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

Michał Gmurek, Rusolut



October 10-12, 2023 | Prague, CZ



Data Recovery from Aircraft Black Box







etep



MECHANICAL

	Specification	Remark
Size	189.5 (231.8 iRIPS	DxWxH
	/219.5 iEE) x 126.2	±1mm
	x 101 mm	
Weight	≈ 3.30kg / 3.75kg	ED155/ ED112
	≈ 4.85kg	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	Configuration/Control
Ethernet	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: 260 C, 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.

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.



Sentinel Under High temperature fire test



Hydraulic press test





Crash test



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





Impact test



Sandbox













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.







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 lfremer 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 ...)





High pressure test

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**.





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

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

🧇 🛃 📙 🍤 🖛	Gérer	SSD ETEP v8 (E:)		-		×
Fichier Accueil Partage	Affichage Outils de le	cteur				^ ?
Épingler à Copier Coller Accès rapide Presse-papiers	Déplacer vers - X Suj Copier vers - Rer Organiser	nommer • Nouveau	Propriétés	 Sélectionn Aucun Inverser la Sélectior 	er tout sélection nner	
← → * ↑ ♥ > CePC	> SSD ETEP v8 (E:)		√ Ō	Rechercher dans	: SSD ETE	م
 Accès rapide Bureau Téléchargemu Téléchargemu Documents Images Images Img docLAB ang OneDrive Ce PC 	Vom xQUICK-F.txt xFULL-F.txt NTFS.EXE autorun.ico mfc100.dll msvcr100.dll EVENTLOG.TXT AUTORUN.INF	Modifié I 10/12/20 10/12/20 24/09/20 17/11/20 19/02/20 22/04/20 25/01/20	e Tyr 18 14:20 Do 18 14:20 Do 18 16:27 Ap 16 16:10 Icô 11 23:03 Ext 11 00:40 Ext 09 11:11 Do 08 11:28 Inf	cument texte cument texte plication ine ension de l'app ension de l'app cument texte ormations de c	Taille 1 882 153 4 295 756 128 1	Ко Ко Ко Ко Ко
🧼 SSD ETEP v8 (E:) 🗸					r	
8 élément(s)						

Real-world test...

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

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 highcapacity 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

Case Workspace Plugins Databases		Case File system	n viewer			
Delete Copy Paste Open images Send solution to Db Extract area	Author: Rusolut ID: emory chips: 1 ystals: 1 Help cent	port II 24 Er Barrow Check headers Barrow Save image set Barrow Save Barrow Save Barow S	Save elected system Create unallocated data dump	Correct allocated	Correct unallocated ECC	ted Android data extractor SQLite carver
Element functions Positi So	lution	GPT 🕨 Volume	5 (EXT-family) /data 2.08 GB ► Root ►			
₩ Workspace ×		⊿		•	Name Ext S	ize Last modified
Elements (⇔ MBR ≰ ⇔ GPT	(EVT familie) 16 00 MP		app app-asec	08/13/2014 19:28:46 01/28/1970 22:49:52
Reader Phy image ECC XOR Pair	Log image	Volume0	(Microsoft EAT16) NO NAME 64 00 MB		app-private	09/04/2014 17:03:49
		Volume2	(EXT-family) /persist 4.00 MB		backup	06/08/2014 19:12:01
Block list operations		▶ 💿 Volume3	(EXT-family) /system 1.17 GB		bms	01/28/1970 22:49:54
	Markers table	▷ 💿 Volume4	(EXT-family) 250.00 MB		controlcenter	01/28/1970 22:53:51
Other		⊿ 💿 Volume5	(EXT-family) /data 2.08 GB		dalvik-cache	06/08/2014 19:12:01
		🔺 🗌 🔒 Ro	oot		data	10/10/2014 18:23:07
			app		dontpanic	01/28/1970 22:49:52
Reader Physical			app-asec	🗆 🌮 📙	drm	01/28/1970 22:53:13
image			app-private		efslog	01/28/1970 22:49:52
Bad bute Bad bit			audio		etc	01/28/1970 22:49:53
BCR col, remover col, remover			backup	🗆 🌮 <mark> </mark> 1	fota	01/28/1970 22:49:52
			bms		hdcp	01/28/1970 22:52:56
			controlcenter		last_alog	06/08/2014 18:28:03
			dalvik-cache		last_kmsg	06/08/2014 18:28:02
			data		local	01/28/1970 22:49:53
Y XOR D Pair			dontpanic		lost+found	01/28/1970 22:49:50
			drm		media	08/10/2014 14:42:26
			efslog		mediaserver	01/28/1970 22:49:57
Unite Offsets			etc		misc	04/27/1970 21:03:44
0 0			fota		property	10/03/2014 17:01:13
			hdcp		resource-cache	06/08/2014 18:28:15
L jimage			last_alog		shared	01/28/1970 22:49:52
			last_kmsg		smime	01/28/1970 22:49:52
			local		ssh	01/28/1970 22:49:52
			lost+tound		startupservice	01/28/1970 22:53:10
			media		suntory	01/28/1970 22:49:54

