DOI:
10.1145/3407023.3409188

Cosmic Rays: a Neglected Potential Threat to Evidential Integrity in Digital Forensic Investigations?

Richard E Overill
Department of Informatics
King's College London
London, U.K.
richard.overill@kcl.ac.uk

ABSTRACT

When evidence is recovered from a suspected crime scene and a criminal prosecution is mounted, the defence team may attempt to formulate an alternative non-criminal explanation for the existence of that evidence. Examples from the digital realm include the "Trojan Horse Defence" and the "Inadvertent Download Defence" against the charge of possession of child pornography, both of which have previously been analysed quantitatively.

In this paper, another putative defence for the existence of forensically recovered data and/or meta-data from a seized digital device is described. The potential plausibility of this "Cosmic Ray Defence" under various memory protection conditions is estimated numerically as a function of its associated soft error rate (SER), thus enabling an evaluation to be made of its potential utility as part of a criminal defence strategy, as well as highlighting its possible significance for the conduct of digital forensic investigations. It is based on the invited keynote lecture at the 10th International Workshop on Digital Forensics (WSDF 2017), Reggio Calabria, Italy, 29 August – 1 September 2017.

CCS CONCEPTS

• Security and privacy • Security in hardware • Hardware security implementation • Hardware attacks and countermeasures

KEYWORDS

digital memory devices; scaling properties; high-energy neutrons; extra-terrestrial sources; cosmic rays; digital forensic evidence.

ACM Reference format:

Richard E Overill. 2020. Cosmic Rays: a Neglected Potential Threat to Evidential Integrity in Digital Forensic Investigations? In *Proceedings of ARES 2020, August 25–28, 2020, Virtual Event, Ireland. ACM, New York, NY USA, 6 pages, https://doi.org/10.1145/3407023.3409188*

ARES 2020, August 2020, Virtual Event, Ireland

1 Introduction and Background

A vital aspect of the forensic recovery and preservation of digital evidence for possible future use at trial is that the contents of any recovered or bit-wise imaged memory device has not been altered between its seizure and its forensic examination. Standard precautions include the use of write-blockers during imaging, the use of hashing and adherence to rigorous chain of custody procedures. However, such standard precautions do not take account of potential spontaneous alterations to the digital evidence as a result of the impact of high-energy radiation or particles of extra-terrestrial origin on the memory device during the period of time immediately preceding its seizure. In order to protect against accidental bit flipping, memory devices are routinely equipped with additional bits implementing an error correcting code (ECC), typically Hamming for single bit errors, or Reed–Solomon (RS) or Bose–Chaudhuri–Hocquenghem (BCH) for multiple bit errors. In this way, only multiple bit errors beyond the implemented ECC's capacity would go uncorrected.

However, the technical literature, e.g. [1], makes it clear that the unavoidable corollaries of the continuing scaling of memory devices according to Moore's law are that the voltage separations and charge thresholds between their bistable states decrease and correspondingly that the number of memory bits susceptible to a single high energy impact increases. This leads us to pose the following question: do any current memory technologies exhibit vulnerabilities to transient single event upsets (SEUs or 'soft errors') affecting more bits than the ECC's capacity which could realistically compromise their forensic evidential value, thereby offering a potentially plausible Cosmic Ray Defence (CRD) at trial? However, before proceeding it is necessary to clarify one point. We are not concerned here with permanent damage to memory modules, such as may be caused by terrestrial lightning strikes or large power grid spikes, since these are readily detectable by means of self-test diagnostic circuitry [32]. Our focus here is on events that may potentially alter digital evidence while leaving a forensic trace detectable only (if at all) at the scanning electron microscope (SEM) [33] level of detail, and which might hence form a plausible basis for a future legal defence stratagem.

