Backup & Recovery

We'll talk about:

How to backup the data.

Types of backups.

How to restore the data from backups.

How the data might get lost?

Faulty hardware:

- Storage devices (most likely to crash)

Human errors:

- Dropping a table by mistake
- An erroneous UPDATE statement
- Delete some datafiles by accident
- Dorel unleashed, etc.

Cybercrime:

- Deliberate data lost

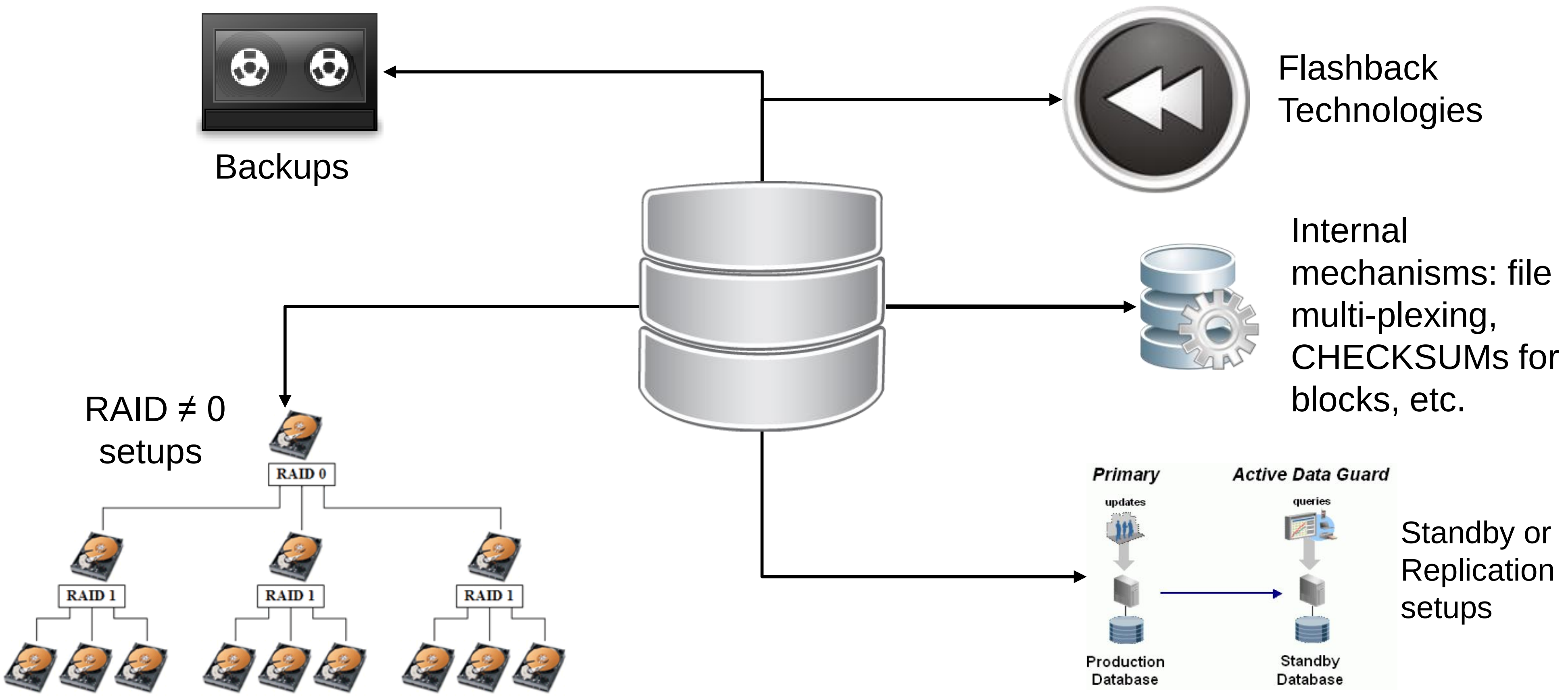
Bugs:

- Right into the firmware (low level/hardware device)
- Into the operating system
- Into the Oracle/DBMS kernel
- Into the client application

Disaster scenarios:

- earthquakes, floods, fire etc.

How to Protect Data



Backups

Flashback Technologies

Internal mechanisms: file multi-plexing, CHECKSUMs for blocks, etc.

RAID ≠ 0 setups

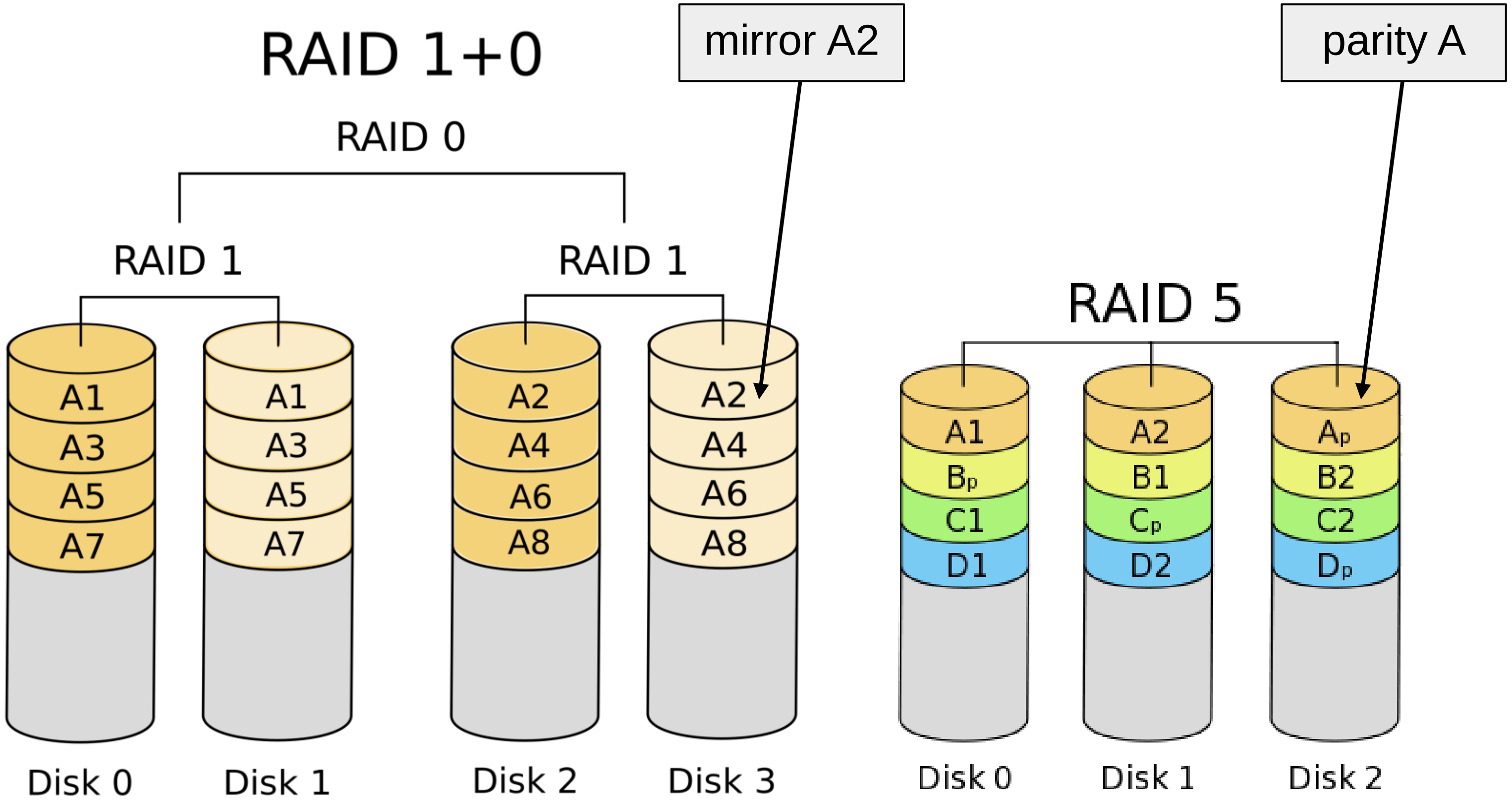
Standby or Replication setups

RAID Setups

RAID10 vs RAID5

- It refers to a specific way of putting together more HDDs so that to have an additional protection level and performance

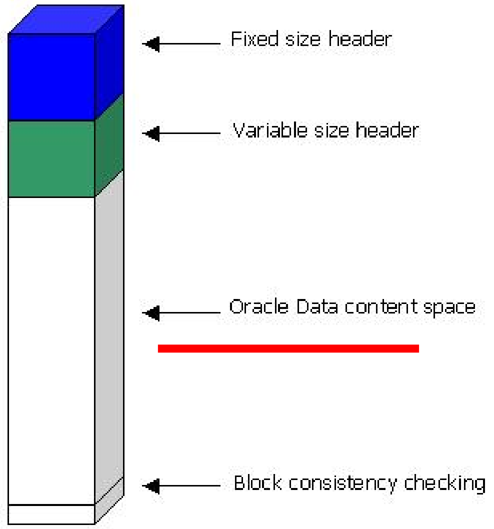
- The most used RAID setups in the DB field are RAID10 and RAID5.

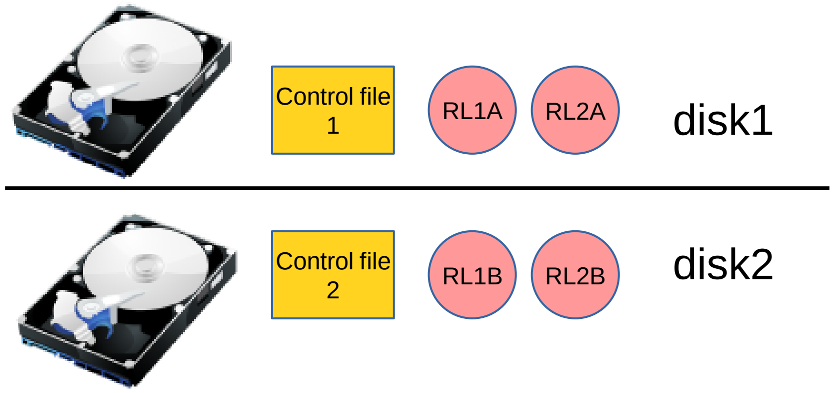


Internal mechanisms for data protection

Oracle Provides

- The ARCHIVELOG mode through which the redolog stream is preserved in archives (offline redologs)
- File multiplexing: the control file or the redologs
- Checking the integrity of the Oracle block (see DB_BLOCK_CHECKING and DB_BLOCK_CHECKSUM)
- The possibility to configure multiple archiving destinations





Backups

What is a Backup

It’s just a copy of the real data.

Important: It’s not a good idea to take a backup into the same disk where the original data resides. If that disk fails, we lost the data and the backups as well.

It can be used:

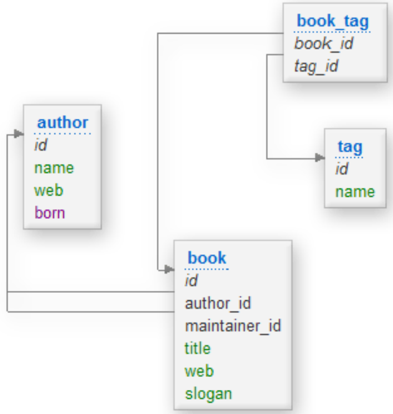
- To recover if the data get lost
- To duplicate the data to other environments (usually TEST or DEVELOPMENT)

Ah, but I don’t have any backups

- To take regular backups is one of the main duties of a DBA.
- The data is exposed to many potential risks which might cause a partial or a total lost.
- The costs to recover when there are no backups are very high and sometimes it’s impossible to get the data back.
- Failing to restore the data in a timely fashion might lead to bankruptcy.

