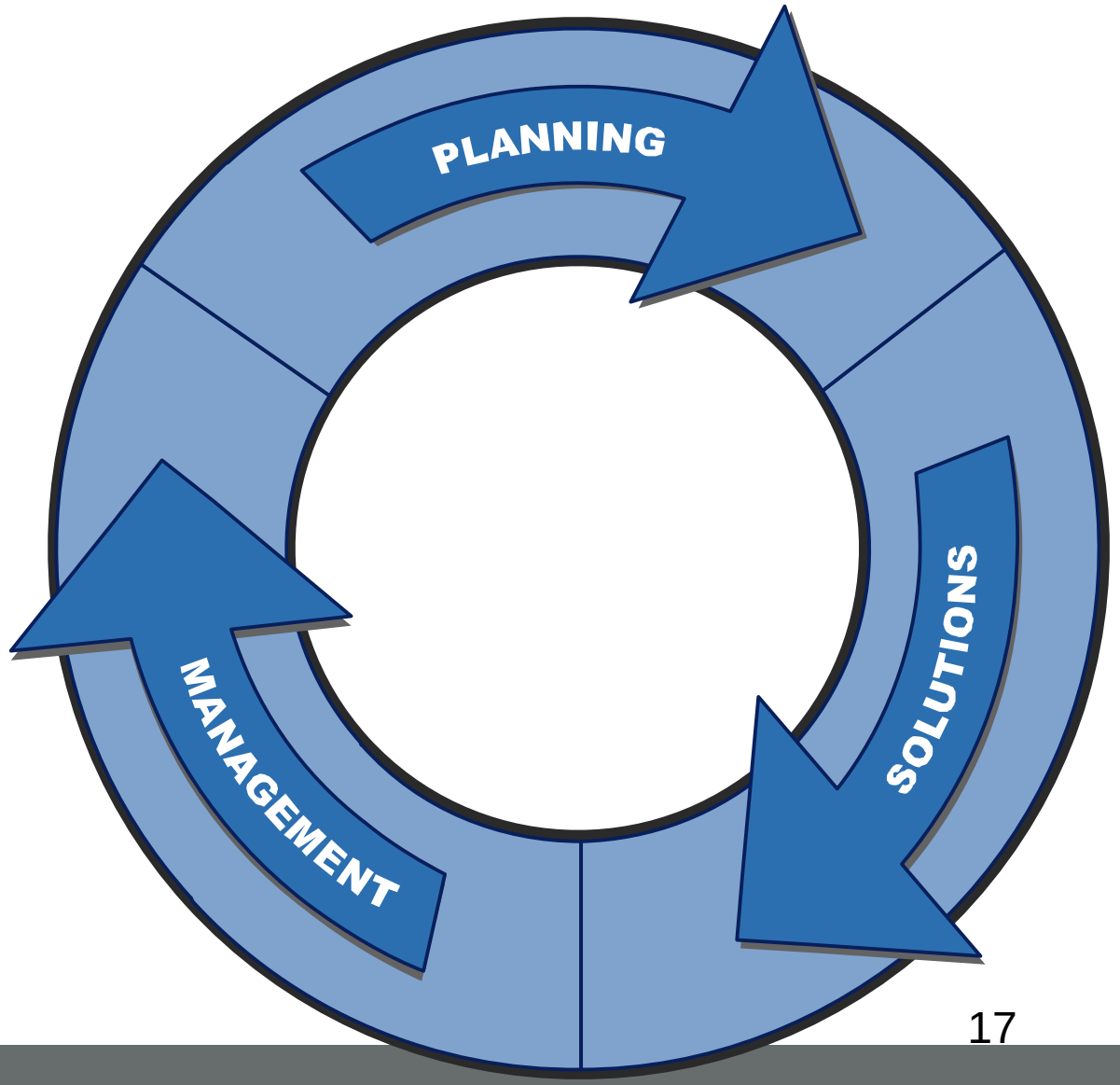
- Niezbyt dobrze rozumiane
- Wymagają rozważenia utworzenia drugiego centrum w innej lokalizacji geograficznej, replikacja danych
- Często postrzegane jako „za drogie” rozwiązania

…ALE..

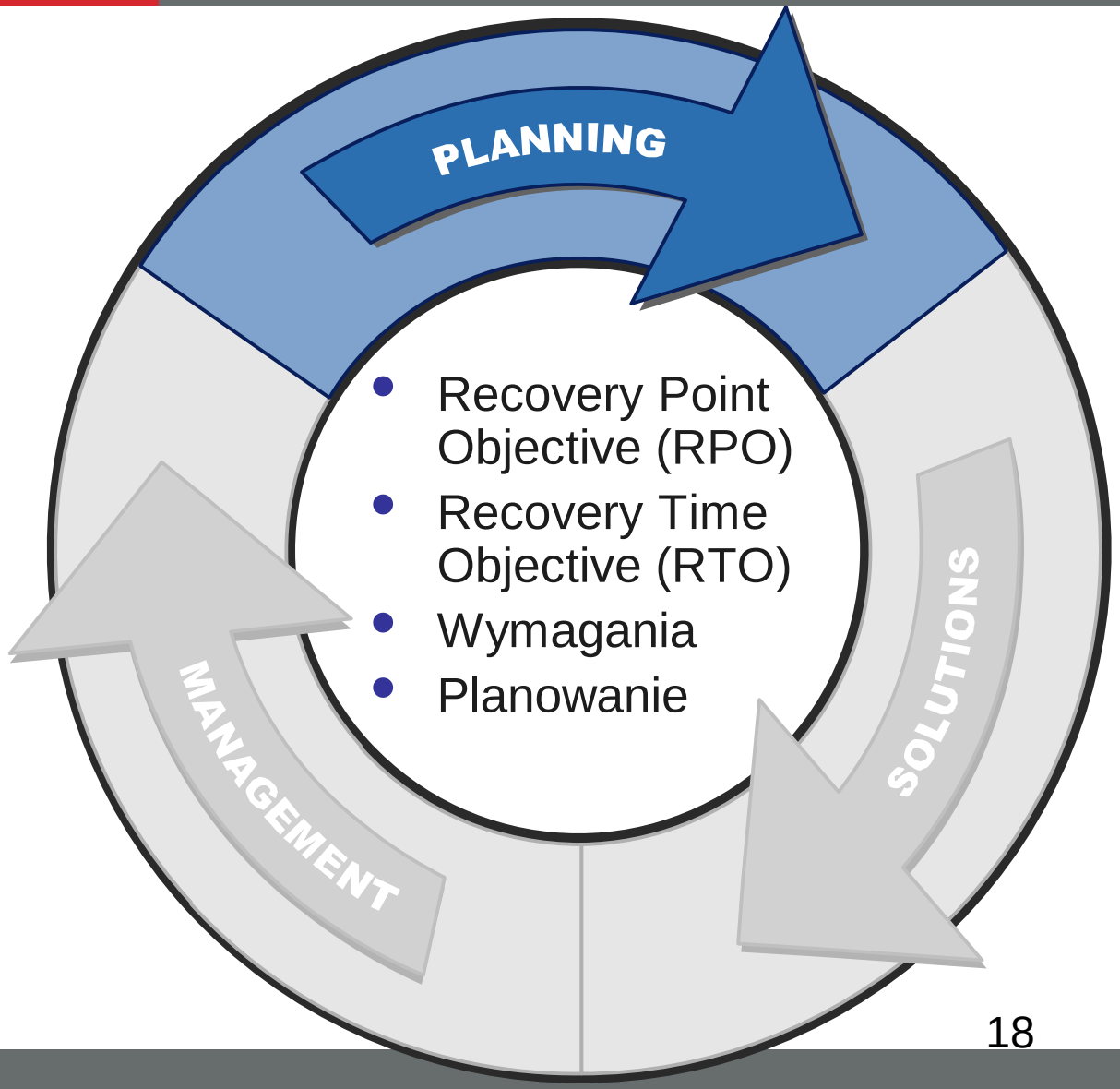



- Większość przedsiębiorstw dotkniętych katastrofą upada !
- Ogromne koszty odtworzenia, strata zysków, strata reputacji, szkody dla marki produktu, strata pozycji lidera na rynku

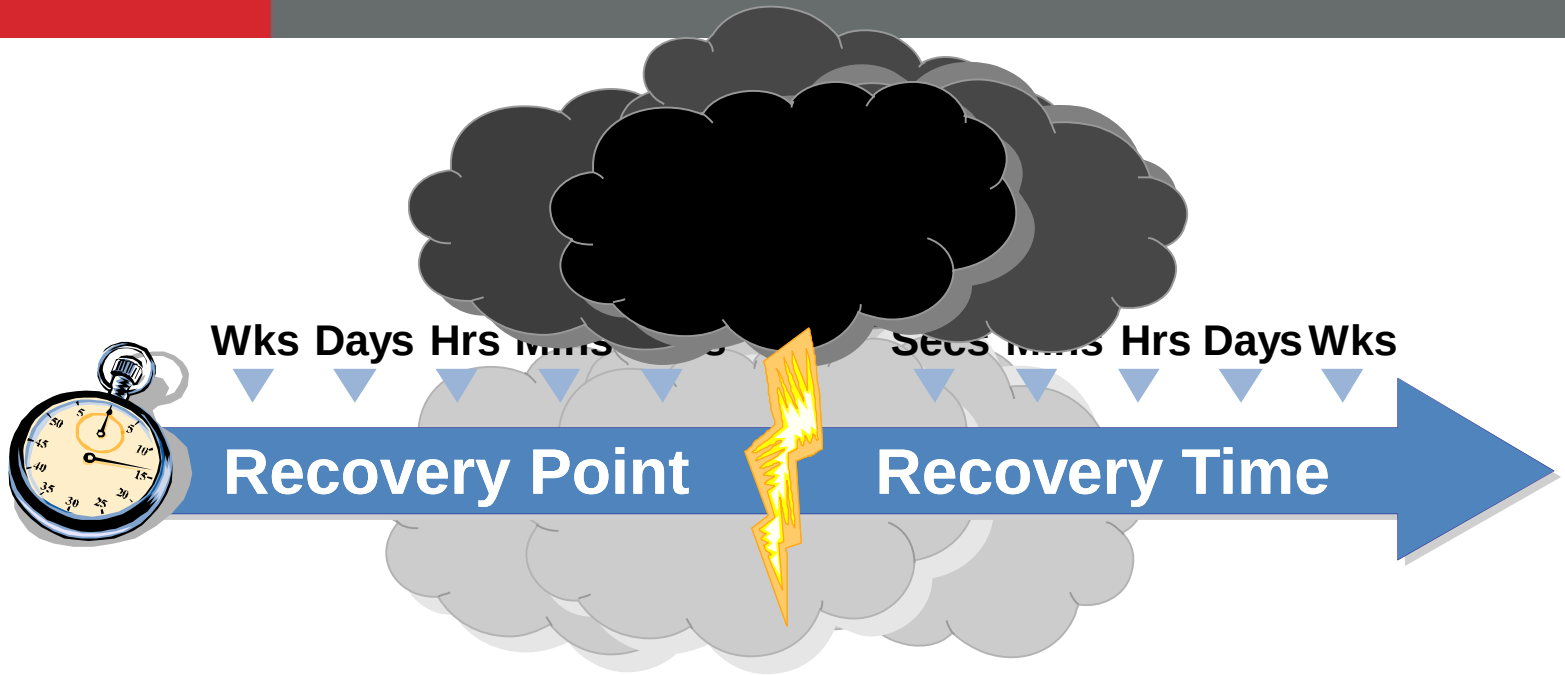
# Fazy procedur DR



# Requirements & Planning



# Terminologia Disaster Recovery

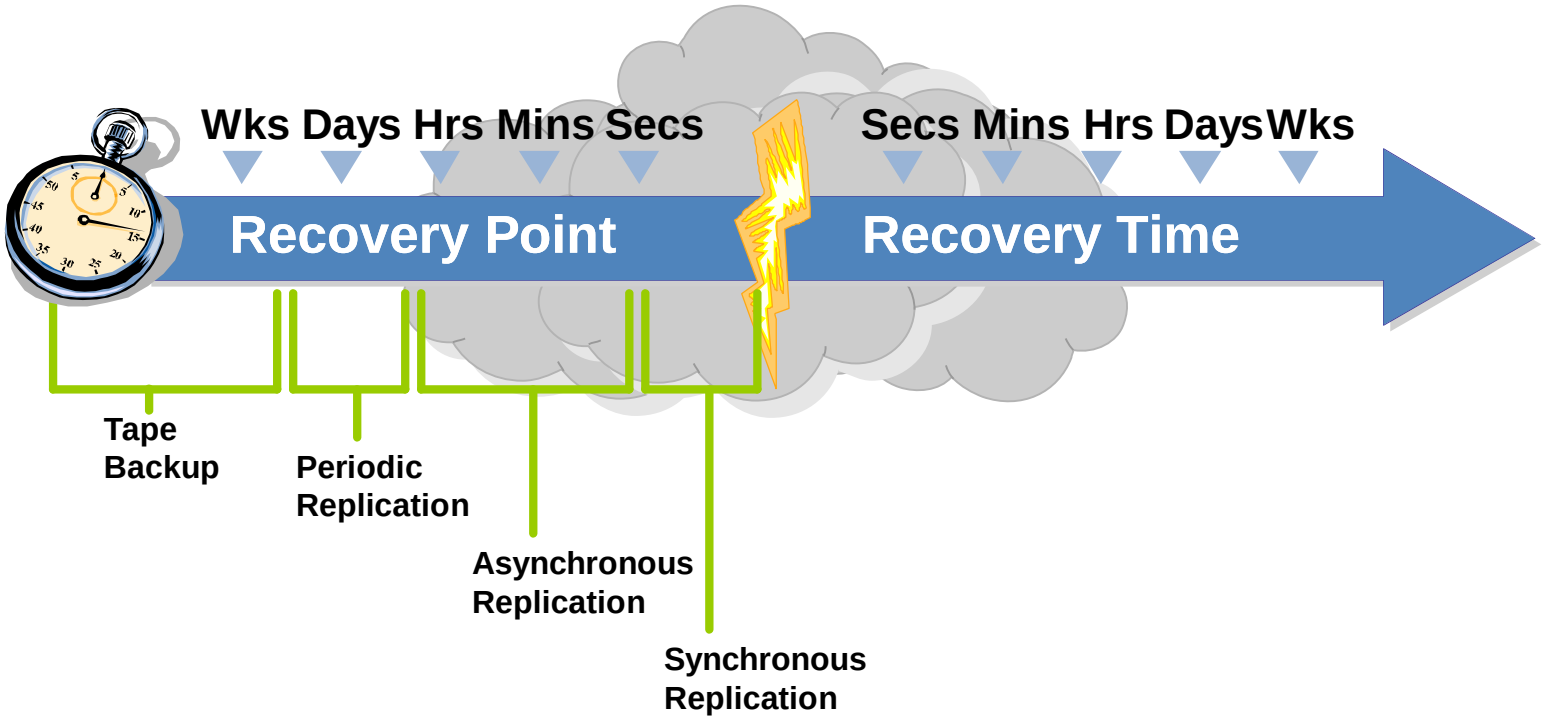



- Recovery Point Objective (RPO) –

  Punkt w czasie, do którego należy przywrócić dane systemów/usług.
- Recovery Time Objective (RTO) –

