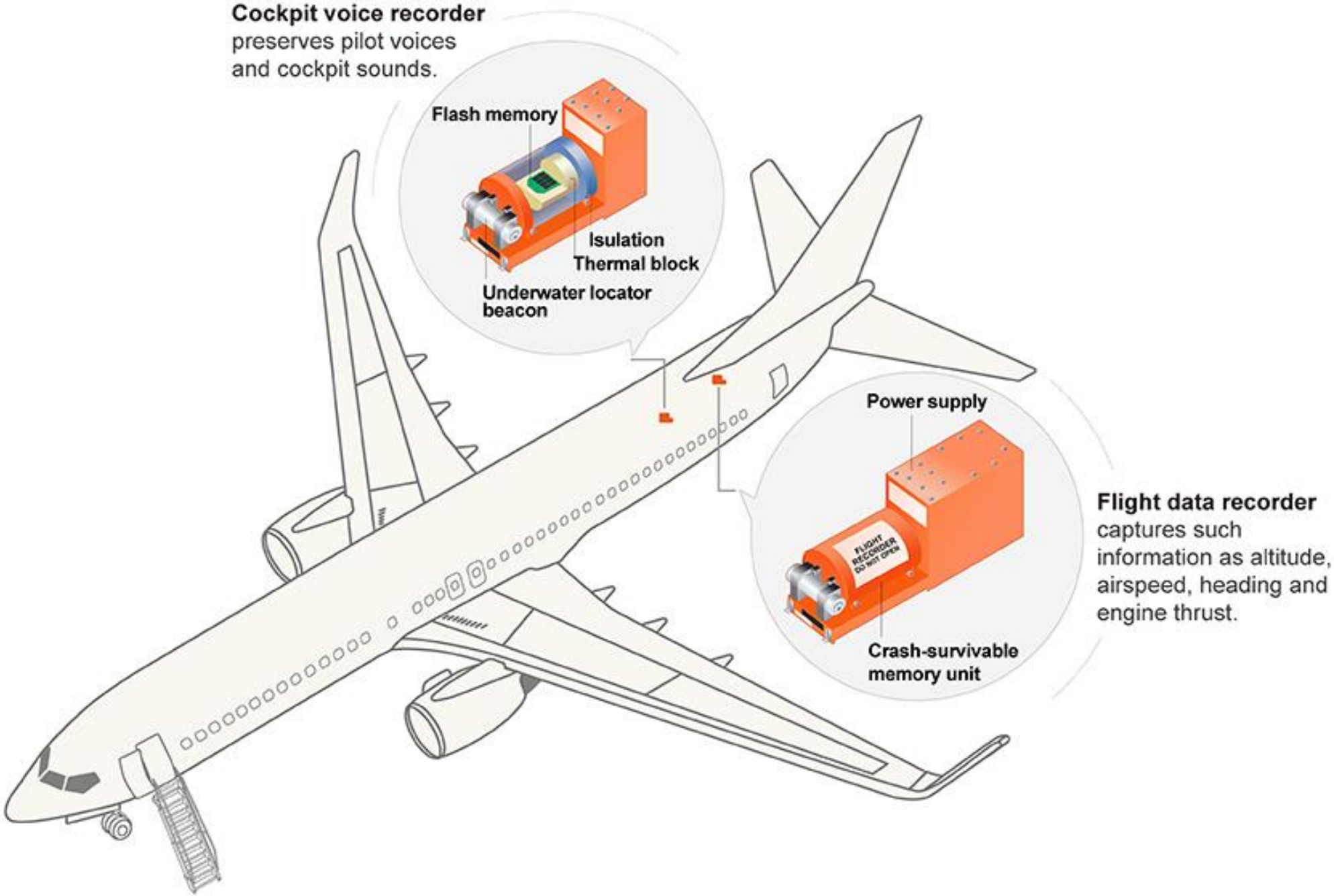
Flash memory technology in Aircraft Black boxes. Data recovery case studies.

Michał Gmurek, Rusolut

LEA-DER TRAINING CONFERENCE & EXPO 2023

October 10-12, 2023 | Prague, CZ

Data Recovery from Aircraft Black Box


Cockpit voice recorder
preserves pilot voices
and cockpit sounds.
Flash memory
Isulation
Thermal block
Underwater locator
beacon
Power supply
FLIGHT
RECORDER
DO NOT OPEN
Crash-survivable
memory unit
Flight data recorder
captures such
information as altitude,
airspeed, heading and
engine thrust.

D.T.MUX Sentinel™

RTCA DO-160 v G TESTED

MILITARY MIL-STD 810 G TESTED

Crash Protected System
from 32 to 128GB

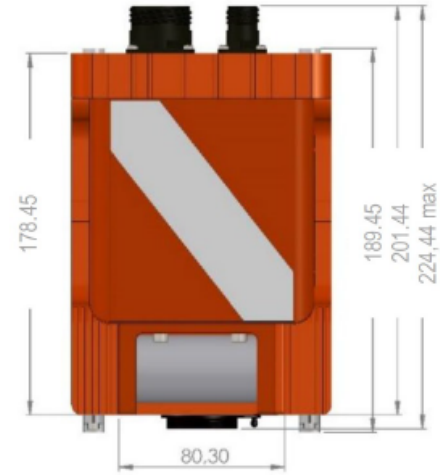
Reference# SEN-XXX

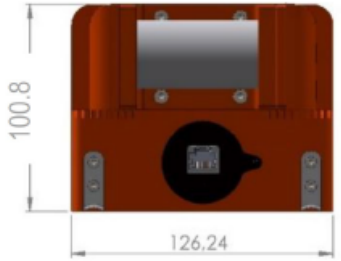
etep

D.T.MUX Sentinel™

MECHANICAL

	Specification	Remark
Size	189.5 (231.8 iRIPS /219.5 iEE) x 126.2 x 101 mm	D x W x H ± 1mm
Weight	≈ 3.30kg / 3.75kg ≈ 4.85kg	ED155/ ED112 iRIPS
Connectors	MIL-DTL-38999	Serie III
Mounting	ARINC 404	Customizable





ELECTRICAL

Input Voltage	28Vdc (16 to 36Vdc)
Power consumption	≈ 12 to 32 watts (28Vdc)
Power Interruption	≈ 200 to 800ms
Standard	MIL-STD-704F / DO-160

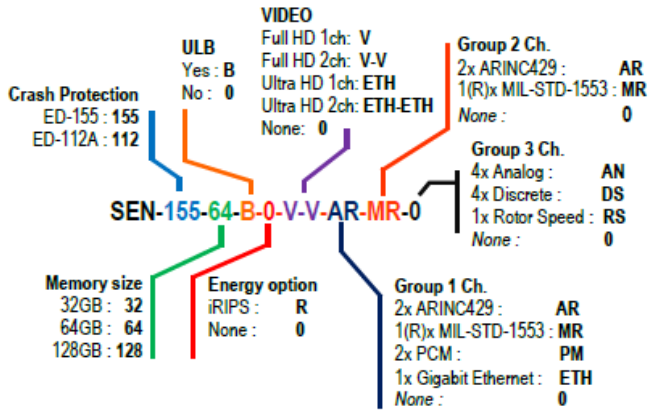
ENVIRONMENTAL

	Specification	Remark
Temperature	-40°C to 65°C	Operating
	-55°C to 90°C	Storage
Cooling	Passive	Convection
Humidity	95%	Non-Cond
Vibration	5Hz to 2KHz	6.29 g RMS
Shocks	20g 11ms	Operating
Acceleration	20g linear 3 axis	Operating
Altitude	+ 60,000 ft	Operating
Decompression	420Kpa/minute	Operating
MTBF	> 90,000 hours	Computed
EMI	DO-160	Rev G

STANDARD FUNCTIONALITY

	Specification
Gigabit Ethernet	Configuration/Control Data download and Streaming
Time synch	GPS Antenna input / Irig B / PTP v2
Voice	4x Audio channels
Recording	IRIG 106 Chapter 10 / DTMUX format
Sensors	Internal 3 Axis Gyro/ G force/ Pressure
COM port	RS-232 Configuration/Maintenance
Status	Status Led / Status output

SENTINEL PART NUMBER COMPOSITION



Environmental specifications

Environmental specifications

The equipment has been designed to meet the environmental specifications applicable to the installation limits as set forth in the version of RTCA/DO-160 in force at the time of certification.

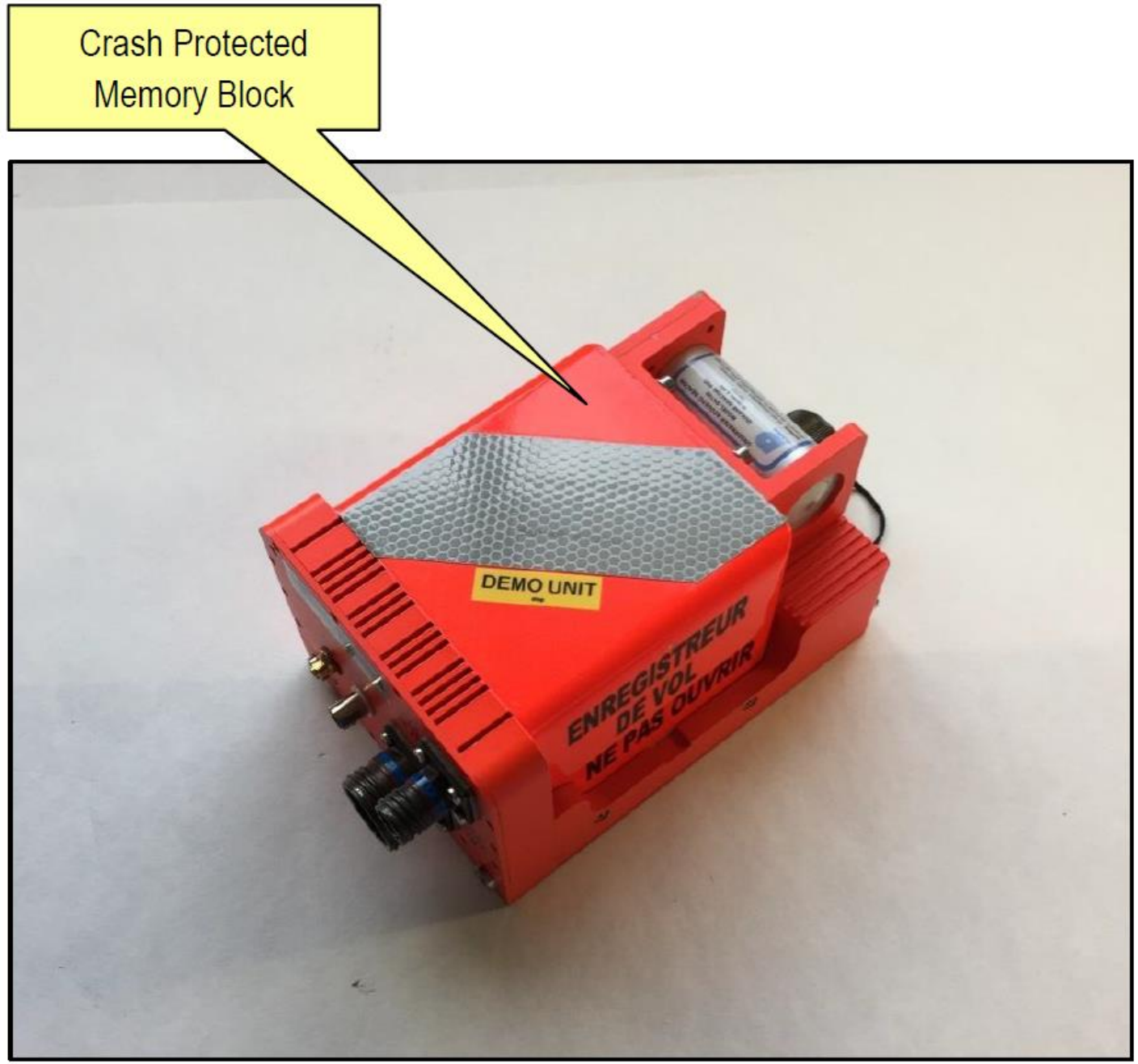
Flight Recording Systems (ED-112), Survivability

- Impact: 3400 Gs, 6.5ms, All Axes
- Pin Penetration: 500 lb., 10 ft.(1/4 in. Pin)
- Static Crush: 5000 lb, 5 min All Axes
- Low Temp Fire: 260C, during 10 hours
- High Temp Fire: 1,100 C, during 60 Min
- Sea Water Immersion: 30 Days
- Deep Sea Pressure: 20,000 ft., 24 Hrs.
- Fluid Immersion: Various Fluids, 48 Hrs.

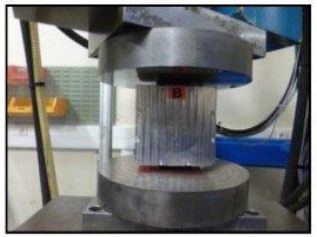
Sentinel Under High temperature fire test

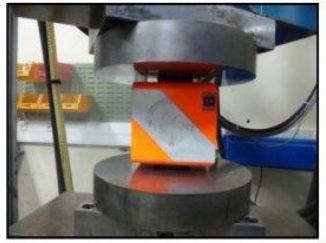
Qualification/Certification

Sentinel "ED-112 type" meets the requirements as specified in the Minimum Operational Performance Specification (MOPS) for flight recording systems ED-112. The system also outperforms many of the crash survival requirements in the Minimum Operational Performance Specification for Crash Protected Airborne Recorder Systems ED-112.


Crash Protected
Memory Block
DEMO UNIT
ENREGISTREUR
DE VOL
NE PAS OUVRIR

Hydraulic press test





Diagonal 1

Diagonal 2

Diagonal 3

Diagonal 4

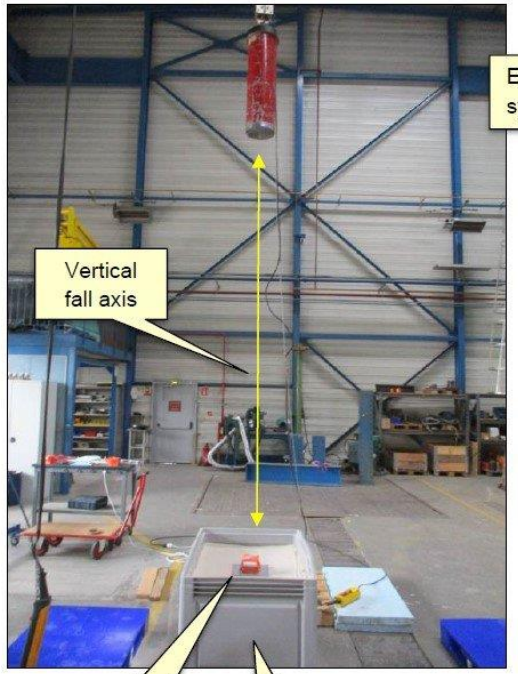
Crash test

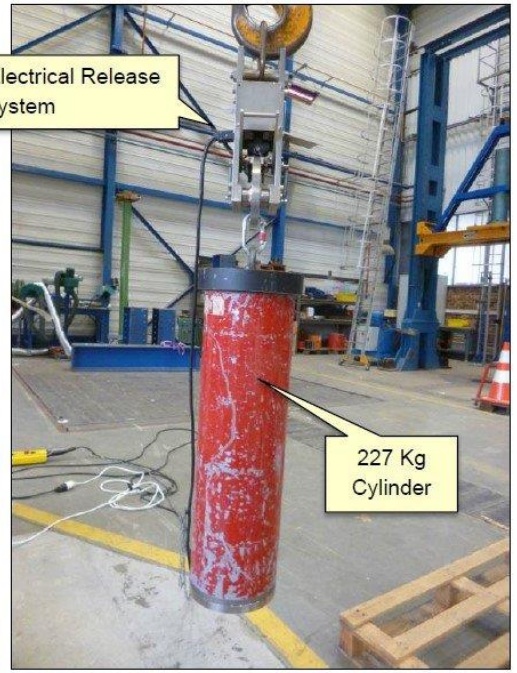

pSi-19-1386, ETEP- Impact Shock Test 02 B X+

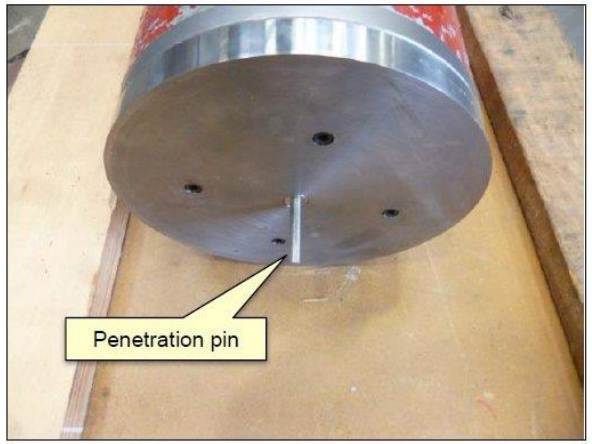

pSi-19-1386, ETEP- Impact Shock Test 02 B X+


pSi-19-1386, ETEP- Impact Shock Test 02 B X+

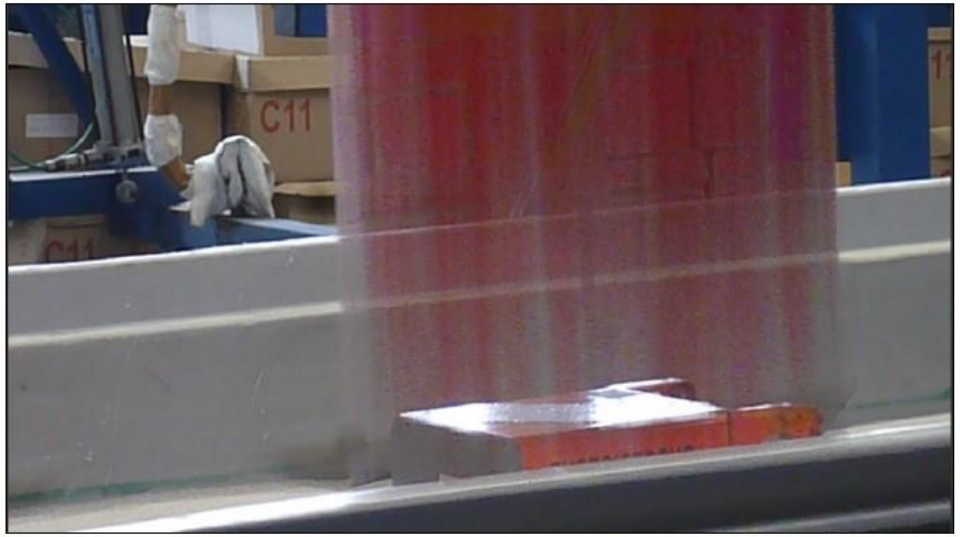
Impact test


Vertical
fall axis
Sentinel CSMU
Sandbox


Electrical Release
system
227 Kg
Cylinder


Penetration pin

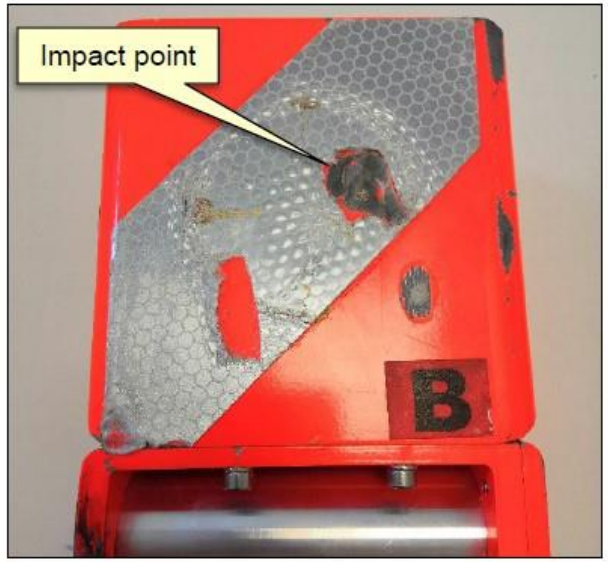

Steel plate

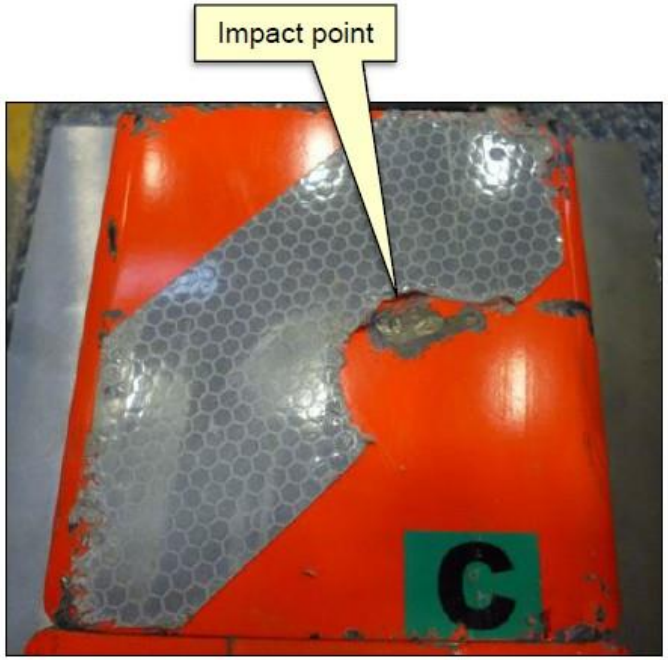

C11

Mechanical crash test results

CSMU “A”, “B” and “C” has successfully pass test sequence, no penetration or deformation of structure has been noted for each one.

Note:
Data contained inside robust memory are not analyzed before end of test sequence.