Types of Backups

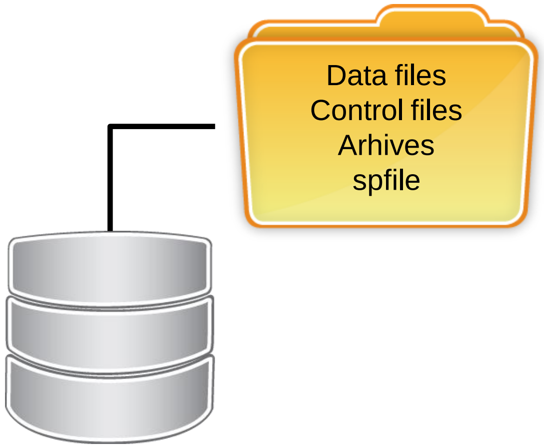
Logical Backup



export

- XML
- CSV
- Export files in a proprietary format (exp, expdp)

Physical Backup



Data files
Control files
Arhives
spfile

copy

- Identical copies
- Special backup files (RMAN)

Logical Backups

PROS:

- Can operate on a DB object (table, stored procedure etc.)
- Allows specifying the records to be backed up (in DataPump, the QUERY parameter)
- Relatively easy to obtain
- OS cross platform format

CONS:

- Not good for big amounts of data (slow)
- Importing logical backups generate redolog
- The database must be open in order to be able to take or restore a logical backup.

Examples of Logical Backups

Starting with Oracle 10g, it is advisable to use DataPump:

```
expdp scott/tiger@db tables=EMP,DEPT directory=TEST_DIR
dumpfile=EMP_DEPT.dmp logfile=expdp.log
```

```
impdp scott/tiger@db tables=EMP,DEPT directory=TEST_DIR
dumpfile=EMP_DEPT.dmp logfile=impdp.log
```

Note: *The old export/import tools are still available but they are deprecated, meaning that Oracle doesn’t provide support for them, nor does new features.*

Challenge

Developers want to start working on FaceBook 2.0. They come to you and ask if you can duplicate the current productive FB schema to a new one called FB2. FB2 should contain the same objects and data as FB.

How would you do it?

Implement the solution using our Oracle playground VM.

Physical Backups

The most common way of taking DB backups

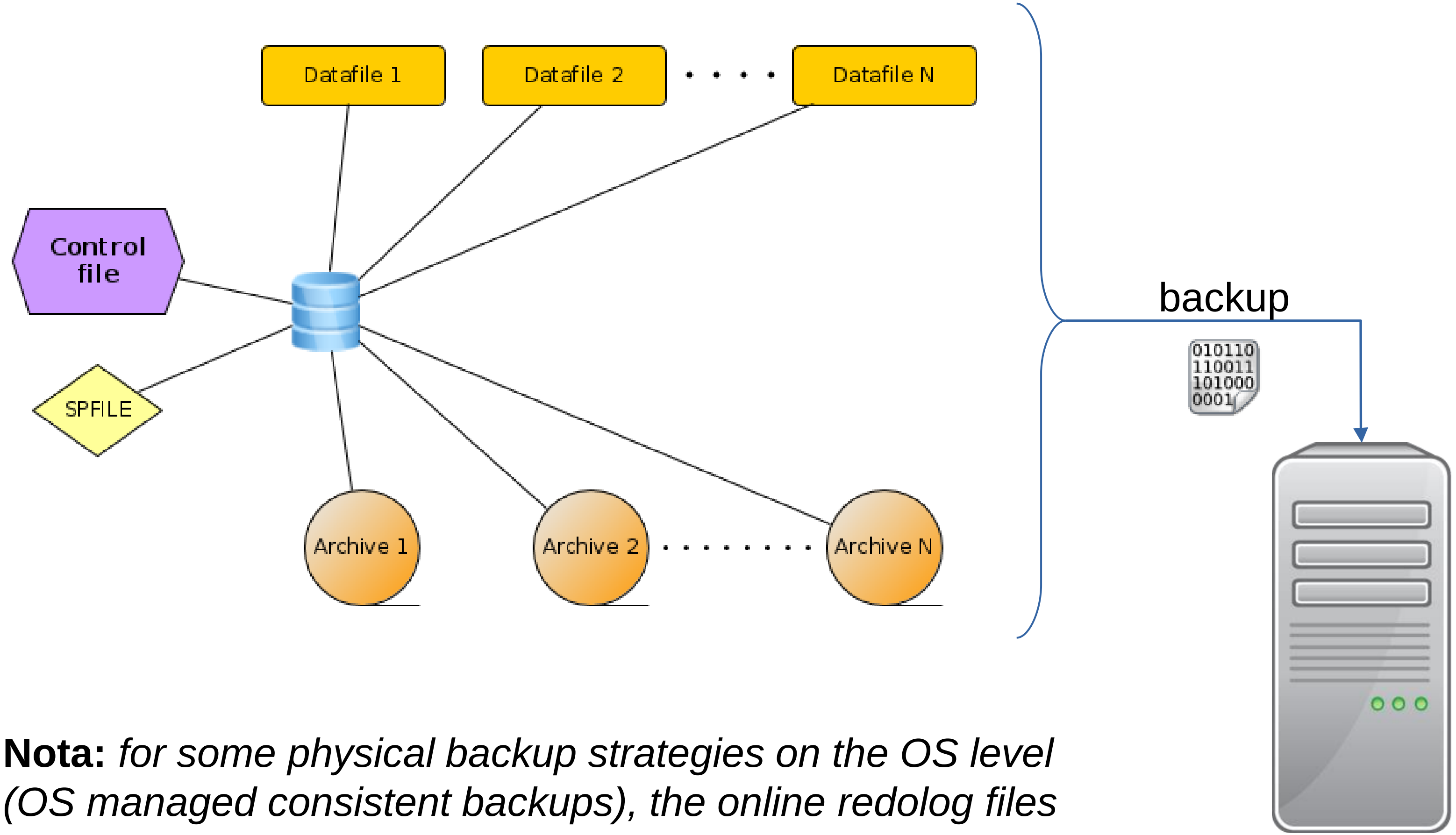
Suitable for backing up big databases

Can be:

- **Consistent backups:** when they are taken with a closed database
- **Inconsistent backups:** when the database is changed while the backup is running (open DB)

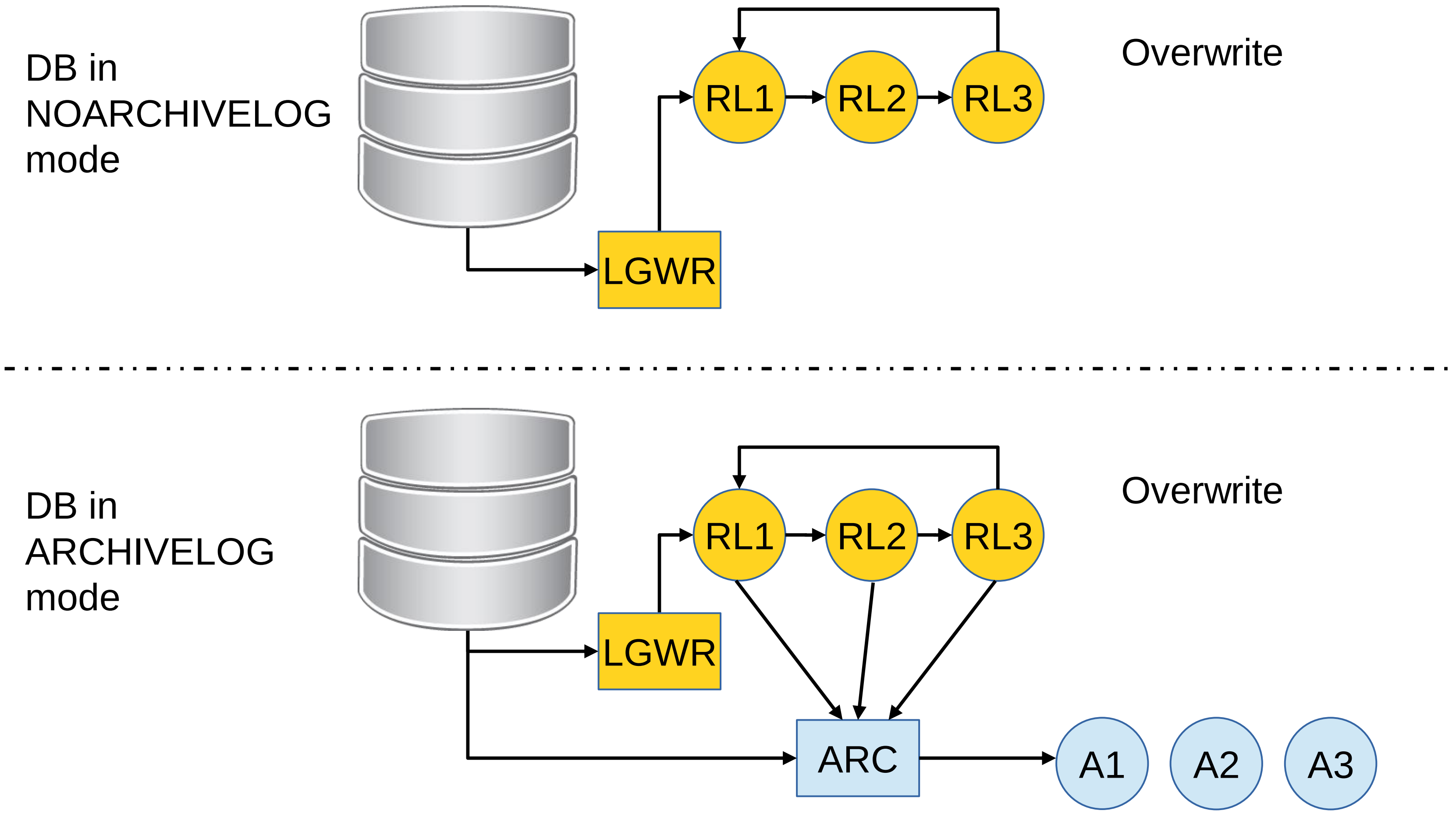
Note: there's also the concept of a consistent logical backup, but in this case it refers to a specific moment in time *(see for expdp the FLASHBACK_TIME and FLASHBACK_SCN parameters).*

Files which are Targeted by a Physical Backup



Nota: *for some physical backup strategies on the OS level (OS managed consistent backups), the online redolog files may also be considered.*

Back to the basics: ARCHIVELOG vs NOARCHIVELOG



DB in NOARCHIVELOG mode

Overwrite

DB in ARCHIVELOG mode

Overwrite

Workshop

Put the database in ARCHIVELOG mode.