2 Cosmic Rays

Cosmic rays, a term originally coined by Robert Millikan around 1914 following their discovery by Victor Hess in 1911–12, refer to a variety of extra-terrestrial phenomena. Primary cosmic rays comprise mainly protons (hydrogen nuclei, about 90%) and alpha particles (helium nuclei, about 10%). Their sources include the Sun, particularly during maxima in the 11-year solar cycle, our galaxy, particularly from black hole(s) located near its centre, and extremely distant extra-galactic objects such as active galactic nuclei (AGNs), quasi-stellar objects (QSOs) and (potentially) gamma ray bursters (GRBs). The solar wind and the terrestrial atmosphere screen the Earth's surface from primary cosmic rays with energies below about 100 MeV. Hence early interest in the effects of cosmic rays was mostly limited to the avionics and aerospace industries where their fluxes are up to two orders of magnitude greater than at ground level. Higher energy primary cosmic rays are transformed by spallation interactions with atmospheric nitrogen (about 80%) and oxygen (about 20%) atoms to produce secondary cosmic rays, ultimately consisting mainly of neutrons (about 96%), electrons, muons (heavy electrons), pions and protons at ground level. It should be noted that because charged particles stream towards the geomagnetic poles along the van Allen belts, there is a pronounced latitude dependence of the ground level cosmic ray flux. It is also known that the cosmic ray flux is far from isotropic. Due to the directional nature of the distant sources the Earth may pass through cones of ejecta as it orbits the Sun and as the solar system revolves around the galactic centre, leading to ground level secondary cosmic ray showers of heightened intensity from time to time.

The energy spectrum of the cosmic rays incident on the upper atmosphere is consistent with the form of a power law:

$$N(E) = K.E^{-\alpha}$$

where *N(E)* is the number of particles with energy *E* and *K* is a proportionality factor. A log–log plot of *N(E) vs*. *E* thus yields a straight line with gradient $-\alpha$ (see *e.g.* [30]), and it is found experimentally that $2.8 < \alpha < 3.0$, depending on the cosmic ray source [2]. However, it is not justifiable to assume that the high-energy ground-level secondary neutrons will have the same energy spectrum as the upper atmospheric cosmic rays. The energy spectrum of secondary cosmic ray neutrons at sea-level has been recorded at New York City (NYC) as a JEDEC standard [27], and the high-energy (>100 MeV) portion of this spectrum [28,29] has been least-squares fitted to a power law by the author, yielding a value of $\alpha = 2.7$, for the purposes of the present work.

Major early experimental and theoretical studies of the effects of secondary cosmic rays on digital memories were published by Ziegler and co-workers at IBM [3–13]. These studies showed that ground level cosmic ray high-energy (>100MeV) secondary neutrons were capable of penetrating up to 50m of concrete [4], and that on average a cosmic ray impact resulting in an SEU occurred about once a month in 256MB of RAM corresponding to a soft error rate (SER) of about 6.5×10^{-13} SEU/b/hr [14] or 650 FIT/Mb (FIT= Failures In Time). In addition, more recent studies have reported that individual SEUs are responsible for MBUs (multiple bit upsets) in which as many as 13 separate bits of 90nm SRAM were flipped [15], with almost 55% of all neutron impacts resulting in MBUs of some form [16]. Mechanistically speaking, high energy cosmic ray neutrons interact with the nuclei of silicon (and oxygen) atoms in the RAM via the strong nuclear force and fracture them into electrically charged fragments that can disrupt virtually any type of solid-state circuit [5]. Note also that the effect of high-energy neutron impact soft errors on DRAMs is of equal concern as for SRAMs [13].

The aim of this contribution is to review the available historical data in the light of the continuing scaling trends in digital memory technologies over the intervening 26 years, and to investigate whether the revised data and associated probabilities may have significant implications both for current digital forensic investigation practices and also for future criminal defence strategies.

It may be of interest to record here that the author first became aware of the likely reality of cosmic ray interactions with digital media around 1979 when a visiting colleague from the University of Calgary happened to remark that the executable file of a large application that was memory resident for very many hours at a time, which he used almost continuously in his research, would occasionally stop working abruptly during execution. These failures occurred irregularly but on average once every several months. The solution was simply to reload the executable and repeat the failed run. After eliminating all other inadvertent tampering mechanisms, we came to the conclusion that cosmic ray strikes on the machine instructions in memory were the most probable cause of these intermittent failures.

3 Memory Technology Scaling

The original IBM experimental and theoretical studies of the effects of secondary cosmic ray particles on digital memories took place between 1978 and 1994 [5]. Given the rather well-attested continuing operation of Moore's law over the following 26 years up to 2020 we would anticipate a $2^{26/2}$ = 8192-fold scaling in memory area technology to have taken place. The revised IBM figure would therefore be that on average a cosmic ray impact resulting in an SEU would occur about once a month in 2TB of RAM, due solely to the area scaling effect. Thus, each individual memory bit is now a much smaller 'target' for a cosmic ray particle than previously, but memory devices have increased in capacity (*i.e.* number of bits) correspondingly.