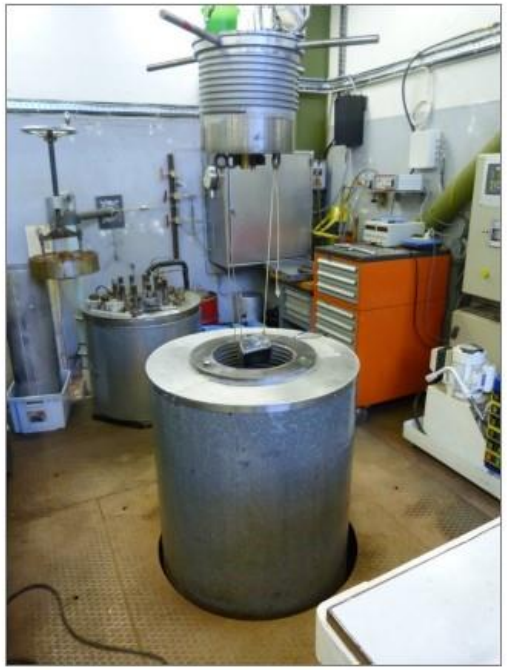


High pressure test

IFREMER is a French institute that undertakes research and expert assessments to advance knowledge on the oceans and their resources, monitor the marine environment and foster the sustainable development of maritime activities.

For more information consult Ifremer website: https://wwz.ifremer.fr/en/

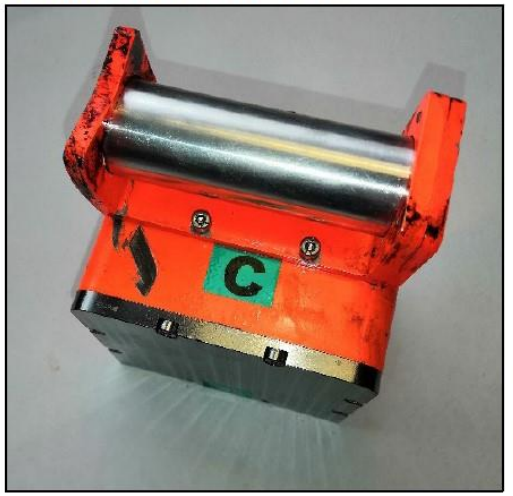
The Sentinel CPM is placed in hyperbaric chamber during 24 hours at 625 Bar, in saltwater to simulate a depth of 6000m. The materials used to protect the recording medium have been shown to be unaffected by sea water (Titanium …)



Ifremer

Pictures Laboratory: IFREMER France (La-Seyne sur-Mer)

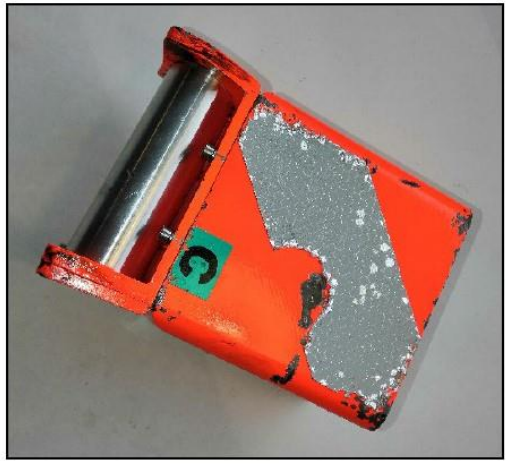
Sentinel CSMU Structure



This test must determinate if the crash protected memory Sentinel can resist to an equivalent depth of 6 000 m (20 000 feet).

We no detected any change of the Sentinel CPM structure after 24 hours at 625 Bar.

After this test in laboratory we don't note any deformation of the structure, and the structure is remains in **full integrity.**



High temperature test

Test has been conducted on Crash Protected memory unit destined to equip Sentinel System. The fire test is started by turning on the main gas valve. Flame temperature, as indicated by the external thermocouples, is continuously monitored. Figure 2 picture show Crash Protected Memory module under high temperature test.

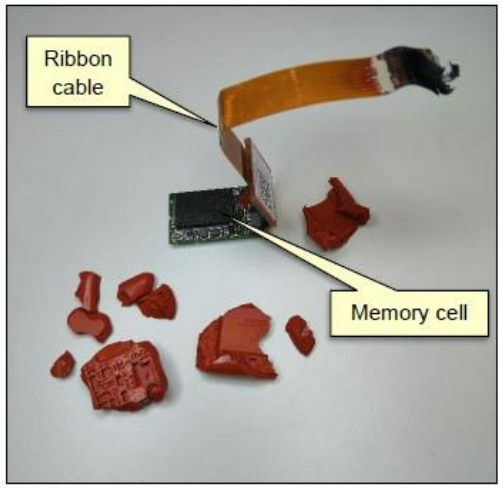
At the end of the test period, the burners have been shut off and the robust memory module has been cool naturally in ambient conditions. The crash Protect memory unit has been removed from the vicinity of the support arrangement.

High temperature test results

The unit is progressively put back to room temperature (natural cooling) the time is approximatively 3 hours before being able to go for opening process.

we don't notice any deformation of the structure and the structure is in **full integrity**. Bright orange paint has disappeared.

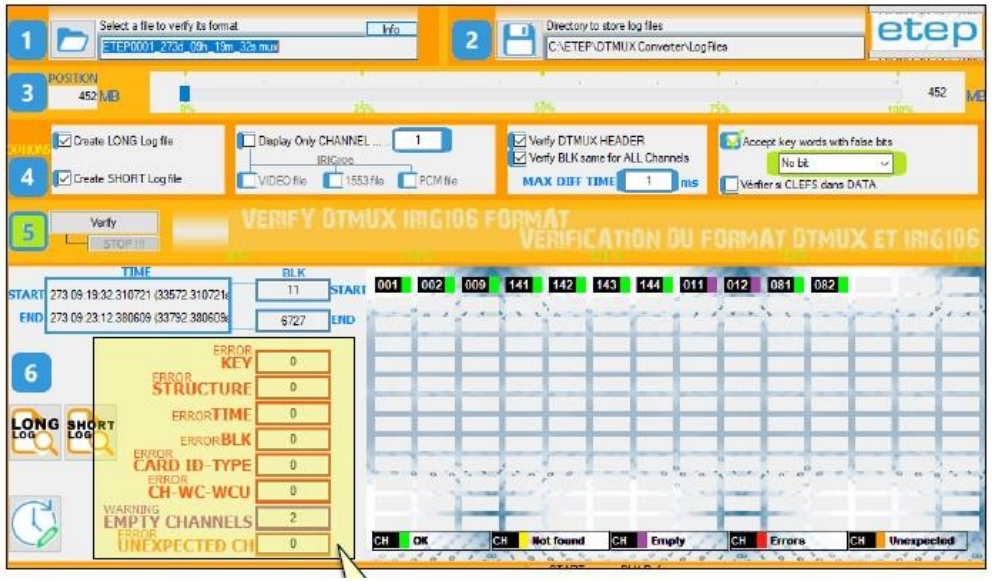
Reached temperature inside enclosure up to 132°C



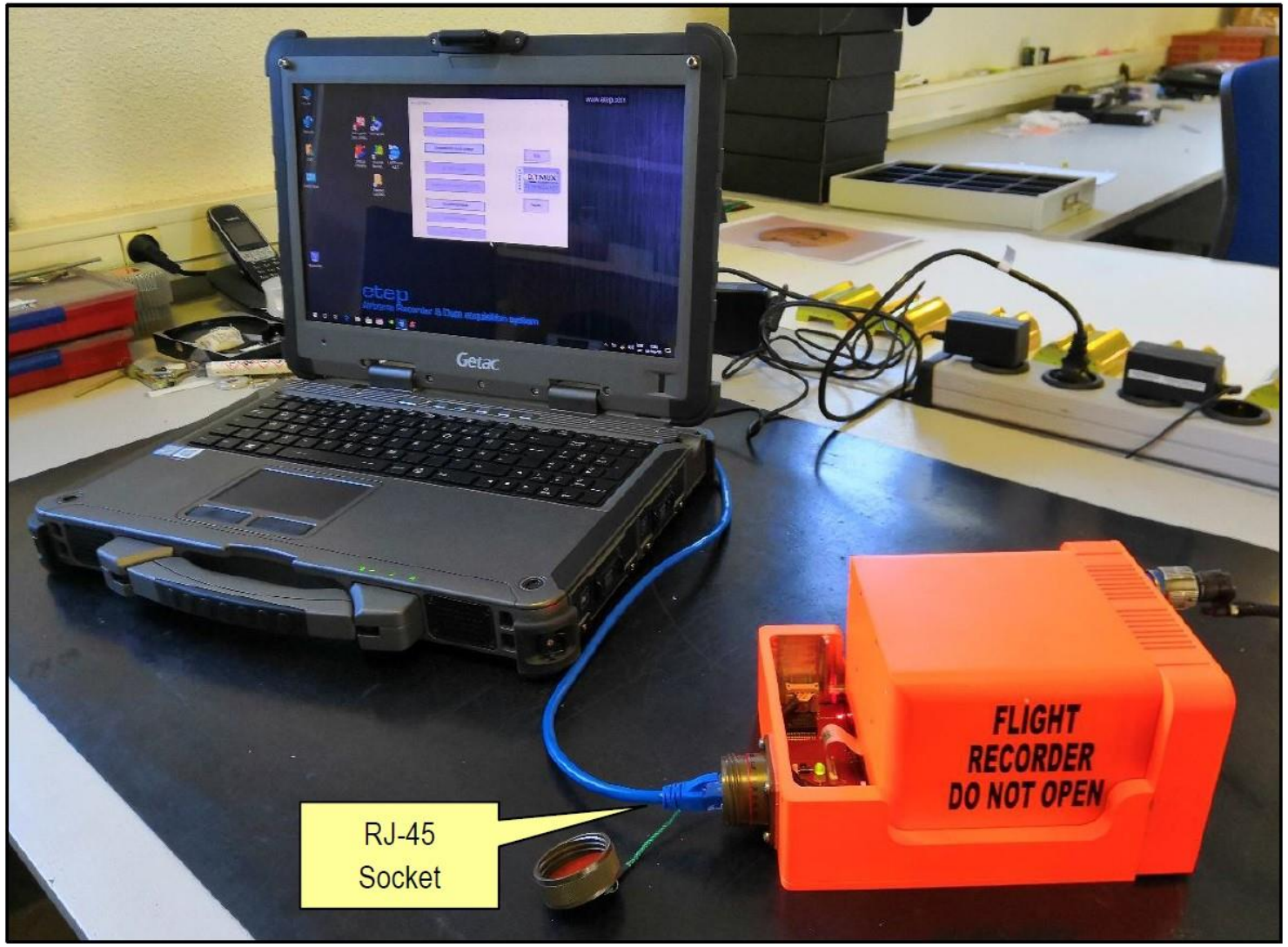
After the test sequence has been performed, this test pattern shall be readily recoverable to establish that the bit error rate defined in Chapter 2-4 has not been exceeded.

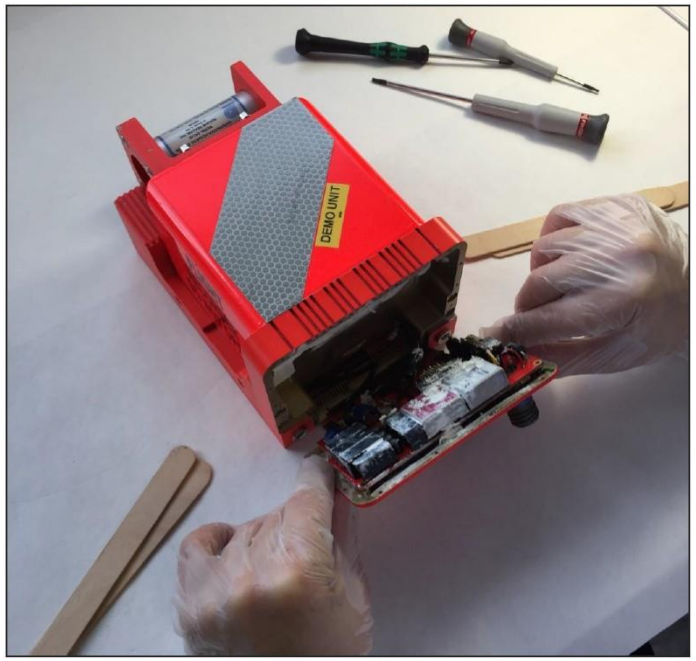
After this test the Sentinel crash protected memory is open to verify if the PCB did not damaged and if the data is still readable. After remove of all insulation protection (Ceramic, white powder material and red silicon protection), we examine the memory PCB.

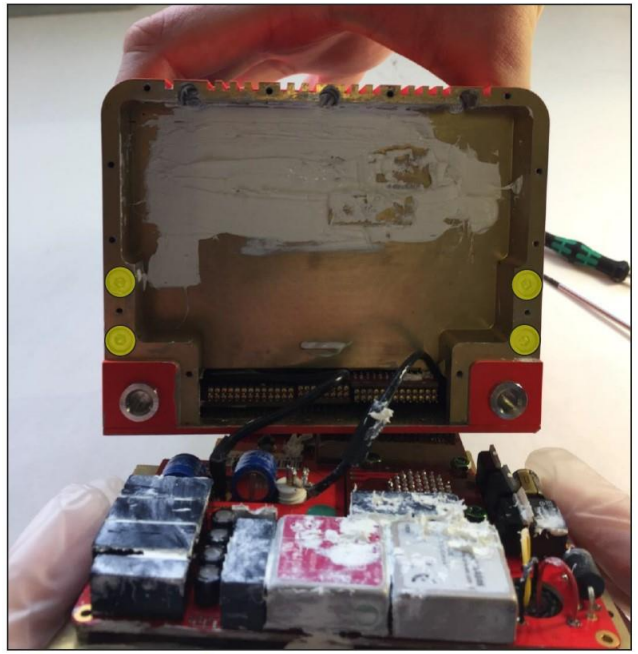
Solid state drive integrity
After a visual inspection, we no detect any damages on solid state drive circuit.
The memory unit was tested to verify if the data is in full integrity.
The data is in full integrity and no present any error.