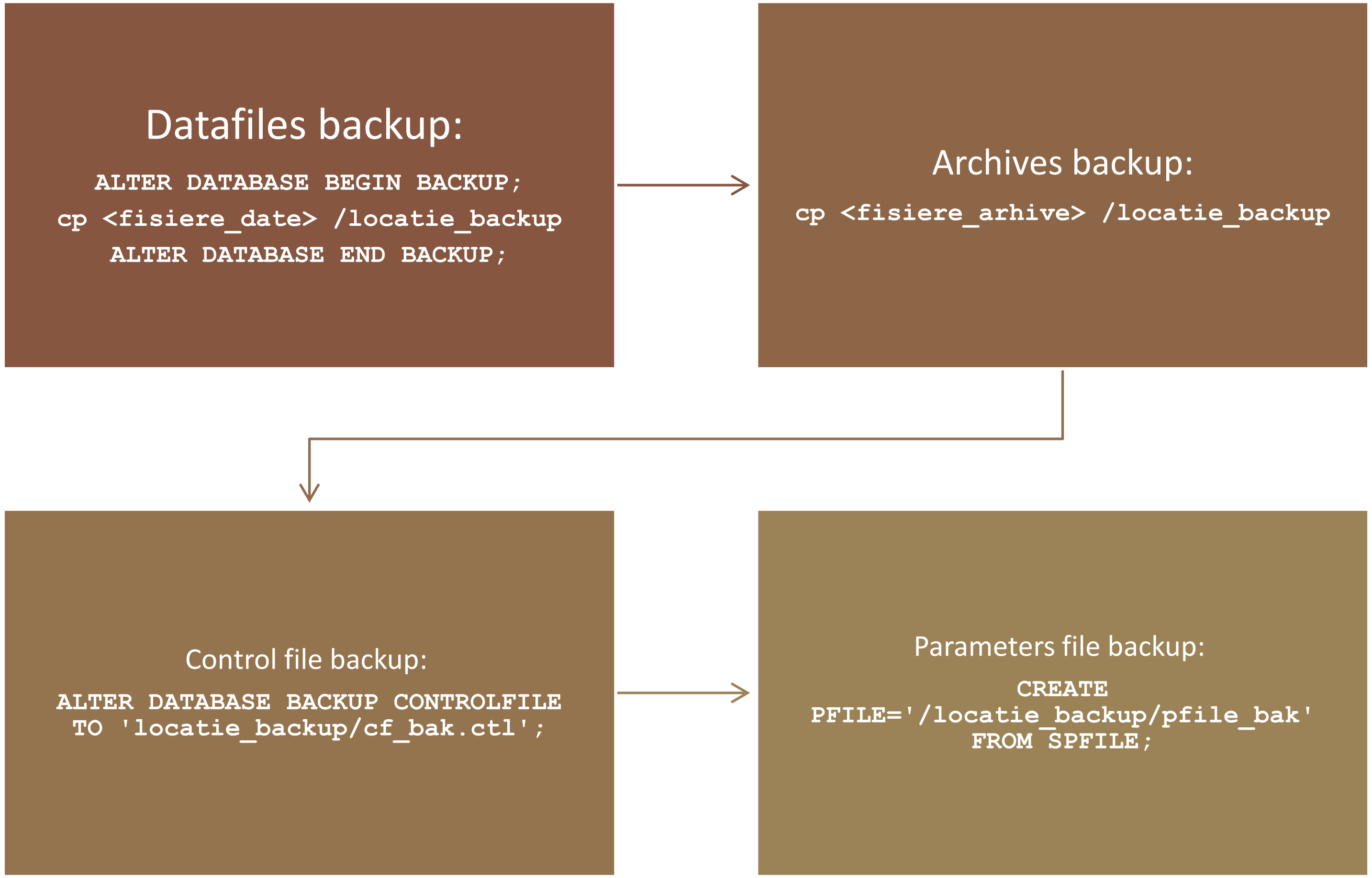
OS Managed Backups

- It uses regular OS commands (cp, scp, xcopy, ftp etc.).

- If the database is opened (for R/W), before initiating the backup, we must ensure the DB is placed in the so-called BACKUP mode.

PROS	CONS
Simplicity as far as the OS commands are concerned	There is the possibility to leave out some database files and thus to invalidate the whole backup.
The only option for those databases older than Oracle 8i	Special care when implementing the retention of the current bakcups.
Fast when combined with facilities of snapshotting or low level replication.	The BACKUP mode may be problematic because it implies a performance penalty (more redo is generated)
Very appealing to sysadmins.	It's not so easy to validate the backups.

Example of an OS Managed Physical Backup



Datafiles backup:

```
ALTER DATABASE BEGIN BACKUP;
cp <fisiere_date> /locatie_backup
ALTER DATABASE END BACKUP;
```

Archives backup:

```
cp <fisiere_arhive> /locatie_backup
```

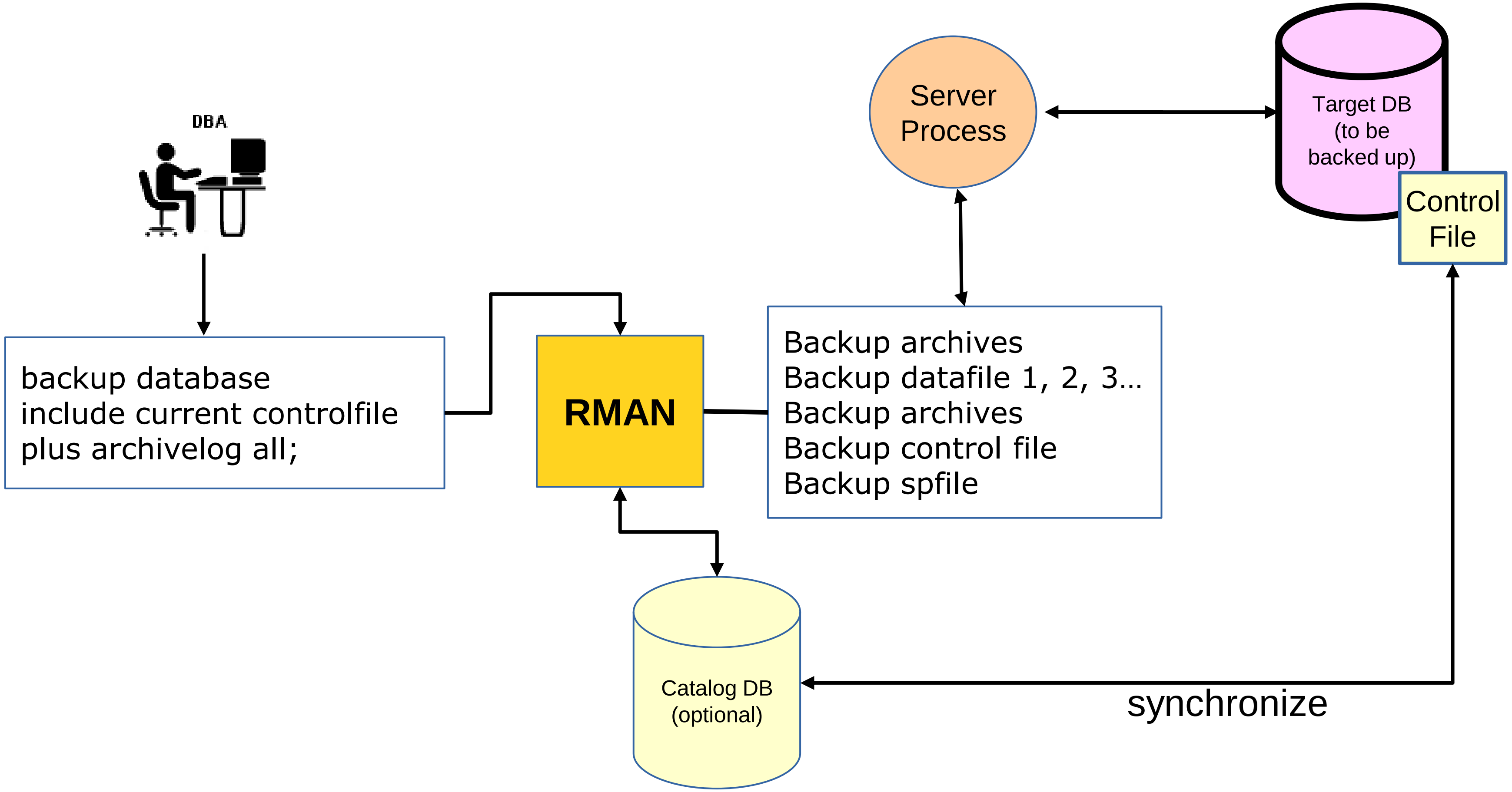
Control file backup:

```
ALTER DATABASE BACKUP CONTROLFILE
TO 'locatie_backup/cf_bak.ctl';
```

Parameters file backup:

```
CREATE
PFILE='/locatie_backup/pfile_bak'
FROM SPFILE;
```

RMAN Overview



backup database
include current controlfile
plus archivelog all;

Backup archives
Backup datafile 1, 2, 3…
Backup archives
Backup control file
Backup spfile

RMAN Backups

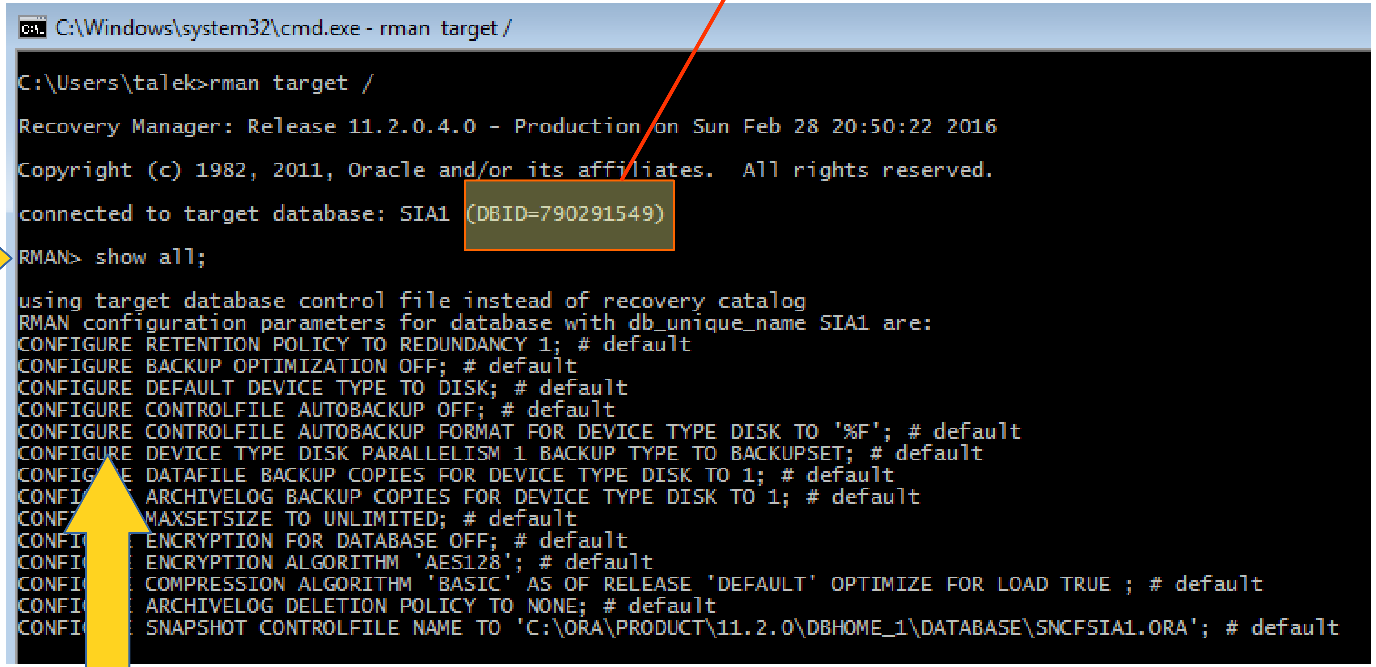
- RMAN (Recovery Manager) is an Oracle tool especially designed to take and manage Oracle backups.

- Backing up with RMAN is the recommended way, as advised by Oracle.

Some PROS	CONS
The DB is not required to be in the BACKUP mode.	It takes time to learn this new tool.
It provides various retention policies.	Subject to various limitations on Oracle Standard Edition (no parallelism, no block recovery)
It can be used to take incremental backups.	
It validates the backups.	
It provides means to manage the RMNA catalog (in the control file or in a separate database)	
It can be easily integrated with tape libraries.	