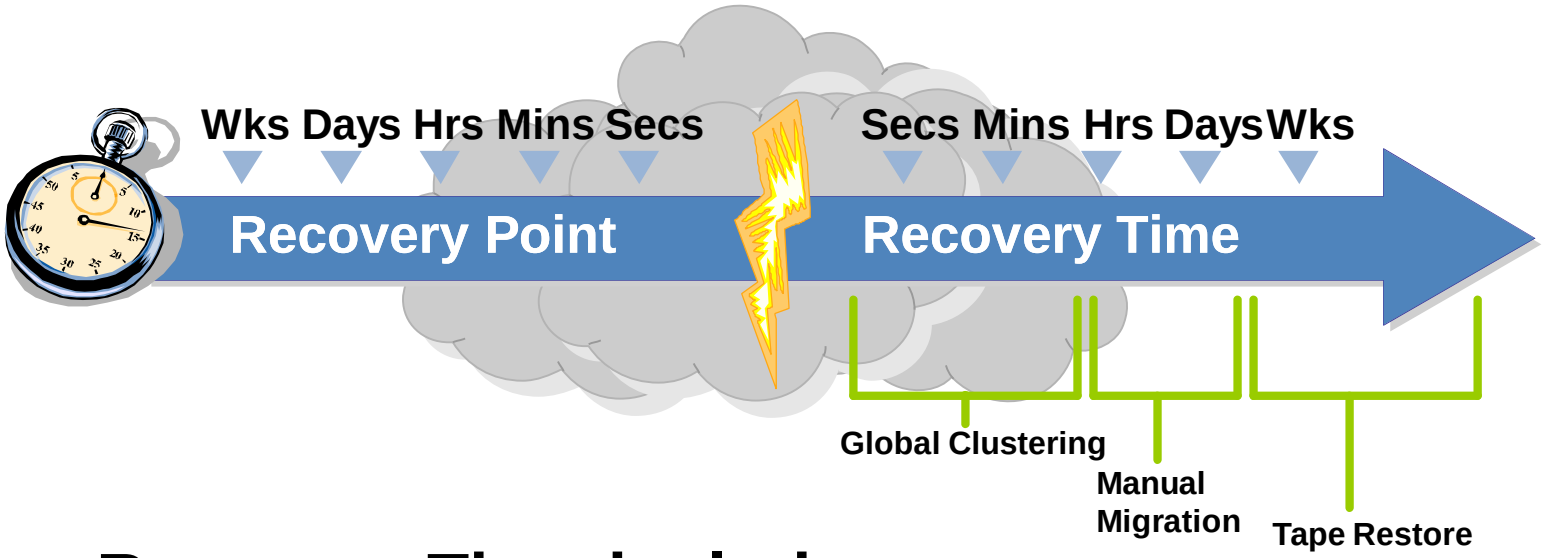
  Maksymalny czas w jakim należy odtworzyć dane systemów/usług.

# Recovery Point Objective (RPO)



# Recovery Time Objective (RTO)

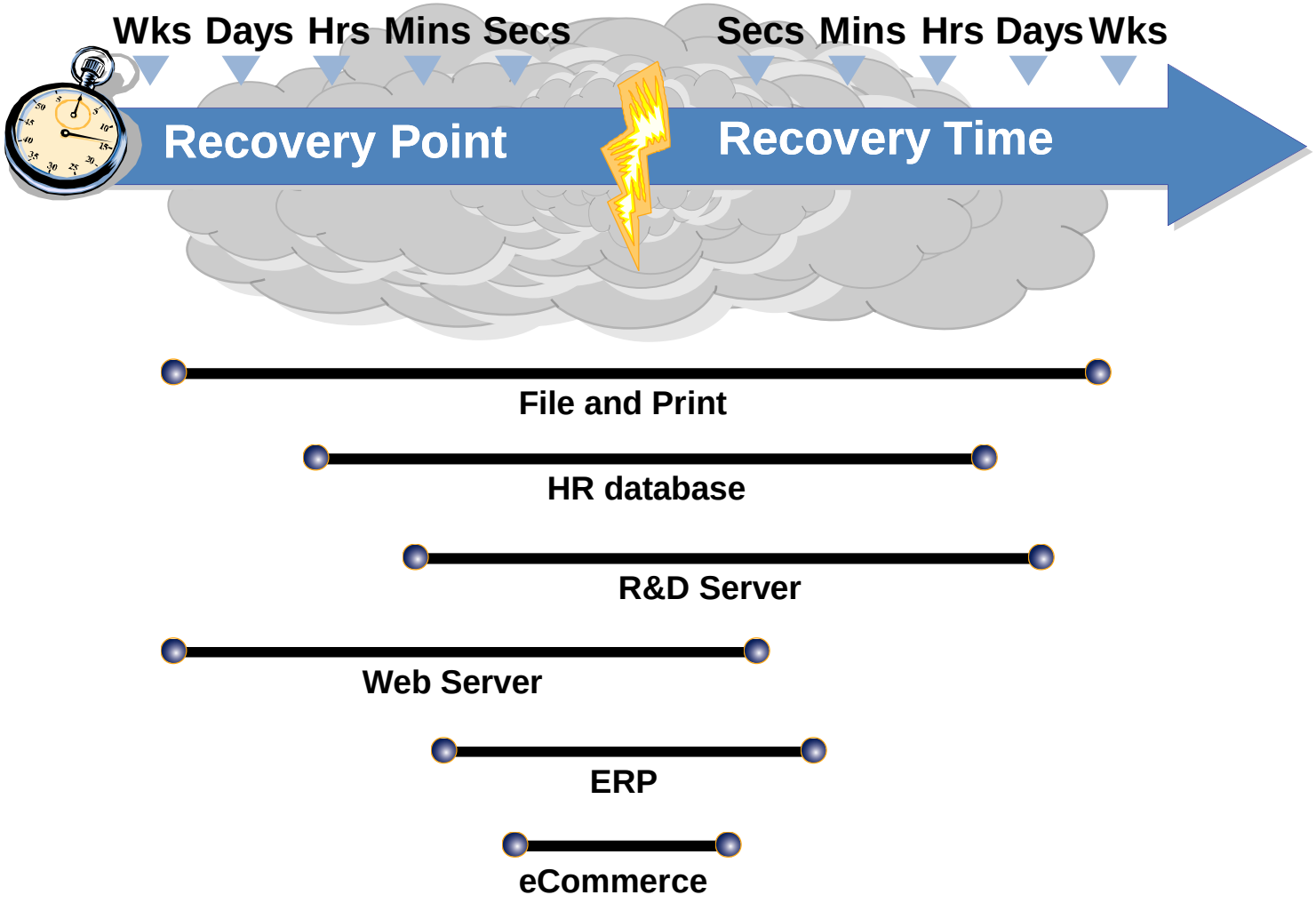
- Business needs drive the technology choice