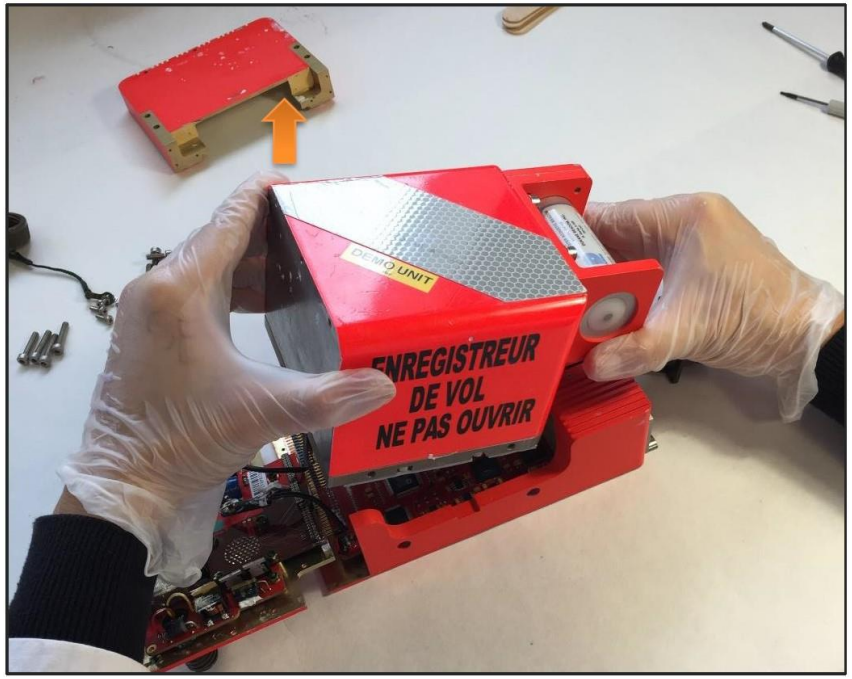


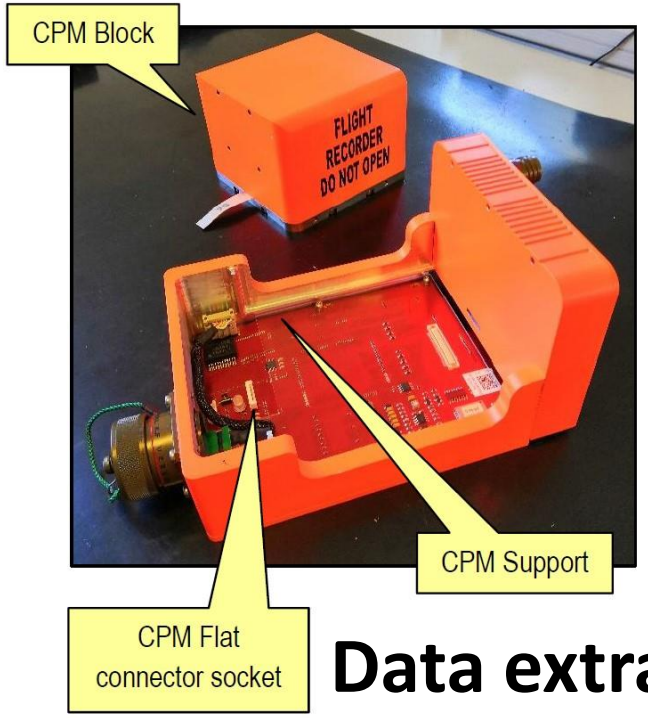
Data extraction via external interface

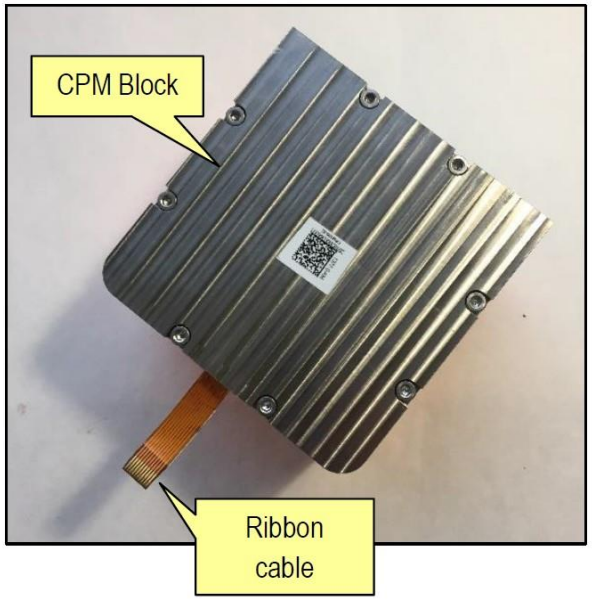




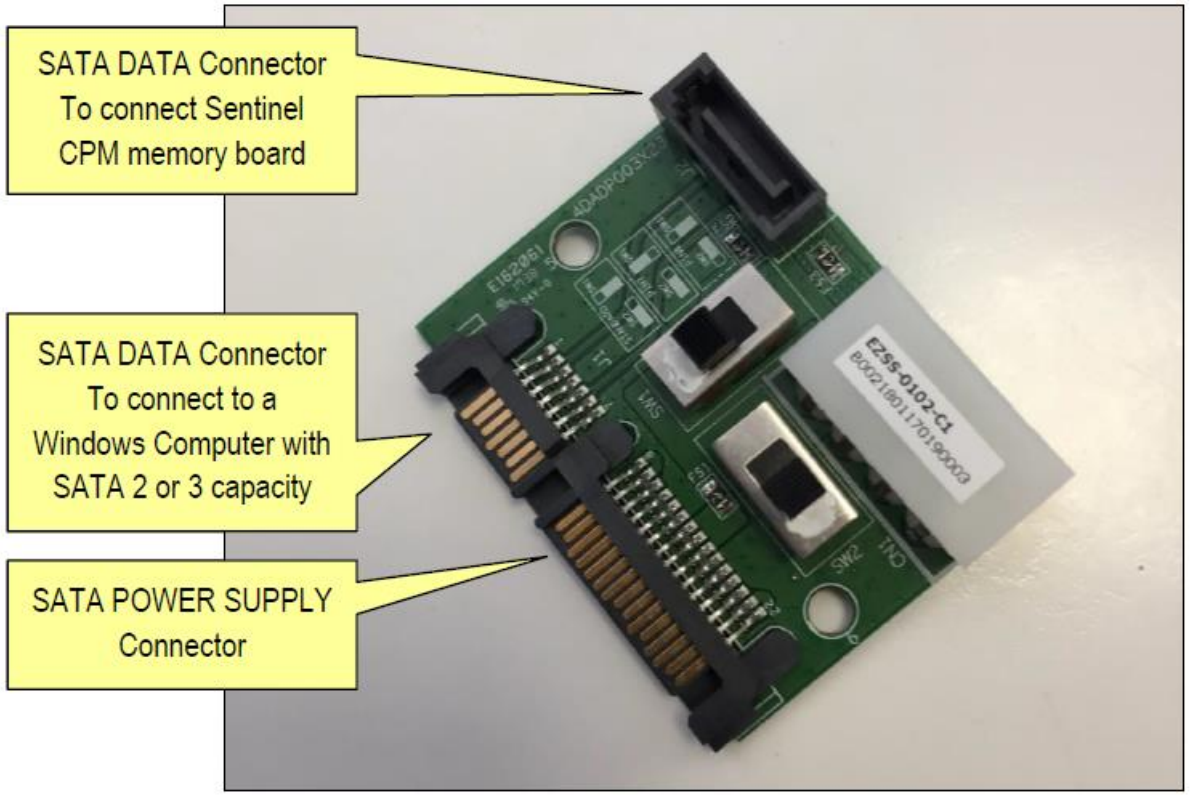


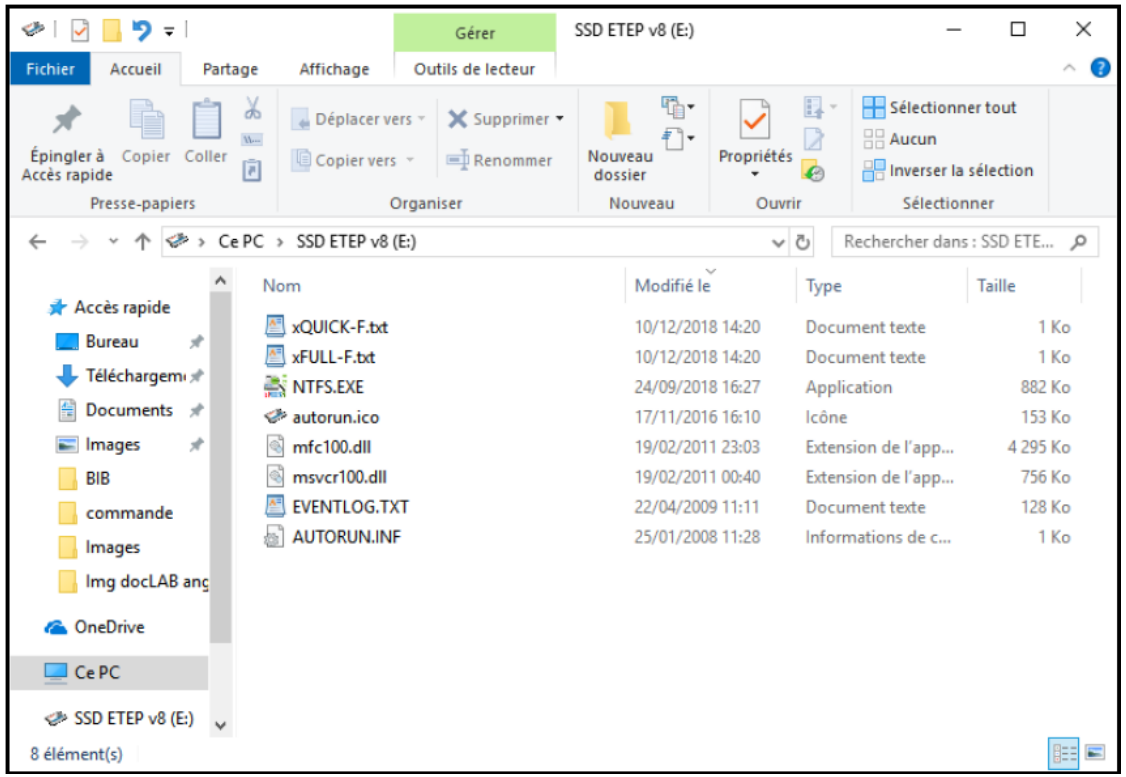






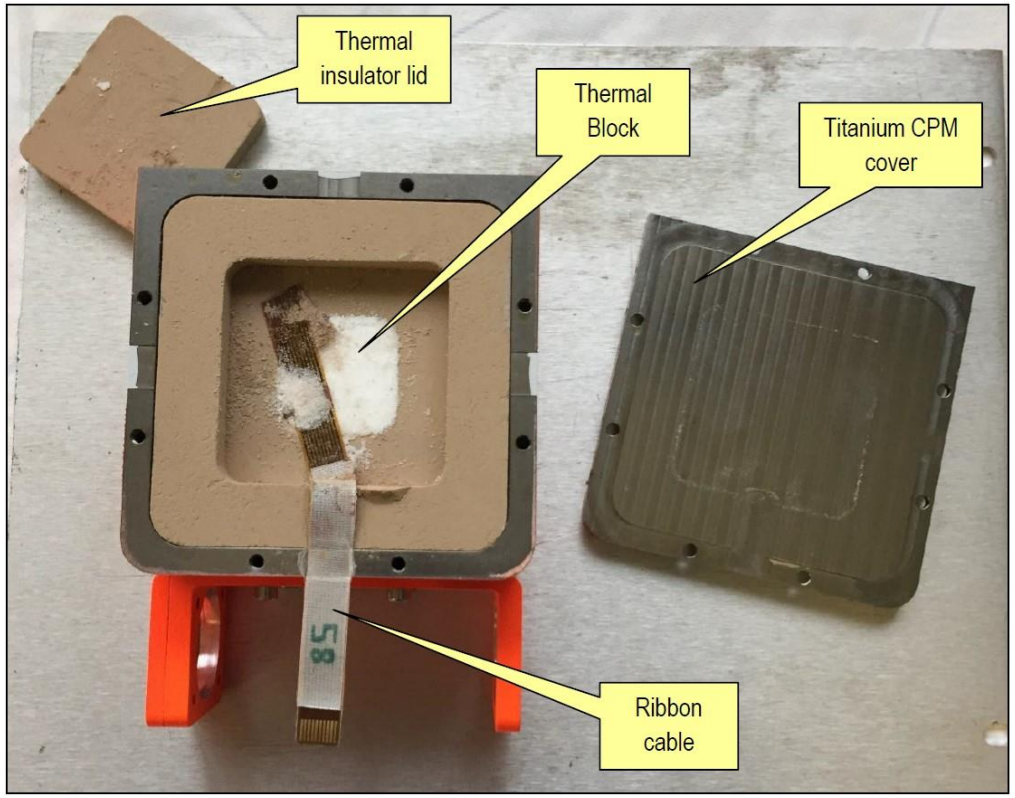
Data extraction via internal SATA

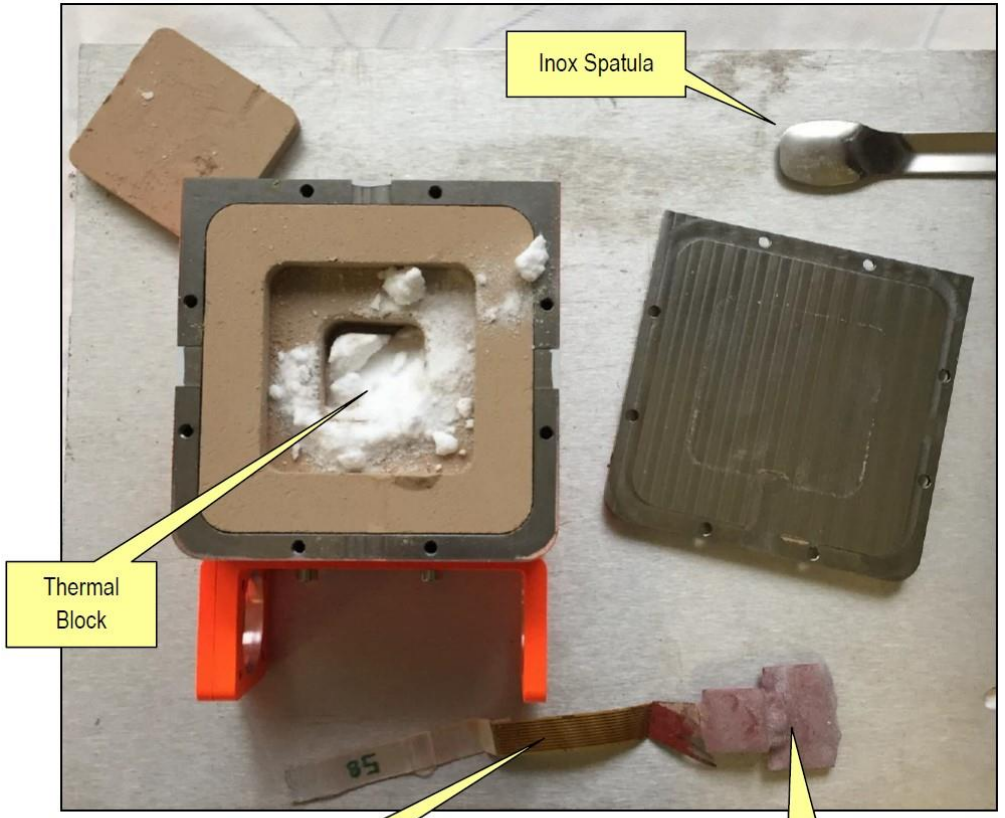

SATA DATA Connector
To connect Sentinel
CPM memory board
SATA DATA Connector
To connect to a
Windows Computer with
SATA 2 or 3 capacity
SATA POWER SUPPLY
Connector


SSD ETEP v8 (E:)
Gérer
Fichier
Accueil
Partage
Affichage
Outils de lecteur
Épingler à Accès rapide
Copier
Coller
Déplacer vers
Copier vers
Supprimer
Renommer
Nouveau dossier
Propriétés
Sélectionner tout
Aucun
Inverser la sélection
Presse-papiers
Organiser
Nouveau
Ouvrir
Sélectionner
Ce PC › SSD ETEP v8 (E:)
Rechercher dans : SSD ETE...
Accès rapide
Bureau
Téléchargem
Documents
Images
BIB
commande
Images
Img docLAB ang
OneDrive
Ce PC
SSD ETEP v8 (E:)
Nom
Modifié le
Type
Taille
xQUICK-F.txt 10/12/2018 14:20 Document texte 1 Ko
xFULL-F.txt 10/12/2018 14:20 Document texte 1 Ko
NTFS.EXE 24/09/2018 16:27 Application 882 Ko
autorun.ico 17/11/2016 16:10 Icône 153 Ko
mfc100.dll 19/02/2011 23:03 Extension de l'app... 4 295 Ko
msvcr100.dll 19/02/2011 00:40 Extension de l'app... 756 Ko
EVENTLOG.TXT 22/04/2009 11:11 Document texte 128 Ko
AUTORUN.INF 25/01/2008 11:28 Informations de c... 1 Ko
8 élément(s)

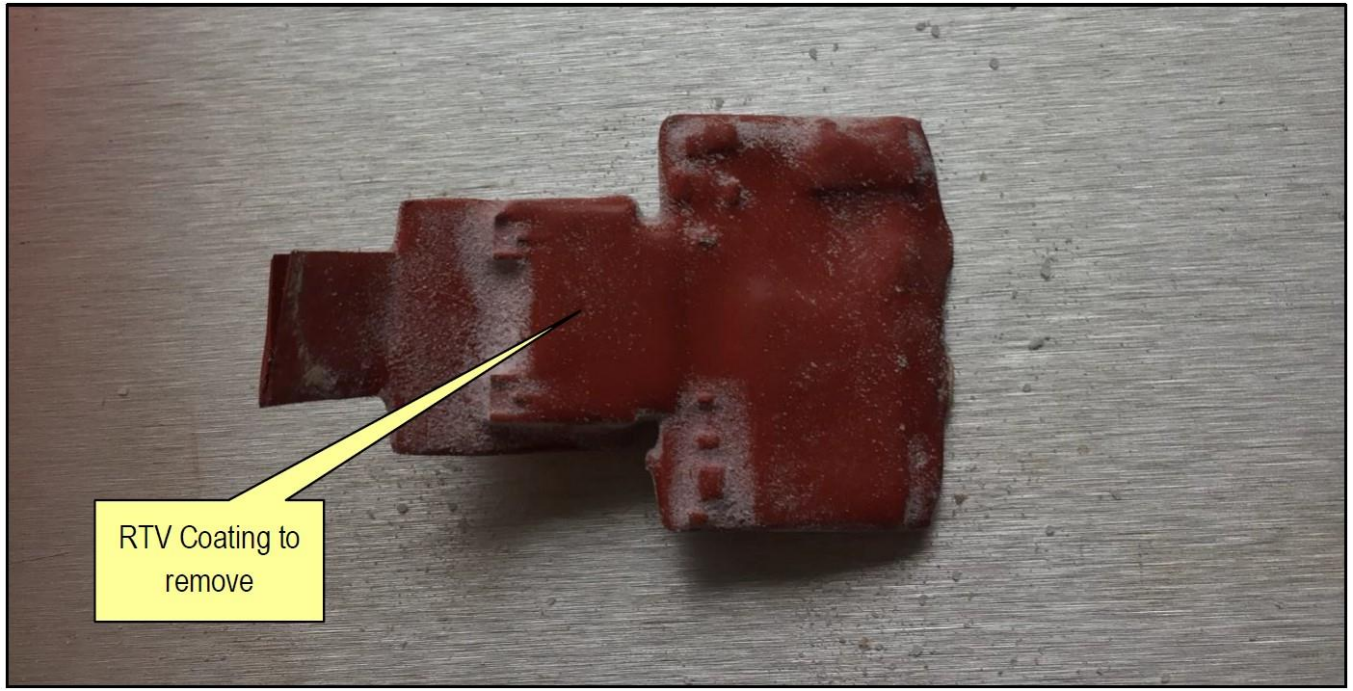
Real-world test...

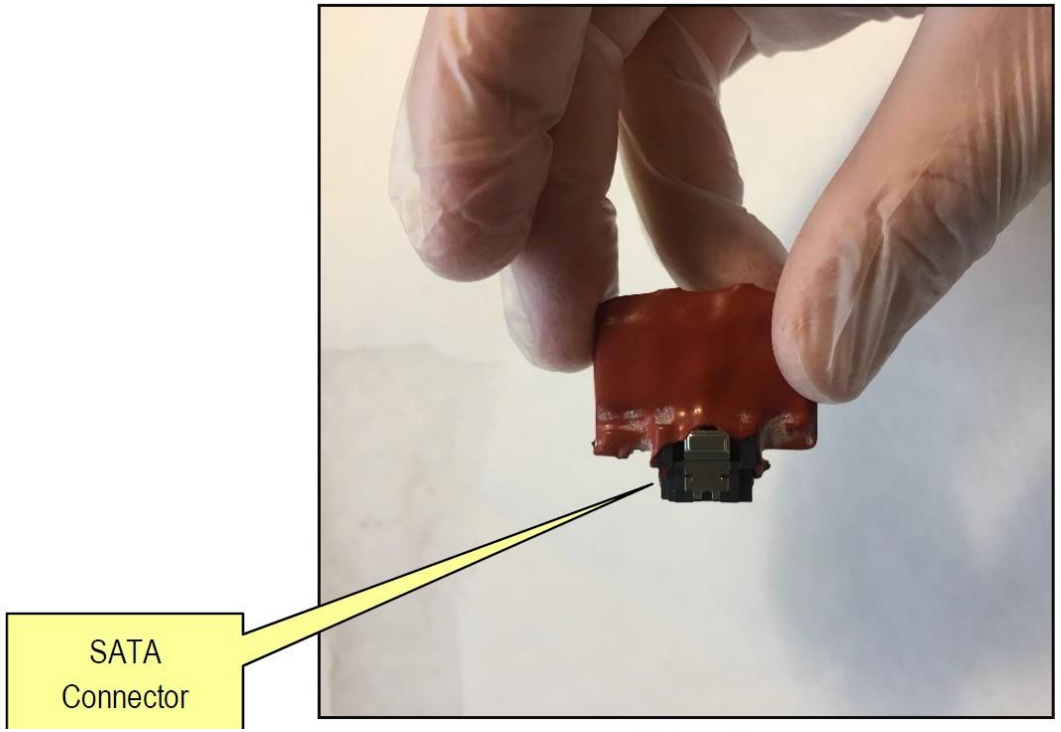
When everything else fails...chips usually don't



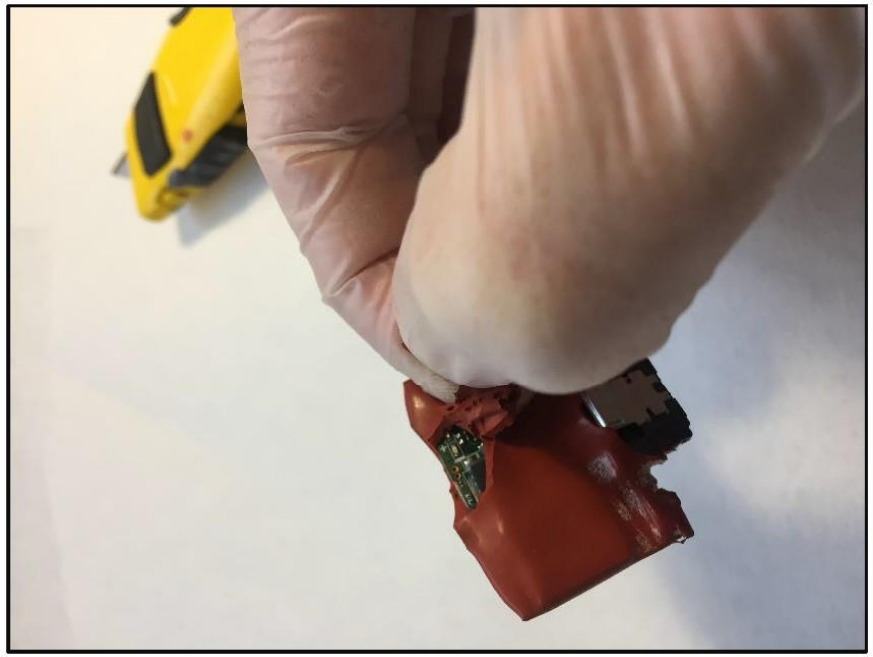


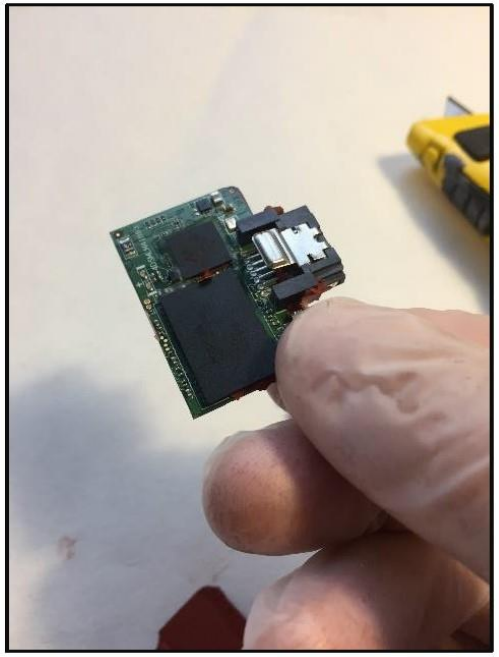
Picture 4





FORTUNATELLY, real-world crash conditions are rare occasion, we were not able to get our hands on damaged device



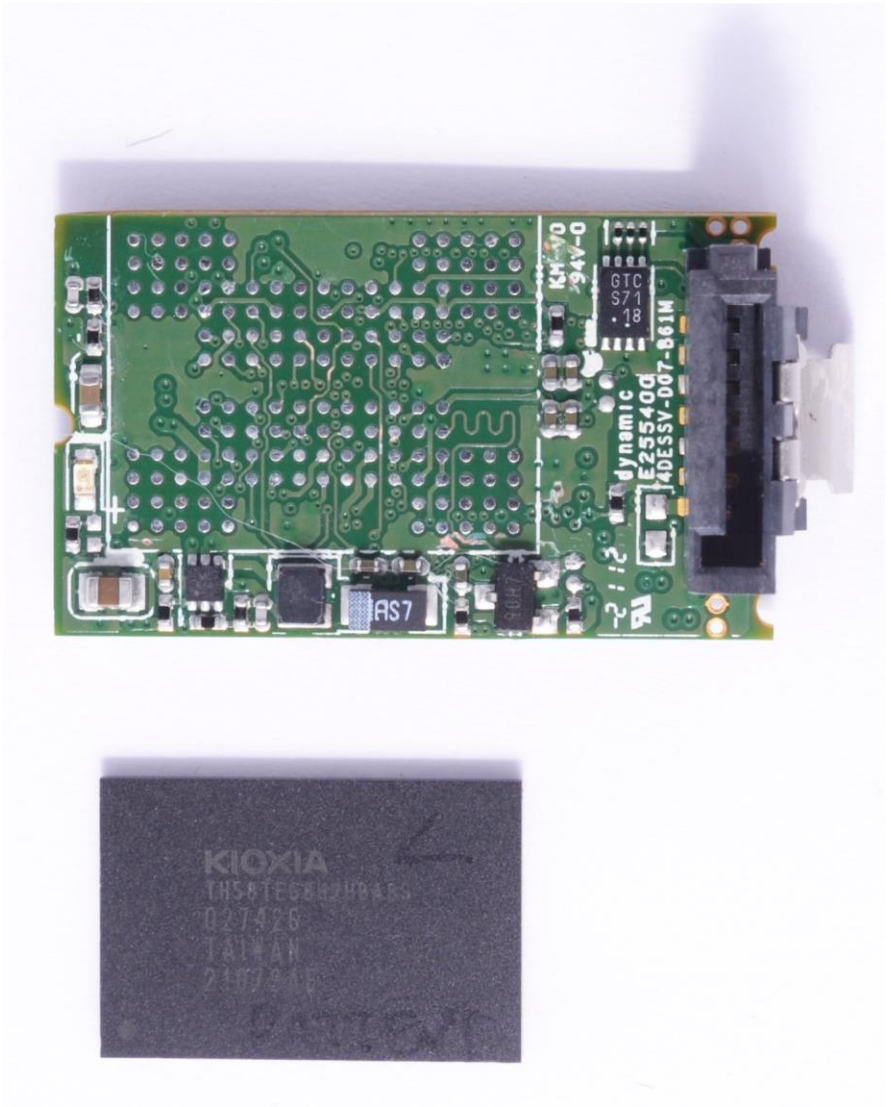


On this side of PCB we can spot NAND memory chip made by Kioxia (Toshiba) with the model name TH58TEG8H2HBA-89