RMAN Configuration

Display all global settings.



```
C:\Users\talek>rman target /

Recovery Manager: Release 11.2.0.4.0 - Production on Sun Feb 28 20:50:22 2016

Copyright (c) 1982, 2011, Oracle and/or its affiliates.  All rights reserved.

connected to target database: SIA1 (DBID=790291549)

RMAN> show all;

using target database control file instead of recovery catalog
RMAN configuration parameters for database with db_unique_name SIA1 are:
CONFIGURE RETENTION POLICY TO REDUNDANCY 1; # default
CONFIGURE BACKUP OPTIMIZATION OFF; # default
CONFIGURE DEFAULT DEVICE TYPE TO DISK; # default
CONFIGURE CONTROLFILE AUTOBACKUP OFF; # default
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F'; # default
CONFIGURE DEVICE TYPE DISK PARALLELISM 1 BACKUP TYPE TO BACKUPSET; # default
CONFIG  E DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFI     ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONF      MAXSETSIZE TO UNLIMITED; # default
CONFI     ENCRYPTION FOR DATABASE OFF; # default
CONFI     ENCRYPTION ALGORITHM 'AES128'; # default
CONFI     COMPRESSION ALGORITHM 'BASIC' AS OF RELEASE 'DEFAULT' OPTIMIZE FOR LOAD TRUE ; # default
CONFI     ARCHIVELOG DELETION POLICY TO NONE; # default
CONFI     SNAPSHOT CONTROLFILE NAME TO 'C:\ORA\PRODUCT\11.2.0\DBHOME_1\DATABASE\SNCFSIA1.ORA'; # default
```

Important in some crash scenarios.

Example of how to config something in RMAN:
configure device type disk parallelism 2 backup type to compressed backupset;

The Auto-backup Control File Feature

- If this feature is activated, Oracle will take an automatic backup of the control-file and SPFILE on every RMAN backup and whenever a structural DB change (like adding/dropping a new data-file) takes place.

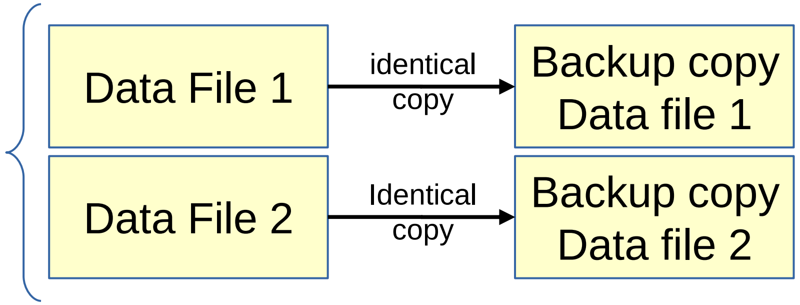
- It is recommended to use this feature especially if no separate DB is used for the RMAN catalog.

```
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE CONTROLFILE AUTOBACKUP FOR DEVICE TYPE DISK
  FORMAT '/backup/%F';
```

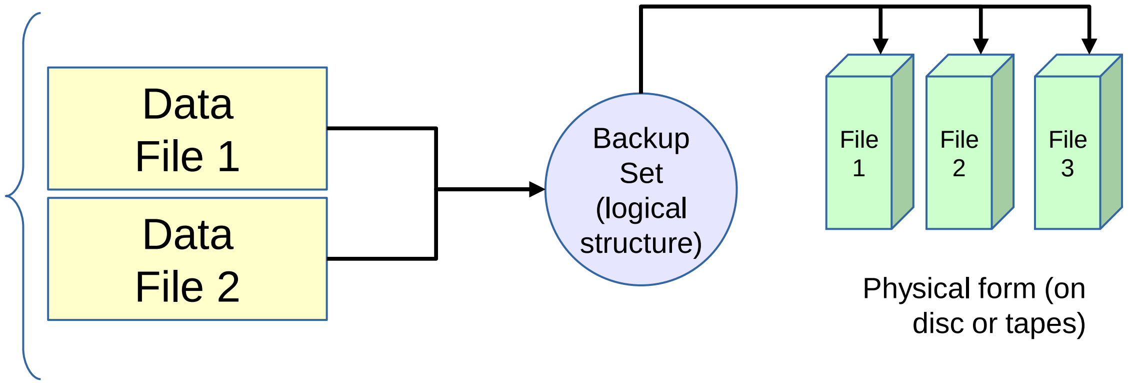
RMAN Backup Files

It’s about those files which are created by RMAN as part of a backup operation.

File copies: identical copies of the source files but in another location and, most likely, having a different name.



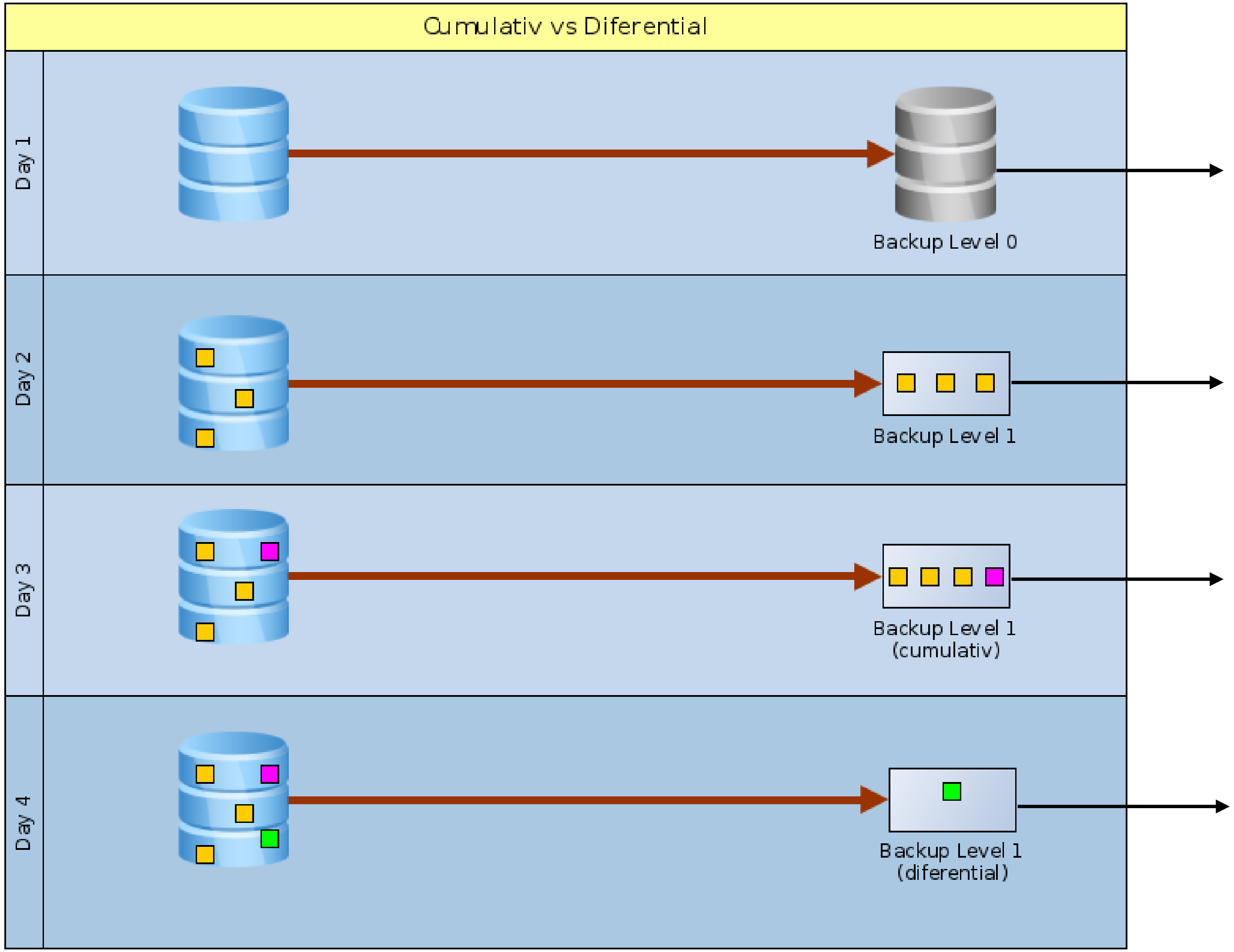
Backupset files: the source files my be combined in the same backupset, compressed etc. One backupset can have one or more backup pieces.


Data File 1
Data File 2
Backup Set (logical structure)
File 1
File 2
File 3
Physical form (on disc or tapes)

Examples of RMAN Backup Commands

```
rman target /
rman target sys/pwd@db catalog user/pwd@catdb

BACKUP AS COPY DATABASE TAG 'FULL_BACKUP_20160210';
BACKUP CURRENT CONTROLFILE;
BACKUP ARCHIVELOG ALL FORMAT '/BACKUP/%U' DELETE INPUT;
BACKUP SPFILE;

RUN {
  ALLOCATE CHANNEL C1 DEVICE TYPE DISK;
  BACKUP AS COMPRESSED BACKUPSET
    CHECK LOGICAL NOEXCLUDE
    (DATABASE
       FILESPERSET 5
       FORMAT '/BACKUP/%d_%s_%p_%t'
       NOT BACKED UP SINCE TIME 'SYSDATE-1'
    ) PLUS ARCHIVELOG FORMAT '/BACKUP/ARCH/%U';
  DELETE NOPROMPT OBSOLETE REDUNDANCY 2;
  RELEASE CHANNEL C1;
}
```

Incremental Backups



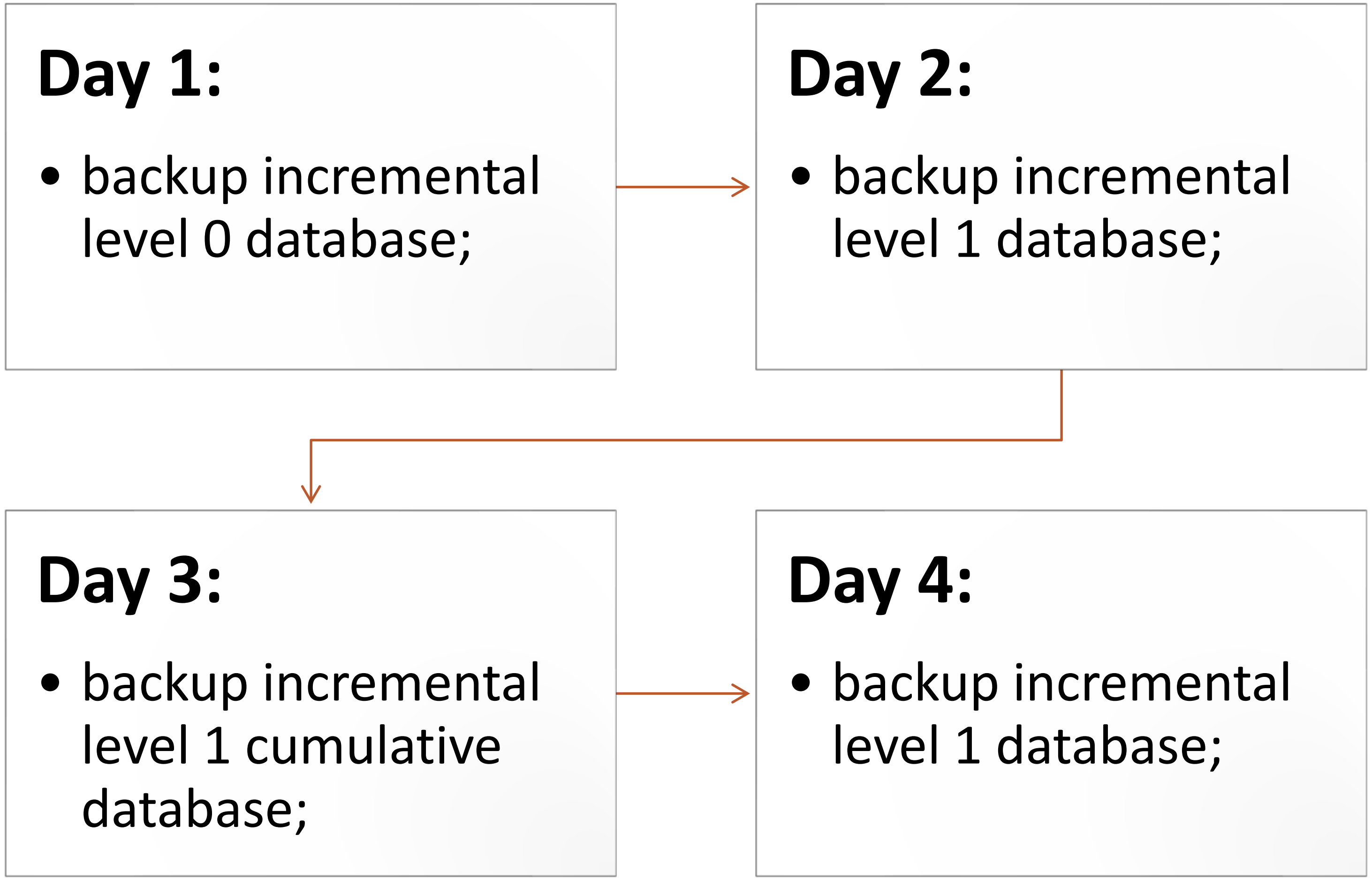
Very similar to a FULL backup.

