Safety of information systems

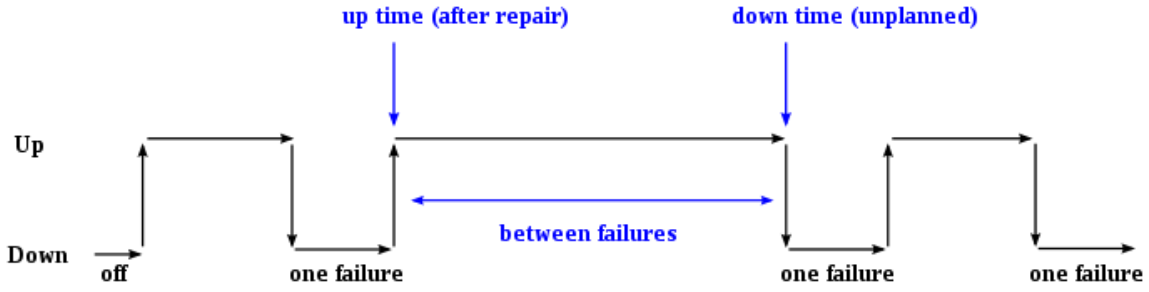
Lecturer: Roman Danel

Fault tolerant systems, disaster tolerant

- **Fault-tolerant System** - a system resistant to failures - failure of the system (electricity, component, network) will not cause significant interruption to the system; solutions through duplication of critical components
- **Disaster Tolerant System -** a system resistant to disasters - just like Fault-tolerant System it uses duplication but additionally it physically separates the backup system (to a different building, different city…).

High Availability & Disaster Recovery

- **Uptime -** refer to periods when a system is available
- **Downtime -** refer to periods when a system is unavailable
- **MTBF - Mean Time Between Failure** - is the predicted elapsed time between inherent failures of a system during operation
- **MTTR - Mean Time to Repair -** represents the average time required to repair a failed component or device
- **Mean time to recovery** - the average time that a device will take to recover from any failure



Time Between Failures = { down time - up time}

Disater Recovery Layer – IBM

Layer 0 – No off-site data
Layer 1 – Data backup with no Hot Site
Layer 2 – Data backup with a Hot Site
Layer 3 – Electronic vaulting
Layer 4 – Point-in-time copies
Layer 5 – Transaction integrity
Layer 6 – Zero or little data loss
Layer 7 – Highly automated, business-integrated solution

High Availability

is a characteristic of a system, which aims to ensure an agreed level of operational performance, usually uptime, for a higher than normal period.

Availability %	Downtime per year	Downtime per month	Downtime per week	Downtime per day
90% ("one nine")	**36.5 days**	**72 hours**	**16.8 hours**	**2.4 hours**
95%	18.25 days	36 hours	8.4 hours	1.2 hours
97%	10.96 days	21.6 hours	5.04 hours	43.2 minutes
98%	7.30 days	14.4 hours	3.36 hours	28.8 minutes
99% ("two nines")	**3.65 days**	**7.20 hours**	**1.68 hours**	**14.4 minutes**
99.5%	1.83 days	3.60 hours	50.4 minutes	7.2 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes	2.88 minutes
99.9% ("three nines")	**8.76 hours**	**43.8 minutes**	**10.1 minutes**	**1.44 minutes**
99.95%	4.38 hours	21.56 minutes	5.04 minutes	43.2 seconds
99.99% ("four nines")	**52.56 minutes**	**4.38 minutes**	**1.01 minutes**	**8.66 seconds**
99.995%	26.28 minutes	2.16 minutes	30.24 seconds	4.32 seconds
99.999% ("five nines")	**5.26 minutes**	**25.9 seconds**	**6.05 seconds**	**864.3 milliseconds**
99.9999% ("six nines")	**31.5 seconds**	**2.59 seconds**	**604.8 milliseconds**	**86.4 milliseconds**
99.99999% ("seven nines")	**3.15 seconds**	**262.97 milliseconds**	**60.48 milliseconds**	**8.64 milliseconds**
99.999999% ("eight nines")	**315.569 milliseconds**	**26.297 milliseconds**	**6.048 milliseconds**	**0.864 milliseconds**
99.9999999% ("nine nines")	**31.5569 milliseconds**	**2.6297 milliseconds**	**0.6048 milliseconds**	**0.0864 milliseconds**

Fault tolerance

Fault tolerance is a property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components. If its operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a naively designed system in which even a small failure can cause total breakdown.

Criteria

- How critical is the component?
- How likely is the component to fail?
- How expensive is it to make the component fault tolerant?

Solution

- Replication
- Redundancy – multiple identical instances
    - Space redundancy – HW, SW ...
    - Time redundancy – computation or data transmission is repeated
- Diversity – multiple different implementations of the same specification

The basic characteristics of fault tolerance:

1. No single point of failure – systems must continue to operate without interruption during the repair process
2. Fault isolation to the failing component
3. Fault containment to prevent propagation of the failure
4. Availability of reversion modes

NIST (National Institute of Standards and Technology) categorizes faults based on locality, cause, duration and effect.

RAID (Redundant Array of Independent Disks) are examples of a fault-tolerant storage devices that uses data redundancy.

DMR (Dual Modular Redundancy) - components of a system are duplicated, providing redundancy in case one should fail.

Business Continuity Management (BCM) - is the process of creating systems of prevention and recovery to deal with potential threats to a company.

Standards for BCM:

- BCP — BS 25999-1, 2006.
- PAS 56