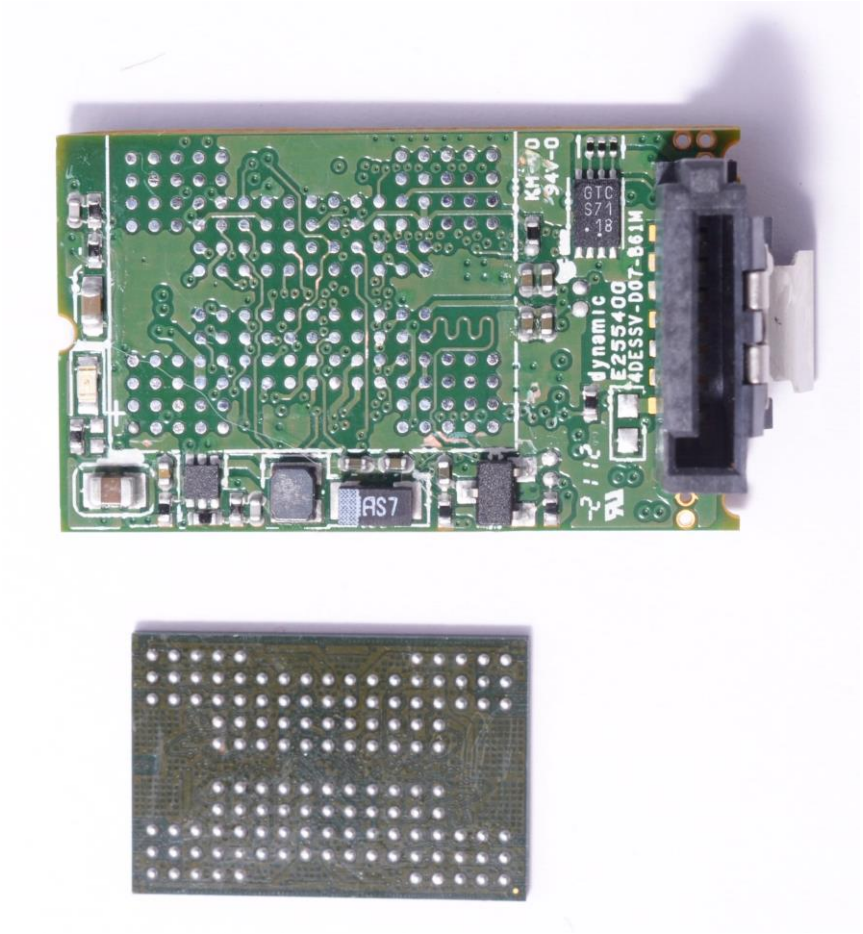
On the other side of PCB we can see the microcontroller

Unsoldered NAND memory – top view

The memory chip was removed from the PCB for further reading using InfraRed rework station and thermal profile of Tmax = 240C (Tdelta ~ 3C/s)



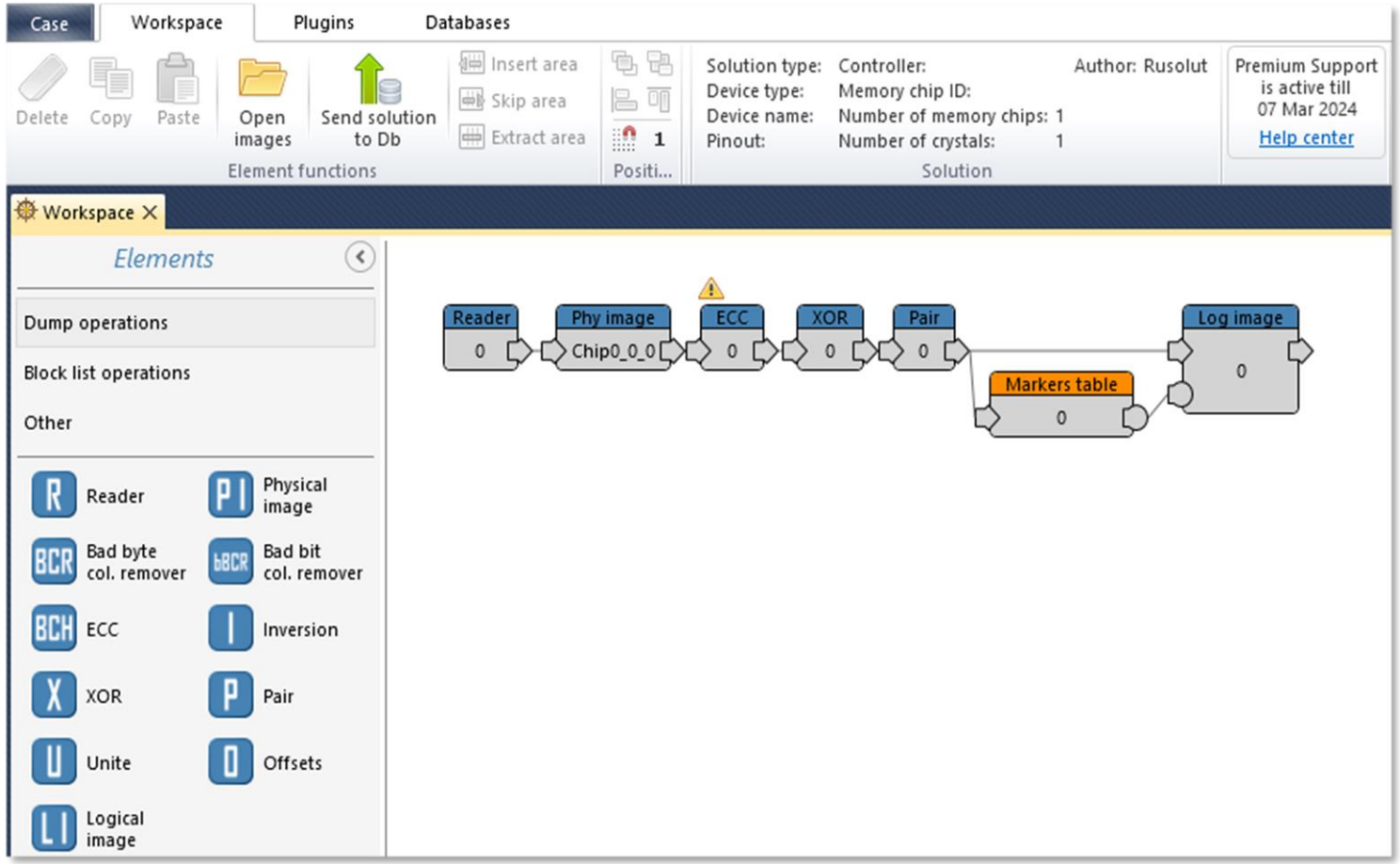
Unsoldered NAND memory – ball view



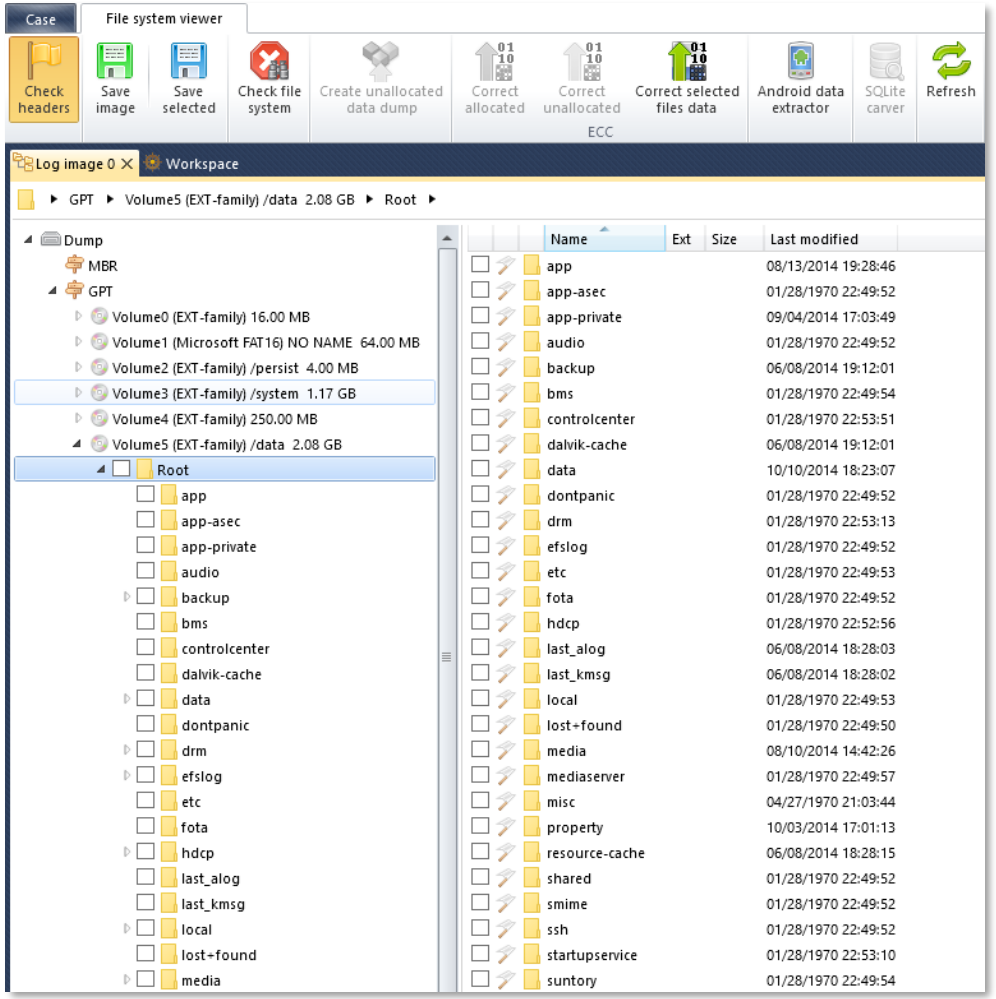
The NAND memory has BGA-132 package which is classics for high-capacity memory chips.
The pads of NAND memory chip have been cleaned with solder wick and then isopropyl alcohol.

Visual NAND Reconstructor

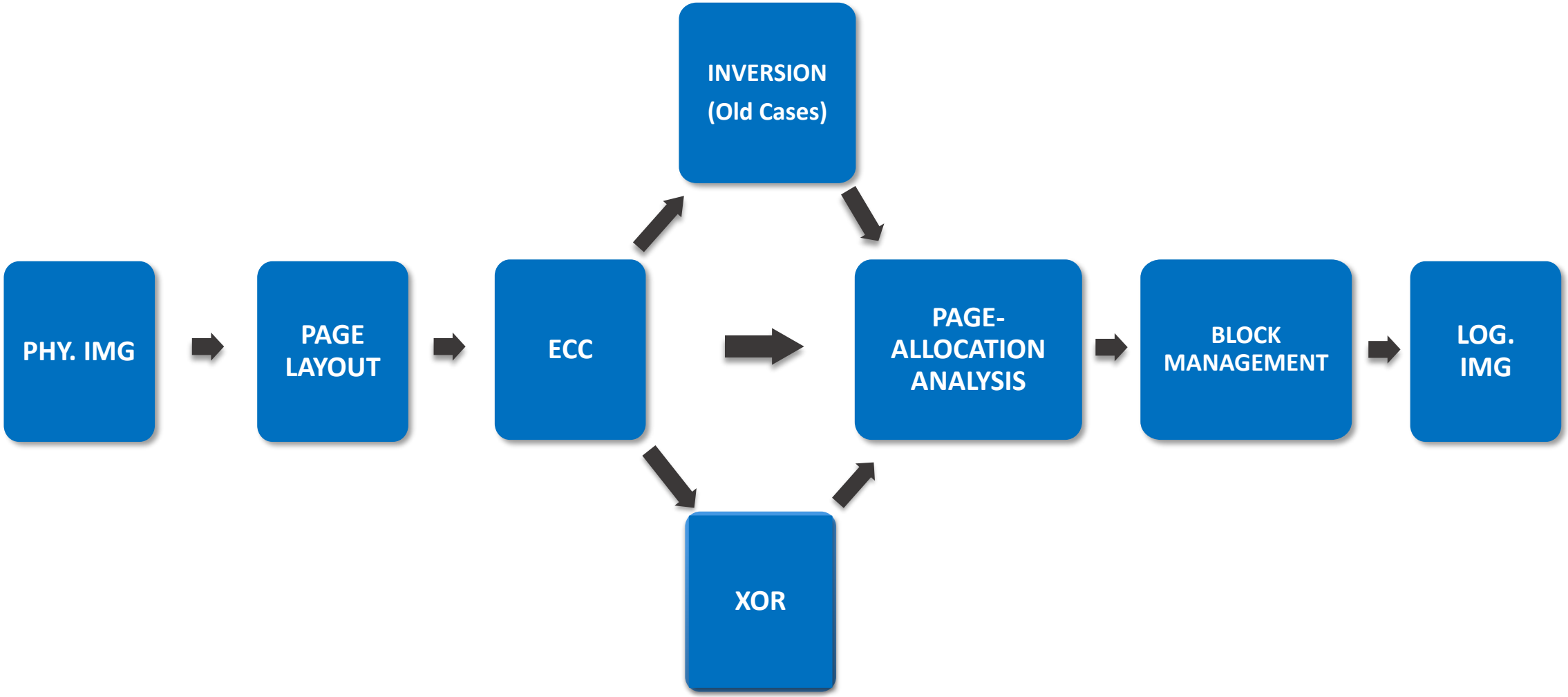
Physical image reconstruction in VNR



Data extraction



Chip-off data recovery procedure

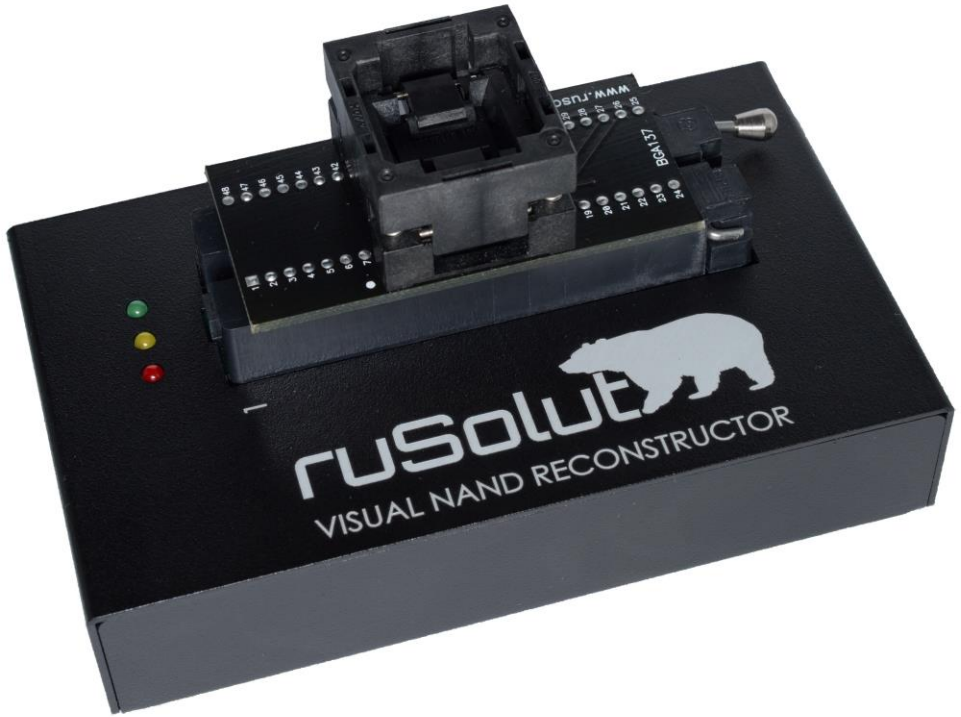


Chip connected to VNR Reader

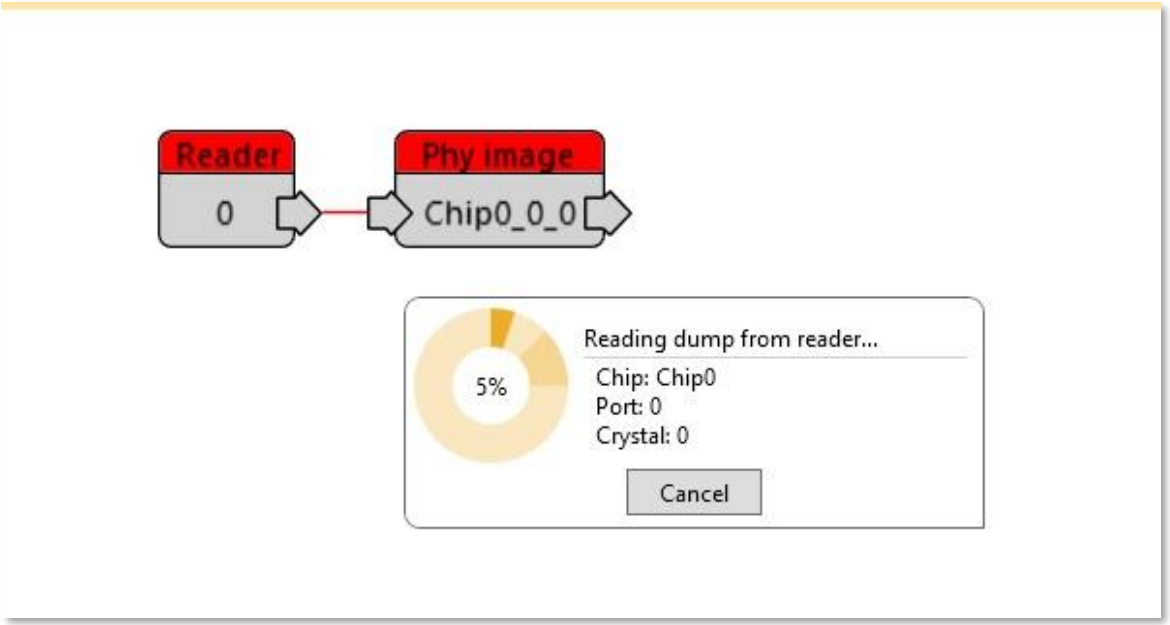
We used Visual Nand Reconstructor Reader from Starter kit in couple with BGA132 adapter from Standard kit for memory chip reading.

Physical image extraction

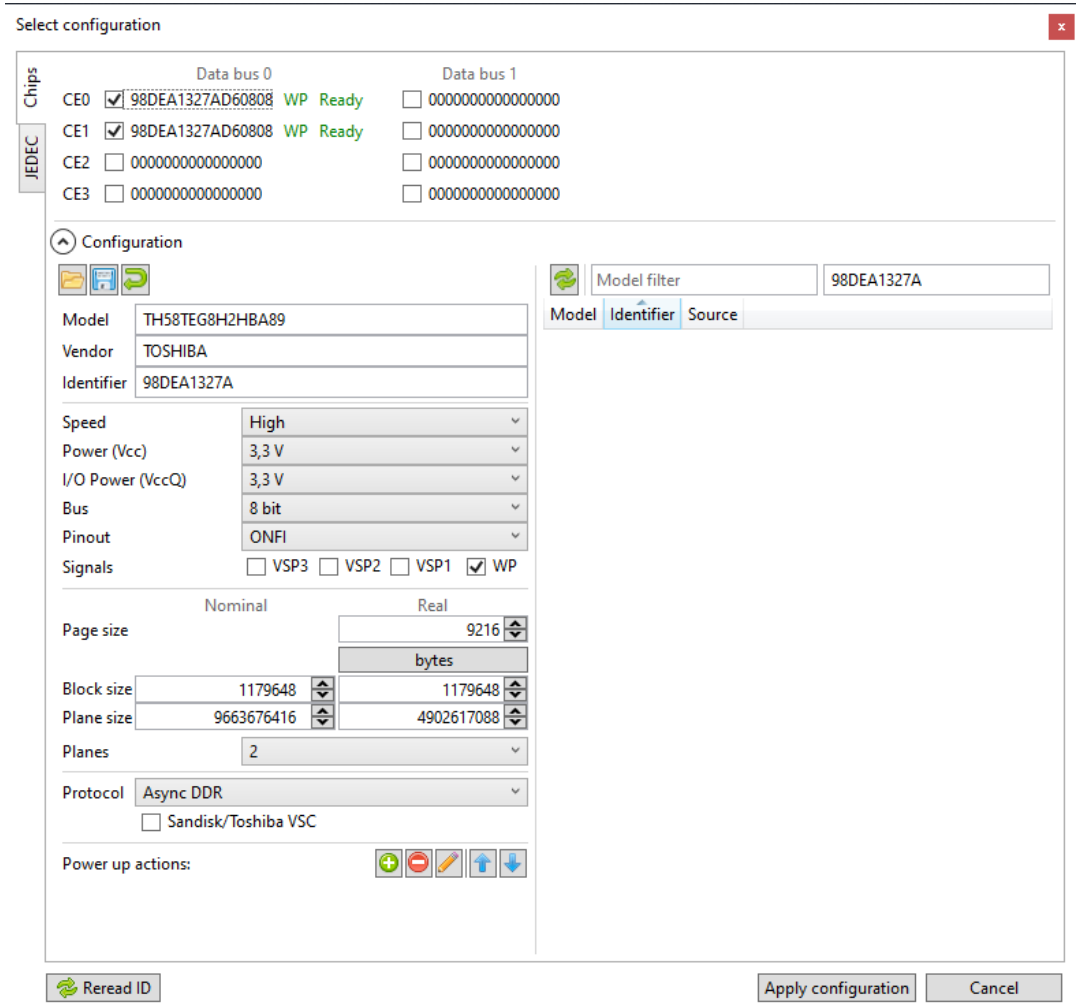
Device in the VNR Reader



Reading initialised in the software



Memory chip identification

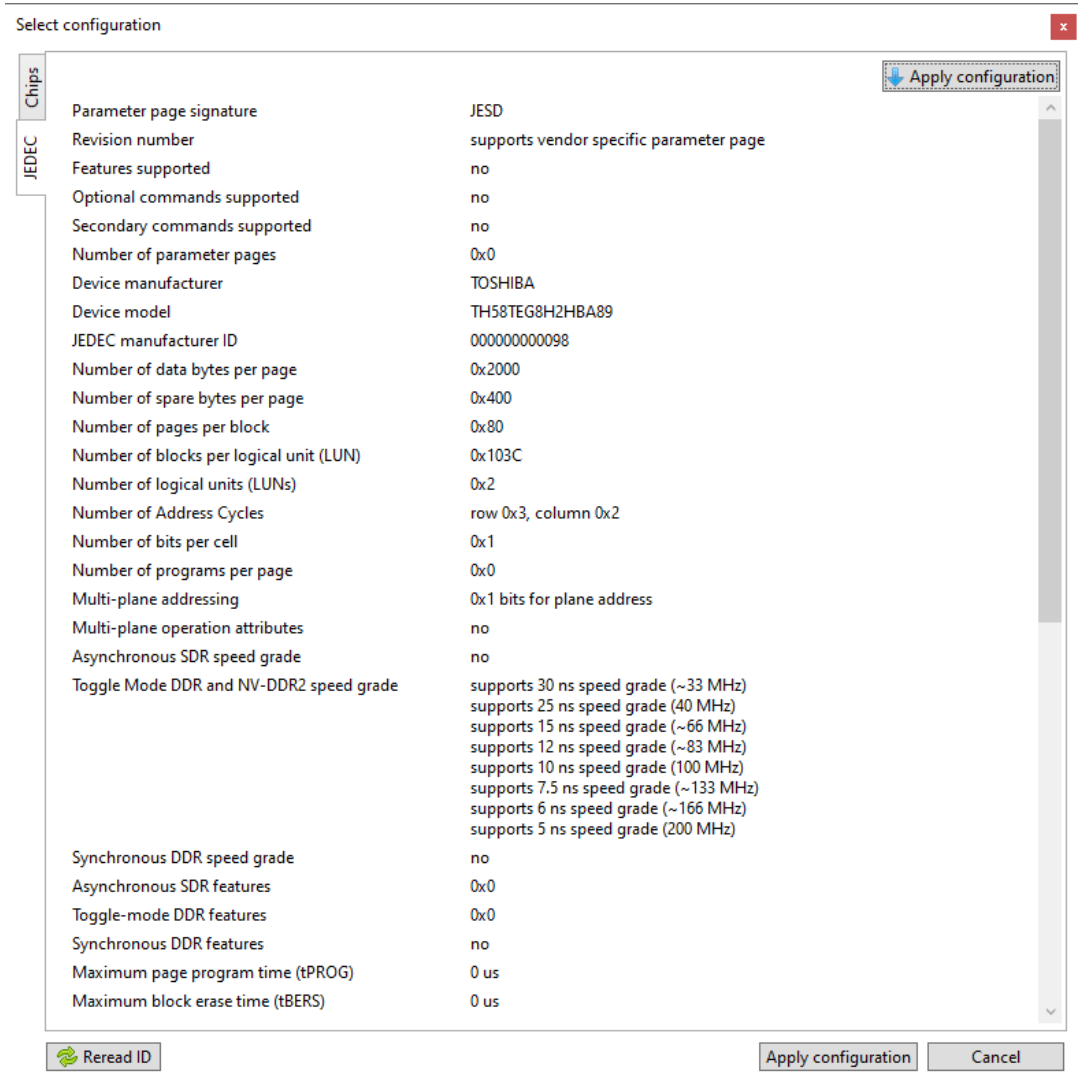


The first step before physical image reading is reading memory chip's ID.

