البنية التحتية لتكنولوجيا المعلومات

الفصل 3

ITIS323

قسم نظم المعلومات 2023-2024

نظرة عامة على المحاضرة

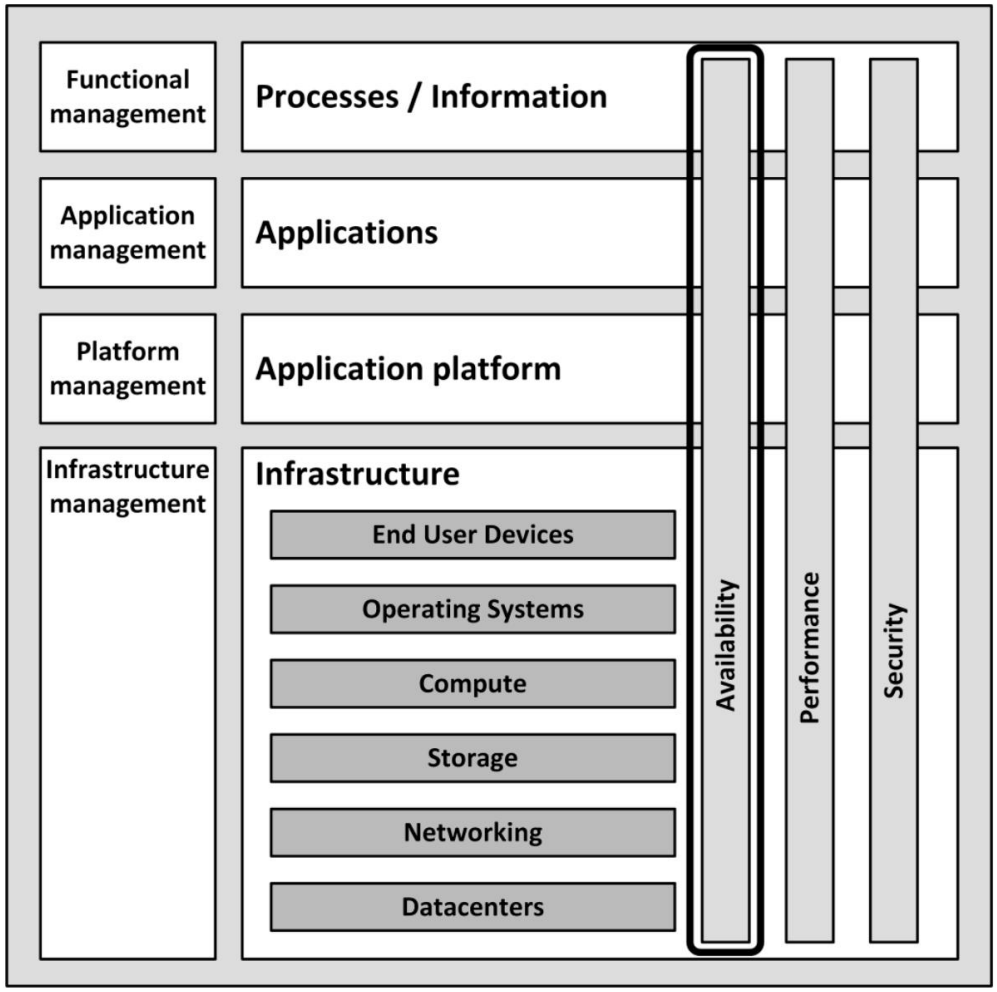
ةمدقم حول التوفر باسح التوفر طسوتم
الوقت بين حالات الفشل

طسوتم (MTBF) وقت الإصلاح ةلثمأ
(MTTR) حسابية

مقدمة

- الجميع يتوقع
البنية التحتية الخاصة بهم لتكون
متاحة في كل وقت

- من المستحيل ضمان
توفر البنية التحتية بنسبة
100%



حساب التوفر

- لا يمكن حساب التوفر أو ضمانه صريح
  - لا يمكن الإبلاغ عنها إلا بعد ذلك، بعد تشغيل النظام لعدة سنوات
- على مر السنين، تم اكتساب الكثير من المعرفة والخبرة حول كيفية تصميم الأنظمة عالية التوفر
  - تجاوز الفشل
  - وفرة
  - برمجة منظمة
  - تجنب نقاط الفشل الفردية (SPOFs)
  - تنفيذ إدارة الأنظمة

