# Fault Tolerance

Dependability

* Specified Service: what behavior should be
* Delivered Service: actual behavior]
* Fault: module deviates from specified behavior

Programming mistake (latent error, if executed, error will happen)

* Error: actual behavior within system differs from specified behavior

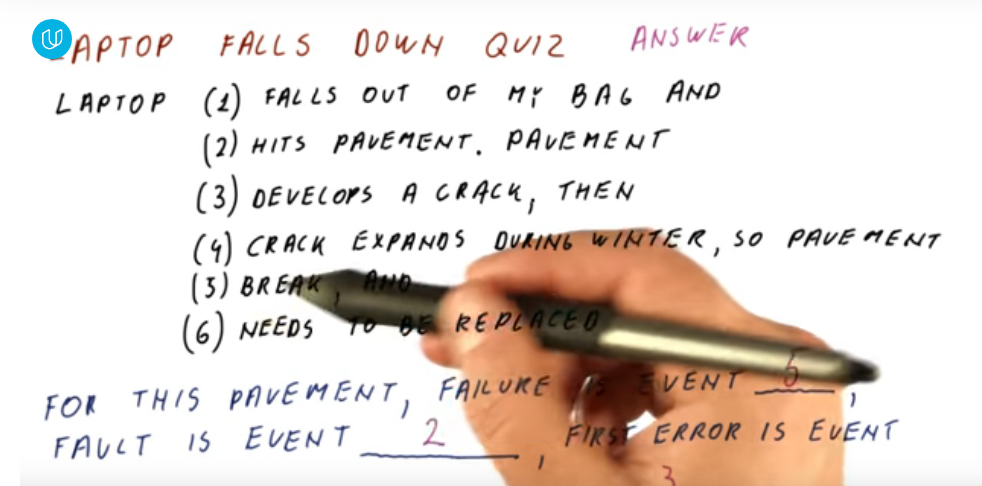
Activated fault (when executed), from latent error to effective error

* Failure: system deviates from specified behavior

Error is resulted by fault. But not every fault results error. For error, if system never use the things related with that error or the error will not cause system working differently, there is no system failure.

图片包含 人员

描述已自动生成



Fault should be latent error. So it is the event might cause problem, which is laptop falling into ground.

## Reliability

System in one of two states:

Service accomplishment: as specified behavior

Service interruption: not expected behavior

Reliability:

* Measure continuous service accomplishment
* Mean time to failure (MTTF):

How long we have service accomplishment until next service interruption

Availability:

* Percentage of overall time that a system is in accomplishment stage
* Mean time to repair (MTTR):

How long it takes to accomplishment once the system is in service interruption

* Availability = MTTF/ (MTTF + MTTR)

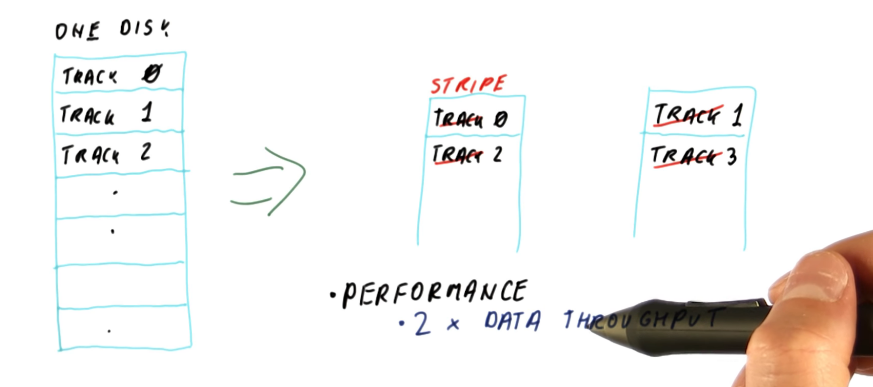
## Fault Tolerance for Memory and Storage

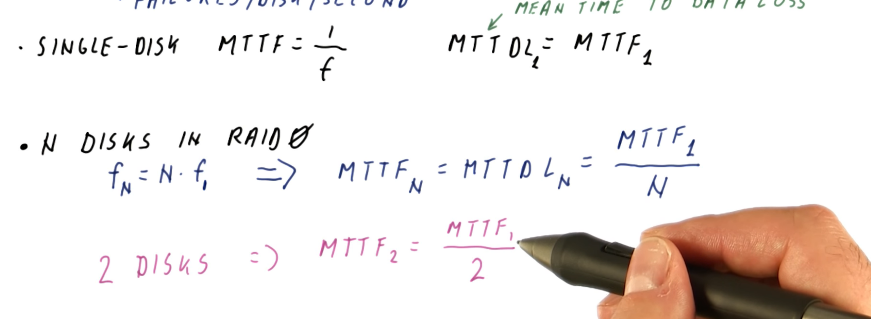
1. Parity (one extra bit, XOR of all bit)
2. ECC, error correction code

## RAID – Redundancy Array of Independent Disks

Several disks play the role of one disk and each disk detects errors using codes

* RAID 0 (twice throughput with 2 disks pretend as 1)





* RAID 1 (mirroring for reliability)

Write to each disk (as 1 disk); Read (2 throughputs after splitting read)

图片包含 人员, 烘干机

描述已自动生成

The probability of second disk failing during repair period: MTTR/MTTF, this is for single time unit that encountering failure. -> Only fail when we can’t fix it. With MTTR/MTTF as the probability of failing, MTTF/MTTR will be the number of possible repairing. After each repairing, the disk can take another MTTF/2. 图片包含 人员

描述已自动生成

* Raid 4 (N disk, with N-1 containing data, and 1 disk has parity blocks, bottle neck is parity block, since other disk also write)

图片包含 人员

描述已自动生成图片包含 文字

描述已自动生成\

* Raid 5 (Parity for each set of stripes in different disk)

图片包含 文字

描述已自动生成

We need 2 disks for reading and each disk is accessed 2. -> N/2/2