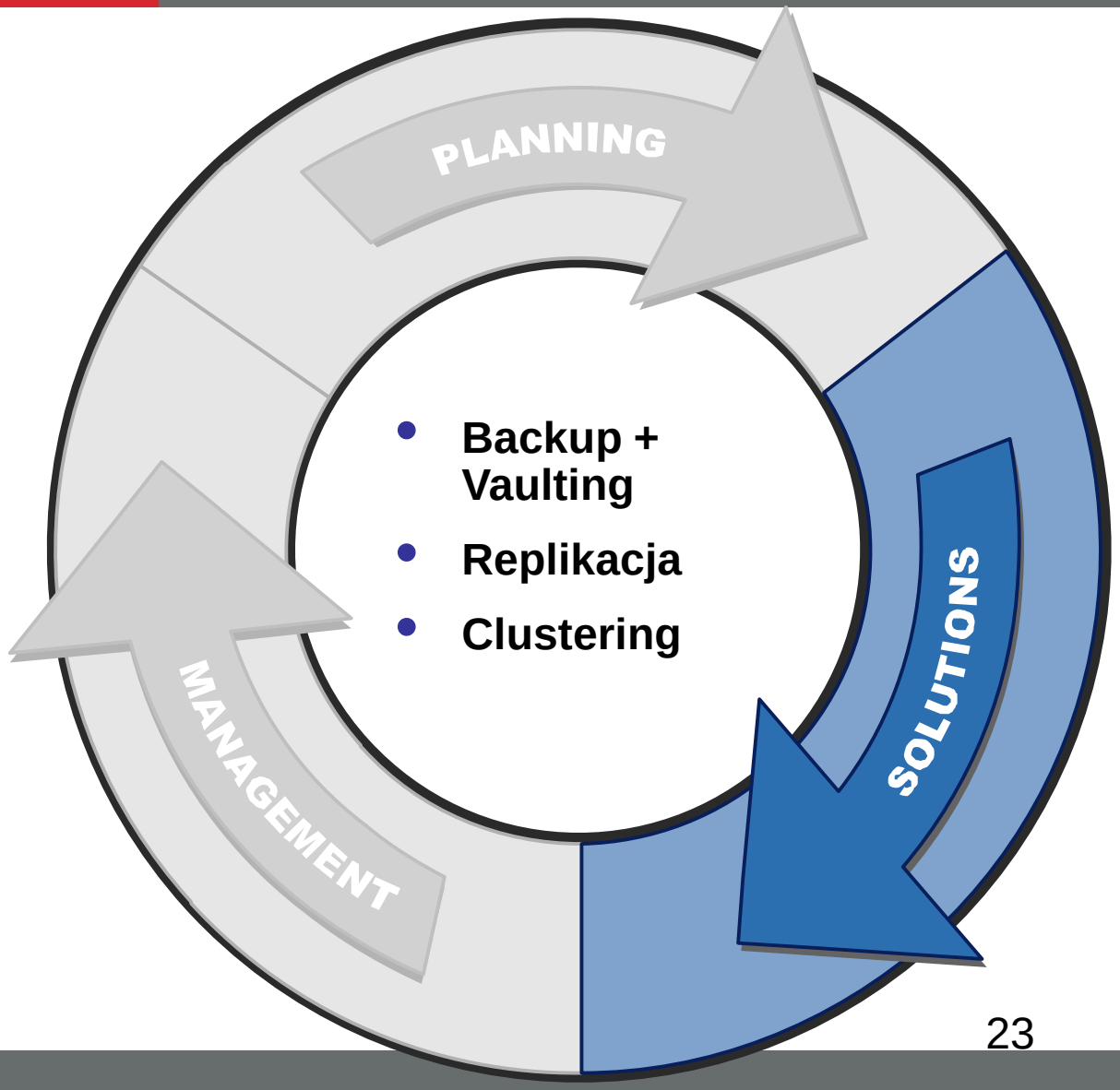

## Recovery Time includes:

- **Fault detection**
- **Recovering data**
- **Bringing apps back online**

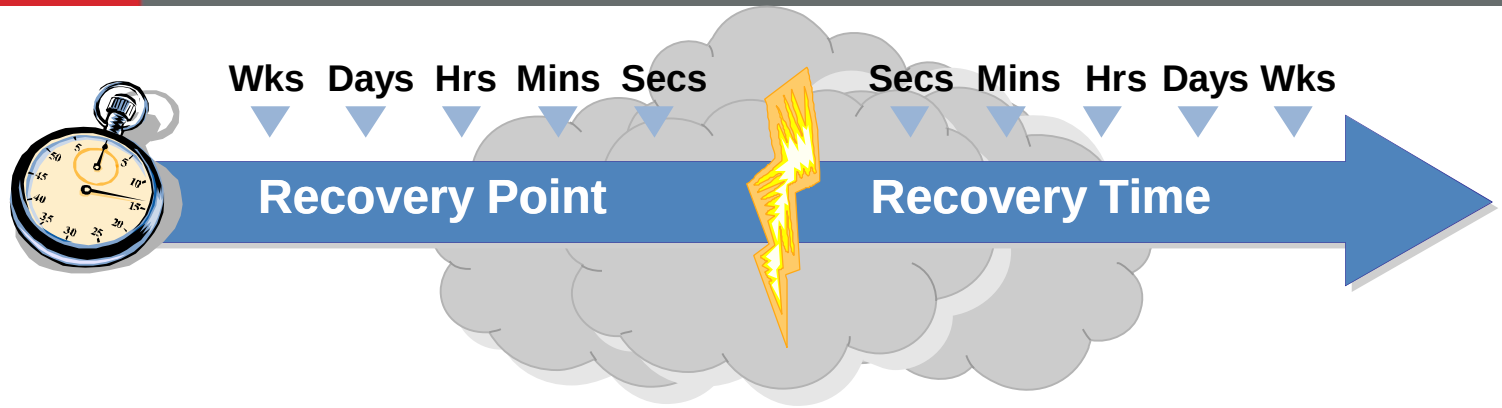
# Szacunki RPO/RTO usług

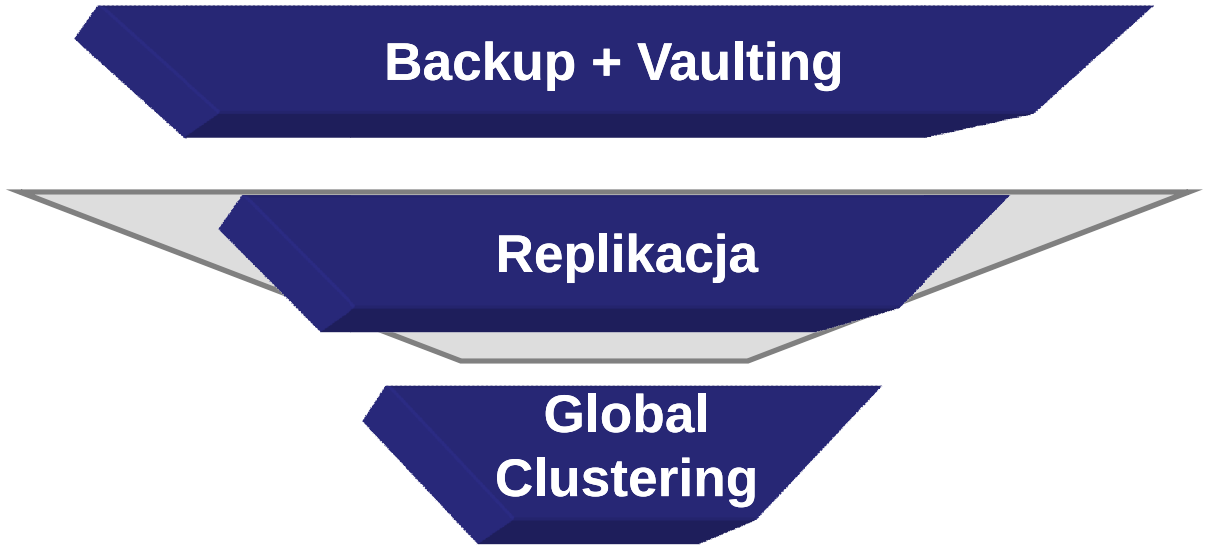


# DR Rozwiązania & Technologia

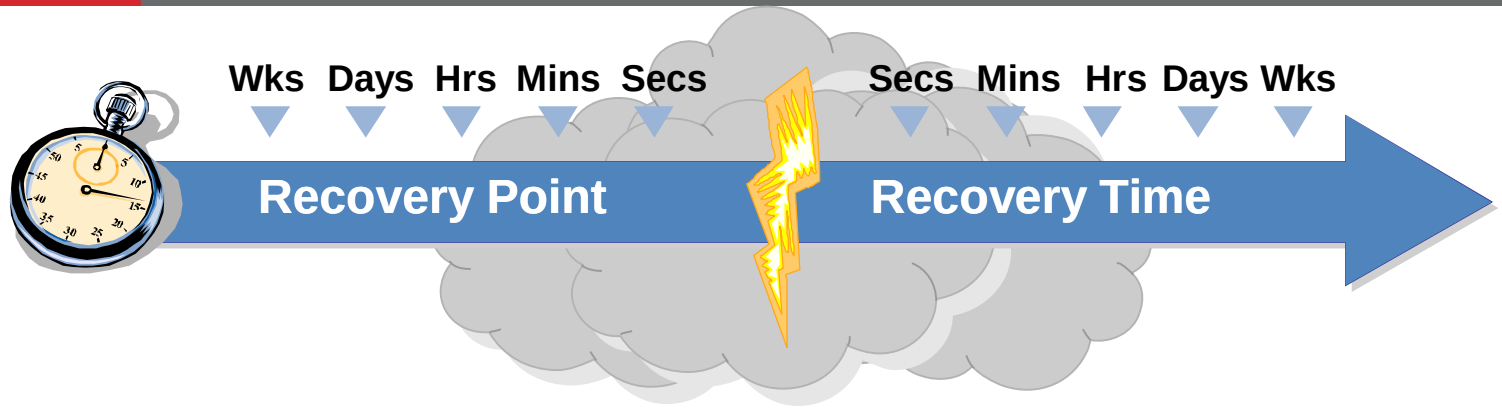


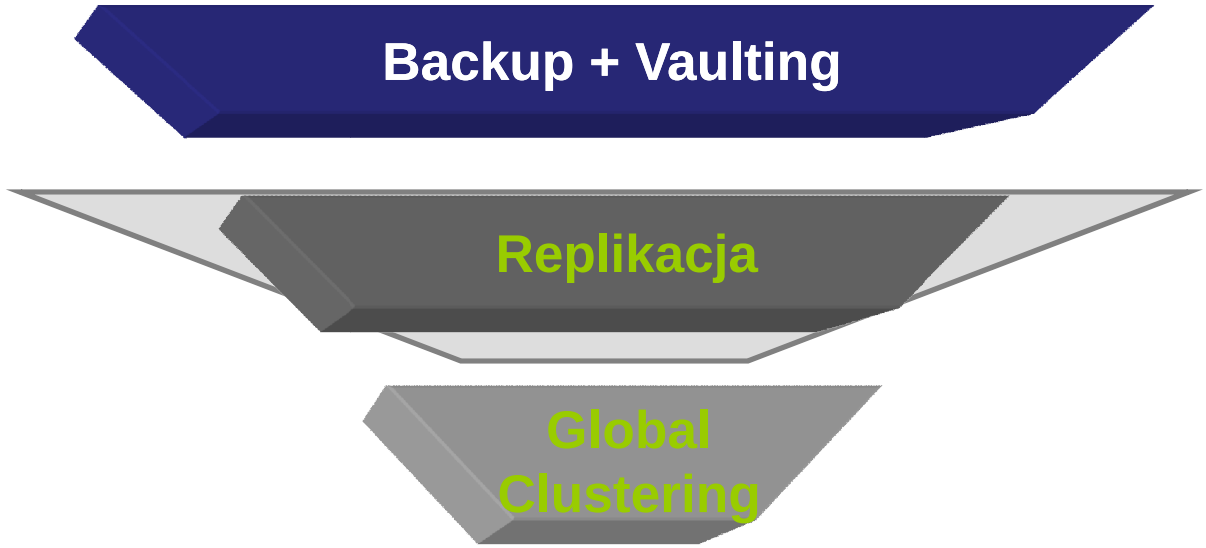
# Technologie DR



# Tape Backup & Vaulting

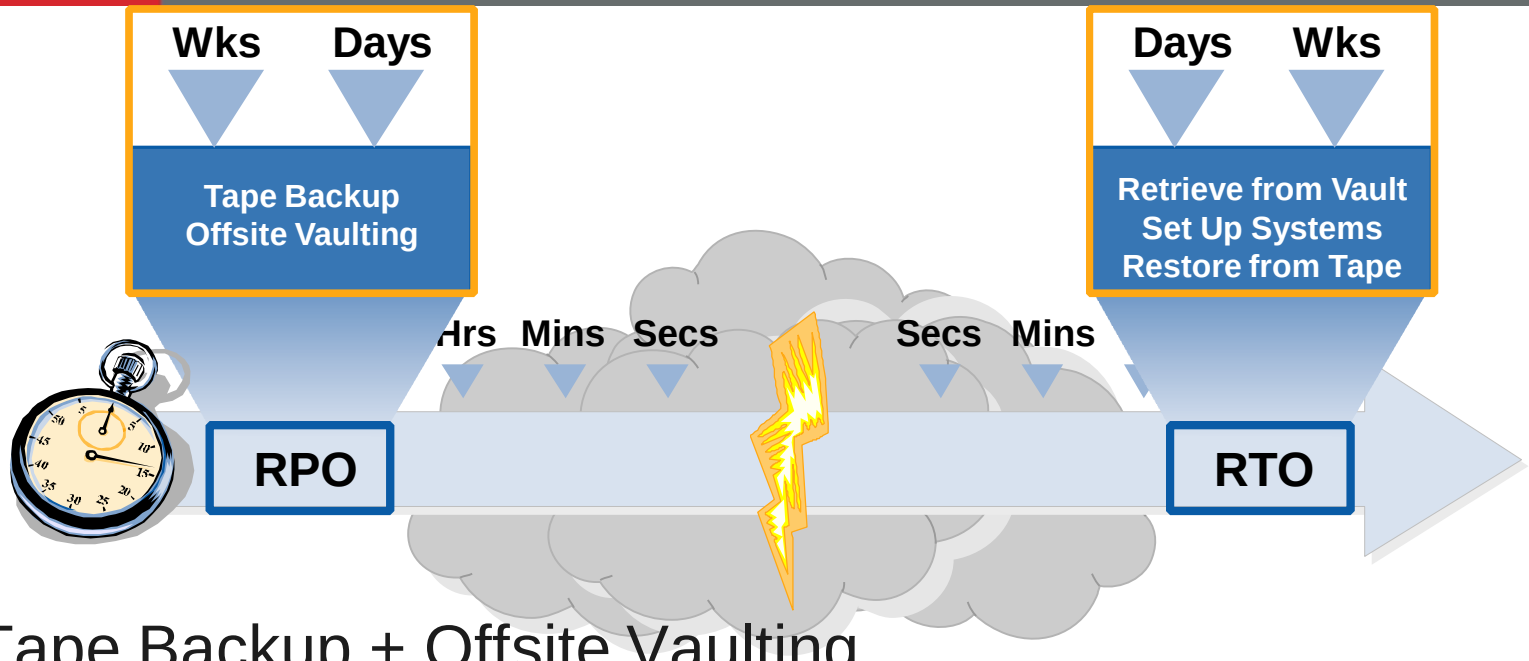


# Backupy w skrócie

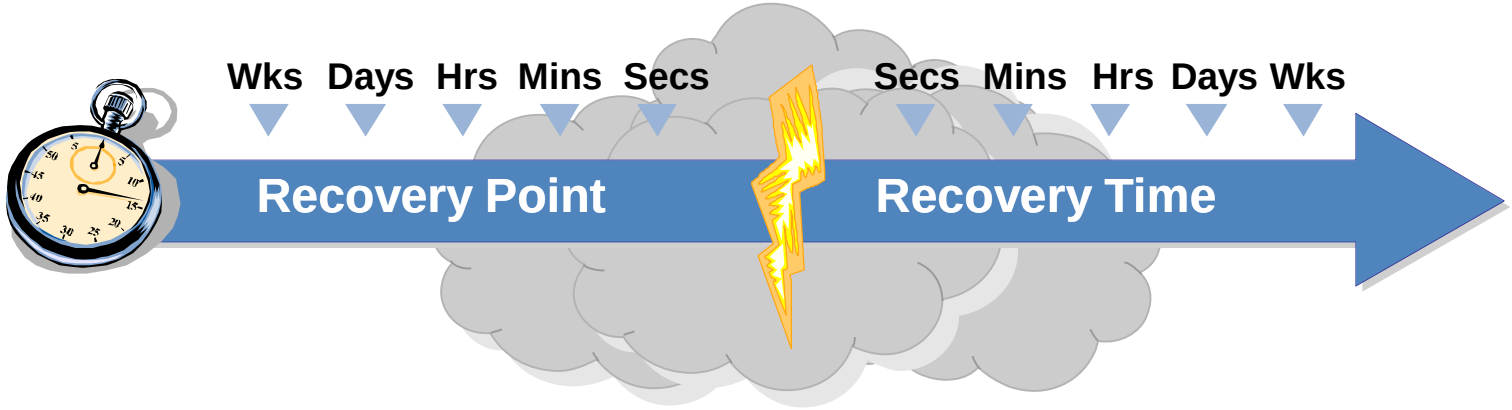
- Backup = podstawowe zabezpieczenie
  - Cold Backup = kilka godzin niedostępności systemu
  - Hot Backup = kilka godzin utraty wydajności systemu, skomplikowana procedura restore
  - Split-mirror backup, ZDB = chwilowa utrata wydajności, konsystentny backup
- Możliwość eksportu nośników do zdalnej lokalizacji. (Podstawowe DR)

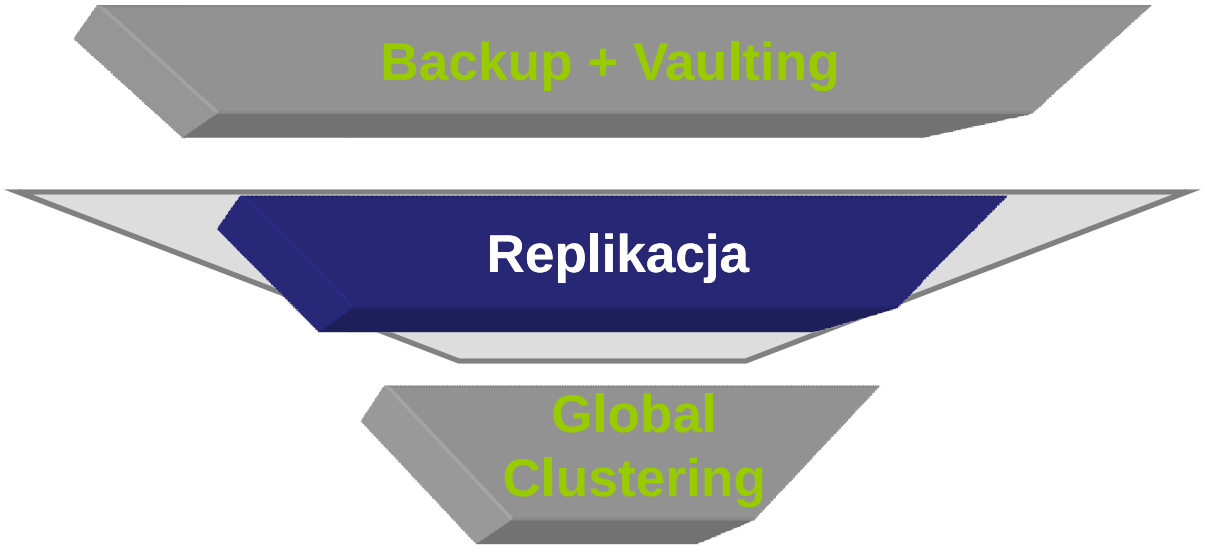
# Restore z backupu




- Tape Backup + Offsite Vaulting
  - **RPO** = Czas wykonania ostatniego backupu *przechowywanego offsite*
  - **RTO** = Czas potrzebny do odtworzenia danych z taśm