حساب التوفر

- يتم التعبير عن توفر النظام عادة كنسبة مئوية من وقت التشغيل في فترة زمنية معينة
  - عادة سنة أو شهر واحد

- مثال لوقت التوقف عن العمل معبرا عنه بـ أ النسبة المئوية سنويا:

التوقف في الاسبوع	التوقف كل شهر		نسبة التوفر
86.2دقيقة 20.2دقيقة	17.5ساعة		99.8%
99.9% (ثلاث تسعات") 99.99% (أربع تسعات") 99.999% ("خمس تسعات") 5.3دقيقة 25.9ثانية 6.1ثانية	8.8ساعة	49.1دقيقة	
1.0دقيقة	52.6دقيقة 4.3دقيقة		

حساب التوفر

- المتطلبات النموذجية المستخدمة في اتفاقيات مستوى الخدمة اليوم هي توفر 99.8% أو 99.9% شهريًا لنظام تكنولوجيا المعلومات الكامل

- توافر البنية التحتية يجب أن يكون كبيرا أعلى
  - عادة في حدود 99.99% أو أعلى
- يُعرف أيضًا وقت التشغيل بنسبة 99.999% بتوفر درجة الناقل

-لمكون واحد

-مستويات التوفر الأعلى لنظام كامل غير شائعة جدًا، حيث يكاد يكون من المستحيل الوصول إليها

حساب التوفر

- من الممارسات الجيدة الاتفاق على الحد الأقصى لتكرار عدم التوفر

عدم التوفر (بالدقائق) (كل سنة)	عدد الأحداث
<= 35	0 - 5
<= 10	5 - 10
<= 5	10 - 20
<=2	20 - 30
<= 1	> 30

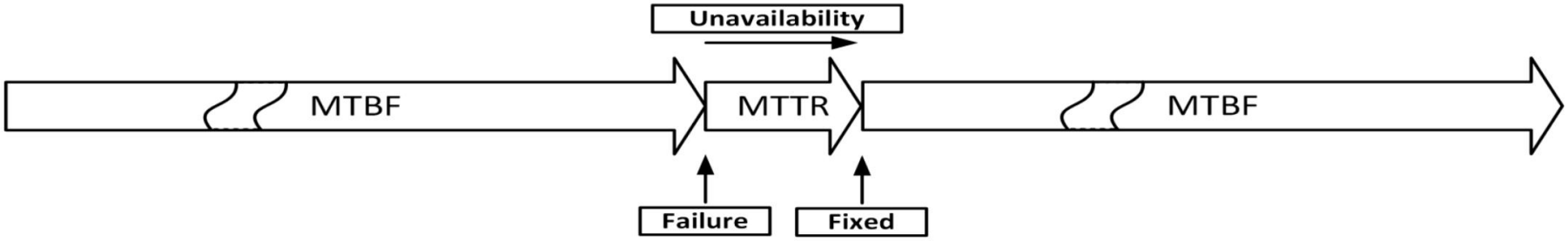
RTTMوMTBF

- متوسط الوقت بين حالات الفشل (MTBF)

-متوسط الوقت الذي يمر بين حالات الفشل

- متوسط الوقت اللازم للإصلاح (MTTR)

-الوقت المستغرق للتعافي من الفشل



MTBFوRTTM

- تتمتع بعض المكونات بمعدل MTBFأعلى من غيرها

- بعض أجهزة MTBالنموذجية:

عنصر	MTBF(ساعات)
القرص الصلب	750.000
مزود الطاقة	100.000
معجب	100.000
تبديل شبكة إيثرنت	350.000
كبش	1,000,000

MTTR

- يمكن إبقاء MTTR منخفضًا عن طريق:
  - وجود عقد خدمة مع المورد
  - وجود قطع الغيار في الموقع
  - التكرار الآلي وتجاوز الفشل

MTTR

- خطوات استكمال الإصلاحات:

-الإخطار بالخطأ (الوقت قبل رؤية المنبه رسالة)