The chip model identifier is 98DEA1327A which belongs to Toshiba/Kioxia manufacturer

The memory chip has multi-die structure and we were able to identify 4 dies/crystals in single package.

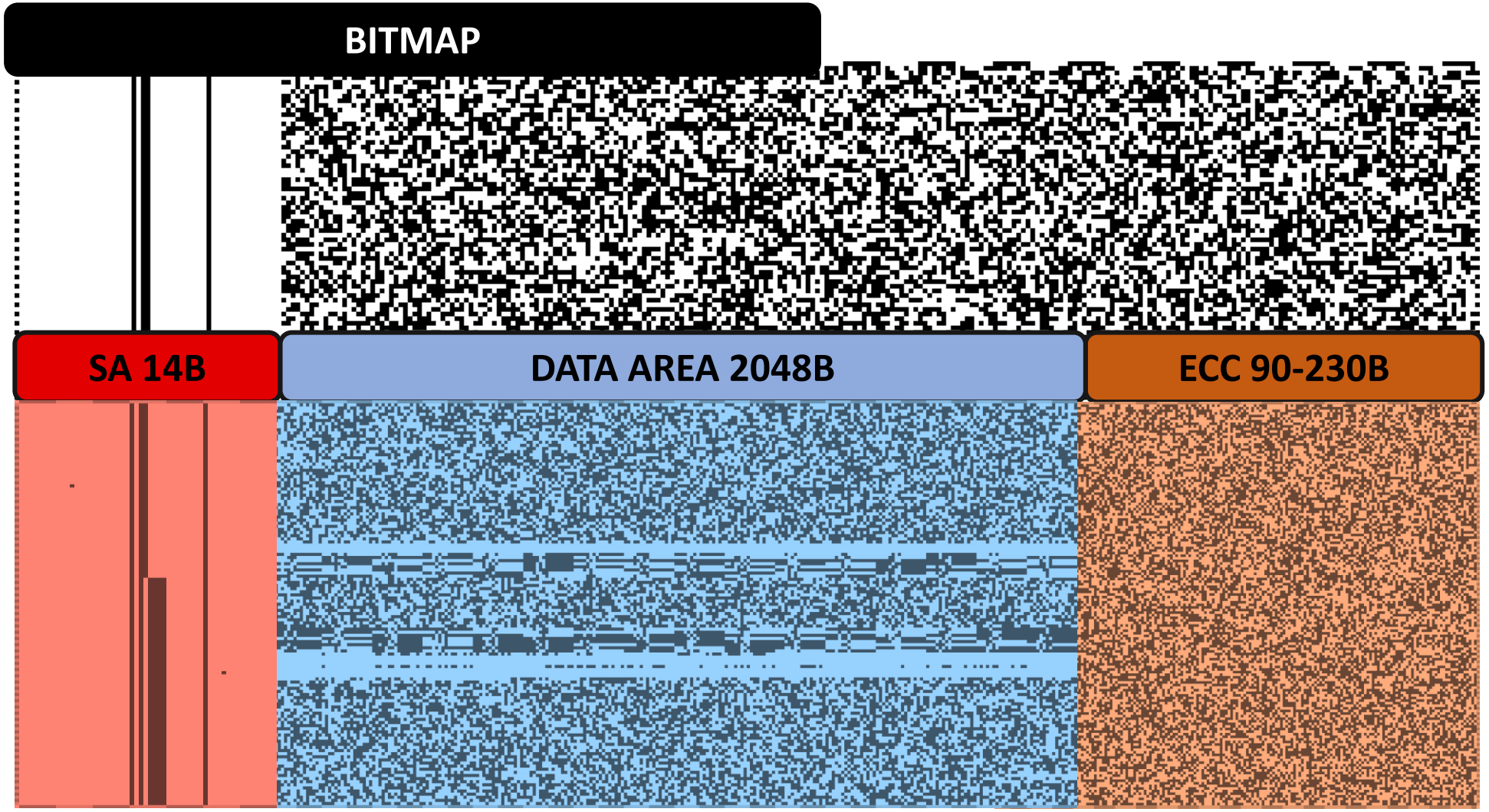
JEDEC data



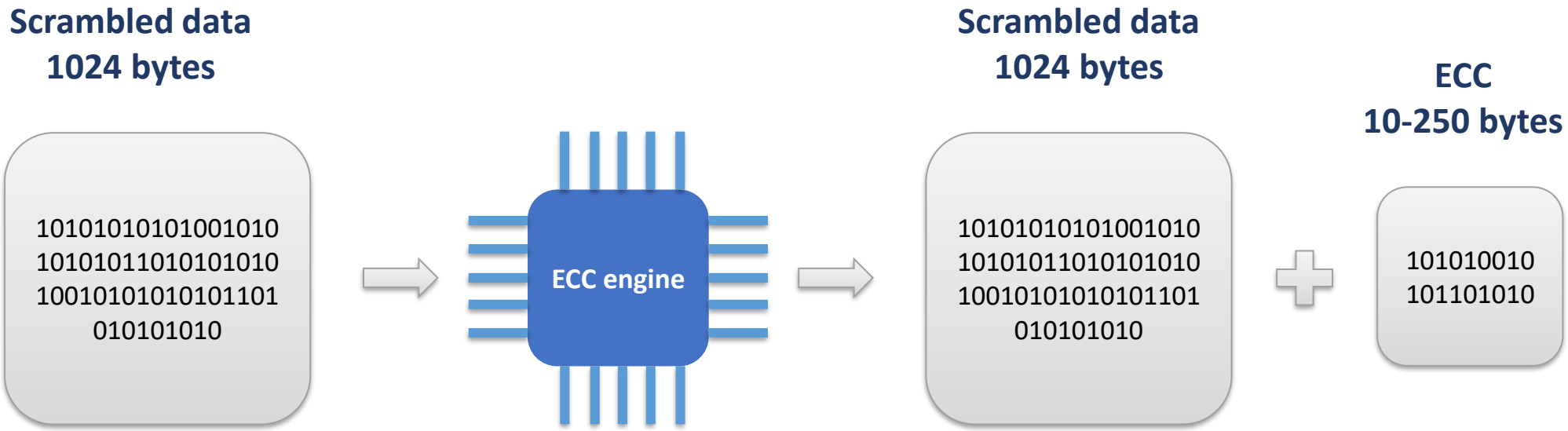
This NAND chip has special JEDEC parameter page that shows basic information about the memory.

As we can see from report:
Number of bits per cell = 1,
which means that memory chip has **SLC architecture, and it is the best choice for the applications where reliability is a KEY factor.**

Page layout



Error Correction Code(ECC)

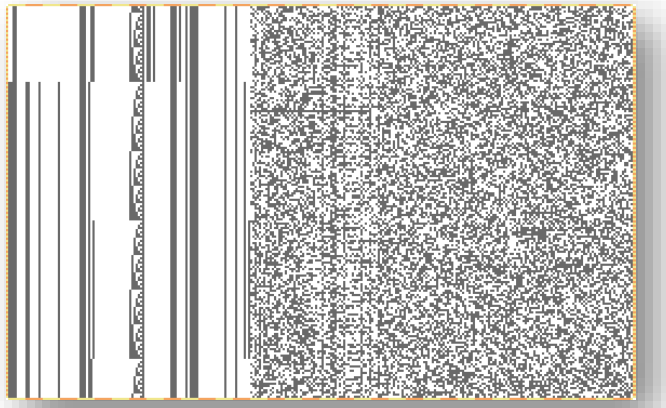


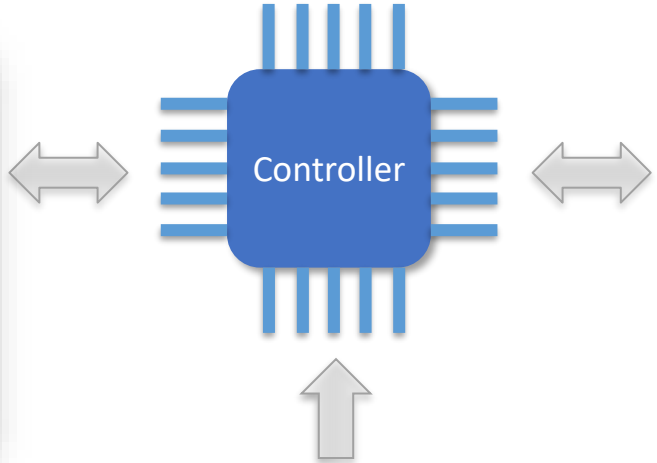
ECC algorithms

- Hamming code (OLD)
- Reed-Solomon code (OLD)
- BCH
- LDPC

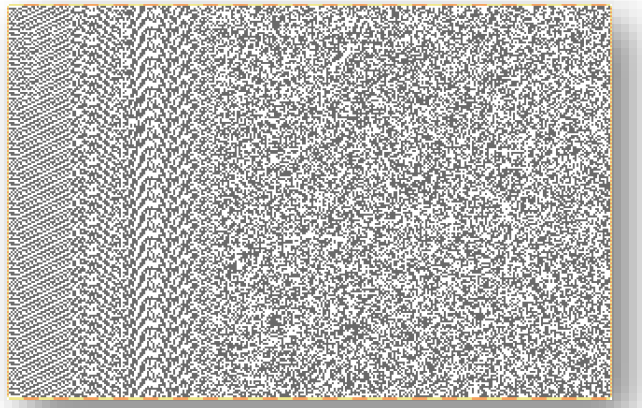
Scrambler XOR key

DATA

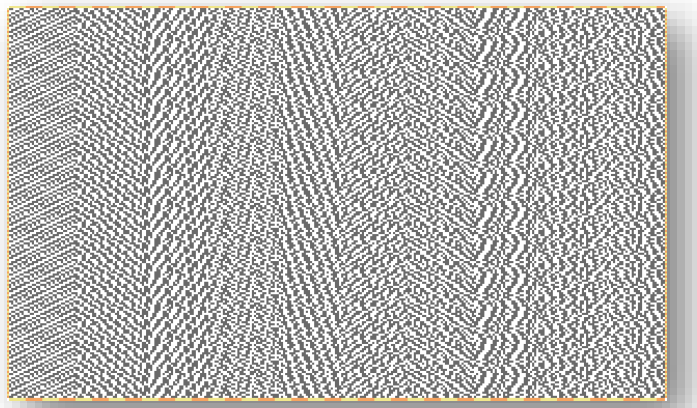




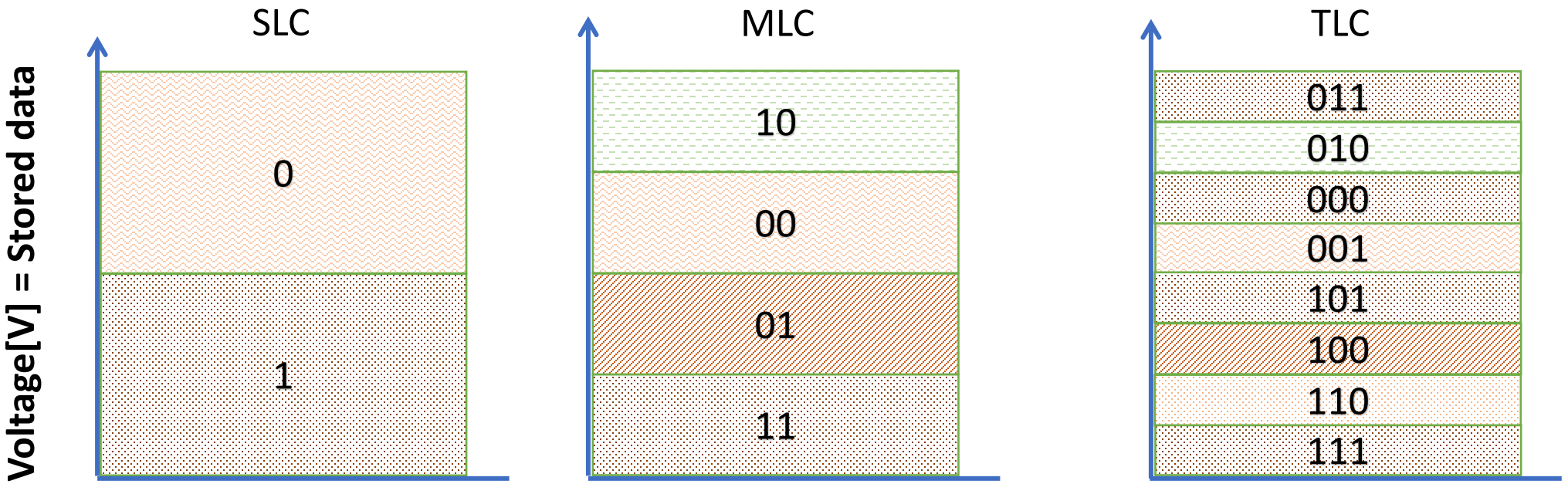
SCRAMBLED DATA



XOR key



NAND memory cell architectures



1 Bit Per Cell
2 Levels
100,000 P/E Cycles

2 Bits Per Cell
4 Levels
10,000 P/E Cycles

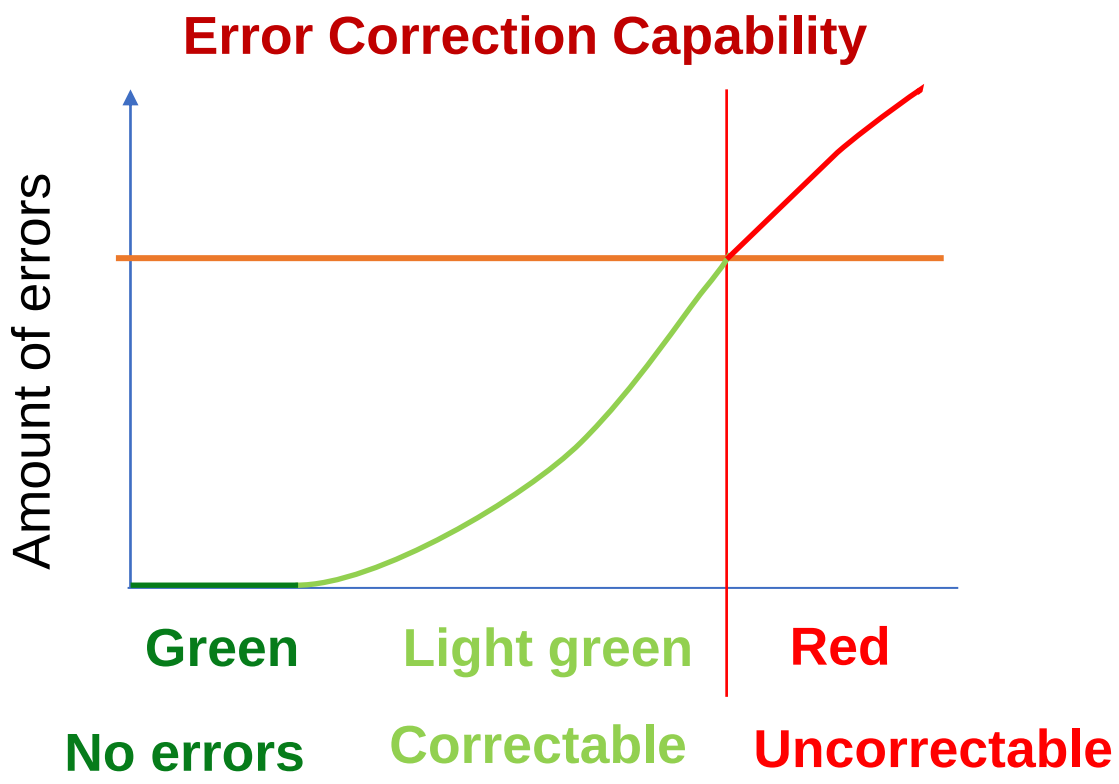
3 Bits Per Cell
8 Levels
1,000 P/E Cycles

