Obsolescence in EMC Risk Assessment: A Case Study on EFT Immunity of Microcontrollers

Qazi Mashaal Khan[1], Mohsen Koohestani[1,2], Mohamed Ramdani[1,2], and Richard Perdriau[1,2]

[1]École Supérieure d'Électronique de l'Ouest (ESEO), Depart. Electrical and Control Engineering, RF-EMC research group, Angers 49107, France

[2]Institute of Electronics and Telecommunications of Rennes (IETR), Rennes 35042, France

E-mail: (qazimashaal.khan, mohsen.koohestani, mohamed.ramdani, richard.perdriau)@eseo.fr

***Abstract*—This paper investigates the obsolescence in EMC risk assessment by conducting an experimental case study on two commercially available Atmel microcontrollers (μCs), i.e. SAM3 and SAM7, the former being more recent but still pin-to-pin compatible. To this end, electrical fast transient (EFT) testing was performed according to the IEC 61000-4-4 standard to identify and clarify the failure occurring in the μCs individual voltage supply pins. The μC crash was considered as the immunity criterion to monitor the failure due to the EFT bursts. Results demonstrate, in a reproducible manner, that SAM3 was more immune to transient disturbances compared to SAM7 on all the considered supply pins, excluding the phase-locked loop. Moreover, regardless of the μC version, the core supply pin was found to be the most susceptible to EFT injection. These results show that replacing a SAM7 μC by a SAM3 μC calls for a detailed EMC analysis, particularly when dealing with obsolescence, since a more modern, compatible IC does not necessarily provide a higher immunity.**

***Index Terms*—EMC, obsolescence, EFT bursts, immunity**

I. Introduction

In recent years, the ever-changing developments in integrated circuit (IC) technology have increasingly challenged IC developers with confronting electromagnetic compatibility (EMC) issues. Microcontrollers (μCs) build up the core of embedded systems [1]. Therefore, their specific EMC characteristics and, in particular, their immunity to electromagnetic interference (EMI), are crucial for proper operation over the entire lifetime of a system [2].

Conducted immunity testing can be carried out either in continuous wave (CW) or in transient mode. Among the latter, electric fast transients (EFTs), defined in IEC 61000-4-4 [3], are among the most widely used for industrial EMC testing [4]. The EFT signal, consisting of a series of bursts, can be injected into either functional or power supply pins of an IC using magnetic or electric coupling. This interferes with the standard behavior of the IC, causing temporary malfunction or even irreversible damage.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 812.790 (MSCA-ETN PETER). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-peter.eu/.

In comparative literature, there are several works reporting information on EFT testing of μCs with different architectures [5]–[7]. However, apart from repeatability, the reasons for the observed failures still have to be clarified in terms of root cause for the ICs selected in those papers.

Unfortunately, that immunity testing is often performed only in a brand new product, not taking into account how the EMC behavior of an IC could evolve within the lifetime of that product. This may result in high risk factors due to EMC-related reliability issues. For example, the following could influence that behavior:

- technological dispersion in IC characteristics (effective channel length, doping, etc)
- ageing due to environmental characteristics (temperature, humidity, vibration, etc)
- obsolescence (replacing an IC by another functionally identical or pin-to-pin compatible IC)

This paper only focuses on obsolescence to provide our contribution to the very vast domain of EMC risk assessment.

Manufacturers are regularly searching for practical and time-efficient techniques for reducing the potential limitations of IC obsolescence [8]. If an IC has become obsolete, it should be verified that its successor will not be more susceptible, in order to ensure that the whole system complies with at least the same performance level according to EMC standards.

In the current study, EFT testing was performed on two 32-bit μCs (Atmel/Microchip SAM7S256 [9] and SAM3S4B [10]), the latter being the a more recent version ideal for migration from SAM7 [10]. These tests were carried out to identify and further clarify the failure caused by the EFT injection into the individual voltage supply pins of the μCs. Both μCs have identical peripherals and pinouts, but with different core architectures (ARM7TDMI and Cortex-M3, respectively) and flash memory voltages; software can be ported from SAM7 to SAM3 with only minimal changes.