-معالجة التنبيه

-العثور على السبب الجذري للخطأ

-البحث عن معلومات الإصلاح

-الحصول على قطع الغيار من المخزن

-حضور الفني إلى مركز البيانات مع المكون الاحتياطي

-إصلاح الخطأ جسديا

-إعادة تشغيل واختبار المكون

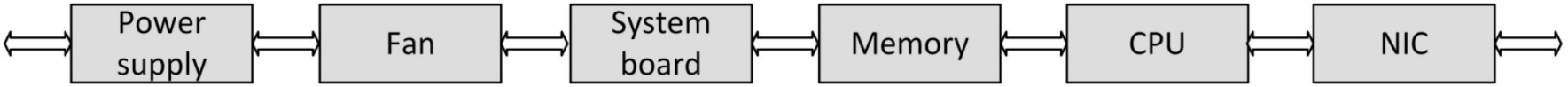
أمثلة الحساب

- $$\text{Availability} = \frac{\text{MTBF}}{(\text{MTBF} + \text{MTTR})} \times 100\%$$

عنصر	MTTR (ح)	MTBF (ح)		التوفر في٪
مزود الطاقة		100.000 8		99.99200
معجب		100.000 8		99.99200
لوحة النظام		300000 8		99.99733
ذاكرة		1,000,000 8		99.99920
وحدة المعالجة المركزية		500000 8		99.99840
شبكة واجهه المستخدم وحدة التحكم (نيك)	250.000	8	0.9999680	99.99680

أمثلة الحساب

- المكونات التسلسلية: عيب واحد يؤدي إلى التوقف عن العمل



- مثال: توفر النظام أعلاه هو:

- Serial components: One defect leads to downtime
- Example: the above system's availability is:

$$0.9999200 \times 0.9999200 \times 0.9999733 \times 0.9999920 \times 0.9999840 \times 0.9999680 = 0.99977 = \mathbf{99.977}\%$$

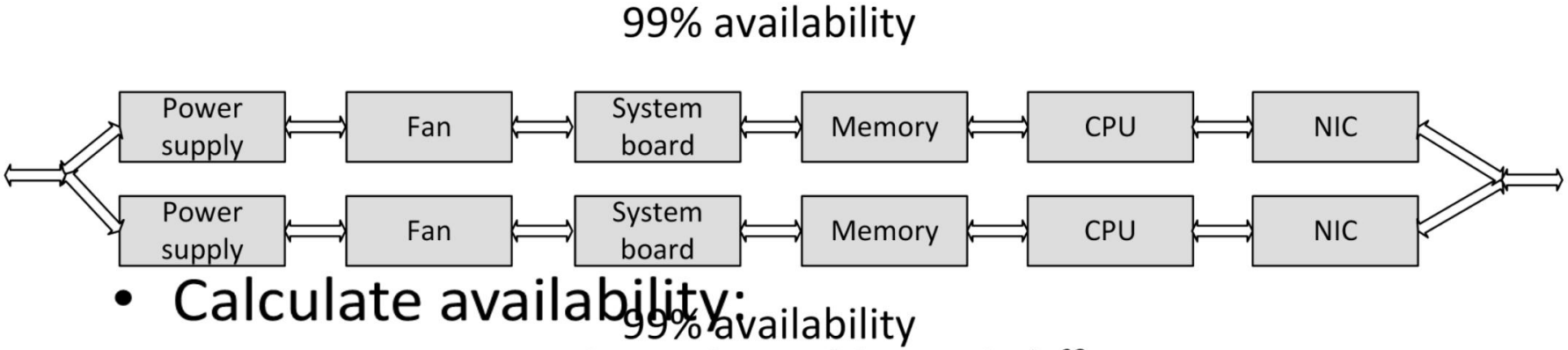
(each components' availability is at least 99.99%)

(توفر كل مكون على الأقل 99.99%)

أمثلة الحساب

- Parallel components: One defect: no downtime!
- But beware of SPOFs!

•المكونات المتوازية: عيب واحد: لا يوجد توقف! •ولكن حذار من SPOFs!



- Calculate availability:

$$A = 1 - (1 - A_1)^n$$

•حساب مدى التوفر:

- Total availability $= 1 - (1 - 0.99)^2$ = 99.99%

•إجمالي التوفر 99.99% =

النهاية

أي سؤال.....؟

البنية التحتية لتكنولوجيا المعلومات

الفصل 4
ITIS323

قسم المعلومات
أنظمة 2023-2024

نظرة عامة على المحاضرة

رداصم□عدم التوفر □الأخطاء البشرية □الأخطاء
البرمجية □الصيانة المخططة □العيوب المادية □

منحنى حوض الاستحمام □المشكلات البيئية □تعقيد
البنية التحتية زواجت□ رارك□ت□ل□ا□الفشل - عجارت□ل□