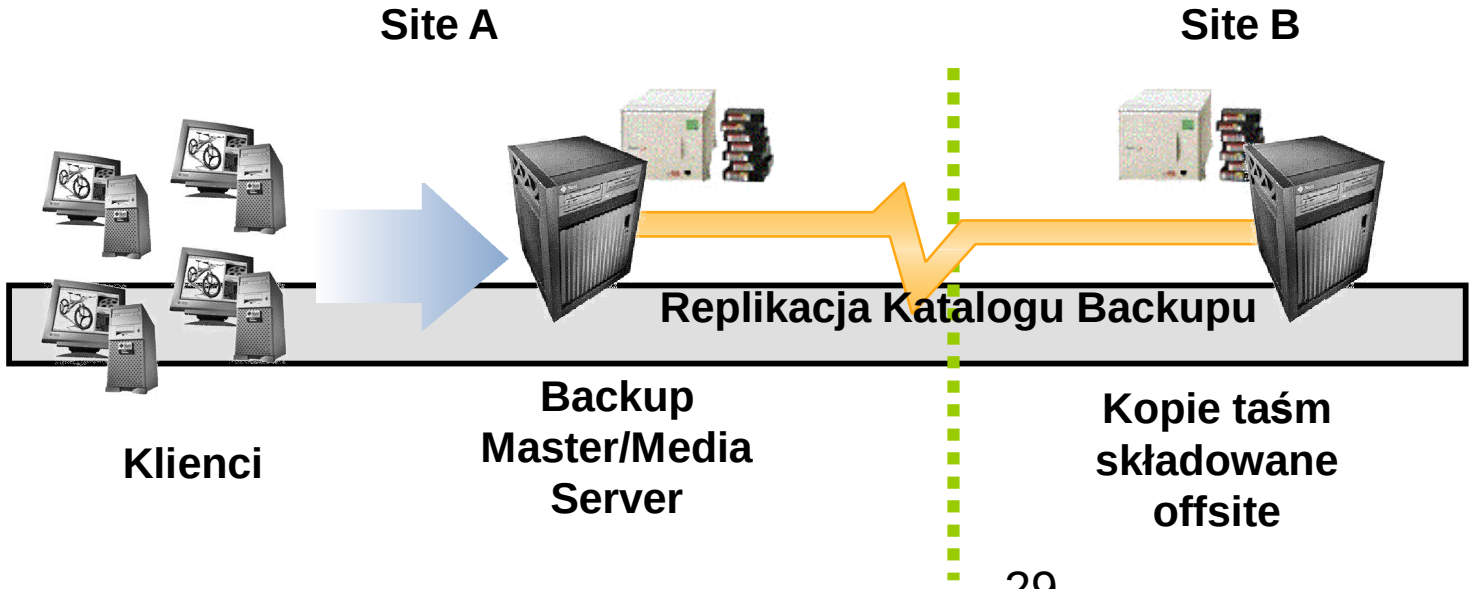
# Replikacja & Mirroring



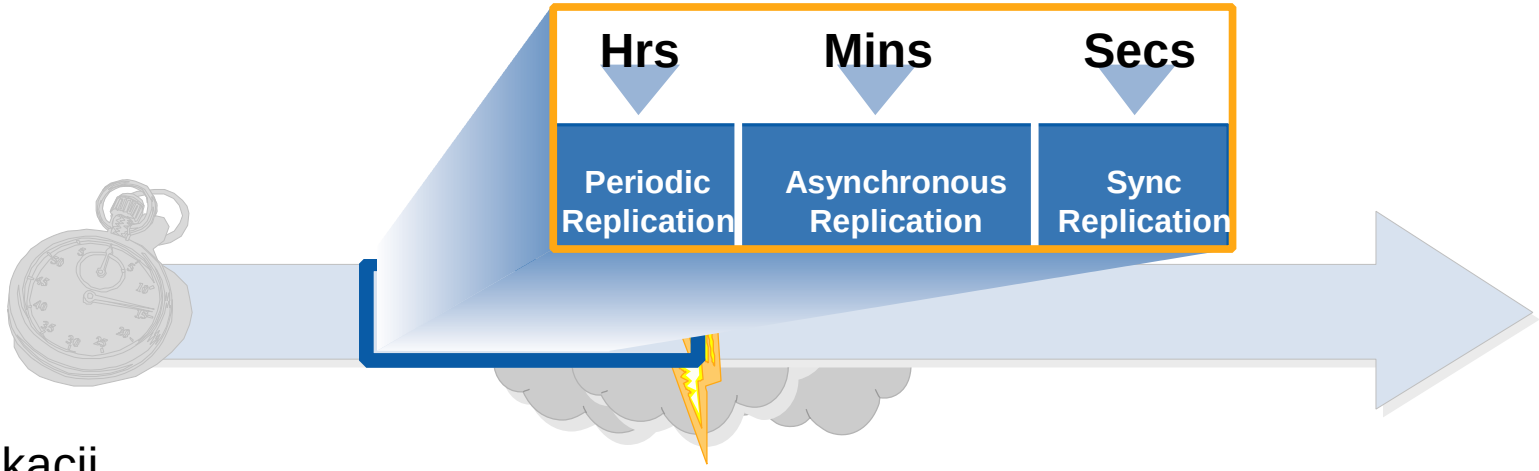



# Backup z replikacją katalogu

- Replikacja katalogu backupowego skraca czas RTO
  - Nie ma potrzeby rekatalogowania taśm
  - Nie ma potrzeby odtwarzania serwera backupu
  - Proces odtwarzania serwerów można zacząć od razu



# Replikacja & Mirroring




Tryby replikacji

- Synchroniczna
- Asynchroniczna
- Periodyczna

Możliwości techniczne

- Volume Management
- Replikacja hardware'owa
- Replikacja software'owa

- Synchroniczna vs Asynchroniczna
  - Synchroniczna = 100% kopia, wymaga szerokiego pasma, obniża wydajność systemu produkcyjnego.
  - Asynchroniczna = wierność kopii zależna od szerokości pasma, w razie awarii dane nie są w 100% aktualne, nie wpływa na wydajność systemu produkcyjnego.

# Replikacja synchroniczna

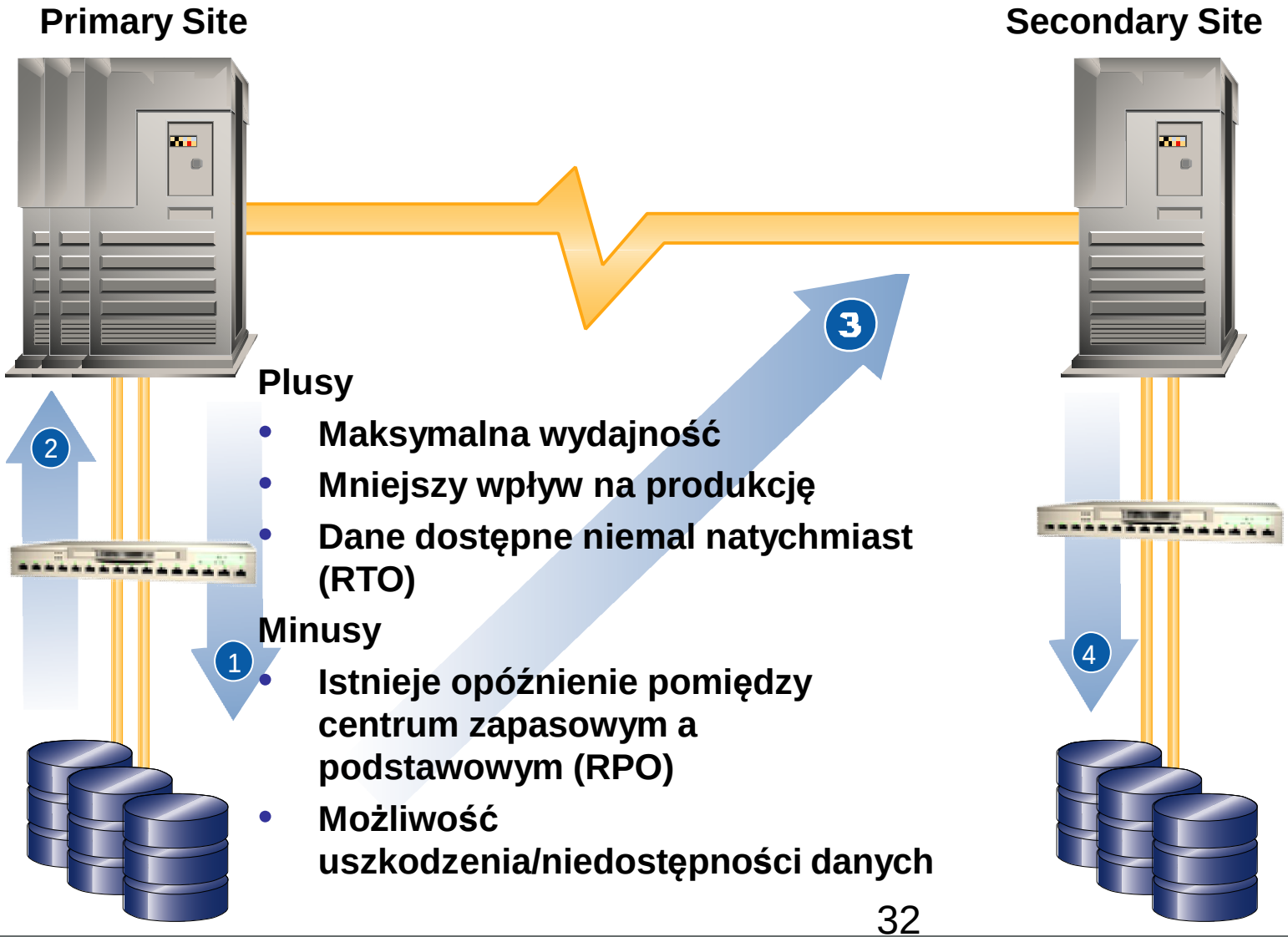

**Plusy**

- **Aktualność danych (RPO)**
- **Dane dostępne od razu (RTO)**

**Minusy**

- **Wymaga „szerokiego” łącza**
- **Opóźnienie na łączu powoduje opóźnienie pracy lokalnej**

# Replikacja asynchroniczna



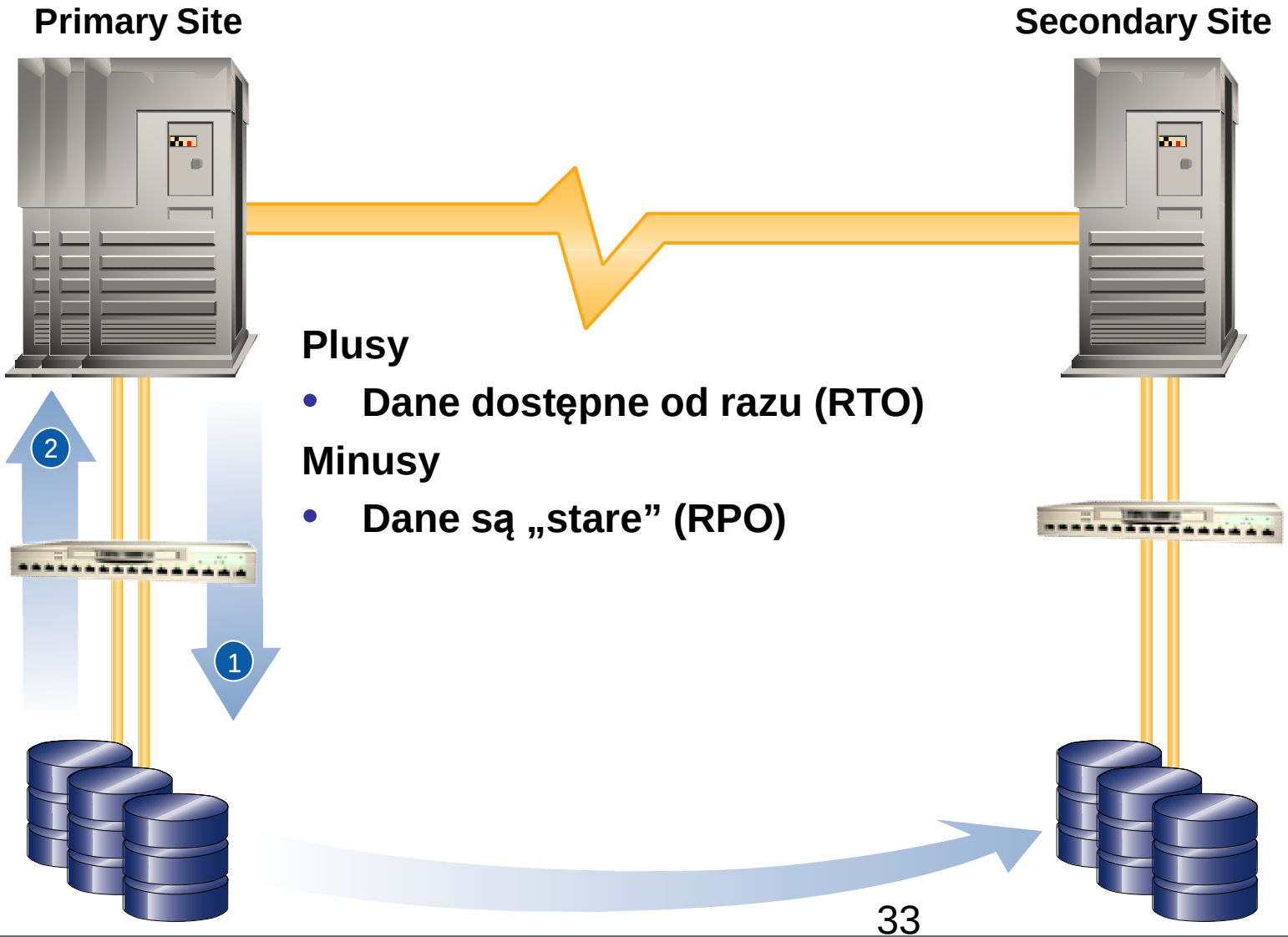

**Plusy**

- **Maksymalna wydajność**
- **Mniejszy wpływ na produkcję**
- **Dane dostępne niemal natychmiast (RTO)**

**Minusy**

- **Istnieje opóźnienie pomiędzy centrum zapasowym a podstawowym (RPO)**
- **Możliwość uszkodzenia/niedostępności danych**