It has all changed blocks since the last backup.

It has all changed blocks since the last level 0 backup.

It has just those changed blocks since the last backup (level 1, day 3)

Incremental Backups Flow



Day 1:

- backup incremental level 0 database;

Day 2:

- backup incremental level 1 database;

Day 3:

- backup incremental level 1 cumulative database;

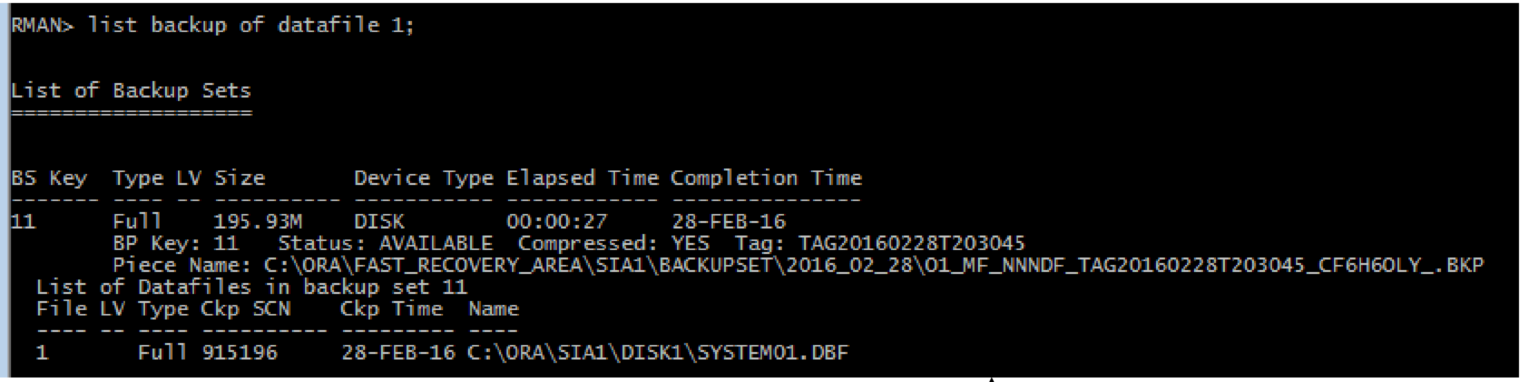
Day 4:

- backup incremental level 1 database;

Workshop

WHILE THE DATABASE IS UP & RUNNING, FULLY BACKUP IT USING RMAN UTILITY.

List Available RMAN Backups



```
RMAN> list backup of datafile 1;


List of Backup Sets
===================


BS Key  Type LV Size       Device Type Elapsed Time Completion Time
------- ---- -- ---------- ----------- ------------ ---------------
11      Full    195.93M    DISK        00:00:27     28-FEB-16
        BP Key: 11   Status: AVAILABLE  Compressed: YES  Tag: TAG20160228T203045
        Piece Name: C:\ORA\FAST_RECOVERY_AREA\SIA1\BACKUPSET\2016_02_28\O1_MF_NNNDF_TAG20160228T203045_CF6H6OLY_.BKP
  List of Datafiles in backup set 11
  File LV Type Ckp SCN    Ckp Time  Name
  ---- -- ---- ---------- --------- ----
  1       Full 915196     28-FEB-16 C:\ORA\SIA1\DISK1\SYSTEM01.DBF
```

```
LIST BACKUP OF DATAFILE 1;
LIST BACKUP OF DATABASE;
LIST BACKUP SUMMARY;
LIST BACKUPSET TAG 'FULL_BACKUP_20160210';
LIST COPY OF DATAFILE 2 COMPLETED BETWEEN
'10-DEC-2015' AND '17-JAN-2016';
```

Backups Retention

When a backup is considered obsolete.

The following backup retention policies are provided by RMAN:

- **REDUNDANCY policy:** a backup becomes obosolete as soon as there are at least N more recent backups.
- **RECOVERY WINDOW policy:** a backup is considered obsolete if cannot (or is not practical to) be used to recover the database as it was N days ago.
- **Explicit retention:** using the KEEP clause of the CHANGE command. It can be an explicit date or FOREVER if the intention is to keep that backup indefinitely.

Retention Related RMAN Commands

```
CONFIGURE RETENTION POLICY
 TO REDUNDANCY 2;
CONFIGURE RETENTION POLICY
 TO RECOVERY WINDOW OF 7 DAYS;
```

Global retention configuration.

```
REPORT OBSOLETE;
REPORT OBSOLETE REDUNDANCY 3;
```

Listing obsolete backups.

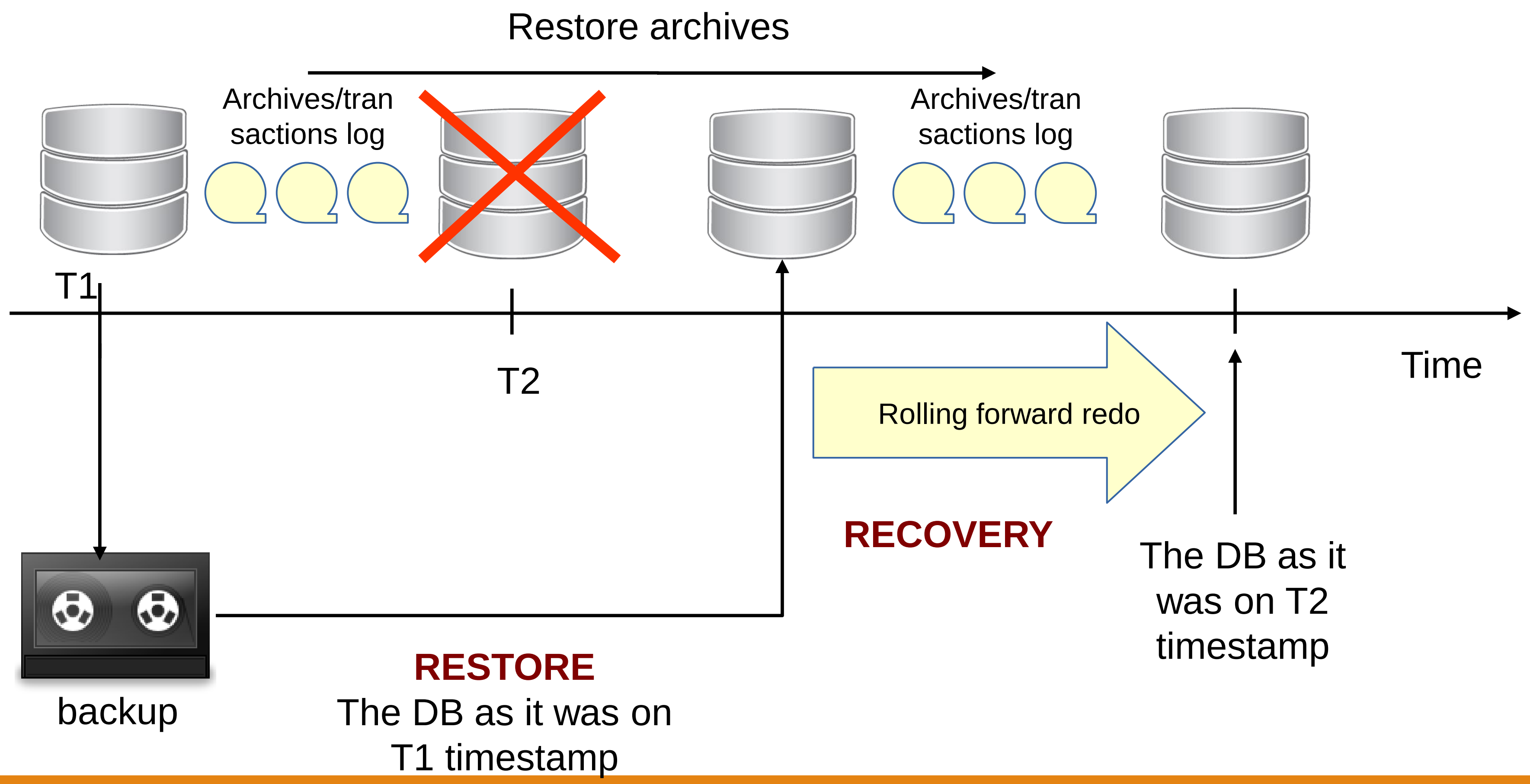
```
DELETE OBSOLETE;
DELETE OBSOLETE REDUNDANCY 4;
```

Delete obsolete backups.

```
CHANGE BACKUPSET 123 KEEP UNTIL
      'SYSDATE+180';
CHANGE DATAFILECOPY
'/tmp/control01.ctl' KEEP FOREVER;
```

Explicit retention settings.

Restore vs. Recovery



Restore archives

Archives/transactions log

T1

T2

Archives/transactions log

Time

Rolling forward redo

RECOVERY

The DB as it was on T2 timestamp

backup

RESTORE
The DB as it was on T1 timestamp

Recovery Types

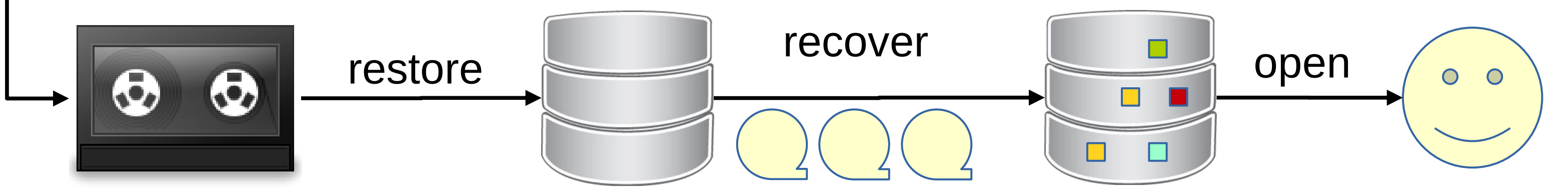
The recovery may be:

- **Complete:** when all the changes from the redo files (offline and online) are applied.
- **Incomplete:** when the database is recovered using a partial rolling forward from the redolog stream, ending up with a image of the database as it was on a specific time in the past, discarding all the other changes after that time (changes which are recorded into the “tail” of redolog stream).