عجارت□ل□ا□الموقع الساخن - عجارت□ل□ا□الموقع البارد
- عجارت□ل□ا□موقع دافئ ل□امع□أل□ا□الاستمرارية RPOو
□RTO □RPOو RTO

مصادر عدم التوفر -الإنسان

أخطاء

80% •من حالات انقطاع التيار التي تؤثر على الخدمات الحيوية للمهام تكون بسبب مشكلات تتعلق بالأشخاص والعمليات. •أمثلة:

- •إجراء اختبار في بيئة الإنتاج
- •إيقاف تشغيل المكون الخطأ للإصلاح
- •تبديل قرص يعمل بشكل جيد بمجموعة RAIDبدلاً من القرص المعيب

- •استعادة الشريط الاحتياطي الخاطئ للإنتاج
- •إزالة الملفات عن طريق الخطأ
  - –مجلدات البريد وملفات التكوين
- •إزالة إدخالات قاعدة البيانات عن طريق الخطأ
  - –إسقاط الجدول xبدلاً من إسقاط الجدول y

مصادر عدم التوفر -الأخطاء البرمجية

- نظرًا لتعقيد معظم البرامج، فمن المستحيل تقريبًا (والمكلف جدًا) إنشاء برامج خالية من الأخطاء

- يمكن لأخطاء البرامج التطبيقية أن تتوقف بالكامل نظام
- أنظمة التشغيل هي برمجيات أيضاً

-أنظمة التشغيل التي تحتوي على أخطاء يمكن أن تؤدي إلى أنظمة الملفات التالفة أو فشل الشبكة أو مصادر عدم التوفر الأخرى

مصادر عدم التوفر –الصيانة المخططة

- في بعض الأحيان هناك حاجة لأداء إدارة الأنظمة مهام:
  - ترقية الأجهزة أو البرامج
  - تنفيذ التغييرات البرمجية
  - ترحيل البيانات
  - إنشاء النسخ الاحتياطية
- يجب أن يتم تنفيذه فقط على أجزاء من البنية التحتية حيث تستمر الأجزاء الأخرى في خدمة العملاء
- أثناء الصيانة المخطط لها، يكون النظام أكثر عرضة للتوقف عن العمل مقارنة بالظروف العادية

- يمكن إدخال SPOF مؤقت
- من الممكن أن يرتكب مديرو الأنظمة الأخطاء

مصادر عدم التوفر -العيوب الجسدية

- كل شيء ينهار في نهاية المطاف
- من المرجح أن تنكسر الأجزاء الميكانيكية أولاً
- أمثلة:

-عادة ما تنكسر مراوح معدات التبريد بسبب الغبار الموجود في المحامل

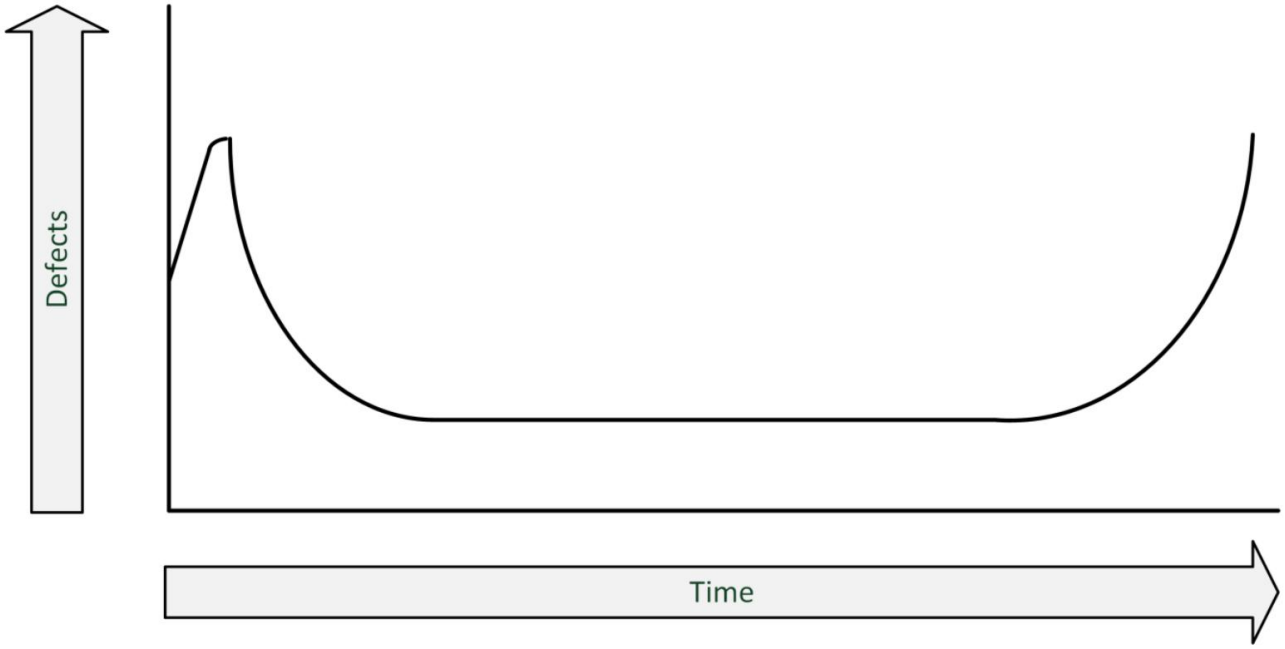
-تحتوي محركات الأقراص على أجزاء متحركة

-الأشرطة معرضة جدًا للعيوب حيث يتم لف الشريط داخل وخارج البكرات طوال الوقت

-تحتوي محركات الأشرطة على قطع ميكانيكية حساسة للغاية يمكن أن تنكسر بسهولة

مصادر عدم التوفر –حوض الاستحمام منحنى

- من المرجح أن يحدث فشل في أحد المكونات عندما يكون المكون جديد
- عندما يستمر أحد المكونات في العمل بعد الشهر الأول، فمن المحتمل أن يستمر في العمل دون عطل حتى نهاية عمره الافتراضي



مصادر عدم التوفر -القضايا البيئية

•يمكن أن تتسبب المشكلات البيئية في التوقف عن العمل:

-مرافق فاشلة

•قوة

•التبريد

–الكوارث

•نار

•الزلازل. •الفيضانات

مصادر عدم التوفر –تعقيد البنية التحتية

- يمكن أن تؤدي إضافة المزيد من المكونات إلى التصميم الشامل للنظام إلى تقويض التوفر العالي
  - حتى لو تم تنفيذ المكونات الإضافية لتحقيق التوفر العالي
- الأنظمة المعقدة
  - لديك المزيد من نقاط الفشل المحتملة
  - يصعب تنفيذها بشكل صحيح
  - يصعب إدارتها
- في بعض الأحيان يكون من الأفضل أن يكون لديك قطعة احتياطية إضافية النظام في الخزانة بدلاً من استخدام أنظمة زائدة عن الحاجة معقدة

وفرة

- التكرار هو الازدواجية الحرجة
المكونات في نظام واحد، لتجنب نقطة فشل واحدة (SPOF)

- أمثلة:

-مكون واحد يحتوي على مصدري طاقة؛ لو
فشل أحدهما، والآخر يتولى المسؤولية

-واجهات شبكية مزدوجة

-الكابلات الزائدة

تجاوز الفشل

- تجاوز الفشل هو التحول (شبه) التلقائي إلى نظام أو مكون احتياطي • أمثلة:

  - تجميع تجاوز الفشل في Windows Server
  - برنامج VMware عالي التوفر
  - قاعدة بيانات Oracle Real Application Cluster (RAC).

تراجع

- التراجع هو التحول اليدوي إلى نظام كمبيوتر احتياطي مماثل في موقع مختلف

- يُستخدم عادةً للتعافي من الكوارث
- ثلاثة أشكال أساسية للحلول الاحتياطية:
  - موقع ساخن
  - موقع بارد
  - موقع دافئ

الاحتياطي -موقع ساخن

•موقع ساخن

-مركز بيانات احتياطي مكون بالكامل

-مجهزة بالكامل بالطاقة والتبريد

-يتم تثبيت التطبيقات على الخوادم

-يتم تحديث البيانات لتعكس الإنتاج بالكامل
نظام

•يتطلب صيانة مستمرة للأجهزة،

البرامج والبيانات والتطبيقات للتأكد من أن الموقع يعكس بدقة حالة موقع الإنتاج في جميع الأوقات

الاحتياطي -الموقع البارد

- جاهز لاستقبال المعدات أثناء حالات الطوارئ، ولكن لا تتوفر أجهزة كمبيوتر في الموقع