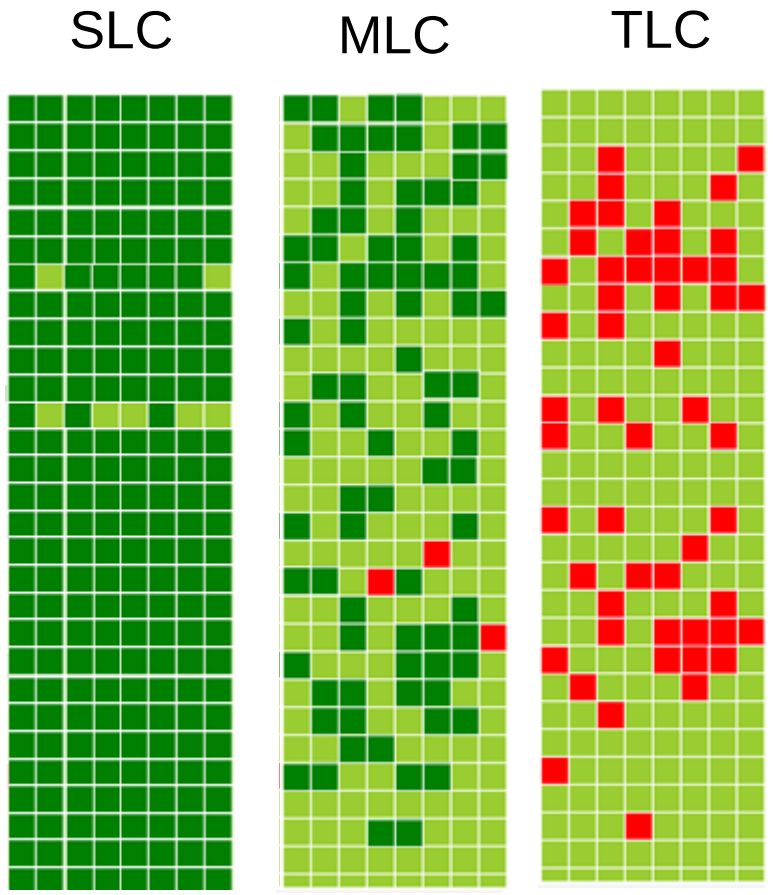
LARGER CAPACITY

LOWER ENDURANCE

LARGER ECC AREA

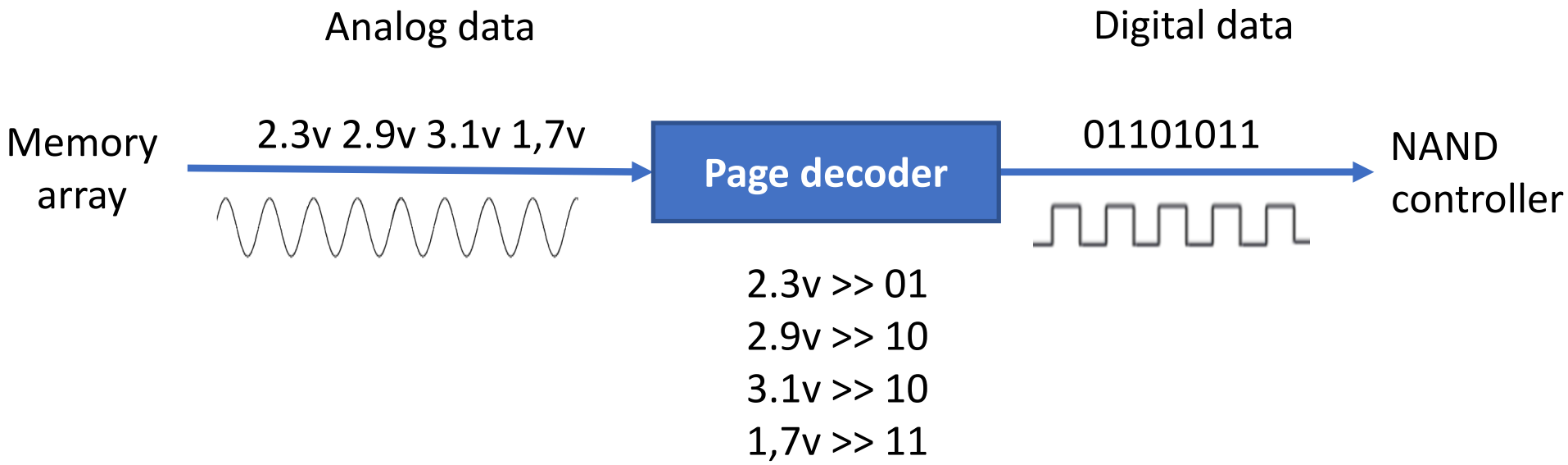
Bit errors in NAND





Page decoder

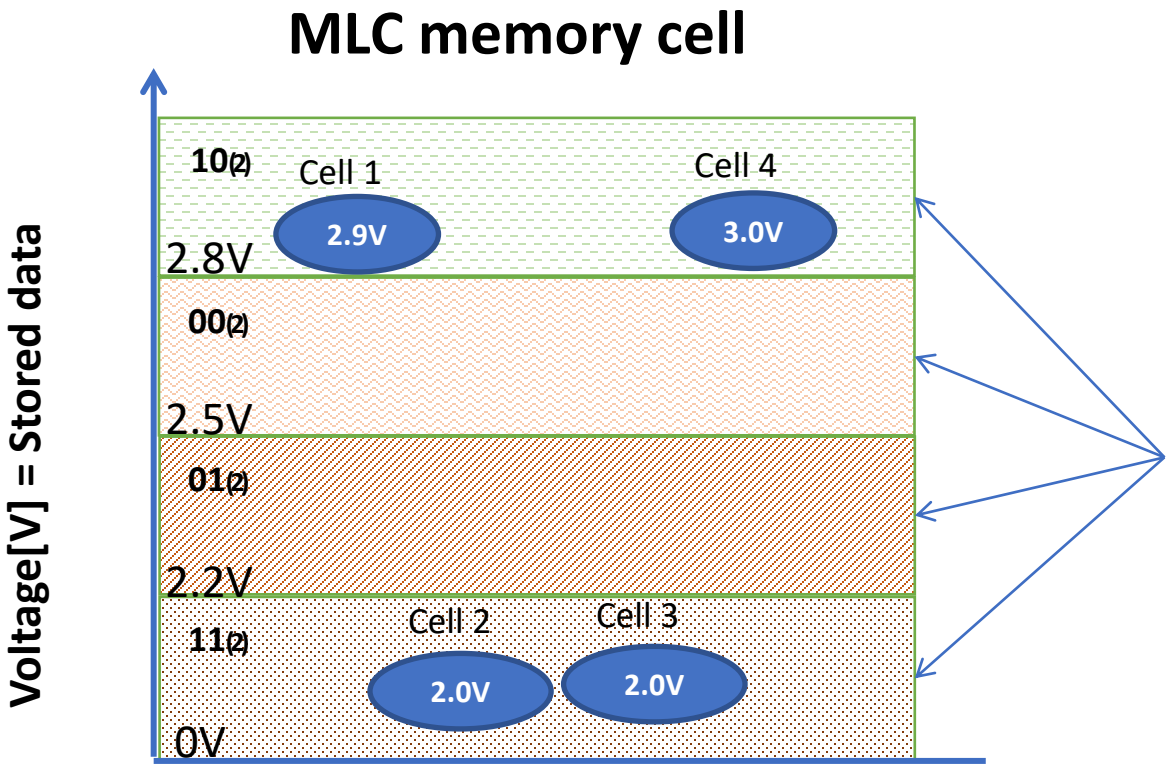
Analog states from cells are converted into digital data



Bits inside memory cell

The data in cell is stored as a voltage level

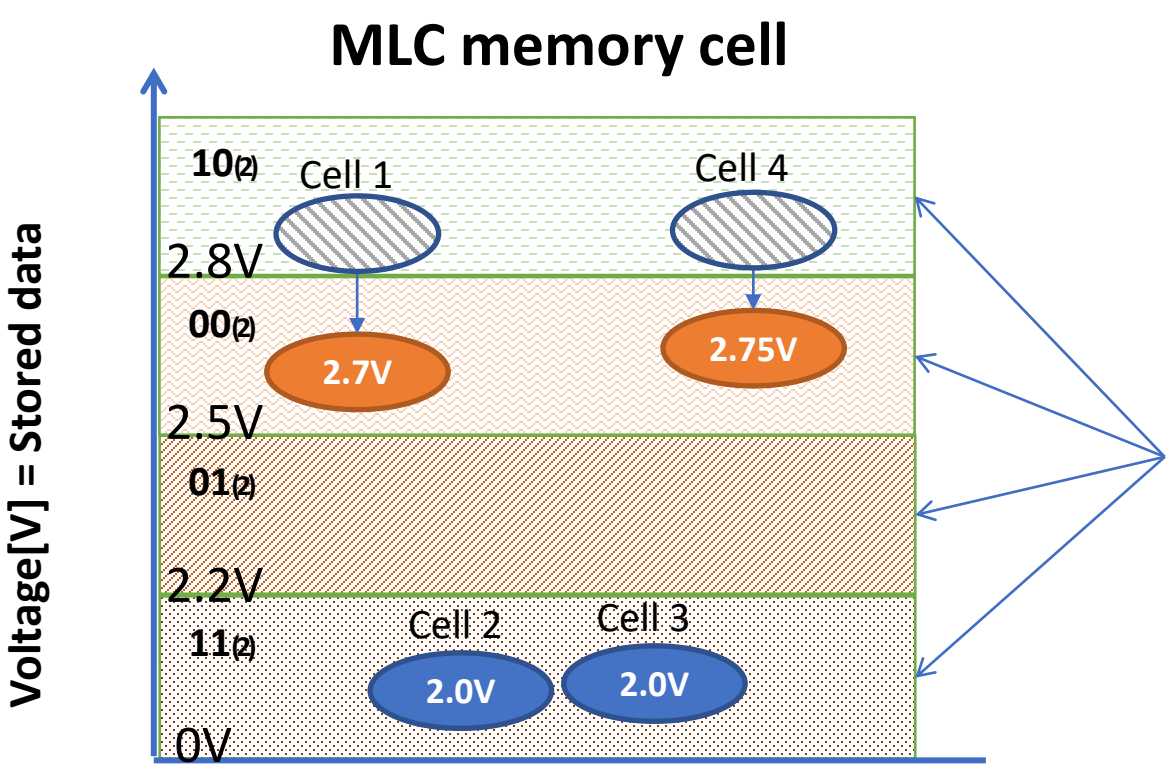
Controller is reading data according to specific zones



Cycle	1	2	3	4	HEX
Initial	10	11	11	10	BE

Retention Error

When charge leaks out from cell we get bit error

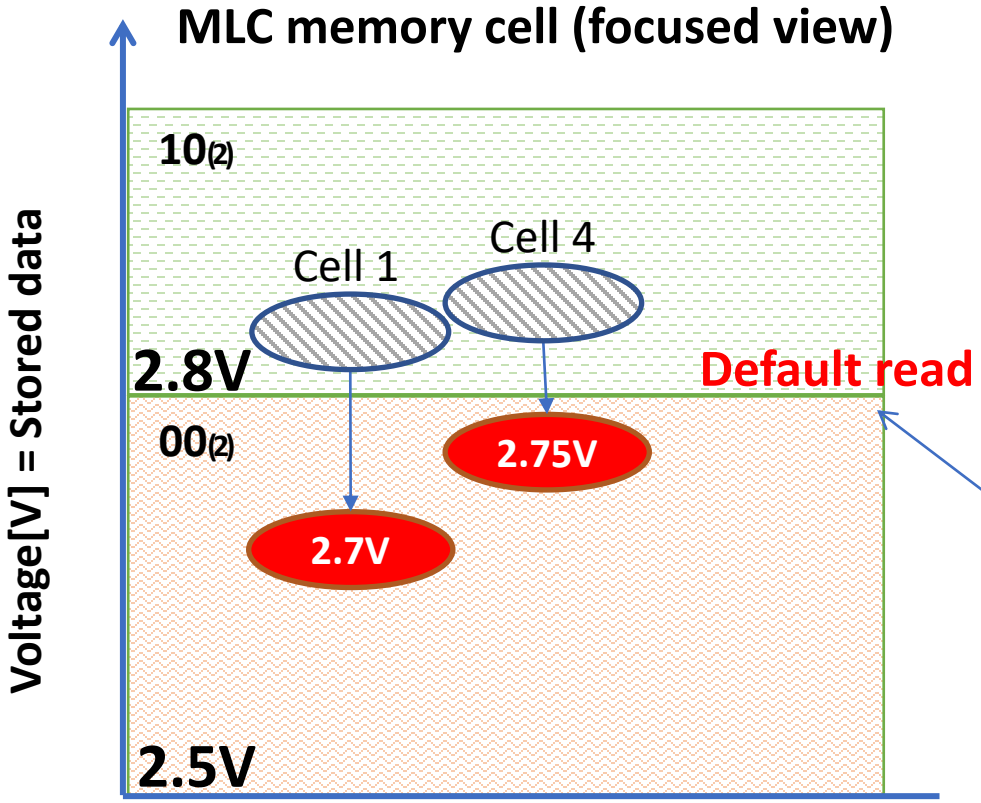


Cycle	1	2	3	4	HEX
Initial	10	11	11	10	BE
Default read	00	11	11	00	3C

Read-Retry Mechanism

When charge leaks out from cell we get bit error

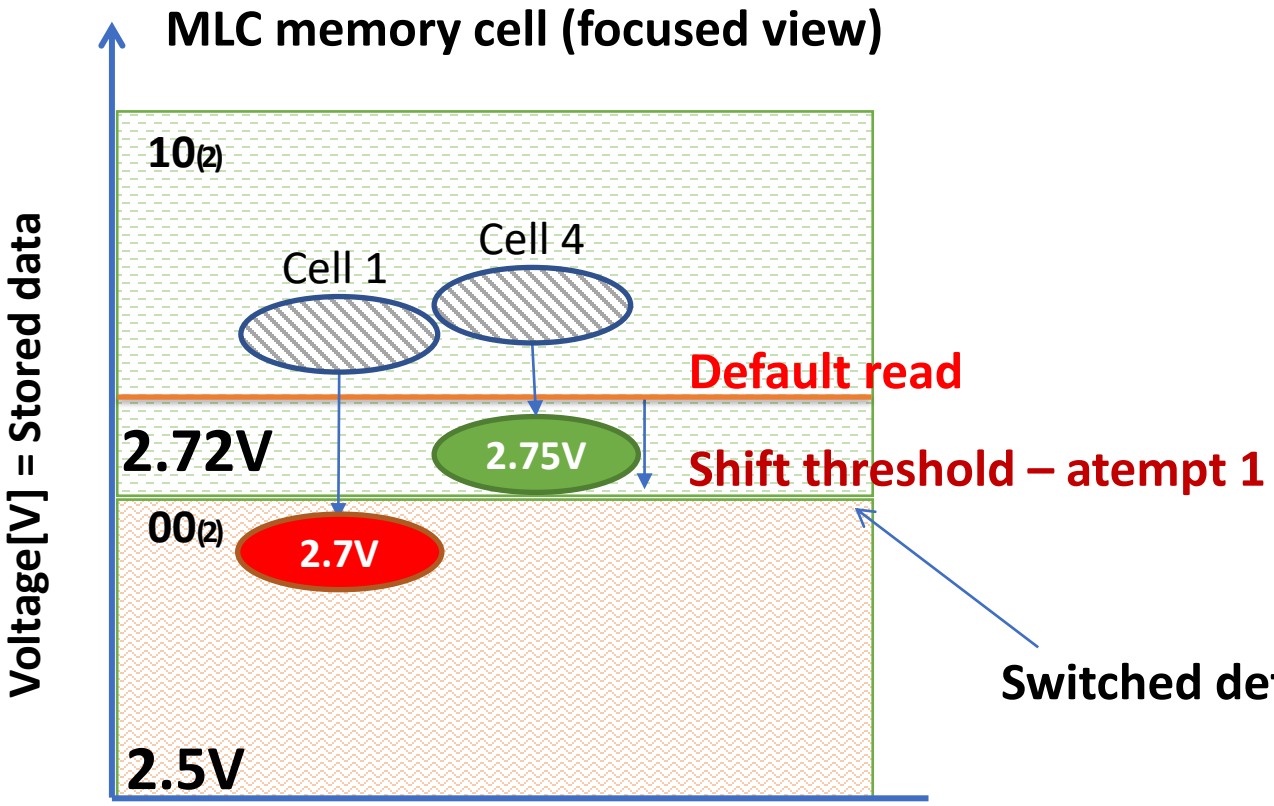
Degraded cell gives wrong data



Cycle	1	2	3	4	HEX
Initial	10	11	11	10	BE
Default read	00	11	11	00	3C

Read-Retry Mechanism #1

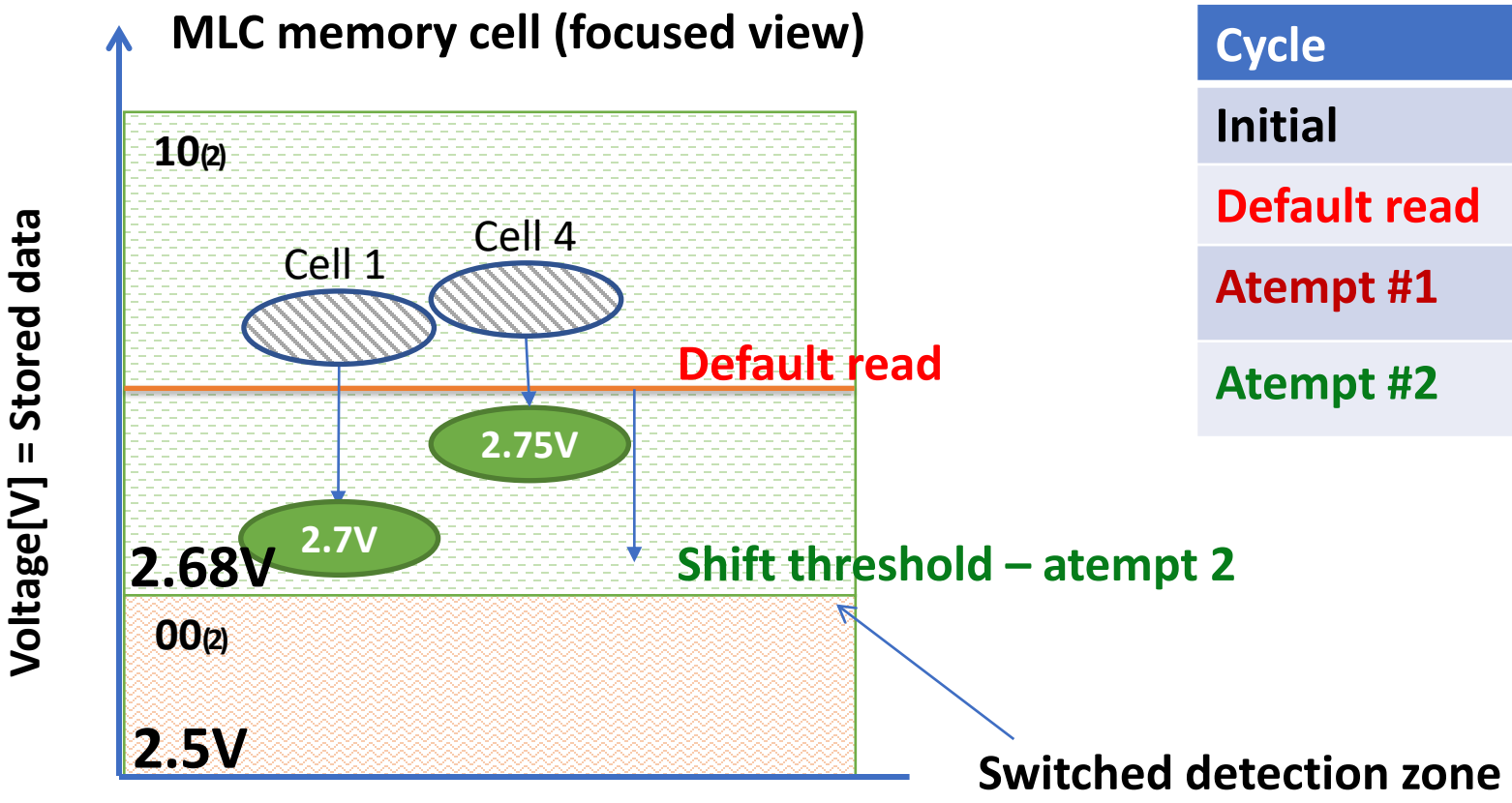
Read retry mechanism helps to shift read voltage thresholds



Cycle	1	2	3	4	HEX
Initial	10	11	11	10	BE
Default read	00	11	11	00	3C
Atempt #1	00	11	11	10	3E