The paper is arranged as follows. Section II describes the devices under test (DUTs) used, the hardware setup configurations, together with the failure criteria employed. Section III addresses the comprehensive analysis of the experimental results. Section IV describes the EMC risk assessment due to obsolescence for the chosen case study, while the concluding contributions of this study are provided in Section V.

978-1-7281-5579-1/20/$31.00 ©2020 IEEE

II. Materials and Methods

This section introduces the configuration of the μC test boards, the hardware setup being employed for EFT testing and the relevant criteria to evaluate the failure of the considered μCs.

A. Description of μCs and Test Boards

The two SAM3 and SAM7 μCs selected for this experiment are pin-to-pin compatible, having similar internal oscillators, external bus interfaces, peripherals and packaging. They require a 3.3 V supply voltage (and, optionally, another 1.8 V supply voltage) to operate reliably and are mounted on identical test boards.

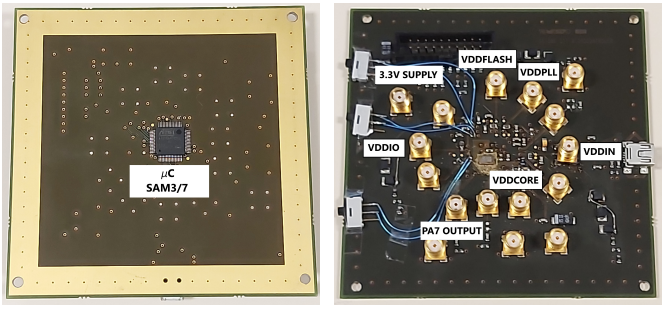
Both μCs use separate 3.3 V power supplies for input/output (I/O) buffers (V_{DDIO}) and for their internal 1.8 V regulator (V_{DDIN}). Only for SAM7, a third 3.3 V power supply is used to power the Flash memory array ($V_{DDFLASH}$), which is replaced by an I/O on SAM3. Either the output of the internal voltage regulator (V_{DDOUT}) or an external supply can be used for the 1.8 V power supplies. Those supplies consist of V_{DDPLL} (powering the PLL and the internal oscillator) and V_{DDCORE} (powering the CPU core and, for SAM3 only, the Flash memory array). Moreover, another difference can be noticed between both μCs: SAM7 uses an external PLL loop filter, while that filter is integrated in the SAM3 (the filter pin is also replaced by an I/O).

Each testboard (Fig. 1) is a 10 × 10 cm standard IEC 62132-2 [11] printed circuit board (PCB) fitted with modular SMA connectors for different power supplies and I/Os. The PA7 pin will be used to monitor the immunity of both μCs. Fig. 2 summarizes the connections that can be set up among all power supplies on both PCBs. As can be seen, each power supply pin is equipped with a zero-ohm series resistor, making it possible to either connect it to the general power supply (J33 for 3.3 V, J34 for 1.8 V) or to the dedicated power supply of an EFT generator to test it individually. Decoupling capacitors are connected to each pin, in order to put the μC in the standard operating conditions recommended by the manufacturer. Since the objective of the study is only a functional comparison, those capacitor values are not critical. Finally, CV1 and CV2 make it possible to switch the 1.8 V supply between the internal voltage regulator output and an external supply.

Both SAM3 and SAM7 are programmed to generate a square wave through PA7. The observed frequency of the wave generated by SAM3 (200 Hz) is twice as that of SAM7 (100 Hz) due to a difference in PLL configurations. Likewise, that difference is not crucial for functional testing.

B. Hardware Setup and Procedure

EFT is a low-energy test, usually (but not always) non-destructive, having a wide spectral frequency content creating problems with sensitive sensors and μCs. During the EFT test, a repetitive voltage transient is induced over either a DC supply line or a functional signal. In this paper, only injection into DC supplies will be considered.