- يجب تثبيت التطبيقات واستعادة البيانات الحالية بالكامل من النسخ الاحتياطية
- إذا كانت لدى المنظمة ميزانية قليلة جدًا لموقع احتياطي، فقد يكون الموقع البارد أفضل من لا شيء

الاحتياطي -موقع دافئ

- مرفق كمبيوتر متوفر بسهولة مزود بالطاقة والتبريد وأجهزة الكمبيوتر، ولكن قد لا يتم تثبيت التطبيقات أو تكوينها

- مزيج بين موقع حار وموقع بارد
- يجب استعادة التطبيقات والبيانات من وسائط النسخ الاحتياطي واختبارها
  - يستغرق هذا عادةً يومًا واحدًا

استمرارية الأعمال

•يتم تعريف كارثة تكنولوجيا المعلومات على أنها مشكلة لا يمكن إصلاحها في مركز البيانات، مما يجعل مركز البيانات غير قابل للاستخدام

•الكوارث الطبيعية:

–الفيضانات

-الأعاصير

-الأعاصير

-الزلازل

•كوارث من صنع الإنسان:

-انسكابات المواد الخطرة

–فشل البنية التحتية

–الإرهاب البيولوجي

استمرارية الأعمال

•في حالة وقوع كارثة، يمكن أن تصبح البنية التحتية غير متوفرة، في بعض الحالات لفترة أطول من الزمن

•إدارة استمرارية الأعمال تشمل:

-هو -هي

–إدارة العمليات التجارية

–توافر الأشخاص وأماكن العمل في حالات الكوارث

•يحتوي التخطيط للتعافي من الكوارث (DRP)على مجموعة من التدابير التي يجب اتخاذها في حالة وقوع كارثة، عندما يجب استيعاب (أجزاء من) البنية التحتية لتكنولوجيا المعلومات في موقع بديل

RPOو RTO

- RPOو RTO هما هدفان في حالة وقوع كارثة
- هدف وقت الاسترداد (RTO)
  - الحد الأقصى للمدة التي يمكن خلالها أ

يجب استعادة العمليات التجارية بعد وقوع الكارثة، وذلك لتجنب العواقب غير المقبولة (مثل الإفلاس)

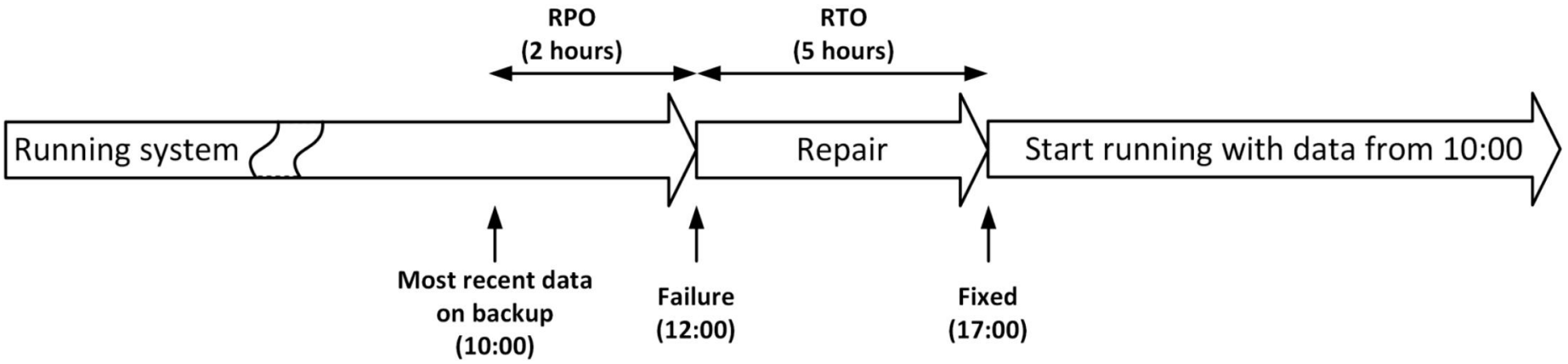
RPOو RTO

•هدف نقطة الاسترداد (RPO)

-النقطة الزمنية التي يجب خلالها استعادة البيانات مع الأخذ في الاعتبار بعض "الخسارة المقبولة" في حالة الكارثة

RPOو RTO •هي أهداف فردية

-لا علاقة لهم



النهاية

أي سؤال....