The Complete Recovery Using RMAN

The Oracle instance is in the mount state:

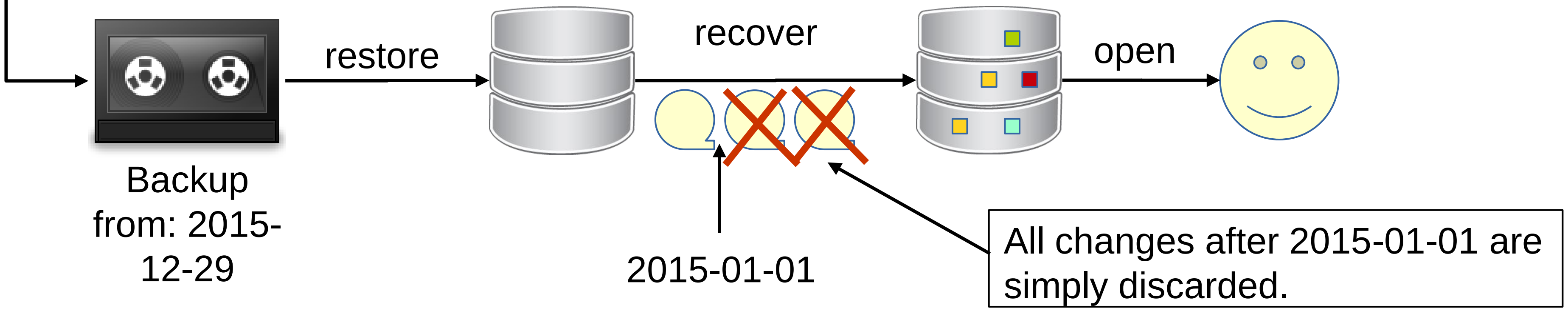
```
rman target /
restore database;
recover database;
alter database open;
```



The Incomplete Recovery Using RMAN

The Oracle instance is in the “MOUNT” state:

```
rman target /
run {
  set until time “to_date('2015-01-01', 'yyyy-mm-dd')”;
  restore database;
  recover database;
  alter database open resetlogs;
}
```



All changes after 2015-01-01 are simply discarded.

Flashback Technologies

Standby/Replication Setups

Crash scenarios.

The backup&recovery strategy plan.

Flashback Technologies

Flashback Overview

May be used to revert the database or a part of it (e.g. a table) as it was in the past

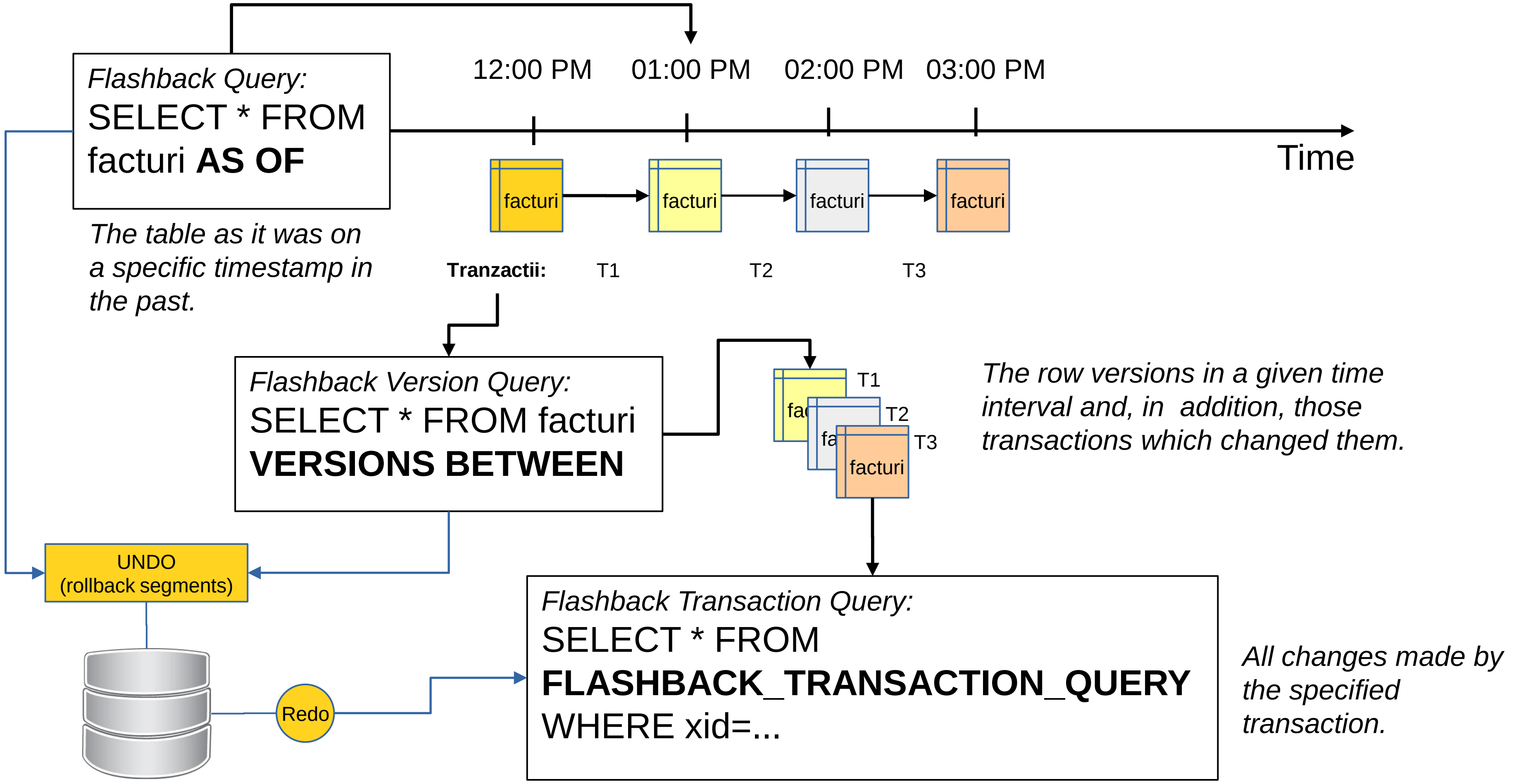
There’s no need for a previous backup

They are (more or less) fast

Especially good for human errors: a wrong UPDATE, dropping a table by accident

Can be used in QA/test databases to revert them to the initial state if, for example, a test suite has changed the database.

View Data from the Past



Flashback Query:
SELECT * FROM facturi **AS OF**

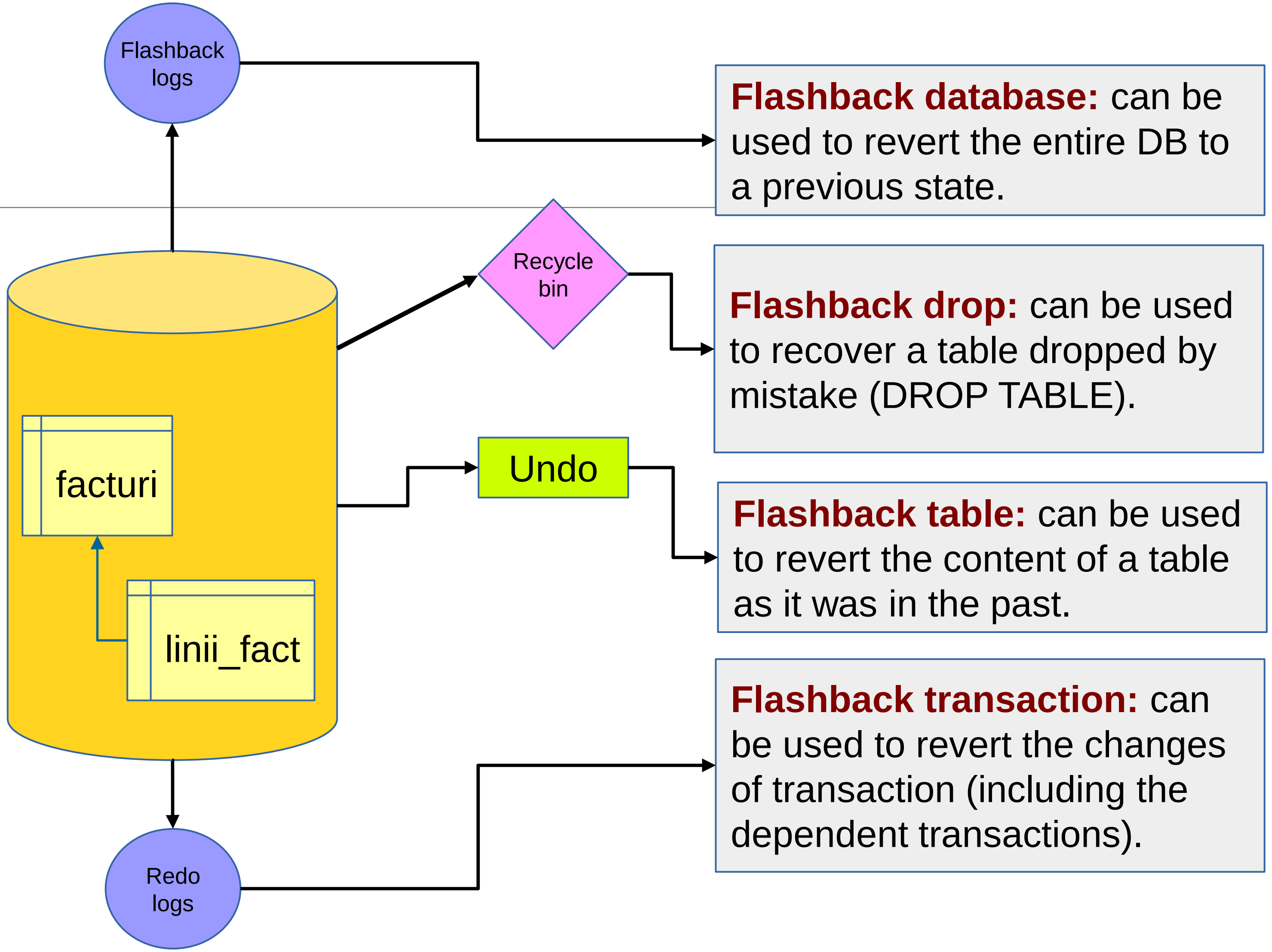
The table as it was on a specific timestamp in the past.

Flashback Version Query:
SELECT * FROM facturi **VERSIONS BETWEEN**

The row versions in a given time interval and, in addition, those transactions which changed them.

Flashback Transaction Query:
SELECT * FROM
FLASHBACK_TRANSACTION_QUERY
WHERE xid=...

All changes made by the specified transaction.



Flashback database: can be used to revert the entire DB to a previous state.

Flashback drop: can be used to recover a table dropped by mistake (DROP TABLE).

Flashback table: can be used to revert the content of a table as it was in the past.