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

-									
CEO DE	Data b	ous 0	Deede	Data bus 1	0000				
	96DEA1327AD0	0808 WP	Ready		0000				
	98DEA1327AD6	0808 WP	Ready		0000				
CE2 [] (000000000000000000000000000000000000000	000		000000000000000000000000000000000000000	0000				
CE3 [] (000000000000000000000000000000000000000	000		000000000000000000000000000000000000000	0000				
Config	uration								
🖻 🗐 🎙					🤣	Model filter		98DEA1327A	
Model	TH58TEG8H2H	HBA89			Model	Identifier	Source		
Vendor	TOSHIBA								
Identifier	98DEA1327A								
Speed		High		~					
Power (Vc	c)	3,3 V		~					
I/O Power	(VccQ)	3,3 V		~					
Bus		8 bit		~					
Pinout		ONFI		~					
Signals		VSP3	VSP2	VSP1 🖌 WP					
Page size	Nom	inal		Real 9216 🗲 bytes					
Block size	1	1179648	\$	1179648 🗢					
Plane size	9663	3676416 🗄	\$	4902617088 🗢					
Planes		2		Ý					
Protocol	Async DDR			¥					
	Sandisk/To	oshiba VSC							
Power up	actions:		9) 🗘 🥖 🔶					

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

		👆 Apply configuration
Parameter page signature	JESD	
Revision number	supports vendor specific parameter page	
Features supported	no	
Optional commands supported	no	
Secondary commands supported	no	
Number of parameter pages	0x0	
Device manufacturer	TOSHIBA	
Device model	TH58TEG8H2HBA89	
JEDEC manufacturer ID	0000000098	
Number of data bytes per page	0x2000	
Number of spare bytes per page	0x400	
Number of pages per block	0x80	
Number of blocks per logical unit (LUN)	0x103C	
Number of logical units (LUNs)	0x2	
Number of Address Cycles	row 0x3, column 0x2	
Number of bits per cell	0x1	
Number of programs per page	0x0	
Multi-plane addressing	0x1 bits for plane address	
Multi-plane operation attributes	no	
Asynchronous SDR speed grade	no	
Toggle Mode DDR and NV-DDR2 speed grade	supports 30 ns speed grade (~33 MHz) supports 25 ns speed grade (40 MHz) supports 15 ns speed grade (~66 MHz) supports 12 ns speed grade (~83 MHz) supports 10 ns speed grade (~133 MHz) supports 7.5 ns speed grade (~133 MHz) supports 6 ns speed grade (~166 MHz) supports 5 ns speed grade (200 MHz)	
Synchronous DDR speed grade	no	
Asynchronous SDR features	0×0	
Toggle-mode DDR features	0×0	
Synchronous DDR features	no	
Maximum page program time (tPROG)	0 us	
Maximum block erase time (tBERS)	0 us	

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.

参 Reread ID

Apply configuration Cancel

Page layout

Error Correction Code(ECC)

Scrambler XOR key

NAND memory cell architectures

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

Retention Error

When charge leaks out from cell we get bit error

Read-Retry Mechanism

When charge leaks out from cell we get bit error

Degraded cell gives wrong data

Read-Retry Mechanism #1

Read retry mechanism helps to shift read voltage thresholds

Read-Retry Mechanism #2

Read retry mechanism helps to shift read voltage thresholds

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

Least Visual Nand Reconstructor - solution		- 🗆	\times
Case Markers table			~
5 / 1 /			
EN = V 0x0 🗢 🆓 🏥 Find repeat. LBN V 🔍			
Markers Block Block edit filter sorter LBN step: 1/1 🚜 🕮 Move to: 0 🕞 🖕 👚 dump blocks by ECC			_
₹			
🕮 Markers table 0 🗙 🚳 Workspace			=
Block markers		Page markers	
Use Bank LBN Address PBN LB RB	LPN Address		- 1
✓ 00 006800 0759900000 D11 □ □	00000000 035B800000		<u>^</u>
▼ 00 006900 08EAA00000 FDA □	00000001 035B802400		
✓ 00 006A00 05E7700000 A7F □	00000002 035B804800		
	00000003 035B806C00		
0 006C00 0210C00000 3AC	00000004 035B809000		
0 006D00 035B800000 5F8	00000005 035B80B400		
□ 0 006E00 072B700000 CBF □	00000006 035B80D800		
	00000007 035B80FC00		
	00000008 0358812000		
	0000009 0358014400		
	0000000R 035B818C00		
	0000000C 035B81B000		
✓ 00 007500 0907500000 100D □ □	0000000D 035B81D400		
✓ 00 007600 03ABF00000 687 □	0000000E 035B81F800		
✓ 00 007700 03DE900000 6E1 □	0000000F 035B821C00		
✓ 00 007800 0106200000 1D2 □	00000010 035B824000		
✓ 00 007900 0765F00000 D27 □ □	00000011 035B826400		
✓ 00 007A00 08E7D00000 FD5 □	00000012 035B828800		
✓ 00 007B00 01B8700000 30F	00000013 035B82AC00		
	00000014 035B82D000		
	00000015 035B82F400		
	00000016 035B831800		
	00000017 035B833C00		
	00000018 035B836000		
✓ 00 008100 05F5800000 A98 □ □	00000019 035B838400		
Position 0x7B from 0x103B	Position 0x0 from 0x3FF		
Event log explorer			
Last active selection: address selected			