However, this does not take into account the concomitant reduction in the electronic charge used to represent a single memory bit that accompanies the area scaling. The critical energy (Ecrit), defined as the minimum energy that needs to be injected into a memory cell in order to induce an SEU, would also scale approximately as 2^{-13} over the 26-year period. This in turn implies that impacts of cosmic rays with correspondingly lower energies would be capable of causing an SEU. In order to account for this effect, it is convenient to re-write the cosmic ray high-energy secondary neutron spectrum power law in terms of probabilities:

$$p(E) = C.E^{-\alpha}$$

where *C* is the probability normalisation factor: The complementary cumulative distribution function (CCDF) of the cosmic ray energy spectrum also takes the form of a power law, but with a decremented exponent [17]:

$$P_{>}(E') = \frac{C}{\alpha - 1}.E'^{-(\alpha-1)}$$

and represents the probability of a cosmic ray particle having an energy *E* greater than some threshold energy *E'*. The ratio of the

CCDFs representing the proportion of cosmic ray particles with energies greater than $E_{crit}/2^{13}$ and the proportion of cosmic ray neutrons with energies greater than E_{crit}:

$$P_{>}\left(\frac{E_{crit}}{2^{13}}\right) : P_{>}(E_{crit}) = (2^{13})^{(\alpha-1)} \sim 2^{22}$$

for α=2.7, gives the increase in the proportion of cosmic ray neutrons capable of causing an SEU due to the reduction in E_{crit}, Each individual memory bit is now very much more susceptible to impacts from a larger number of lower energy cosmic ray neutrons than previously.

In order to incorporate the effect of implementing an ECC with the capacity to correct k bit errors it is necessary to find the ratio of the proportion of cosmic ray neutrons capable of causing an MBU of at least (k+1) bits to the proportion capable of causing an SBU. Under the assumption that most MBUs are caused by a single high-energy SEU, (as opposed to a shower of several simultaneous lower-energy SBUs [15]), this ratio is given by:

$$P_{>}\left(\frac{(k+1)E_{crit}}{2^{13}}\right) : P_{>}\left(\frac{E_{crit}}{2^{13}}\right) = (k+1)^{-(\alpha-1)} \sim \frac{2}{13}$$

for k=2 and α=2.7. Combining the effects of area scaling, charge scaling and the mitigating presence of ECC logic with k=2, we find an upper bound on the rate of cosmic ray induced undetectable SEU events in 2020 to be about $1\times2^{22}\times(2/13)$ SEU per month per 2TB of RAM, which is equivalent to an SER of ~ 79 SEU per month per 256MB of RAM to facilitate direct comparison with the original IBM figure quoted earlier [14].

4 Discussion of Results

It needs to be stressed from the outset that this result represents a worst case (i.e. an upper bound) for the following reasons. Firstly, not every interaction with a sufficiently energetic cosmic ray neutron will necessarily result in an SEU, since its angle of incidence (AoI) determines the extent to which its energy is transferred into the memory device. An orthogonal interaction will dump virtually all the particle's energy whereas a grazing interaction will offload virtually none. Specifically, if all AoIs are considered to be equally probable then the energy transferred is:

$$E_e = E.cos^n\theta$$

where $0 \le \theta \le \pi/2$ is the AoI relative to the surface normal. Since the value of n is not known with certainty but is thought to lie between 1 and 5 [6], we give in Table 1 the values of $cos^n\theta$ averaged over $0 \le \theta \le \pi/2$ for n = 1 to 5, noting that the AoI scale factor varies between *ca.* 2/3 and *ca.*1/3. Secondly, we have assumed that Moore's law has continued to operate consistently throughout the 26-year period (1994 – 2020), doubling the memory bit density every two years, whereas in fact there is some evidence for a falling-off in the past decade [18]. Finally, it is very unlikely that a SEU causing an MBU of k bits would have an energy as low as $k.E_{crit}$ since a proportion of the energy would be dissipated in-between the individual SBU events constituting the MBU. In Table 2 we illustrate the numerical dependence of the estimated SER on the value of the ECC parameter k.