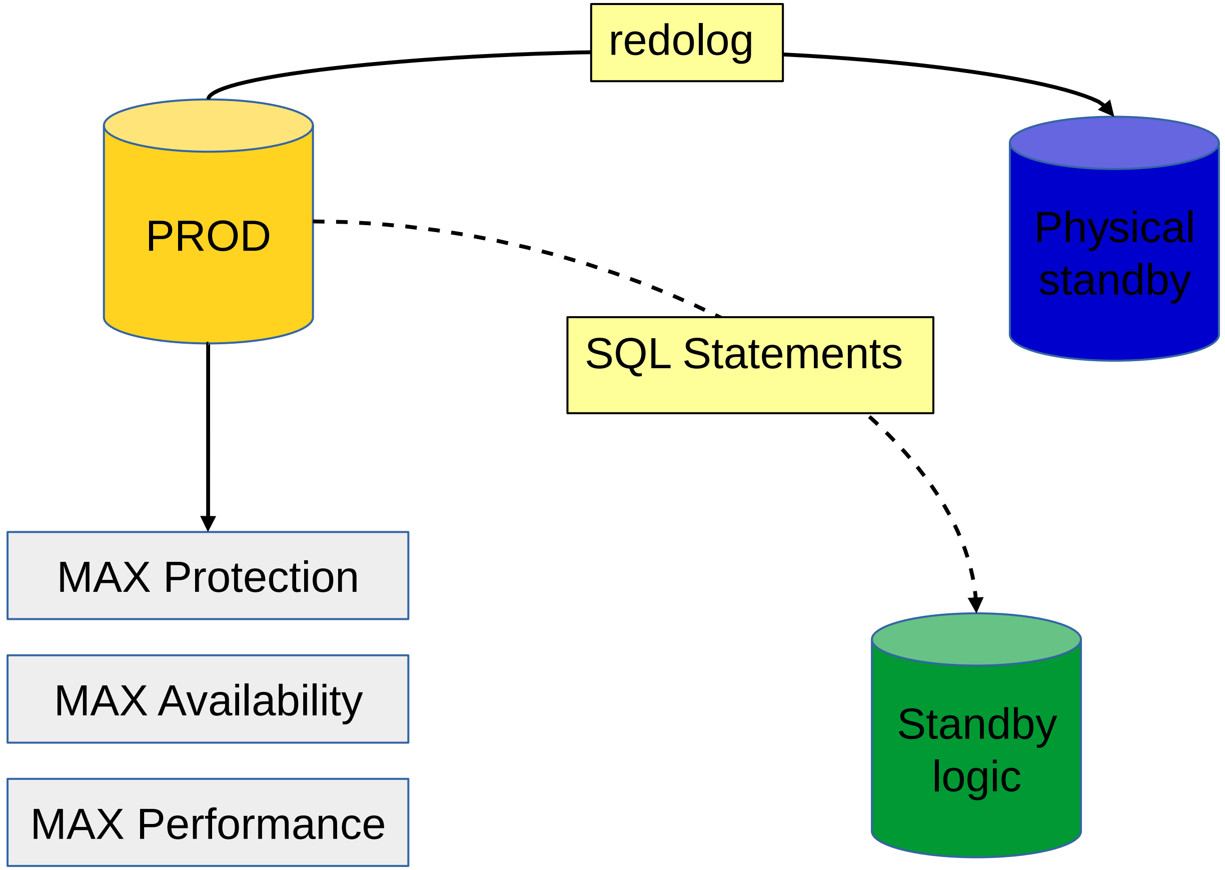
Flashback transaction: can be used to revert the changes of transaction (including the dependent transactions).

Stanby / Replication Setups

- The data is protected by replicating it to another location.
- The data can be recovered even an entire location is lost (wars, flood etc.)
- Usually, the standby database has a passive role and is activated only when the production site is lost.

Reykjavik
Oslo
Helsinki
Stockholm
Tallinn
Riga
Moscow
København
Vilnius
Dublin
London
Amsterdam
Berlin
Warsaw
Bruxelles
Paris
Luxembourg
Praha
Kiev
Bratislava
Vienna
Chişinău
Bern
Budapest
ROMÂNIA
Ljubljana
Zagreb
Bucureşti
Sarajevo
Beograd
Sofiya
Madrid
Lisboa
Roma
Tirane
Skopje
Ankara
Athinai
Tunis
Rabat
Algiers
Nicosia
Beirut
©2001 Amco Press

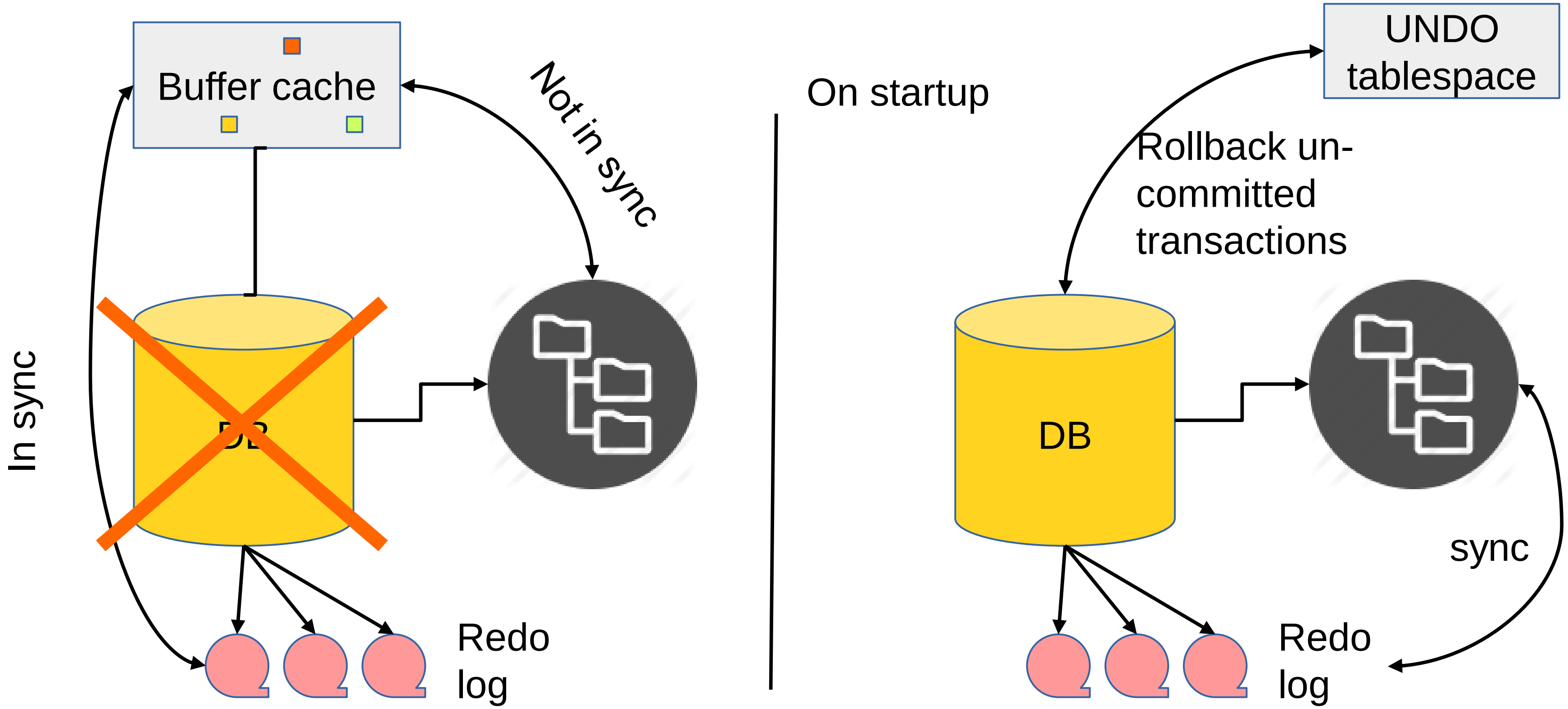
Standby Database Types



Crash Scenarios

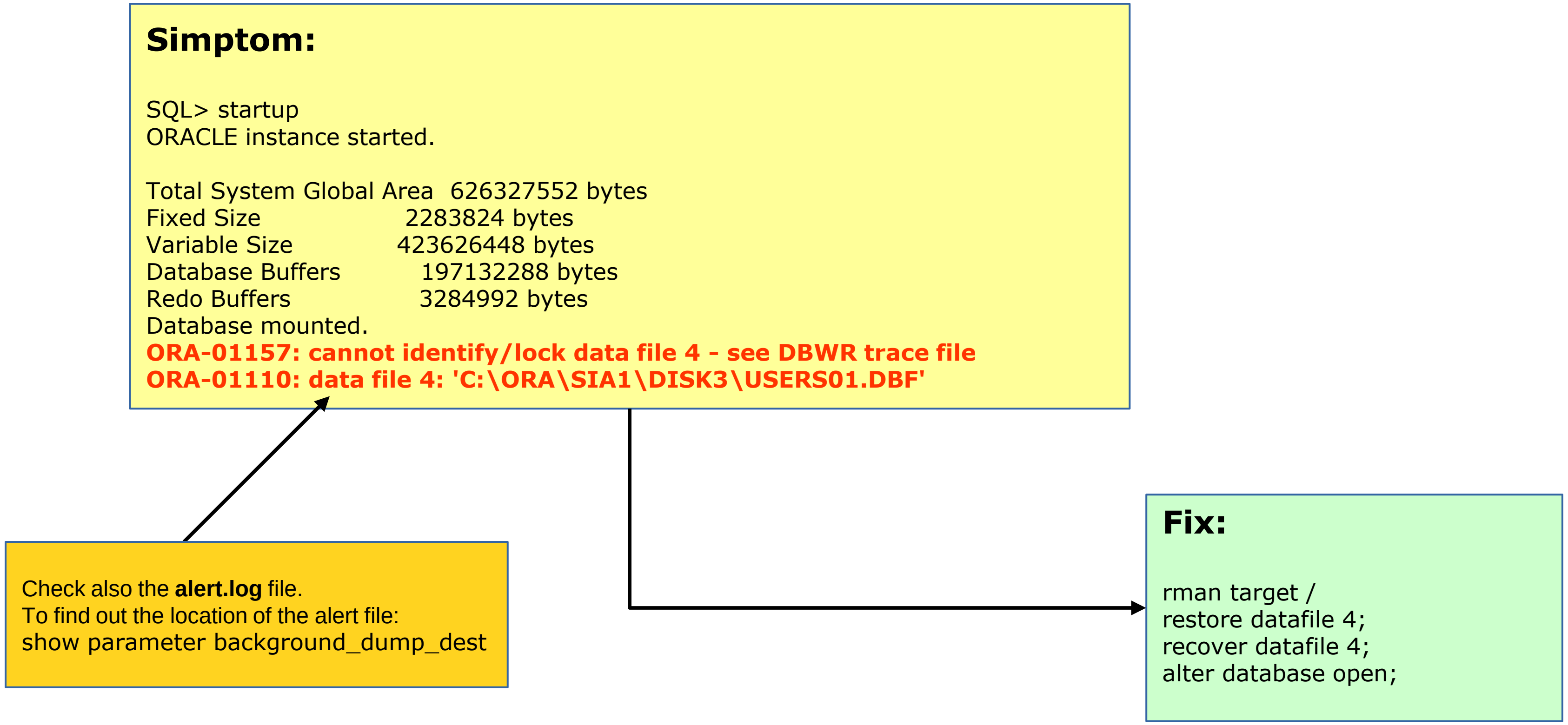
Oracle Instance Crash

A likely cause: Dorel has switched off the server.



Recovering a Datafile

A likely cause: Dorel has removed the file by mistake.



Simptom:

```
SQL> startup
ORACLE instance started.

Total System Global Area  626327552 bytes
Fixed Size                  2283824 bytes
Variable Size             423626448 bytes
Database Buffers            197132288 bytes
Redo Buffers                3284992 bytes
Database mounted.
ORA-01157: cannot identify/lock data file 4 - see DBWR trace file
ORA-01110: data file 4: 'C:\ORA\SIA1\DISK3\USERS01.DBF'
```

Check also the **alert.log** file.
To find out the location of the alert file:
`show parameter background_dump_dest`

Fix:

```
rman target /
restore datafile 4;
recover datafile 4;
alter database open;
```

Simulate a crash scenario where one datafile is deleted by mistake!

Loosing a Control-file

A likely cause: the disk where that controlfile was located has crashed.