# Replikacja periodyczna



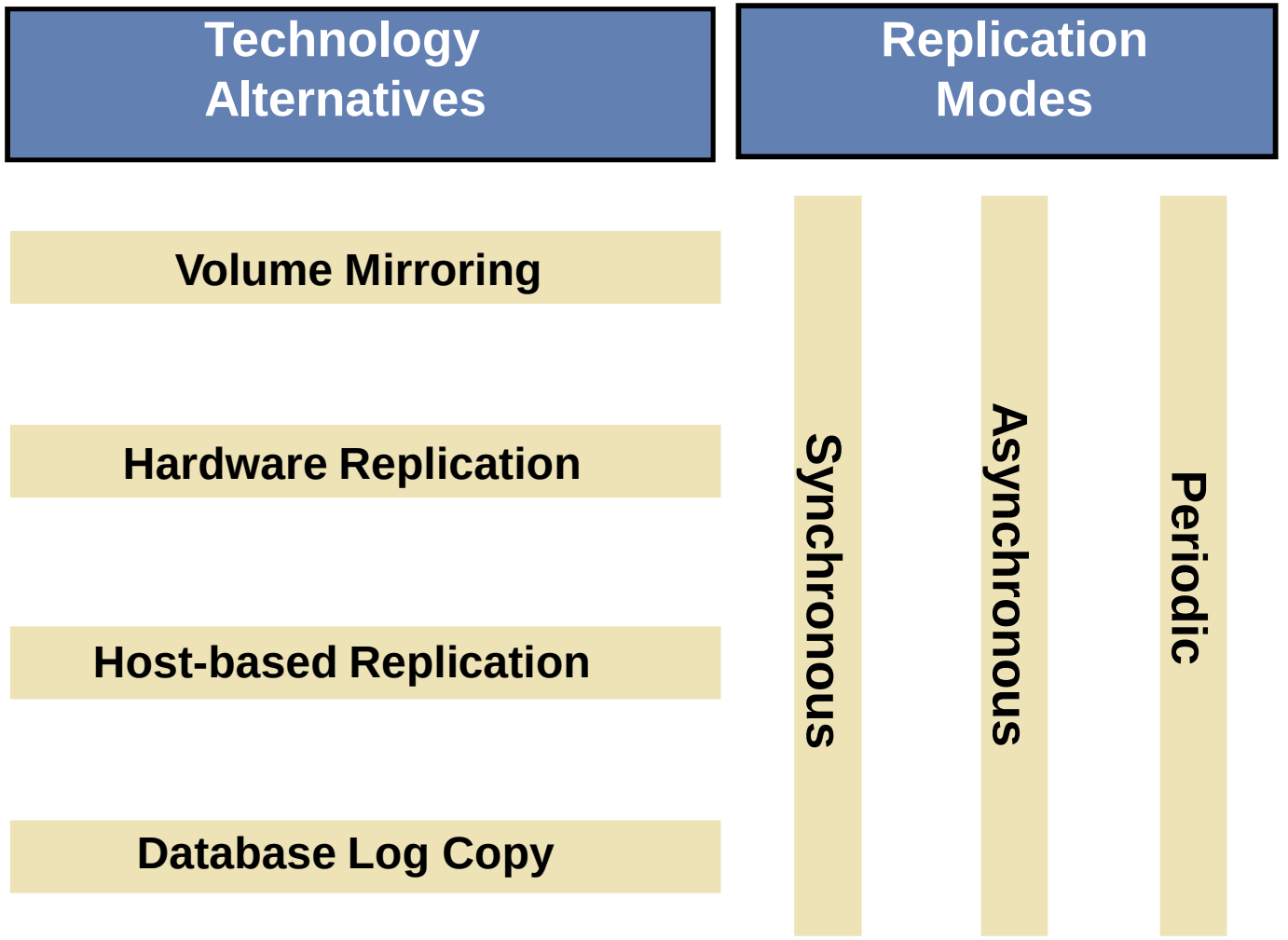

**Plusy**

- **Dane dostępne od razu (RTO)**

**Minusy**

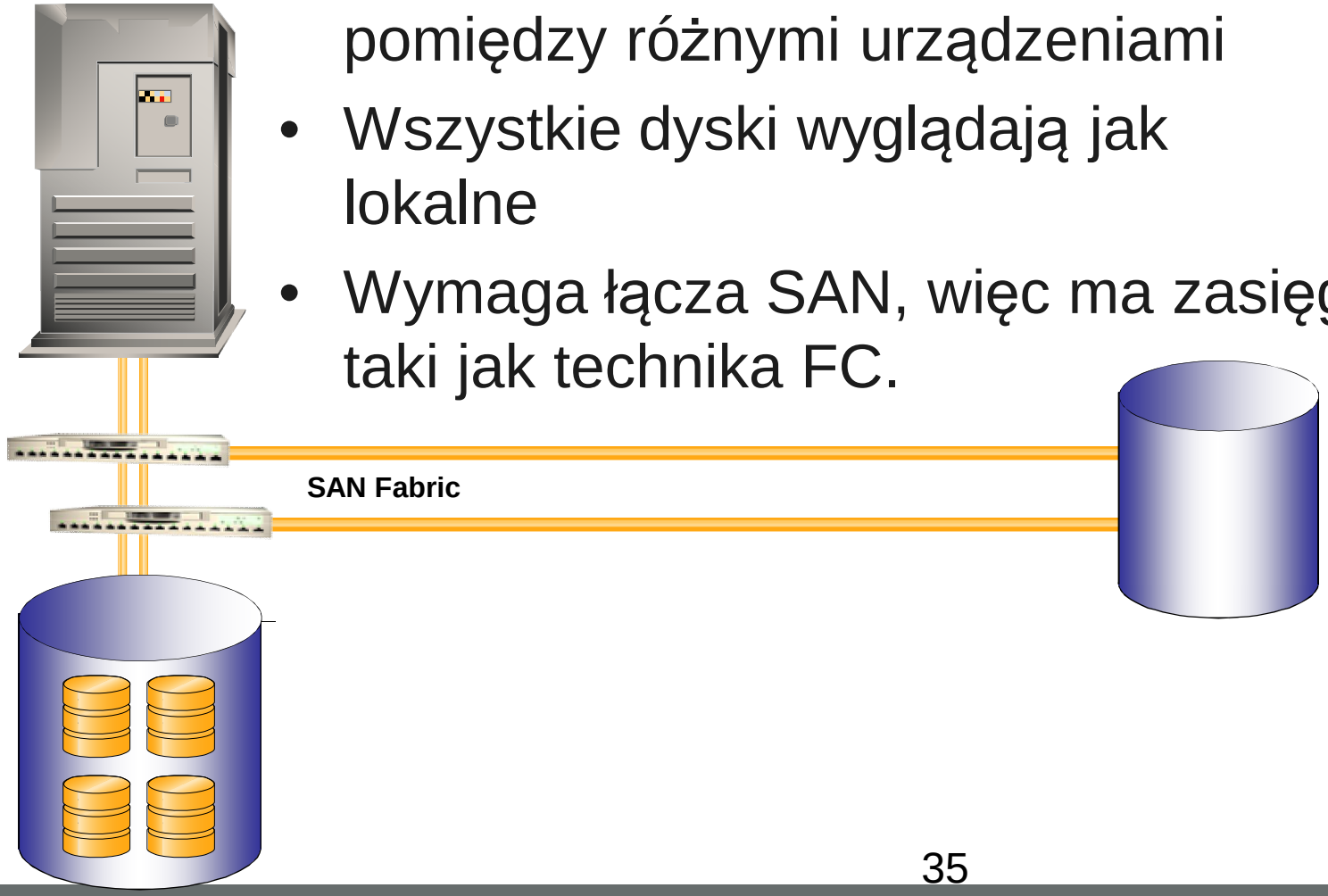
- **Dane są „stare” (RPO)**

# Możliwości replikacji



# Wykorzystanie VM do replikacji (Remote Mirroring)

- Umożliwia replikację danych pomiędzy różnymi urządzeniami
- Wszystkie dyski wyglądają jak lokalne
- Wymaga łącza SAN, więc ma zasięg taki jak technika FC.

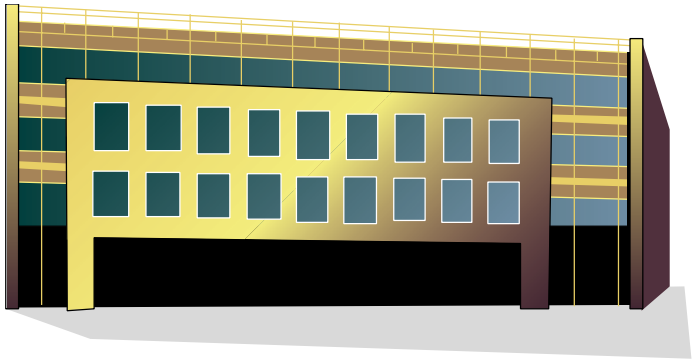


# Remote mirror czy replikacja ?

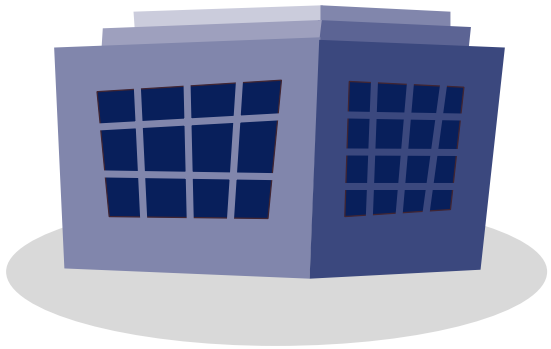
**Logical Volume Mirror**

**Data Replication**

**1 m** **10 m** **1 km** **10 km** **100 km** **1000 km** **10,000 km**



**Primary Site**



**Secondary Site**

# Replikacja hardware'owa

## Plusy

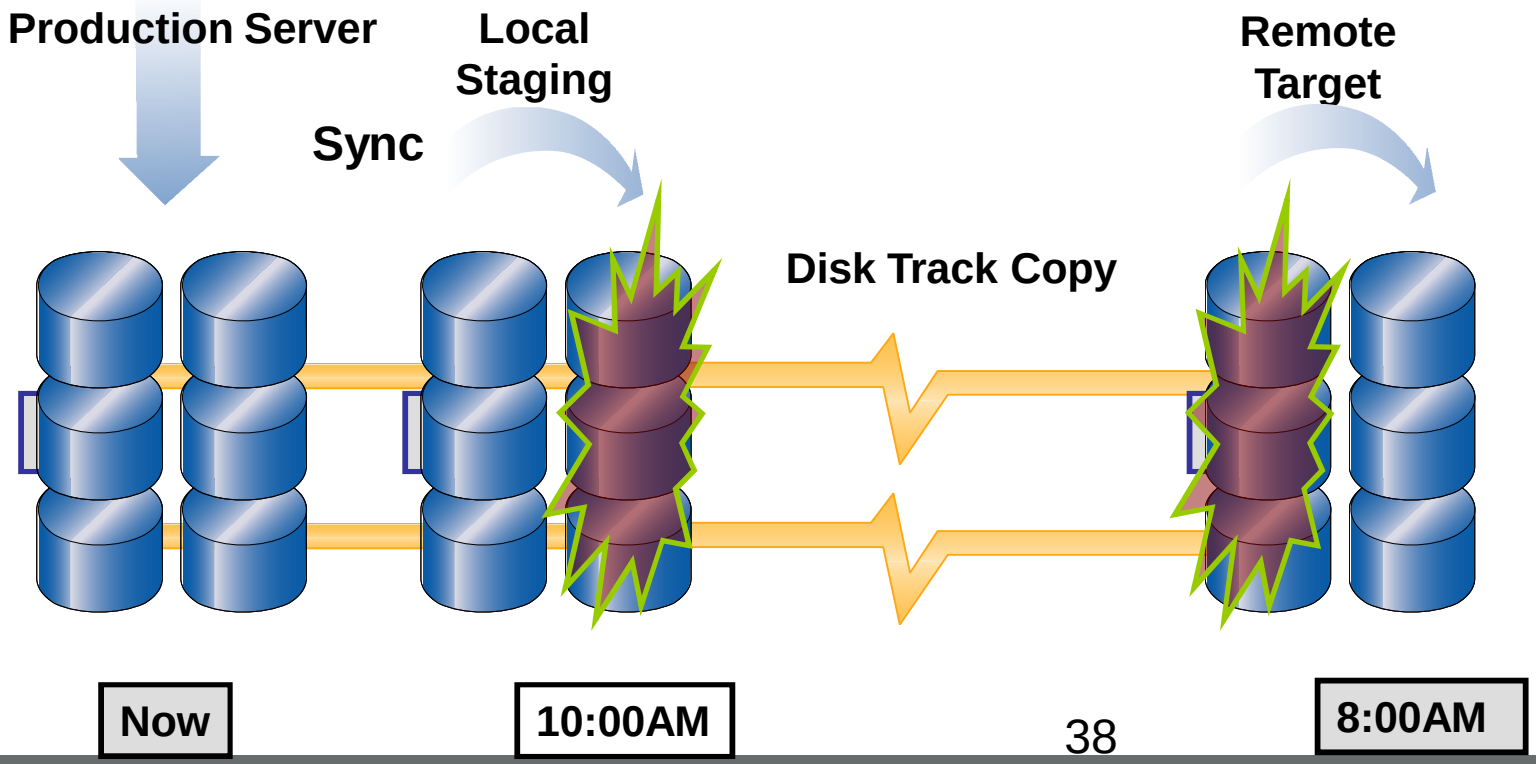
- „Niezależność" od systemu operacyjnego, i jego stanu.