The estimated SER data in Table 2 are of course subject to a number of uncertainties, the largest of which are almost certainly the variations in primary cosmic ray flux with time over the 11-year solar activity ('sun-spot') cycle and with latitude (distance from the geomagnetic north or south pole) on the Earth's surface; ground-based measurements [27] suggest a factor of *ca.*2 both above and below the mean in the variation of the high-energy secondary cosmic ray neutron flux as a result of these two effects. Consequently, there will be a similar uncertainty in the estimated SERs in Table 2, and any value $\boldsymbol{x}$ taken or derived from Table 2 should be treated as a value within the range [0.5$\boldsymbol{x}$, 2.0$\boldsymbol{x}$].

However, it must also be recognised that as memory chip feature sizes continue to move further into the deep nanoscale region, the effects of both quantum mechanical tunneling of electrons and Boltzmann thermal excitation of electrons could also contribute to charge leakage which would have the effect of reducing E_{crit} still further [19]; for example, at chip feature sizes around 50nm, only a few hundred electrons represent each memory bit [20], while feature sizes as low as 16nm are currently in production.

In addition to the use of ECCs, another partial mitigation strategy is memory bit interleaving, a data organisation scheme where there a is much greater insulation barrier between memory bits along the word-line than along the bit-line [21]. Then a cosmic ray neutron strike along the bit-line is much more likely to propagate than a strike along the word-line, and the logical ECCs have a greatly enhanced chance of detecting the MBU.

While early studies focused mainly on bipolar and then on CMOS SRAM and DRAM memory technologies, more recently non-volatile floating gate (FG) Flash memories employing NAND- and NOR-based technologies have been developed. A similar Moore's law scaling trend operates in FG Flash memory [21], and similar area and charge scaling considerations also apply, although the detailed nanoscale SEU mechanisms differ somewhat [22]. Further studies on the radiation hardness characteristics of FG Flash memories have been published, *e.g.* [23, 24], and it is known that at a feature size of 30 nm, an ECC capable of correcting at least 24 bit errors must be used for MLC (multi-level cell) NAND Flash memory technology [25].

In the case of conventional hard disk (HD) ferromagnetic grains, completely different soft error mechanisms are operative since magnetisation, rather than charge, is used to represent each bit. No systematic studies comparable with those for CMOS and Flash memory have been undertaken to determine whether or not cosmic ray impacts are capable of producing hard disk soft errors. However, in order to generate the transient magnetic fields required to cause a HD SEU, accelerated charged particles (alpha particles, protons) of sufficiently high energy would need to be produced at the HD surface, and no viable mechanism for achieving this effect has been proposed.

Note that we have not considered here the effects of alpha particles ejected from the immediate ceramic chip packaging as a result of radioactive decay of trace radionuclide impurities, since these are now known to be more than an order of magnitude smaller than cosmic ray effects [7], and, unlike high-energy neutrons, a sheet of ordinary paper is a perfectly adequate shield for these non-cosmic alpha particles [26].

5 Summary and Conclusions

Given the above considerations, a wily defence lawyer might (perhaps inspired by case of the 2003 Schaerbeek, Belgium

election or the 2008 A330 flight QF72 [31]) attempt to plausibly cast reasonable doubt on the integrity of the recovered digital evidence using a Cosmic Ray Defence (CRD) strategy. Once the device containing the evidence has been seized, bit imaged and hashed, any such bit-flip change(s) can be detected. But during the time interval between the actual creation of the evidential material and its seizure by law enforcement there exists a "window of opportunity" during which the defence side could argue that one or more SEUs may have compromised the integrity of the digital evidence. In order to refute such a claim in a semi-absolute sense, the prosecution would need to demonstrate that appropriate memory bit interleaving and/or adequate ECC was not only implemented but also correctly functioning in the device to prevent this occurrence. This latter point is important since our wily defence counsel might otherwise offer the counterclaim that the ECC circuitry had itself been compromised by a secondary cosmic ray strike, something which could be checked using a SEM. Alternatively, the prosecution could attempt to create a statistical refutation based on the contention that the cosmic ray neutron induced SER derived in Section 3 above was so small as to render the defence's claim implausible beyond all reasonable doubt.