Simptom:

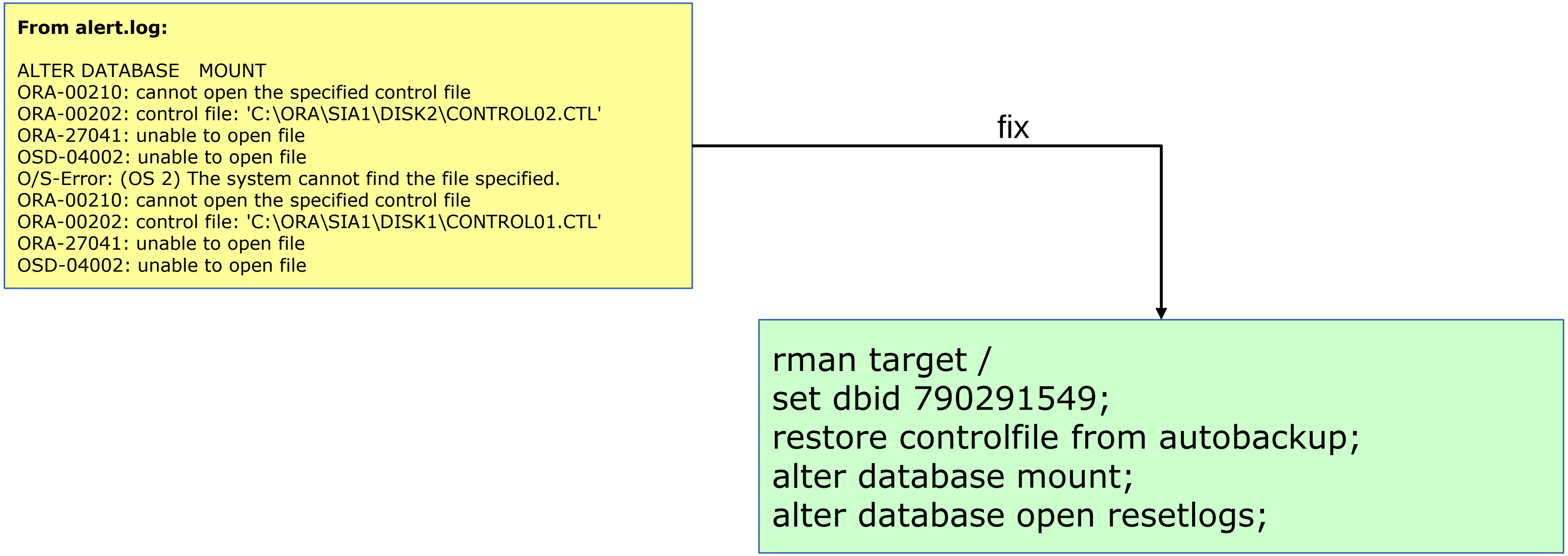
```
SQL> startup
ORACLE instance started.

Total System Global Area  626327552 bytes
Fixed Size                  2283824 bytes
Variable Size             423626448 bytes
Database Buffers          197132288 bytes
Redo Buffers                3284992 bytes
ORA-00205: error in identifying control file, check alert log for more info

In alert.log:

ORA-00210: cannot open the specified control file
ORA-00202: control file: 'C:\ORA\SIA1\DISK2\CONTROL02.CTL'
ORA-27041: unable to open file
OSD-04002: unable to open file
O/S-Error: (OS 2) The system cannot find the file specified.
```

Fixed by

```
SQL> select name from v$controlfile;

NAME
------------------------------------
C:\ORA\SIA1\DISK1\CONTROL01.CTL
C:\ORA\SIA1\DISK2\CONTROL02.CTL

copy C:\ORA\SIA1\DISK1\CONTROL01.CTL C:\ORA\SIA1\DISK2\CONTROL02.CTL

SQL> alter database mount;
SQL> alter database open;
```

All Control-files are Lost

A likely cause: Dorel has deleted all control-files or the disks have crashed.



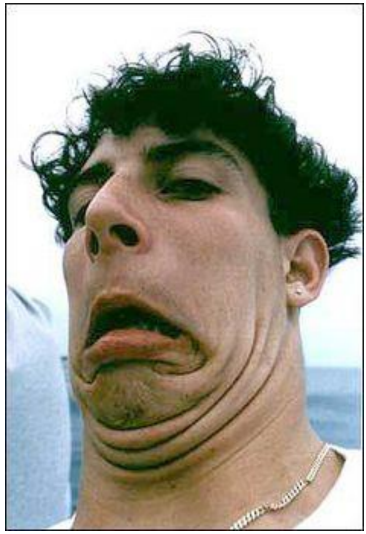
From alert.log:

```
ALTER DATABASE   MOUNT
ORA-00210: cannot open the specified control file
ORA-00202: control file: 'C:\ORA\SIA1\DISK2\CONTROL02.CTL'
ORA-27041: unable to open file
OSD-04002: unable to open file
O/S-Error: (OS 2) The system cannot find the file specified.
ORA-00210: cannot open the specified control file
ORA-00202: control file: 'C:\ORA\SIA1\DISK1\CONTROL01.CTL'
ORA-27041: unable to open file
OSD-04002: unable to open file
```

```
rman target /
set dbid 790291549;
restore controlfile from autobackup;
alter database mount;
alter database open resetlogs;
```

A Table Has Been Dropped

A likely cause: Dorel was mad because his salary wasn't raised, therefore he dropped the ANGAJATI table.



Dorel

DROP TABLE ANGAJATI!

FLASHBACK TABLE ANGAJATI TO BEFORE DROP;

The DBA

A New Password has been set, but for the Wrong User

Scenario:

- The DBA is requested to reset “ZOREL”’s password.
- By mistake, our DBA resets “DOREL”’s password instead of “ZOREL”’s.

```
alter user DOREL identified by "parola_noua";
```

Noooo!

```
SQL> select password from user$
as of timestamp sysdate-1/24
where name='DOREL';

PASSWORD
-----------------
FB63AE2ACC4630F4

SQL> alter user dorel identified
by values 'FB63AE2ACC4630F4';

User altered.
```

```
alter user ZOREL identified by "parola_noua";
```

Hands-on Practice

⛔ Marius Moga is complaining that he can’t access FB anymore. The DBA is engaged to reset Marius’ password. Unfortunately, by mistake, the DBA resets Marius Teicu’s password instead!

✋ Give DBA a hand and help him recover from this error!

The Backup & Recovery Strategy

It defines the acceptable data loss tolerance

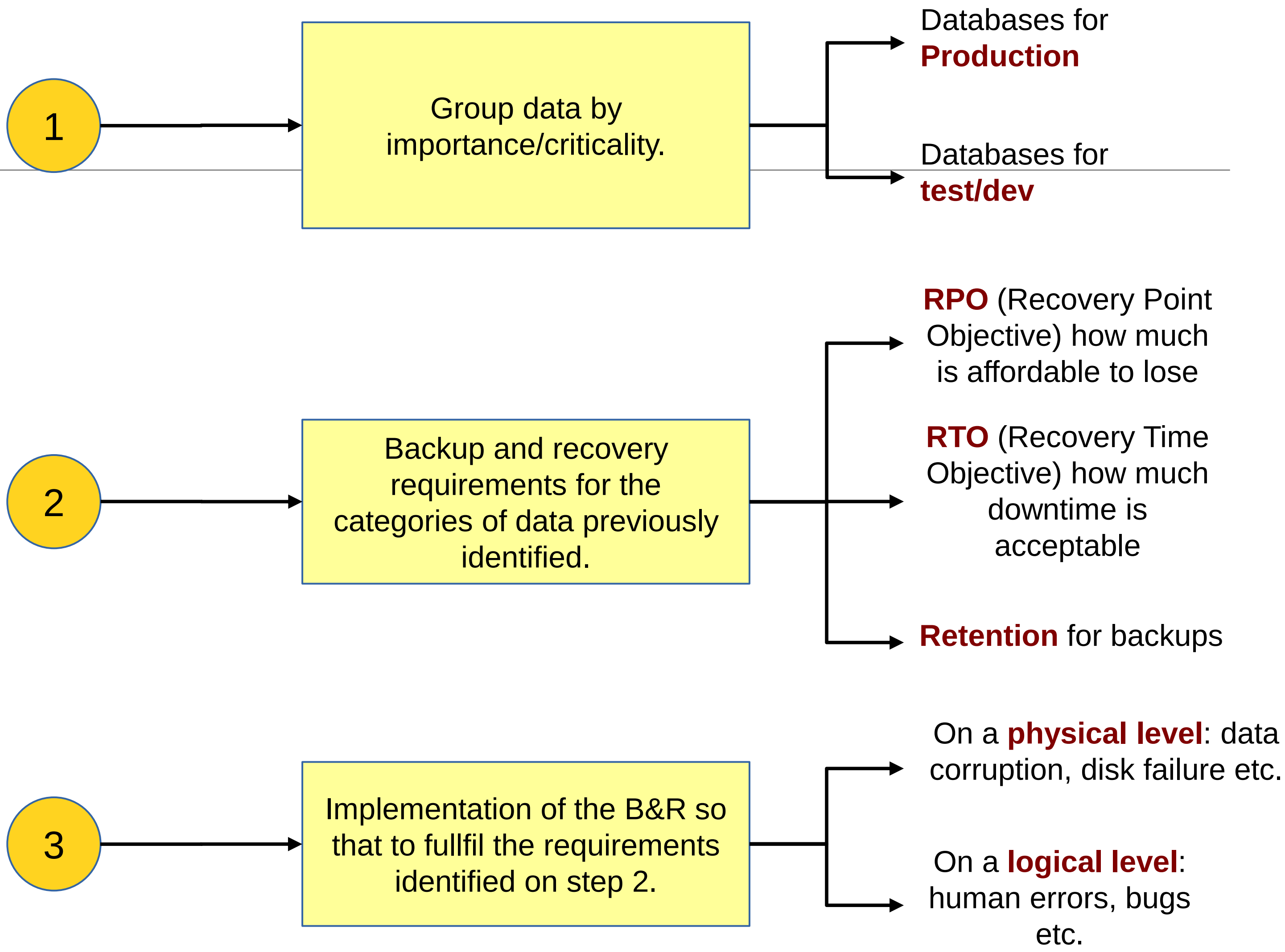
The data from the last X (minutes/hours/days) are acceptable to be lost.

Example: RPO = 15min, it means that the implemented backup and recovery strategy MUST ensure the recoverability of the data, at least as it was 15 minutes ago, before the database crashed.

It defines the downtime tolerance: how much time the database can remain inaccesible because of a major crash.

RTO = The time needed to identify the problem + The time to actually recover the database or to failover to the STANDBY database etc.)

RTO can be agreed on different levels: the entire database, on a tablespace level, a table or even on specific rows.



1

Group data by importance/criticality.

Databases for **Production**

Databases for **test/dev**

2

Backup and recovery requirements for the categories of data previously identified.

RPO (Recovery Point Objective) how much is affordable to lose

RTO (Recovery Time Objective) how much downtime is acceptable

Retention for backups

3

Implementation of the B&R so that to fullfil the requirements identified on step 2.

On a **physical level**: data corruption, disk failure etc.

On a **logical level**: human errors, bugs etc.

	Requirement	Goal	Implementation
PROD	RPO	30 minutes	ARCHIVE_LAG, STANDBY database, A FULL daily backup + incremental backups on every 30 minutes.
	RTO	2 hours	Restore/recovering from RMAN backups Activate the STANDBY database Flashback Table Flashback Database
	Backups Retention	7 days	A “recovery window” retention enforced on the RMAN level.
TEST	RPO	7 days	A full RMAN backup once a week.
	RTO	3 days	Restore/recover from RMAN backups Flashback Database
	Backups Retention	One copy on disk	A “redundancy 1” RMAN retention policy.

Testing the Backup & Recovery Strategy

Using BACKUP VALIDATE or RESTORE VALIDATE commands

Testing the workflow (the steps) required to restore the database.

Testing the failover to the standby database.

The tests should take place on a regular basis (once a year, on every 6 months etc.)