## Minusy

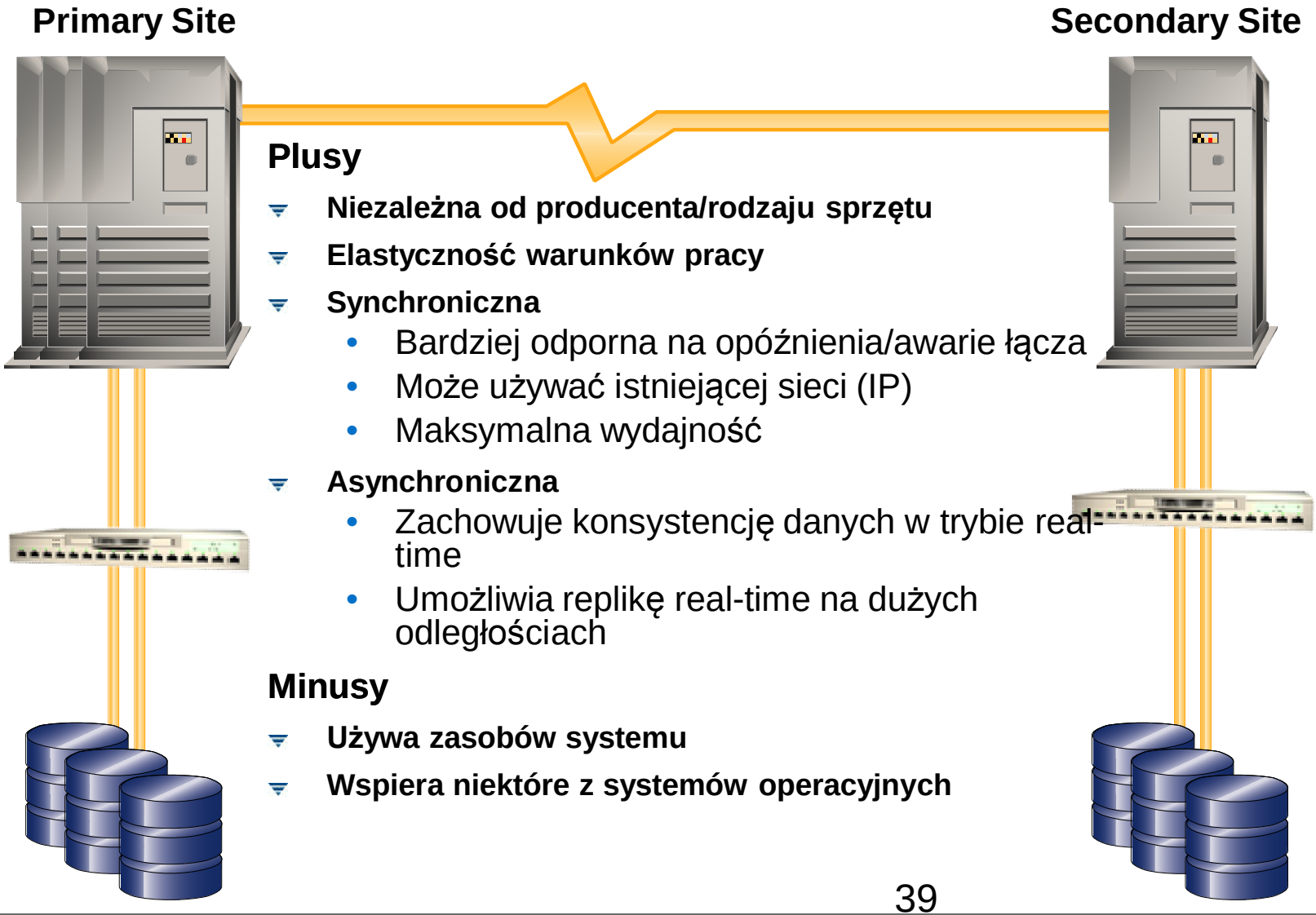
- Przywiązanie do jednego producenta
  - Wyższy koszt per MB/GB/TB
  - Wyższy koszt wdrożenia rozwiązania/licencji
- Tryb synchroniczny
  - Praktyka pokazuje znaczny wpływ na wydajność produkcji
  - Tryb ten w rozwiązaniu jest wygodniejszy, tańszy, elastyczniejszy.
- Tryb asynchroniczny
  - Problemy z integralnością danych (jest na poziomie HW, nie SW)
  - "Asynchroniczna" replikacja często oznacza "periodyczną"
- Periodyczna
  - „Stare" dane
  - Wymaga znacznie więcej dysków (nawet 5X – 7X więcej)

# Replikacja sprzętowa - Async/Periodyczna

- Wymaga używania snapshotów do zachowania konsystencji
- Wymaga dużo więcej dysków
- Dane są „starsze” (RPO)



# Replikacja software'owa



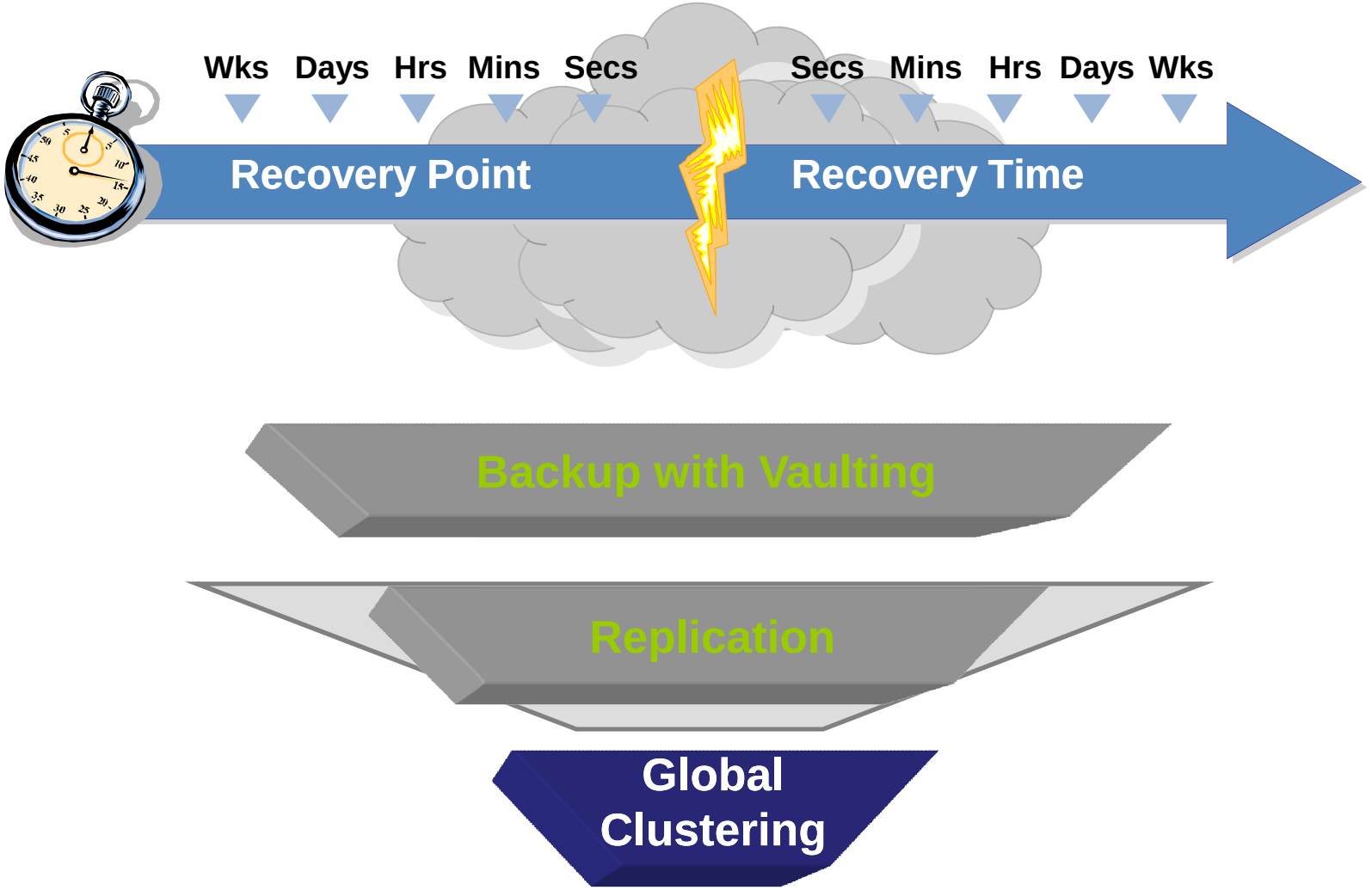

**Plusy**

- **Niezależna od producenta/rodzaju sprzętu**
- **Elastyczność warunków pracy**
- **Synchroniczna**
  - Bardziej odporna na opóźnienia/awarie łącza
  - Może używać istniejącej sieci (IP)
  - Maksymalna wydajność
- **Asynchroniczna**
  - Zachowuje konsystencję danych w trybie real-time
  - Umożliwia replikę real-time na dużych odległościach

**Minusy**

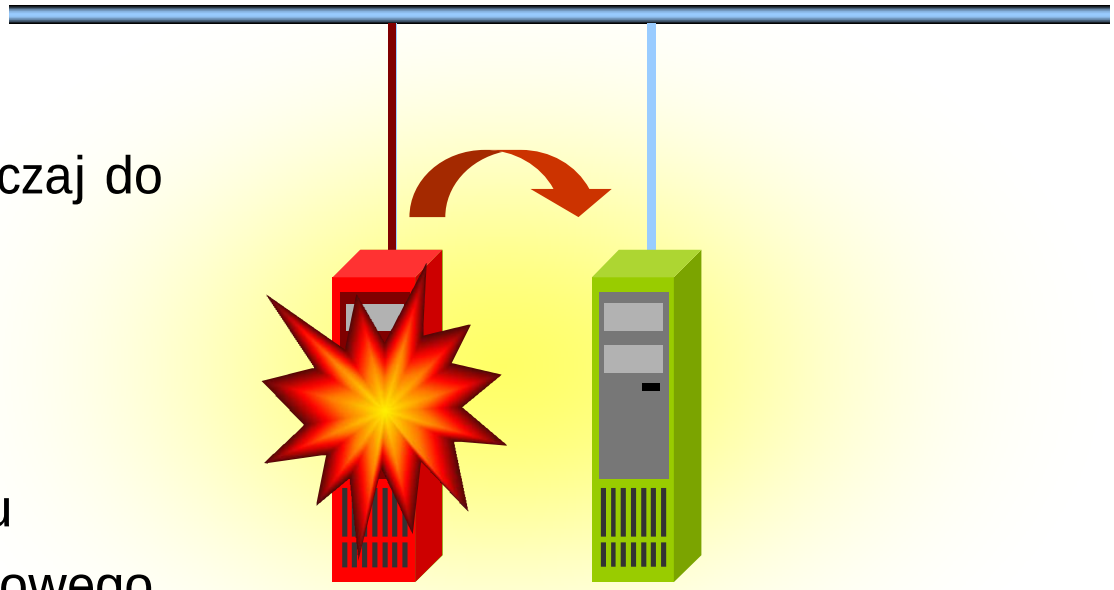
- **Używa zasobów systemu**
- **Wspiera niektóre z systemów operacyjnych**

# Clustering



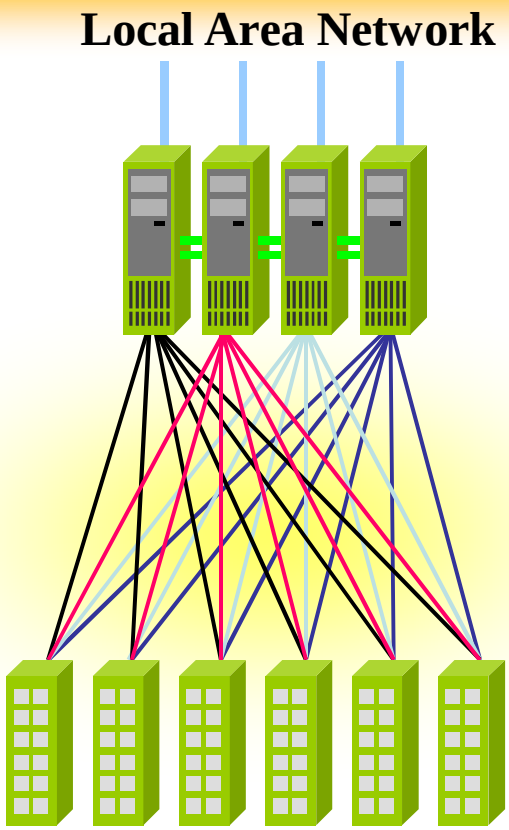
# Klastry

- Tradycyjny klaster
  - Ograniczony zazwyczaj do dwóch node'ów, rozstawionych na odległość ok. 25m
  - Wymaga 100% redundancji sprzętu
- Możliwość natychmiastowego Disaster Recovery, bez udziału obsługi
- DR ograniczone do klas Oprogramowanie, System



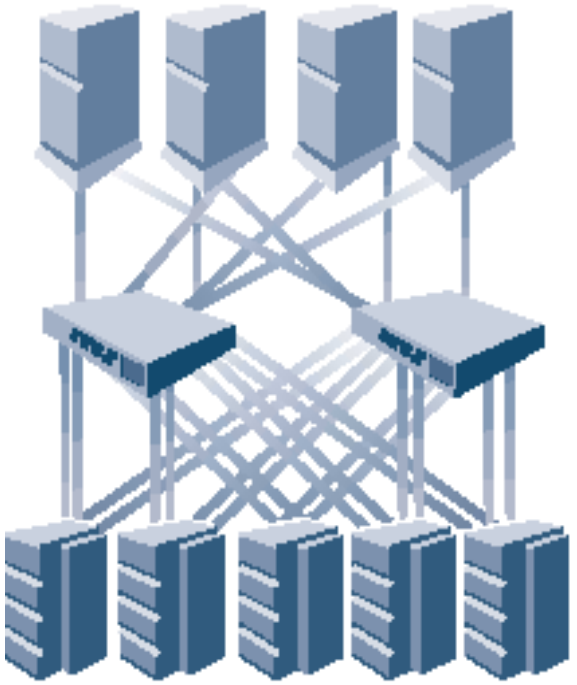
# Klastry cd...