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

File system reconstructed from NAND physical image

4	Visual Nand Reconstructor - solution	- 🗆 🗙
Case File system viewer		G
Image Image	Image: Correct selected rated Image: Corret selected rated	
Coffsets 1 🗙 🝭 Workspace		=
► MBR ► Volume0 (Microsoft NTFS) SSDv9 29.82 GB ► Root ►		
	Name Ext Size Last modified	
	R251-275 06/07/2022 16:07:37	î
Volume0 (Microsoft NTFS) SSDV9 29.82 GB	K2/b-300 06/07/2022 16:07:37 D D D	
A C Root	RS01-325 06/07/2022 16:07/37	
	System volume information 00/07/2022 16:0715	
R051-075	SATTOPY Store CP - CP	
		-
	Stitmap 954.09 KB 06/07/2022 16:07/13	
K331-375 Sustan Valuma Information		
	Image: Number of the state of the	
	voluck F tyt 256 bytes 06/07/2022 16:07:35	
Event log explorer		
st active selection: address selected		

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

4	Visual Nand Reconstructor - solution	- 🗆 🗙
Case File system viewer		G
Image Image	Image: Correct selected rated Image: Corret selected rated	
Coffsets 1 🗙 🝭 Workspace		=
► MBR ► Volume0 (Microsoft NTFS) SSDv9 29.82 GB ► Root ►		
	Name Ext Size Last modified	
	R251-275 06/07/2022 16:07:37	î
Volume0 (Microsoft NTFS) SSDV9 29.82 GB	K2/b-300 06/07/2022 16:07:37 D D D	
A C Root	K301-325 06/07/2022 16:07/37	
	System volume information 00/07/2022 16:0715	
R051-075	SATTOPY Solution S	
		-
	Stitmap 954.09 KB 06/07/2022 16:07/13	
		=
K331-375 Sustan Valuma Information		
	Image: Number of the state of the	
	voluck F tyt 256 bytes 06/07/2022 16:07:35	
Event log explorer		
st active selection: address selected		

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	80	09	0A	0B	0C	0 D	0E	0 F	
3D	1E	8 F	C7	DO	E8	F4	7A	0F	87	43	Α1	FF	7 F	3F	1F	=.□ÇĐèôz.‡C;ÿ ?.
40	00	90	00	15	91	23	43	01	6C	26	25	1E	39	05	00	@.□.`#C. <mark>1</mark> &%.9
30	0.3	00	00	00	00	00	00	00	00	7C	80	08	05	09	4C	0 €L
24	54	45	4D	50	зA	2B	33	32	2E	39	31	0D	0A	24	50	\$TEMP:+32.91\$P
52	45	53	53	зA	31	30	30	34	2E	35	30	0D	$_{0}A$	24	47	RESS:1004.50\$G
59	52	4 F	53	зA	58	2B	30	30	30	20	59	2D	30	30	30	YROS:X+000 Y-000
20	5A	2D	30	30	30	0 D	^{0}A	24	47	50	52	4D	43	2C	30	Z-000\$GPRMC,0
35	35	34	30	34	2E	30	30	30	2C	<u>56</u>	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.

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

		New Case			
ontroller Select controller model					
Find controller	AU_universal	AU6986	AU6987	AU6989ANHL	
Filter controllers by vendor	AU6989SN	AU6989SNCS	AU6989SNHL	AU6990	
AlcorMicro(AU) Black blob					
Chipsbank(CBM) FirstChip(FC)	AU6998SN	AU69xx	Black blob 1	Black blob 2	
Indilinx(IDX) Innostor(IS)	Black blob 3	Black blob 4	Black blob 5	Black blob 6	
Intel ITEtech(IT) IMicron(IM)	Black blob 7	Black blob 8	Black blob 9	CBM_universal	
Marvell(88SS) Other	CBM2098E	CBM2099	CBM2199	FC universal	
Phison(PS) Samsung		CDINEODD		C_universui	
SanDisk SiliconMotion(SM)	FC1178	FC1179	FC1250-TC-AL	FC1610-TC-AL	
Skymedi(SK) SolidStateSystem(SSS) Toshiba(TC)	FC8708-C	IDX_universal	IS_universal	IS817	
	IS902	IS903	IS916	IS916EN	

New Case						
Monolithic device Select monolithic device						
Filter monolithic device by memory chip ID Filter monolithic device by vendor Apacer CENTON Freecom Generic			•			
Generic GoodRAM Hama HEMA Integral Intenso Kingston Lexar no name Other Panasonic						
Platinum pqi Pretec Samsung Sandisk Sony SP Toshiba Transcend Verbatim						
			< Back Next > Skip			

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!

October 10-12, 2023 | Prague, CZ