For two simple illustrations of such a statistical refutation consider the following two scenarios. Firstly, consider a standard workstation with a 32GB non-ECC RAM would be expected to undergo *ca.* 91 SEUs during the one-hour period prior to backing-up its contents to a HD; the probability of any one specific bit undergoing an SEU during that time interval is simply given by $91 / (32G\times8) \sim .4 \times 10^{-9}$ per hour. Secondly, consider a standard workstation with a 4TB NAND MLC Flash SSD with each 512B block protected by an ECC with $k = 24$. Each block would be expected to have suffered *ca.* 2.2/½M SEUs and the entire SSD would experience $(4T/512) \times (2.2/½M) \sim 35{,}200$ SEUs during the month prior to its being seized; the probability of any one specific bit undergoing an SEU during that time interval is similarly given by $35{,}200 / (4T\times8) \sim .9 \times 10^{-9}$ per month. To gain some sense of scale and perspective, it is worth comparing the two probabilities above with that of a random collision in a 32-bit hash function which is $2^{-32} \sim .25 \times 10^{-9}$.

It should be recalled at this juncture that some of the SEUs in the two examples above may in fact be MBUs, as opposed to SBUs, provided that the energy of the incident secondary neutron is sufficiently high. This consideration could increase the estimated probabilities by at most one order of magnitude.

To revert to the question posed in the Introduction, the SER rates displayed in Table 2 and the two exemplar scenarios described above demonstrate that undetected bit-flips due to secondary high-energy cosmic ray neutrons do occur at a predictable measurable rate, and thus *in principle* offer the basis for a putative CRD. The question as to whether this amounts to anything approaching a plausible legal defence strategy *in practice* is another matter entirely. It will depend on, amongst other things, whether the integrity of every single bit of the data is equally crucial to the case, *e.g.* with a large financial spreadsheet. If only a small subset of the data, or perhaps just the 24 bytes of file meta-data relating to creation, last modification and last access times and dates, are considered crucial to the case, then there is a much smaller effective cross-section (or 'target') for the neutrons to disrupt and a consequently smaller probability of a forensically significant SEU in support of the hypothetical CRD.

However, in the final analysis it will be up to the investigators, prosecutors, and ultimately the courts, to decide whether such potential changes to the digital evidence are significant in the detailed context of the case being tried. For example, if the metadata and/or the exact contents of one or more critical files are crucial to a particular case and are believed not to have been backed-up elsewhere, either automatically (*e.g.* in the cloud) or manually, for a significant amount of time, such a scenario might be deemed potentially suitable for the CRD. Contexts in which there is inherently little or no data redundancy, such as some areas of IoT device forensics, are more likely to present potential opportunities for this kind of defence since it would be difficult or even impossible to reconstruct the data under question from other digitally independent sources which have been forensically recovered during the investigation.

Turning to the implications for digital forensic investigations, the fact that there exists a non-zero (although numerically small) probability that in the time interval between its creation and its forensic recovery or backing-up, digital evidence may have undergone a number of bitwise alterations that have left no obvious traces places the outcome phenomenologically in a similar league with data tampering. Data destruction is another matter, however, and although this can be achieved by the very highest energy secondary neutrons literally smashing through one or more of the memory capacitor structures, it leaves a trail of destruction which is clearly visible using a SEM.

From what has been said above it will also be clear that digital forensic investigators will need to acquaint themselves with the detailed technical characteristics of the memory device in question if a CRD is anticipated; in particular, the capacity k of the ECC (if any) and the block size over which it is implemented will be crucial to any evaluation of plausibility. For dealing with memory technologies dating from earlier than 2020 it is simply necessary to recompute the relevant estimated SER using the appropriate year since 1994.

Finally, a small historical lesson may also be drawn. The first Trojan Horse Defence (THD) [34,35] was successful at least in part because its low plausibility was not appreciated with any degree of certainty at the time of the trial; however, subsequent quantitative analysis based on complexity theory was able to attach probabilities to each of a number of different THD scenarios [36]. The putative Inadvertent Download Defence (IDD) against the possession of small quantities of child pornography has also been analysed quantitatively using statistical Urn methods to determine its plausibility with numerical data from two actual cases that ultimately did not go to trial [37]. The present contribution is another example of proactively analysing a putative novel defence stratagem in order that it is well understood before it is offered at a trial, unlike the original THD. The corollary of this is that the evidently low SERs in Table 2 and the two worked examples above may effectively deter our wily defence counsel from deciding to run a CRD, in which case this paper will have served its purpose in another way. From a philosophy of science perspective, the apparently negative result of a very low plausibility for the CRD may also result in the positive consequence that the courts will be unlikely to ever be confronted with it.

n	$\langle \cos^n\theta \rangle$
1	2/π
2	1/2
3	4/(3π)
4	3/8
5	16/(15π)