- Klaster rozszerzony
  - Klaster wielonodowy, lecz wciąż ograniczony długością magistral SCSI, bez możliwości redundancji łączy
  - Skomplikowane połączenia pomiędzy serwerami a urządzeniami dyskowymi, bardziej podatny na awarie
- Możliwość natychmiastowego Disaster Recovery, bez udziału obsługi
- DR ograniczone do klas Oprogramowanie, System



# <99,999% Klastry „kampusowe”

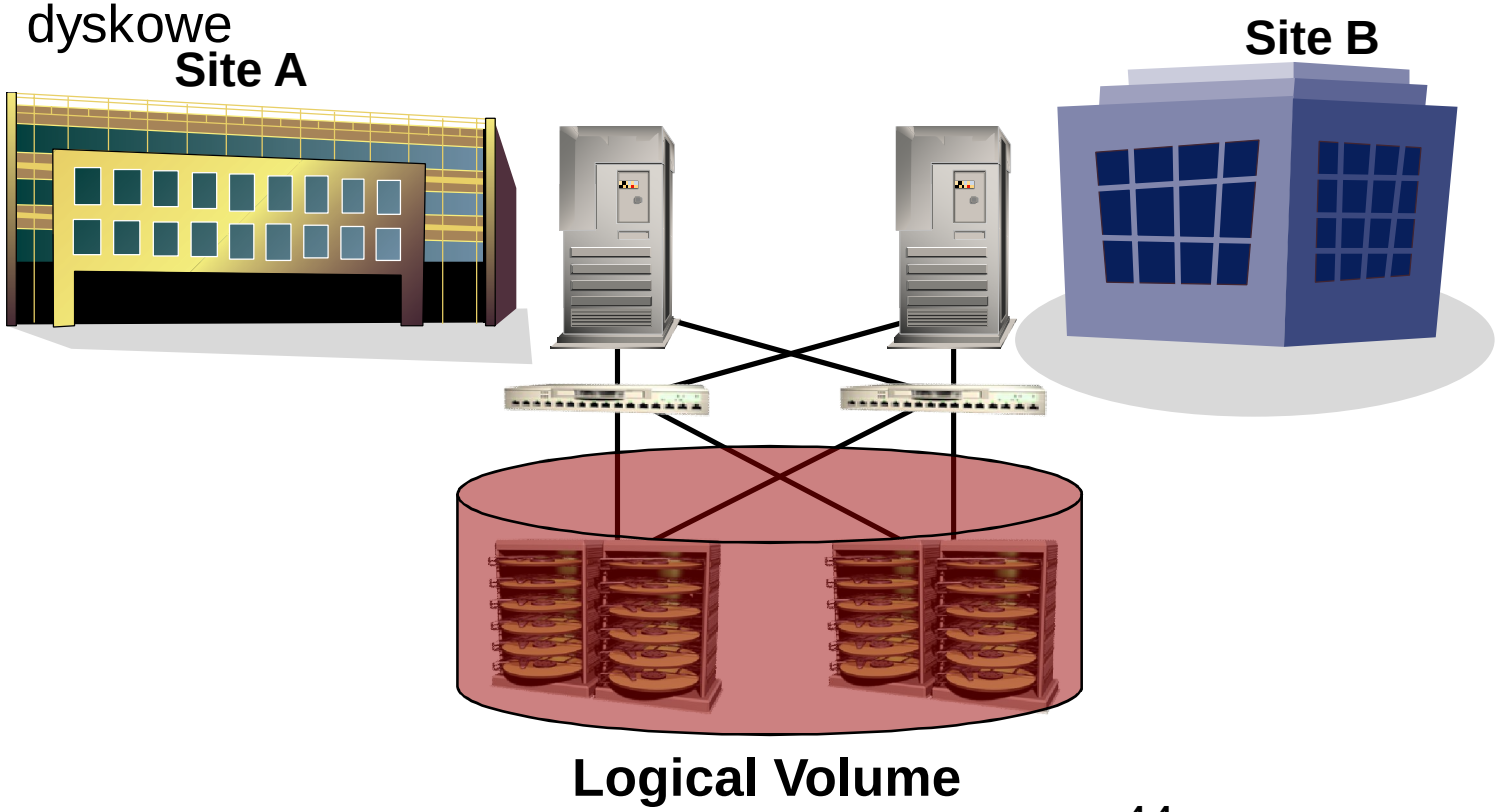
- Klaster multi-nodowy w środowisku Storage Area Network (stretched)
  - Klaster wielonodowy, używający łączy FibreChannel (proste połączenia, redundancja łączy, długość segmentu ograniczona technologią FC)
  - Odporny na awarię, failover na poziomie aplikacji (policy-based)
- Możliwość automatycznego Disaster Recovery, z przeniesieniem aplikacji
- DR we wszystkich klasach zasięgu



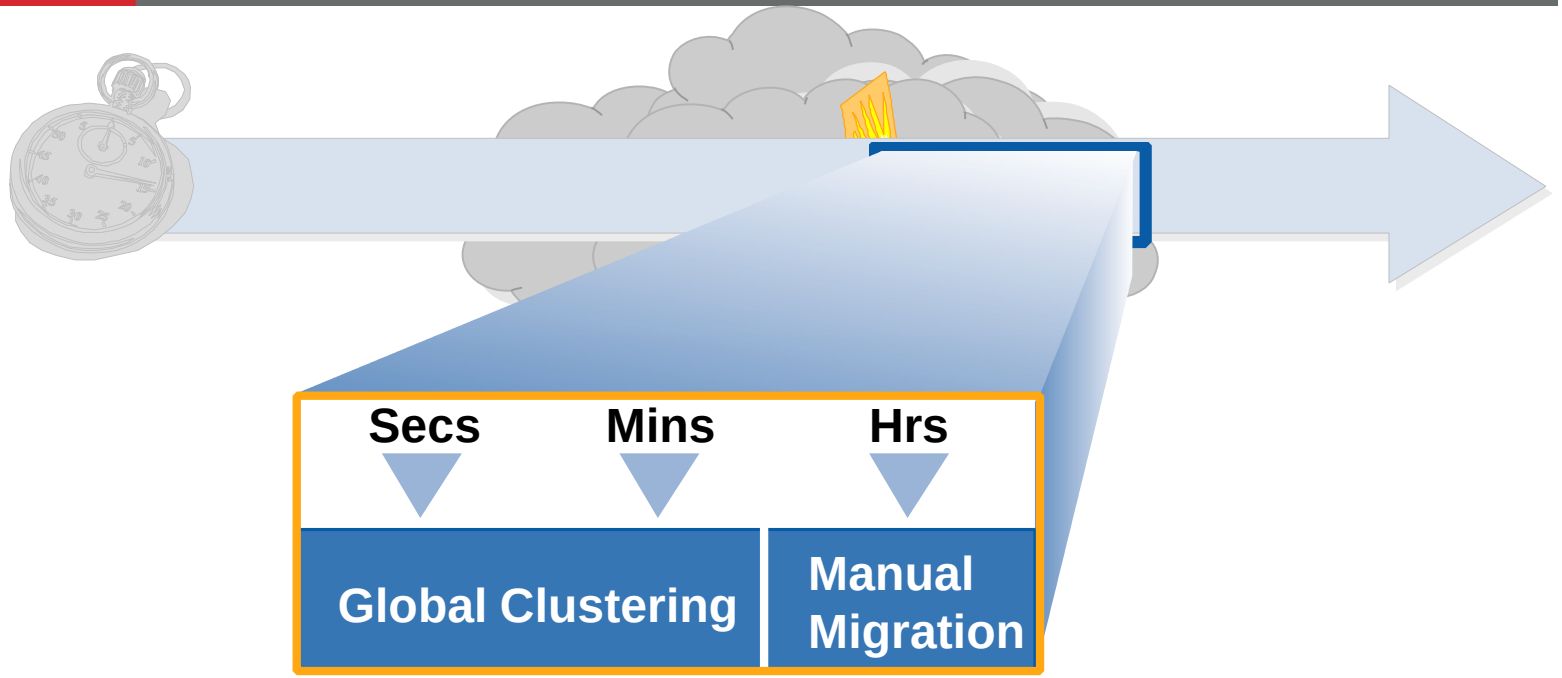
BiG Vent

# Klastry „kampusowe”

- **Klaster rozciągnięty pomiędzy budynkami**
  - Wykorzystuje sieć SAN do współdzielenia urządzeń dysków
  - Wykorzystuje software’owy RemoteMirror, jako zasoby dyskowe



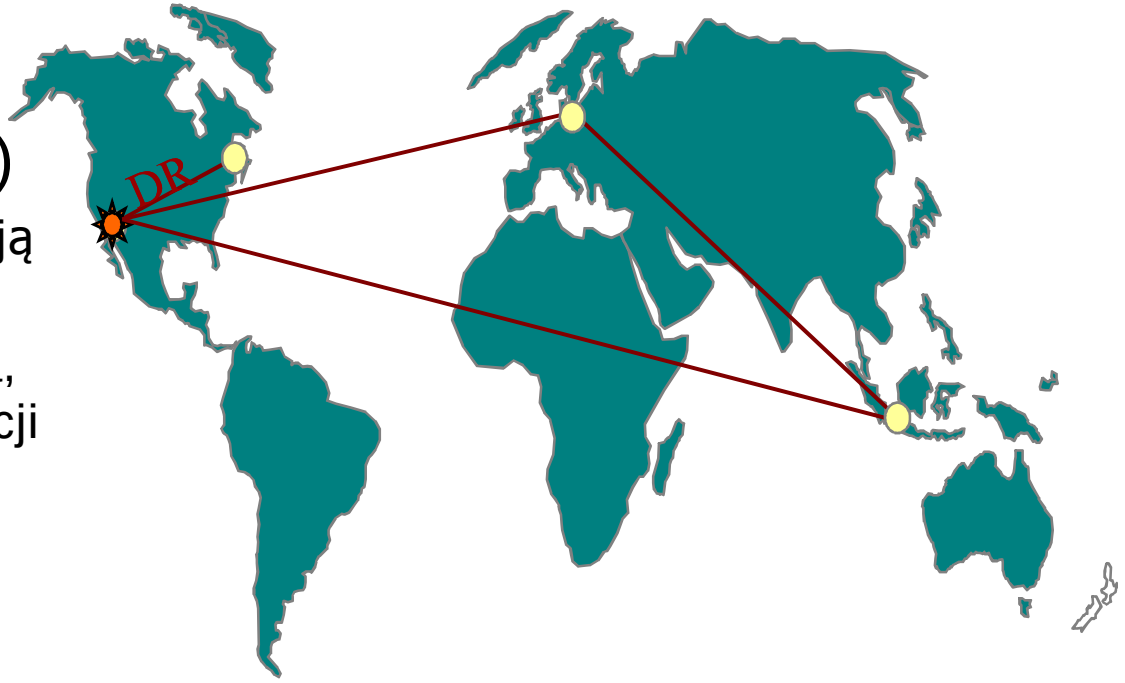
# Global Clustering




- **Założenia „klastra klastrów”**
  - **Wykorzystuje klastry lokalne**
  - **Wykorzystuje replikację**
  - **Failover usługi następuje najpierw lokalnie w ośrodku, dopiero jeśli to niemożliwe następuje przełączenie usługi do innego ośrodka**

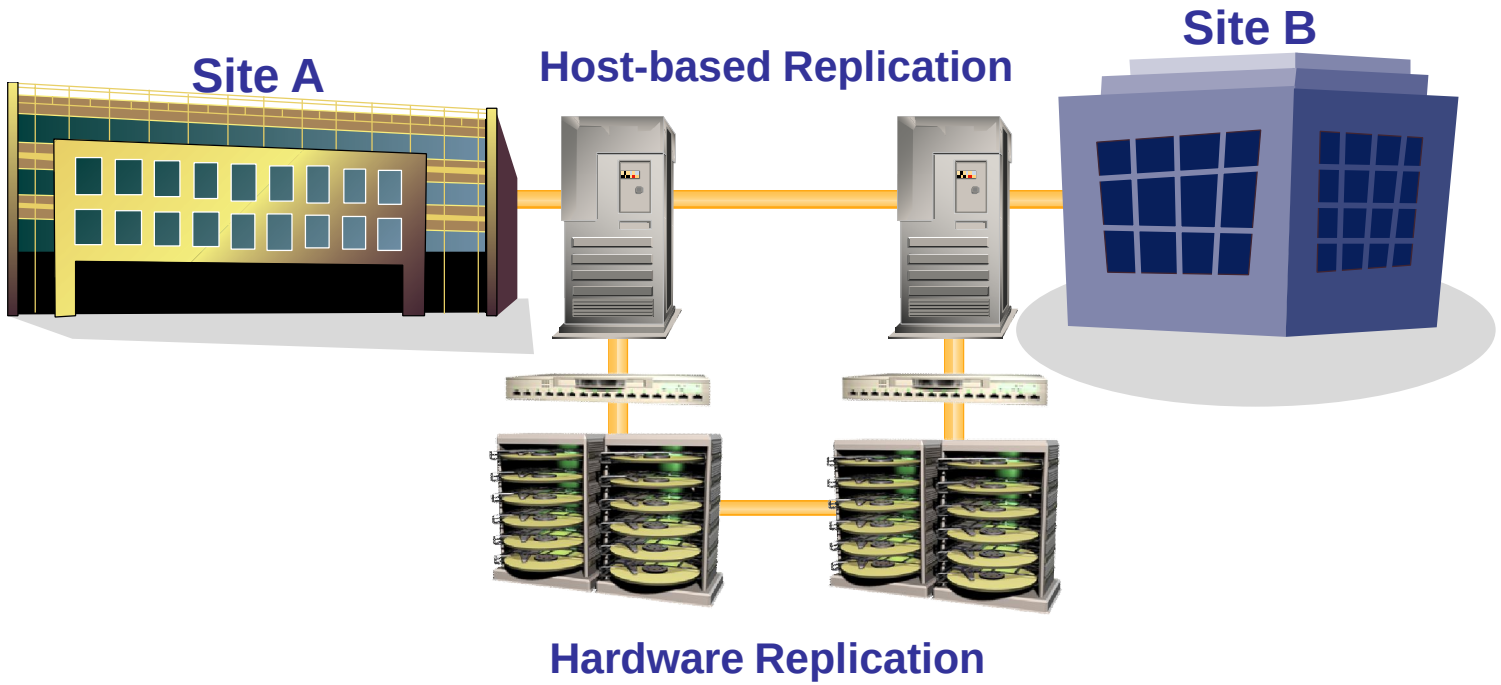
# BiG Vent <= 99,9999 Klastry WAN

- Klastry na duże odległości (GEOCluster)
  - Połącznie klastra z replikacją danych
  - Dynamiczna rekonfiguracja, failover na poziomie aplikacji (policy-based)
- Możliwość automatycznego Disaster Recovery, z przeniesieniem aplikacji typu mission-critical
- DR we wszystkich klasach zasięgu
- Szczyt współczesnej technologii