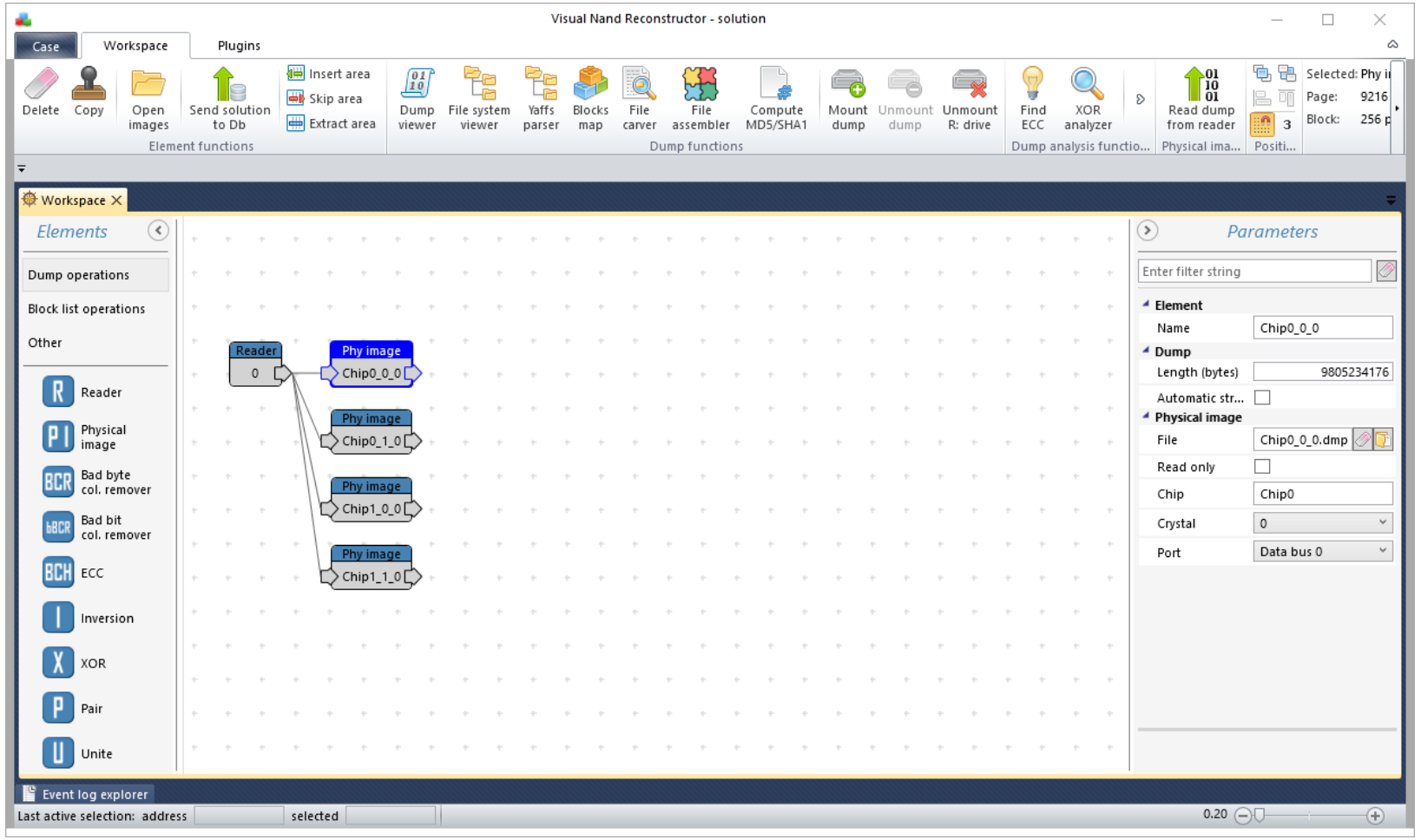
Read-Retry Mechanism #2

Read retry mechanism helps to shift read voltage thresholds



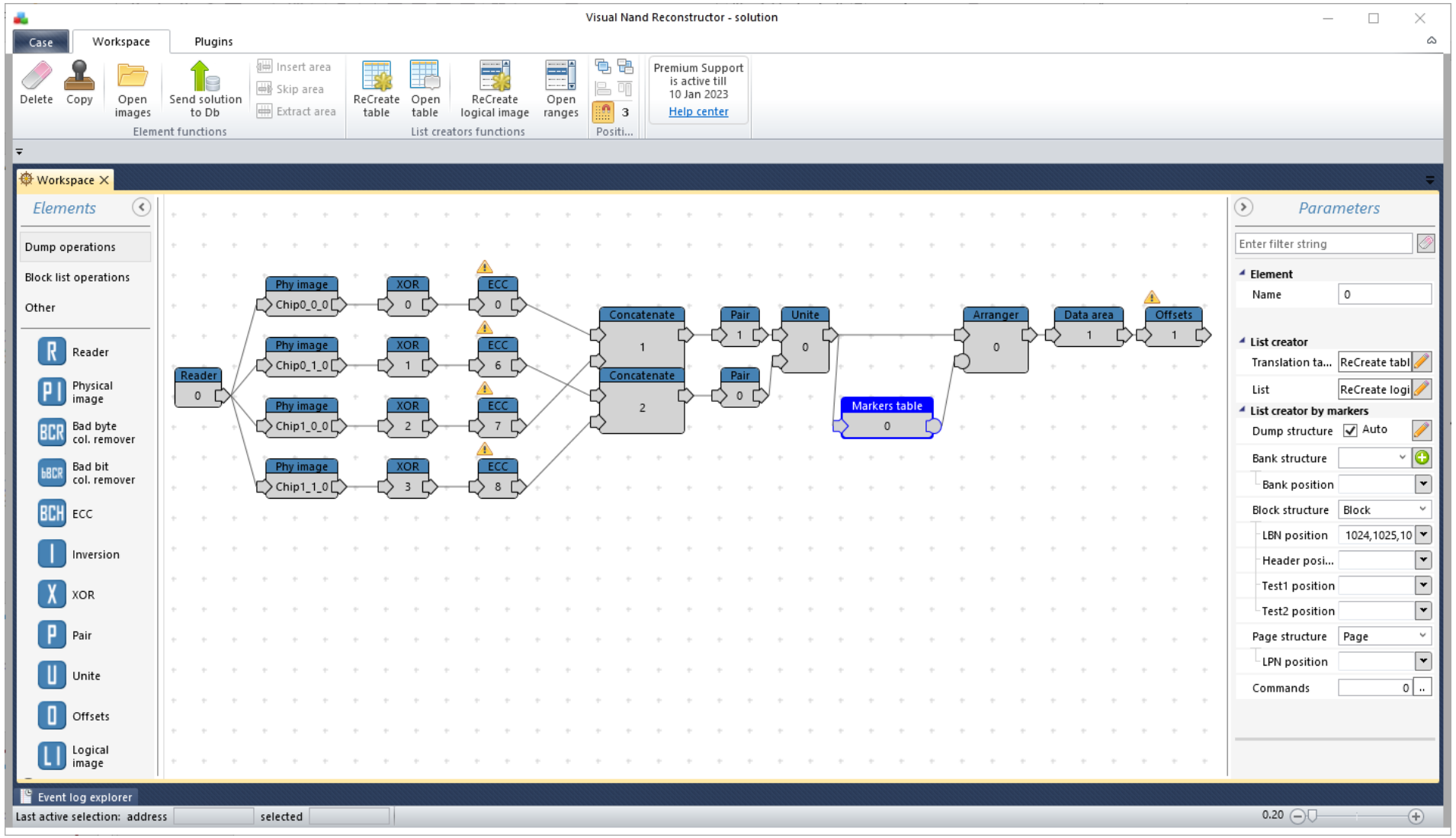
Cycle	1	2	3	4	HEX
Initial	10	11	11	10	BE
Default read	00	11	11	00	3C
Atempt #1	00	11	11	10	3E
Atempt #2	10	11	11	10	BE

Physical image extraction from NAND



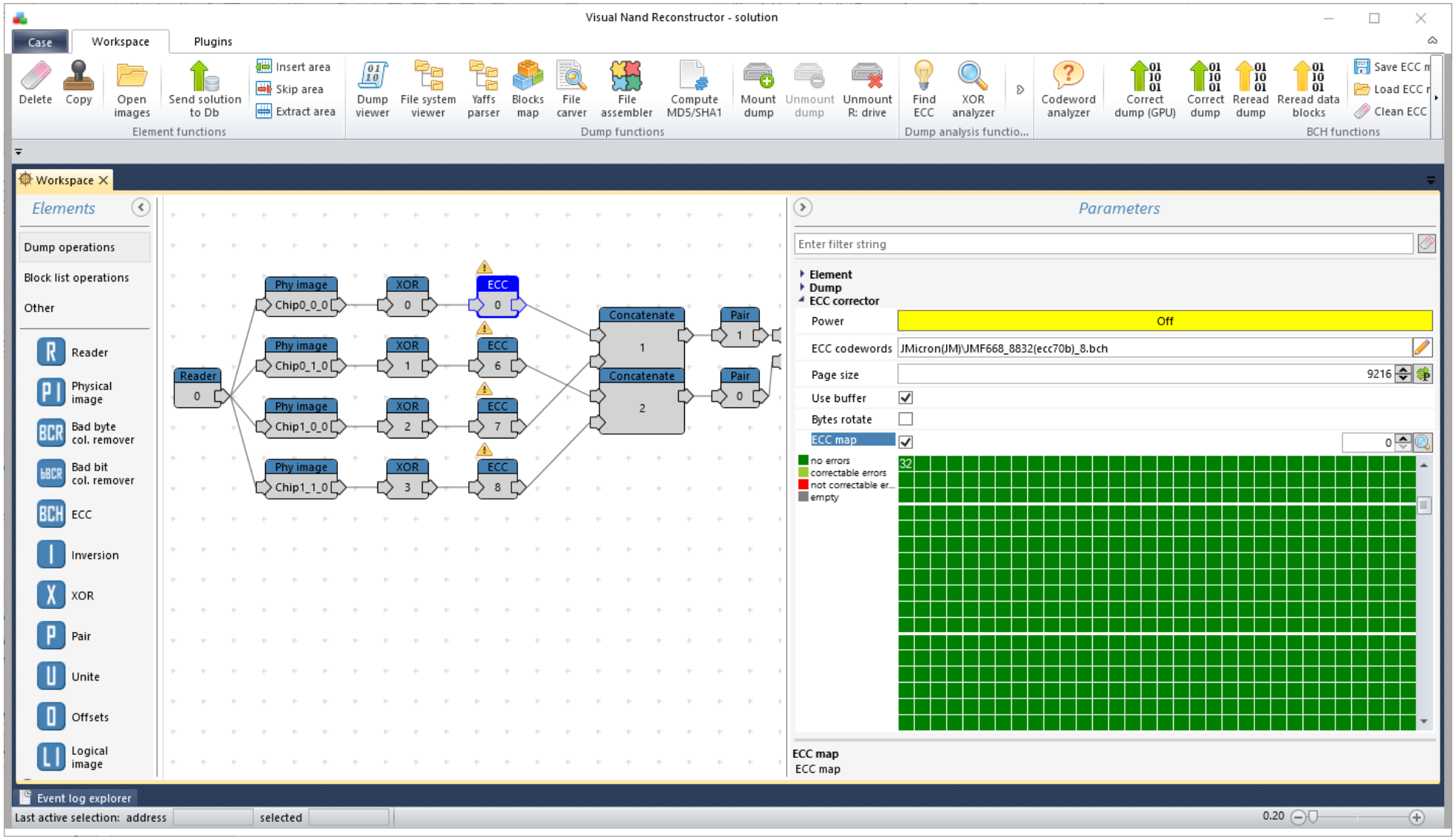
We used Visual NAND Reconstructor for memory chip reading and physical image processing.
In total 4 dumps/physical images were extracted out of the NAND.

Reconstruction of controller’s workflow

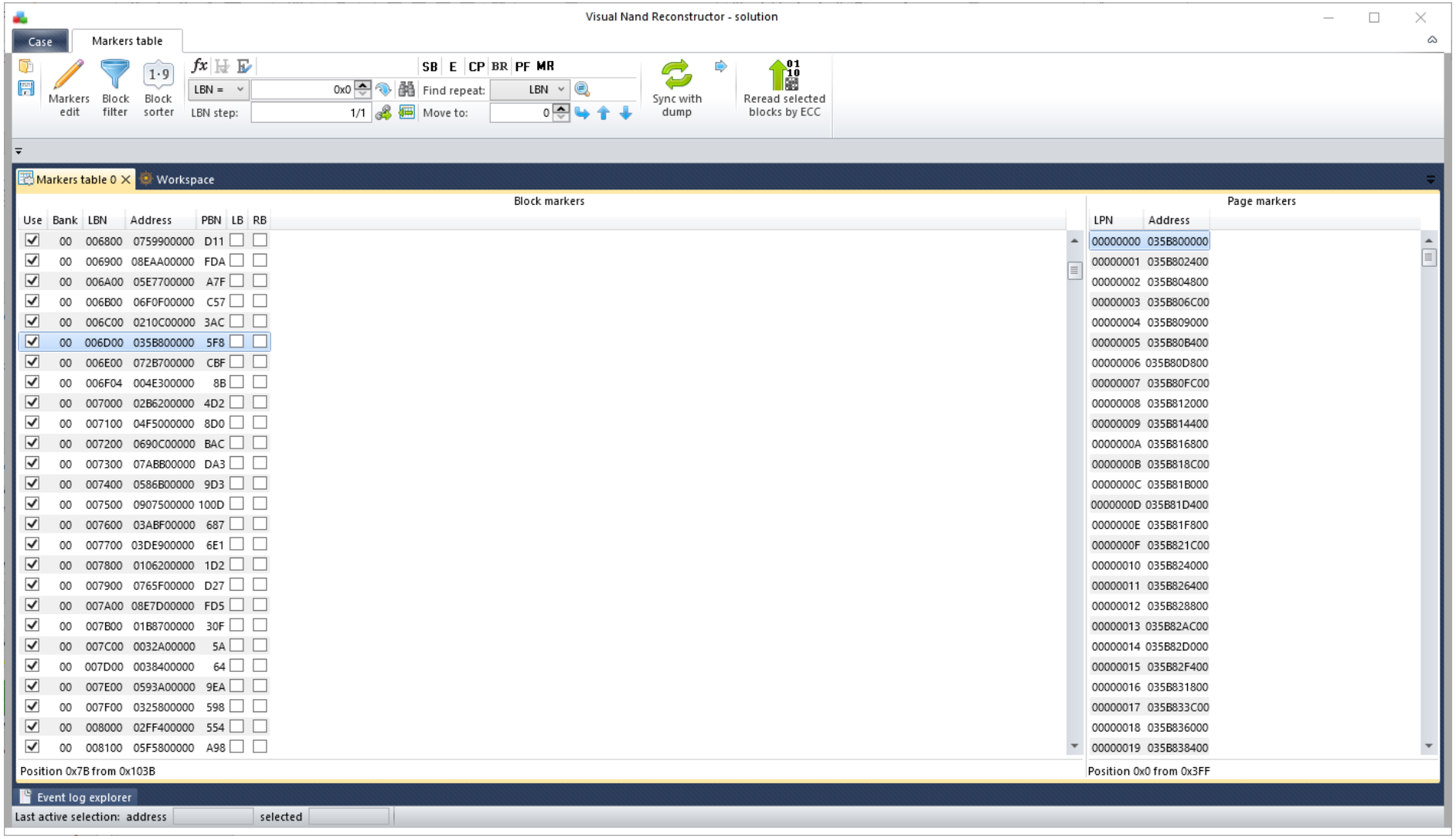


Physical image has been converted to logical image through controller’s emulation process

ECC algorithm for bit error correction has been found and errors got corrected

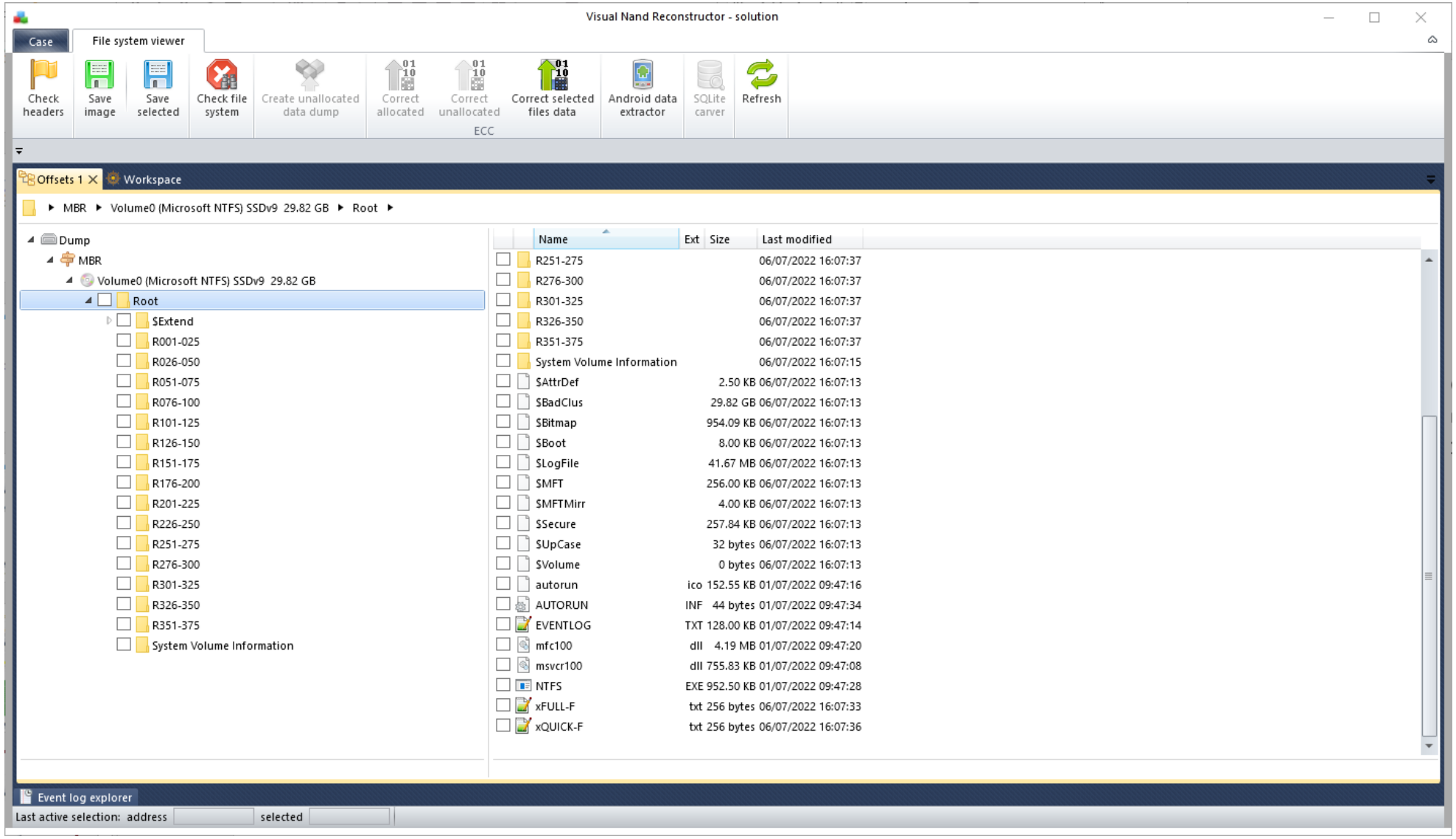


Block translation



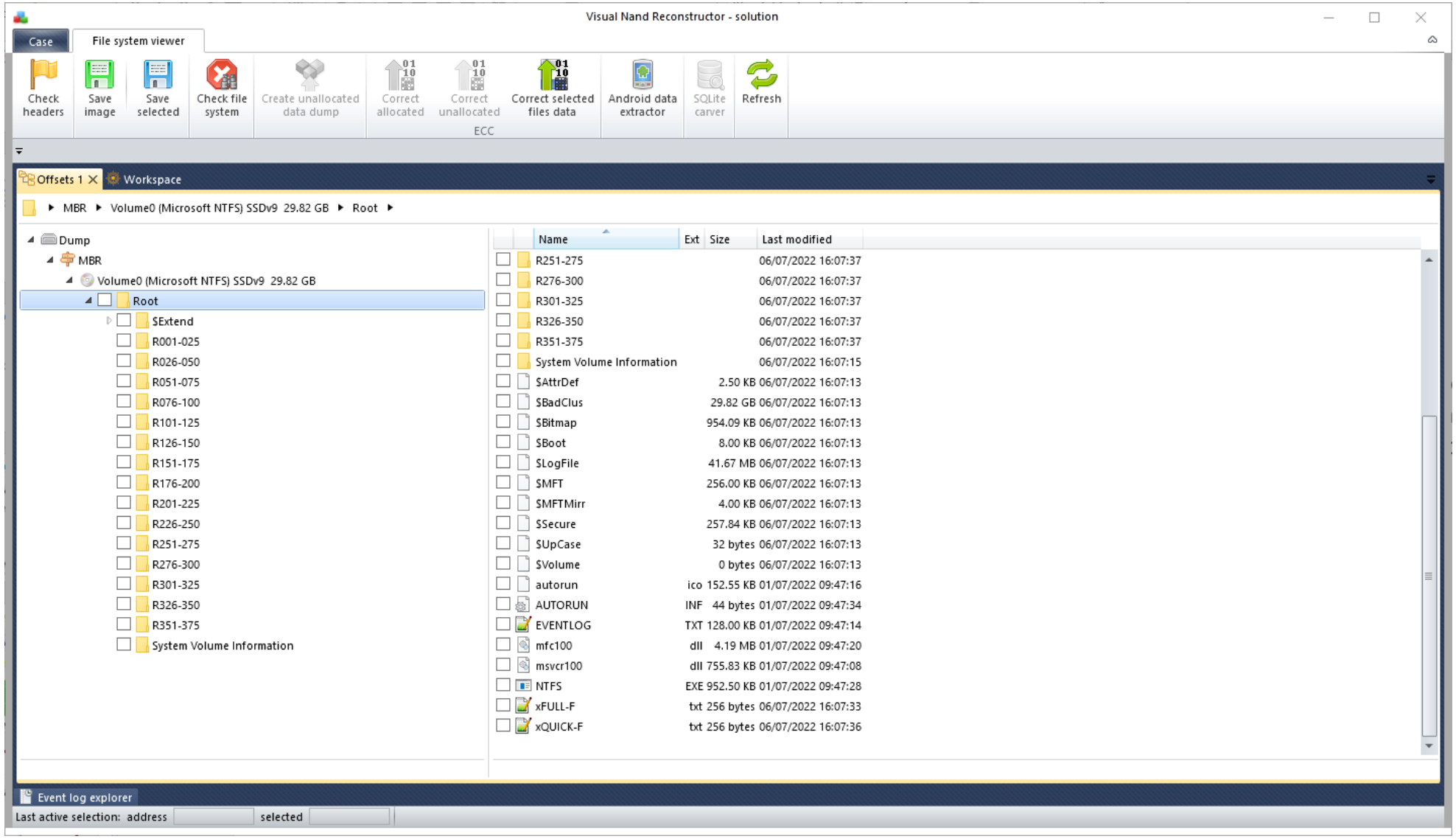
Blocks have been properly reorganized according to the logical block number (LBN)

File system reconstructed from NAND physical image



We have been able to successfully reconstruct file system for this SSD, and solution should generally work on all devices with same controller, NAND and capacity.

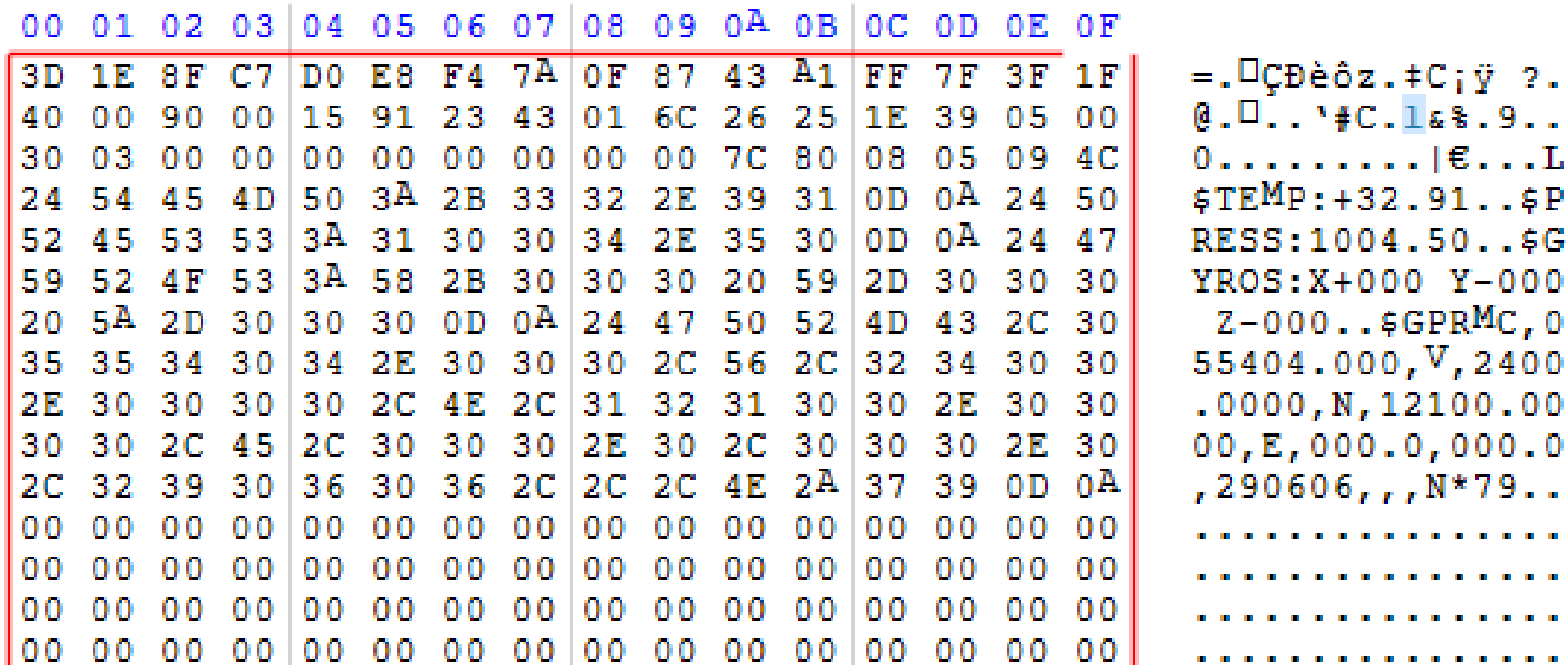
File system reconstructed from NAND physical image



We have been able to successfully reconstruct file system for this SSD, and solution should generally work on all devices with same controller, NAND and capacity.