Table 1. Average values of $\cos^n\theta$

k	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
	512	158	79	48	33	24	19	15	12	10
k	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
	8.7	7.5	6.5	5.8	5.1	4.6	4.1	3.8	3.4	3.1
k	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**
	2.9	2.7	2.5	2.3	2.2	2.0	1.9	1.8	1.7	1.6

Table 2. Estimated SER values (/month/256MB) as a function of k (for α = 2.7)

ABBREVIATIONS

AGN active galactic nucleus
AoI angle of incidence
B byte; b bit
BCH Bose–Chaudhuri–Hocquenghem ECC
CCDF complementary cumulative distribution function
CMOS complementary metal oxide
CRD cosmic ray defence
DRAM dynamic RAM
ECC error correcting code
FG floating gate
FIT failures in time (per billion device hours operation)
GRB gamma ray burster
MBU multiple bit upsets
HD hard disk
IDD inadvertent download defence
IoT internet of things
MeV mega-electron volts
MLC multi-level cell
QSO quasi-stellar object
RAM random access memory
RS Reed–Solomon ECC
SBU single bit upsets
SEM scanning electron microscope
SER soft error rate
SEU single event upsets
SLC single-level cell
SRAM static RAM
SSD solid state disk
THD Trojan horse defence

REFERENCES

[1] P Hazucha and C Svensson. 2000. Impact of CMOS technology scaling on the atmospheric neutron soft error rate. *IEEE Trans. Nucl. Sci*., 47 (6) (December 2000) 2586–2594.

[2] J D Hague, B R Becker, M S Gold and J A J Matthews. 2007. Power laws and the cosmic ray energy spectrum. *Astroparticle Phys*., 27 (5) (June 2007) 455–464.

[3] J F Ziegler and W A Lanford. 1979. Effect of cosmic rays on computer memories. *Science*, 206 (4420) (1979) 776–788.

[4] J F Ziegler. 1981. The effect of concrete shielding on cosmic ray induced soft fails in electronic systems. *IEEE Trans. Electron. Dev*., 28 (5) (1981) 560–565.

[5] J F Ziegler *et al.* 1996. IBM experiments in soft fails in computer electronics (1978 – 1994). *IBM J. Res. Devel*., 40 (1) (January 1996) 3–18.

[6] J F Ziegler. 1996. Terrestrial cosmic rays. *IBM J. Res. Devel*., 40 (1) (January 1996) 19–39.

[7] T J O'Gorman *et al.* 1996. Field testing for cosmic ray soft errors in semiconductor memories. *IBM J. Res. Devel*., 40 (1) (January 1996) 41–50.

[8] J F Ziegler *et al.* 1996. Accelerated testing for cosmic soft error rate. *IBM J. Res. Devel.* 40 (1) (January 1996) 51–72.

[9] J F Ziegler. 1998. Terrestrial cosmic ray intensities. *IBM J. Res. Devel*., 42 (1) (January 1998) 117–139.

[10] J F Ziegler *et al.* 1998. Cosmic ray soft error rates of 160Mb DRAM memory chips. *IEEE J. Solid-State Circuits*, 33 (2) (February 1998) 246–252.

[11] G J Hofman *et al.* 2000. Light-hadron induced SER and scaling relations for 16- and 64-Mb DRAMs. *IEEE Trans. Nucl. Sci*., 47 (2) (April 2000) 403–407.

[12] J F Ziegler. 2004. Trends in electronic reliability – Effects of terrestrial cosmic -rays, (2004) http://www.srim.org/SER/SERTrends.htm

[13] T J Dell. 2008. System RAS implications of DRAM soft errors, *IBM J. Res. Devel.*, 52 (3) (May 2008) 307–314.

[14] E Normand. 1996. Single event upset at ground level. *IEEE Trans. Nucl. Sci.*, 43 (6) (December 1996) 2742–2750.

[15] R Naseer and J Draper. 2008. Parallel double error correcting code design to mitigate multi-bit upsets in SRAMs. In *Proc 34th IEEE European Solid-State Circuits Conference (ESSCIRC)*, (2008) 222–225.

[16] Z Wang, M Karpovsky and K J Kulikowski. 2010. Design of memories with concurrent error detection and correction by non-linear SEC-DED codes. *J. Electron. Test.*, 26 (2010) 559–580.

[17] M E J Newman. 2005. Power laws, Pareto distributions and Zipf's law. *Contemp. Phys.*, 46 (5) (2005) 323–351.