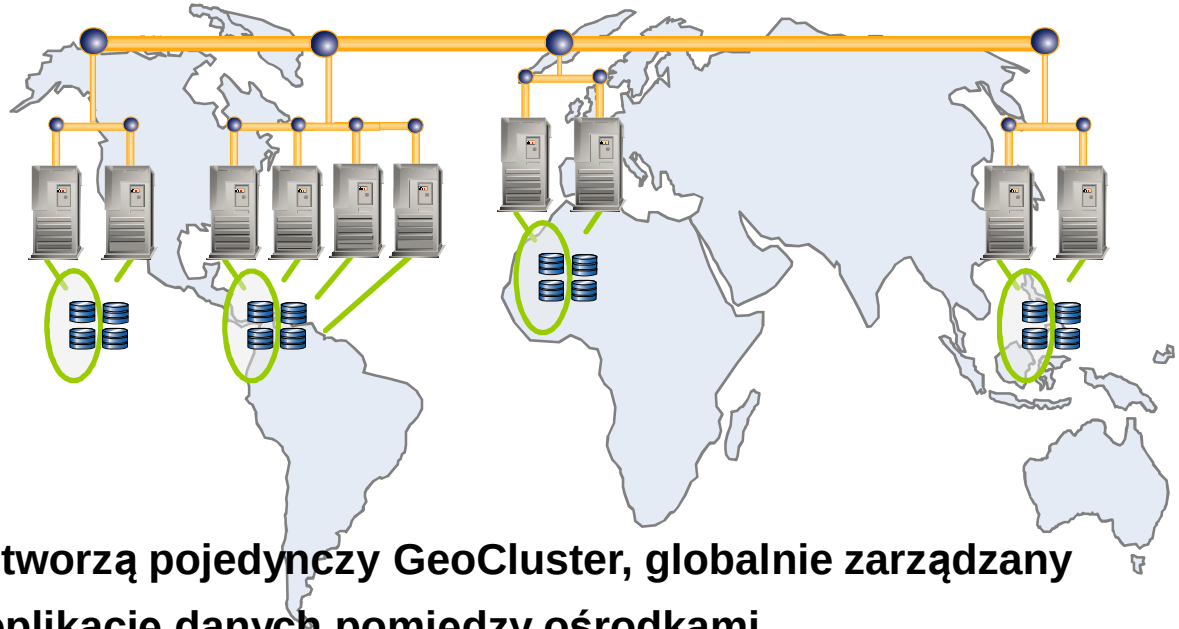


# Klastry „shared-nothing” z replikacją HW

- **Klaster obejmujący (zazwyczaj 2) ośrodki**
  - Pojedynczy klaster rozciągnięty pomiędzy ośrodkami
  - Wykorzystuje replikację danych



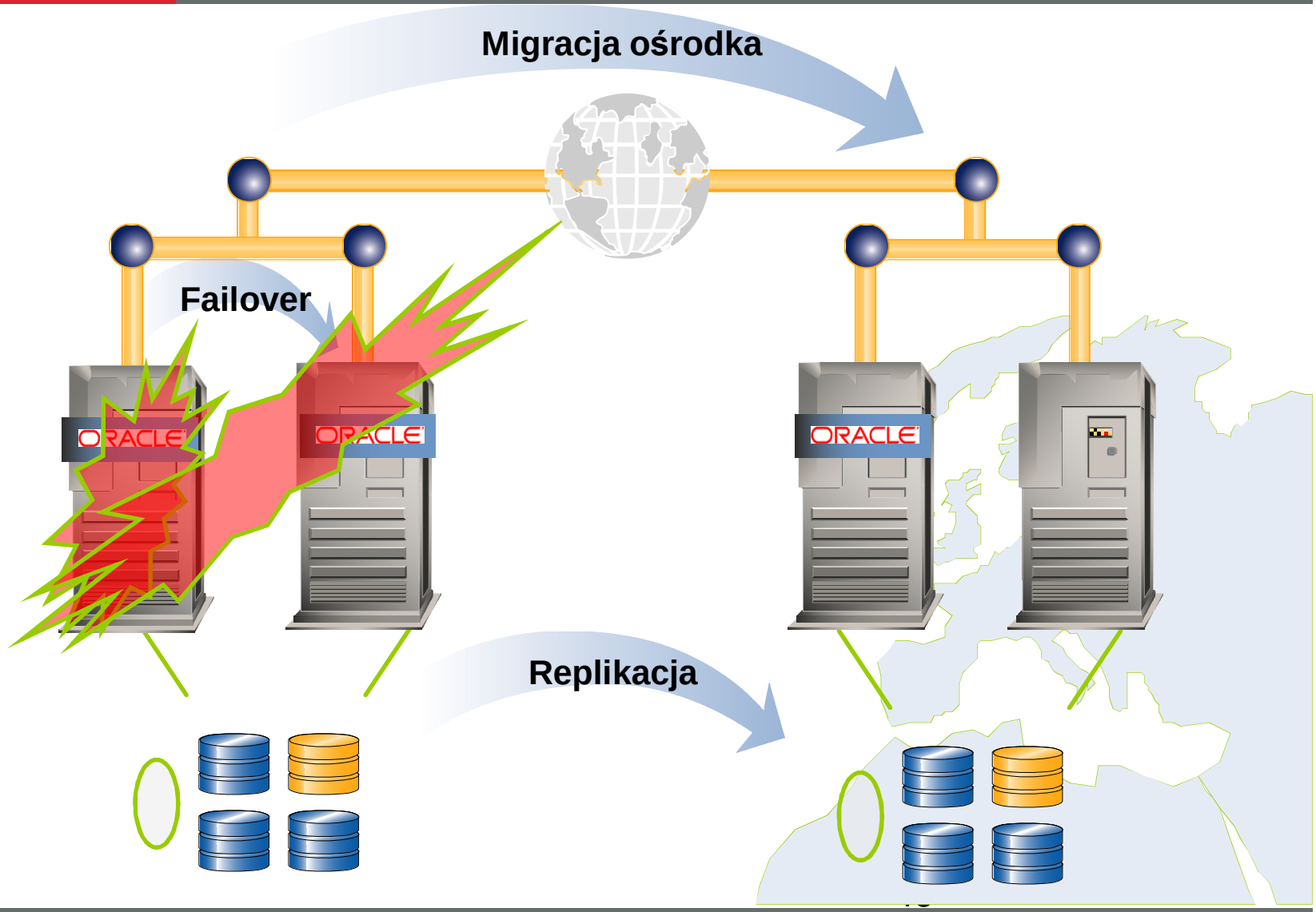
# Global Clustering – Klaster klastrów



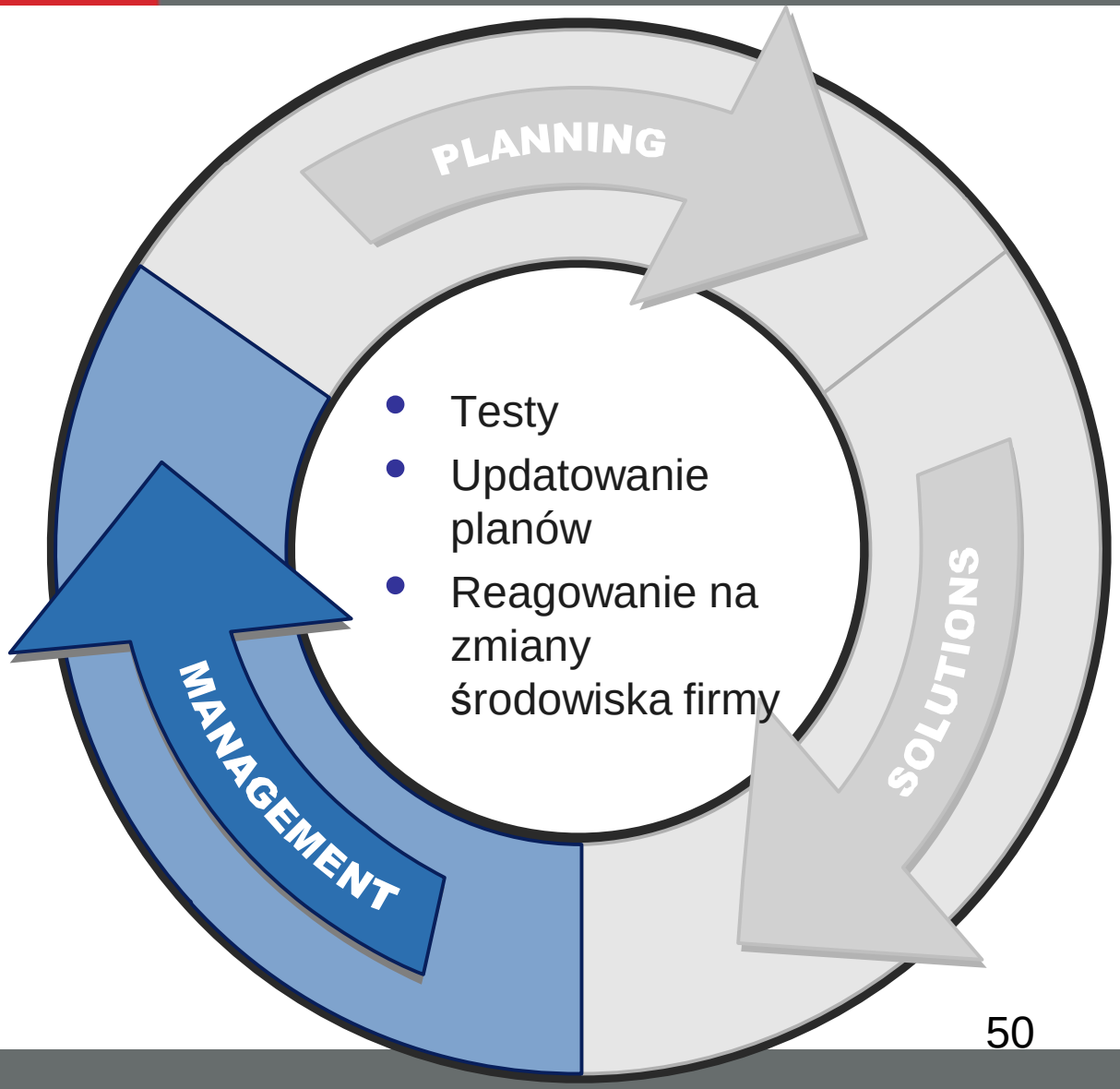
- **Lokalne klastry tworzą pojedynczy GeoCluster, globalnie zarządzany**
- **Wykorzystują replikację danych pomiędzy ośrodkami**
- **Zabezpieczają przed awarią całych centrów danych**
- **Failover usługi następuje najpierw lokalnie w ośrodku, dopiero jeśli to niemożliwe następuje przełączenie usługi do innego ośrodka**
- **Operacje failover następują wskutek decyzji administratora**
- **Komunikacja pomiędzy ośrodkami odbywa się z użyciem publicznych dostawców łączy WAN.**

BiG Vent

# Global Clustering: Wide Area Availability



# Nieprzerwany nadzór nad DR !!!

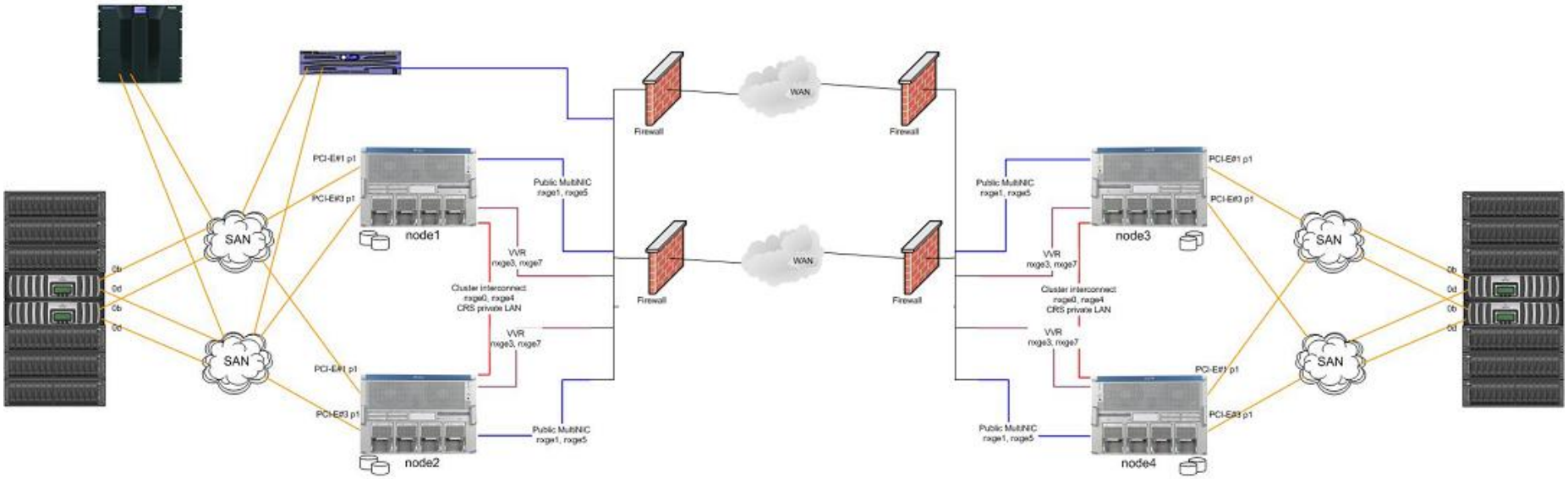


# Systemy HA

**W ramach rozwiązań wysokiej dostępności implementujemy następujące produkty:**

- **Veritas Cluster Server - Symantec**
- **HACMP – IBM**
- **Sun Cluster - Sun Microsystem**
- **Real Application Cluster – Oracle**
- **Veritas Volume Replicator - Symantec**
- **Mirror View, BCV, SRDF – EMC**
- **ShadowImage – Hitachi**
- **Global Cluster Manager - Symantec**

# Case study




1. Zastosowanie równolegle pracujących urządzeń
2. Umieszczenie krytycznych elementów systemu w 2 centrach danych klasy DataCenter oddalonych od siebie o 25 km ( Warszawa Centrum, Piaseczno)
3. Zastosowanie mechanizmów automatycznego przełączania usług pomiędzy lokalizacjami ( dotyczy aplikacji , bazy danych i dostępu do systemu)
4. Replikacje danych w sieci korporacyjnej WAN pomiędzy lokalizacjami
5. Rozłożenie obciążenia pomiędzy lokalizacjami

# Plany DR ? Zapasowe Centra Danych ? Niech się nigdy nie przydadzą...