Example of recovered file

Flight parameters. Temperature. Pressure and geographic location.



00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
3D	1E	8F	C7	D0	E8	F4	7A	0F	87	43	A1	FF	7F	3F	1F	=.□ÇÐèôz.‡C¡ÿ ?.
40	00	90	00	15	91	23	43	01	6C	26	25	1E	39	05	00	@.□..'#C.l&%.9..
30	03	00	00	00	00	00	00	00	00	7C	80	08	05	09	4C	0.........|€...L
24	54	45	4D	50	3A	2B	33	32	2E	39	31	0D	0A	24	50	$TEMP:+32.91..$P
52	45	53	53	3A	31	30	30	34	2E	35	30	0D	0A	24	47	RESS:1004.50..$G
59	52	4F	53	3A	58	2B	30	30	30	20	59	2D	30	30	30	YROS:X+000 Y-000
20	5A	2D	30	30	30	0D	0A	24	47	50	52	4D	43	2C	30	Z-000..$GPRMC,0
35	35	34	30	34	2E	30	30	30	2C	56	2C	32	34	30	30	55404.000,V,2400
2E	30	30	30	30	2C	4E	2C	31	32	31	30	30	2E	30	30	.0000,N,12100.00
30	30	2C	45	2C	30	30	30	2E	30	2C	30	30	30	2E	30	00,E,000.0,000.0
2C	32	39	30	36	30	36	2C	2C	2C	4E	2A	37	39	0D	0A	,290606,,,N*79..
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

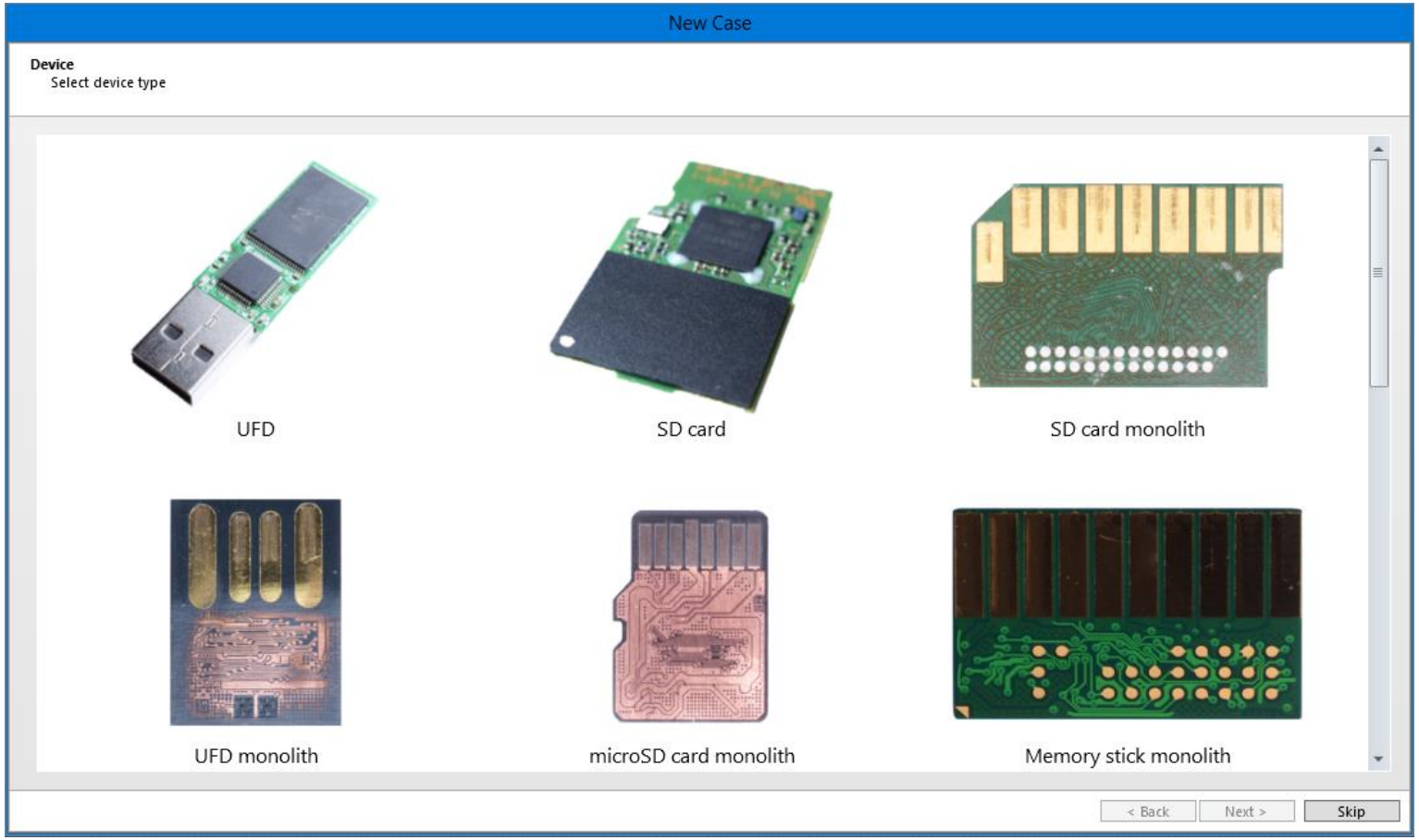
Conclusion:

The SLC memory chip used in this device is very reliable. Even in the critical scenario of thermal damage, there's still high chance of successful data recovery. As long as memory chip is not cracked physically, the flight recorder is failproof.

Controller's data translation algorithm was fully reverse engineered and logical image was reconstructed.

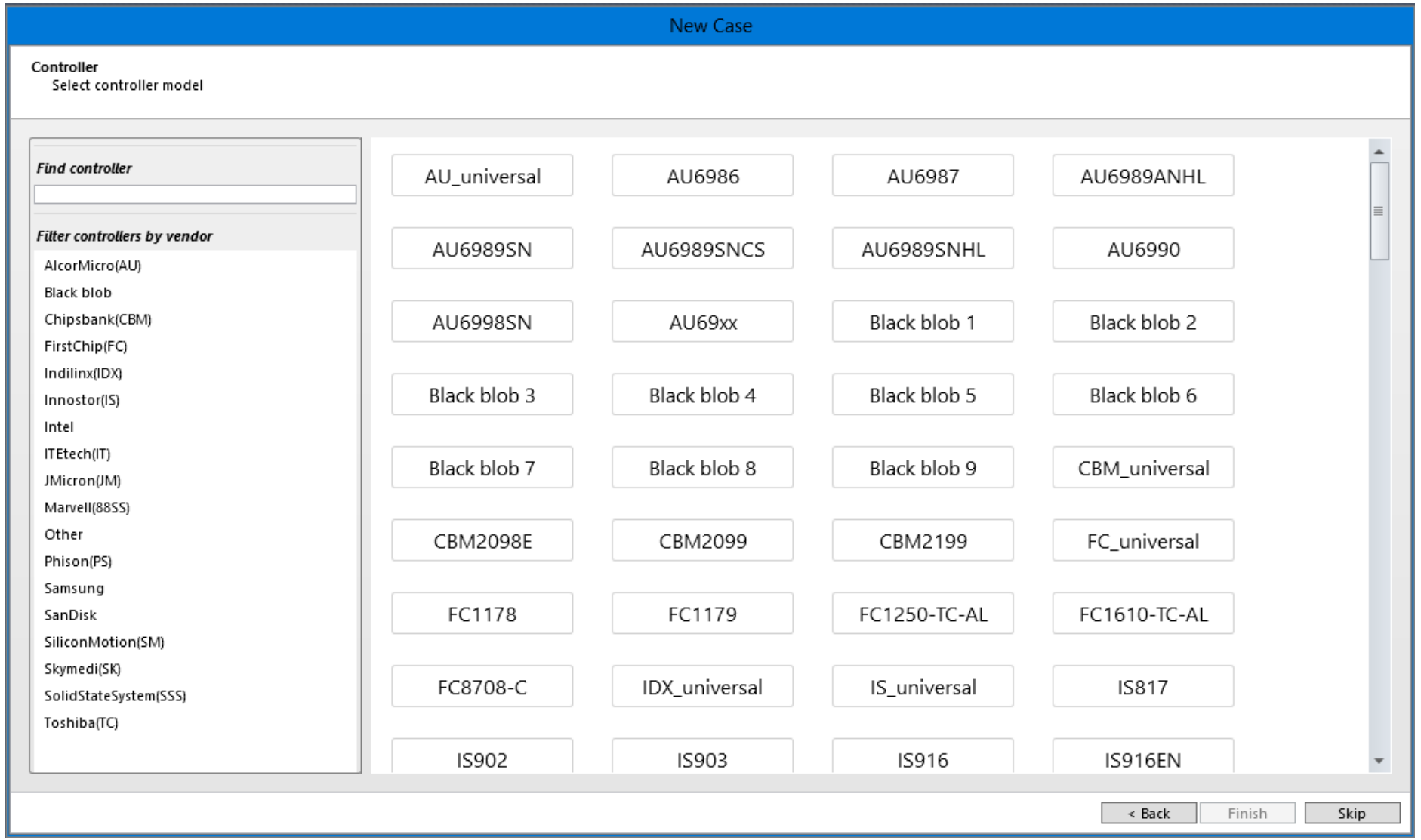
It can be fed to the vendor's software for the flight accident data extraction.

Database of Solutions

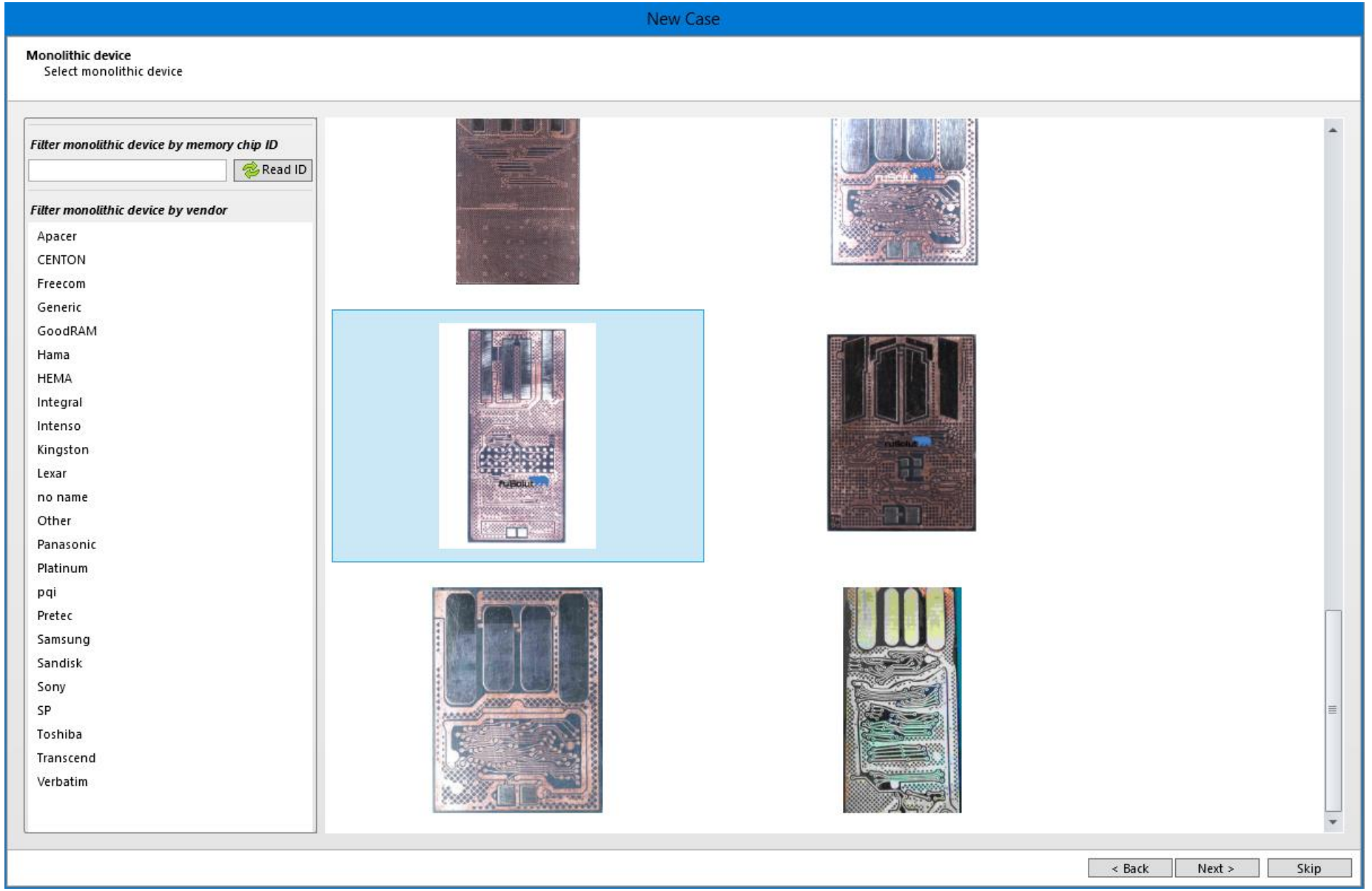


- Integrated into VNR
- Dynamically updated
- Local, with Cloud sync
- Automatically adjustable solutions

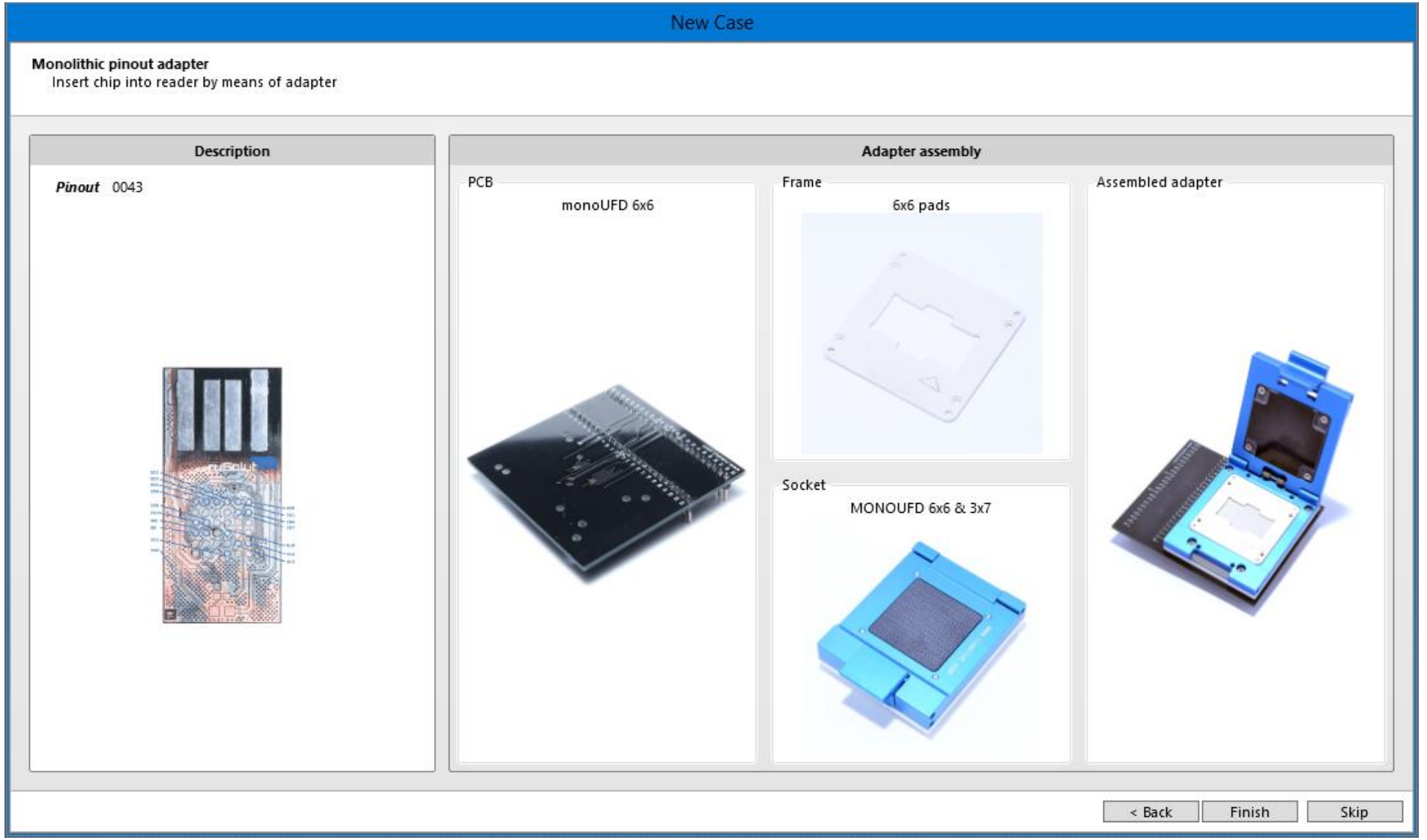
Database of Solutions



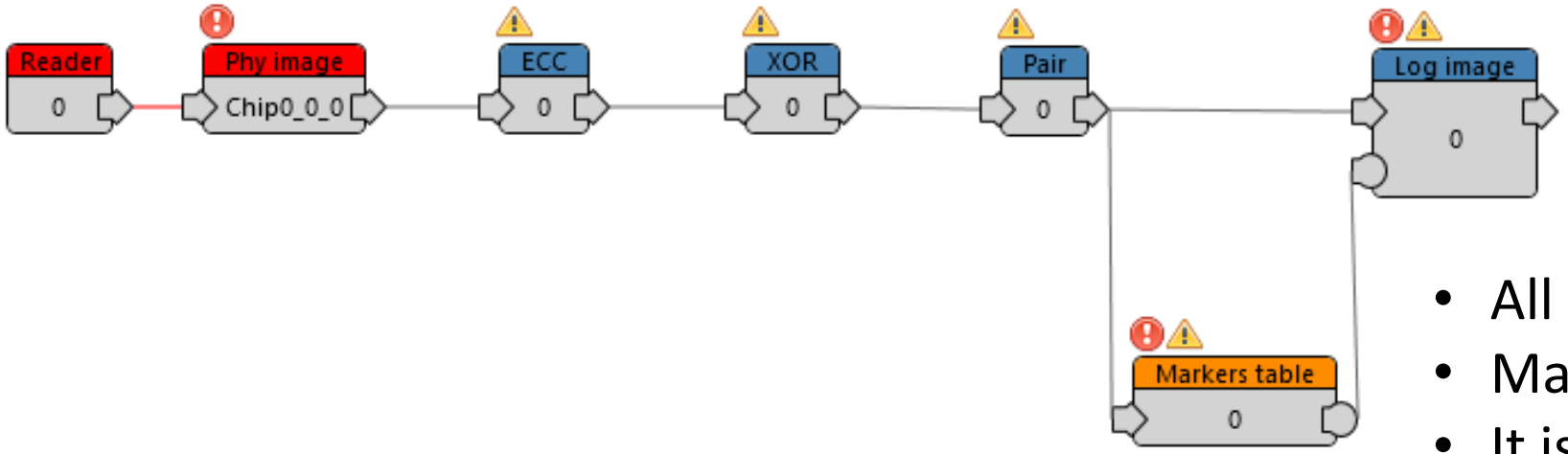
Database of Solutions

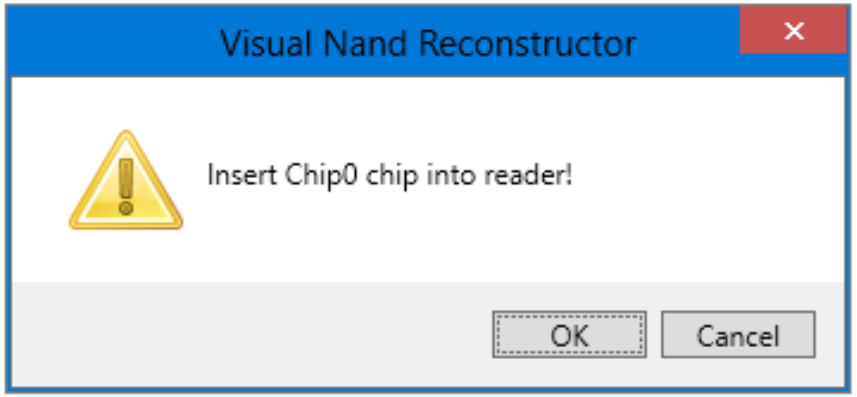


Database of Solutions



Database of Solutions – Full solution





- All parameters are defined
- Markers table is fully set up
- It is necessary just to read a chip and run the reread to fix bit errors

Thank you!