[18] V V Zhirnov, R K. Cavin III, J A. Hutchby and G I Bourianoff. 2003. Limits to binary logic switch scaling—a gedanken model. *Proc. IEEE*, 91 (11), (November 2003) 1934–1939.

[19] D Rittman. 2006. CMOS nanometer scaling limited, Tayden Design (July 2006), http://tayden.com/publications/CMOS Nanometer Designs Scaling Limited.pdf

[20] S Gerardin *et al.* 2012. Neutron-induced upsets in NAND floating gate memories. *IEEE Trans. Dev. Mat. Reliab.*, 12 (2) (June 2012) 437–444.

[21] M Bagatin, S Gerardin and A Paccagnella. 2017. Space and terrestrial radiation effects in flash memories. *Semicond. Sci. Technol*., 32 (2017) #033003.

[22] J C McNulty and C D Hillman. 2008. Current concerns regarding solid state drive reliability. In *Proc. IDEMA Reliability Symposium*, San Jose, CA (September 2008).

[23] M Bagatin, G Cellere, S Gerardin and A Paccagnella. 2010. Radiation effects on NAND flash memories. In *Inside NAND Flash Memories* (Eds. R Micheloni, L Crippa & A Marelli), Springer (2010), Ch.19, 537–571.

[24] E Verrelli and D Tsoukalas. 2011. Radiation hardness of flash and nanoparticle memories. In *Flash Memories* (Ed. I Stievano), InTech (2011) Ch.11, 211–240.

[25] R Novotny, J Kadlec and R Kuchta. 2015. NAND flash memory organization and operations. *J. Info. Tech. Soft. Eng*., 5 (1) (2015) #1000139.

[26] L Lantz II. 1996. Soft errors induced by alpha particles. *IEEE Trans. Reliab*., 45 (2) (June 1996) 174–179.

[27] JEDEC. 2006. Measurement and Reporting of Alpha Particles and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices: JESD89A. *JEDEC Standard*, JEDEC Sold State Technology Association, Arlington, VA., USA, No.89, (2006) 1–85.

[28] M S Gordon, P Goldhagen, K P Rodbell, T H Zabel, H H K Tang, J M Clem and P Bailey. 2005. Measurement of the Flux and Energy Spectrum of Cosmic-Ray Induced Neutrons on the Ground. *IEEE Trans. Nucl. Sci*., 51 (6) (Dec. 2004) 3427–3434; *erratum*: *ibid.*, 52 (6) (Dec. 2005) 2703.

[29] E Ibe. 2011. Terrestrial Neutron-Induced Failures in Semiconductor Devices and Relevant Systems. In *Dependability in Electronic Systems* (Eds. N. Kanekawa *et al*.), Springer (2011), 7–63.

[30] Wikipedia. 2019. Cosmic ray flux versus particle energy. (8 January 2019). https://commons.wikimedia.org/wiki/File:Cosmic_ray_flux_versus_particle_energy.svg

[31] Vanderbilt University. 2017. Alien particles from outer space are wreaking low-grade havoc on personal electronic devices. (17 February 2017).

https://news.vanderbilt.edu/2017/02/17/alien-particles-from-outer-space-are-wreaking-low-grade-havoc-on-personal-electronic-devices/

[32] T J Bergfield, D Niggemeyer and E M Rudnick. 2000. Diagnostic testing of embedded memories using BIST. In *Proc. IEEE Conf. on Design, Automation and Test in Europe (DATE)*, Paris, March 2000, 305–309.

[33] E Menzel and E Kubalek. 1983. Fundamentals of electron beam testing of integrated circuits. SCANNING 5 (1983) 103–122.

[34] E George. 2004. UK computer misuse act – the Trojan virus defence. *Digital Invest.*, 1 (2) (2004) 89–89.

[35] S Bowles and J Hernandez-Castro. 2015. The first 10 years of the Trojan Horse defence. *Computer Fraud & Security*, 2015 (1) (2015) 5-13.

[36] R E Overill and J A M Silomon. 2011. A Complexity Based Forensic Analysis of the Trojan Horse Defence. In *Proc. 4th International Workshop on Digital Forensics (WSDF 2011)*, Vienna, Austria (22–26 August 2011) 764–768.

[37] R E Overill and K P Chow. 2016. An approach to quantifying the plausibility of the inadvertent download defence. *Forensic Sciences Research*, 1 (1) (2016) 28–32.