(a) (b)

Fig. 1. EMC Test Board (SAM3/7) : (a) Front ; (b) Back.

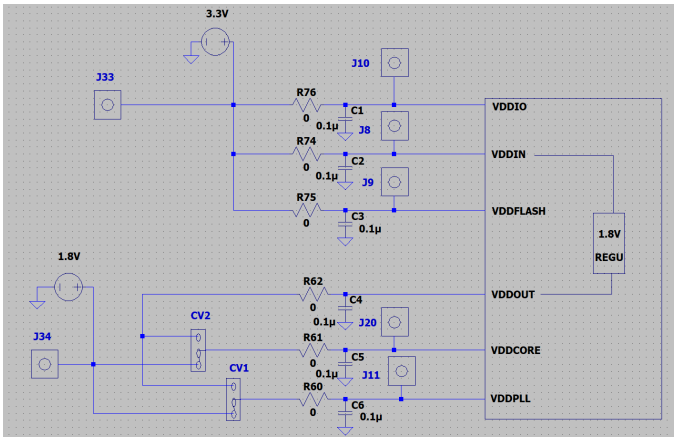


Fig. 2. Schematic of SAM3/7.

According to the standard [3], each individual EFT pulse is characterized by a 5 ns rise time, 50 ns pulse width, 300 ms burst repetition, 5 kHz spike frequency, and 15 ms burst duration. The positive polarity EFT signal is ramped from 250 V to 5 kV in 100 V steps.

The test bench for EFT primarily includes the adapter board for the Device Under Test (DUT), an EMC-Partner 5.1 kV IMU4000 EFT generator [12], a dual-channel Agilent E3631A DC power supply with current monitoring, a Keysight DSOS0204A oscilloscope to monitor the PA7 signal, and a custom optoisolation board. This setup is depicted in Fig. 3. One channel of the power supply is connected to the internal coupler of the EFT generator (making it possible to superimpose the disturbance with the DC voltage), while the other channel is used as an auxiliary supply to power IC pins that should remain undisturbed. Both current limits were set to 1 A.

The customized optoisolation board shown in Fig. 4 is designed with optocouplers to avoid reinjection of high-voltage EFT signals into the oscilloscope. The optocouplers chosen for that board are low-current (1 mA) with inverting 5 V digital outputs. The PA7 output of either μC is connected to the input of one of the optocouplers through a cable connected to the corresponding SMA connector of the DUT. Since that output only delivers around 1.2 mA for both μCs, it can be noted that a slight variation of that current due to injection may

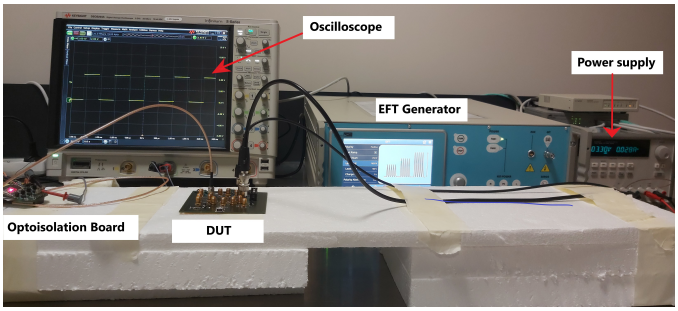


Fig. 3. EFT Test Setup.

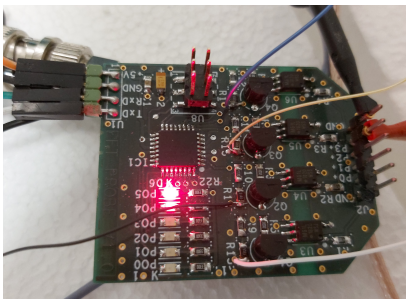


Fig. 4. Custom optoisolating board.

dramatically change the low output level of their outputs, and the voltage-to-voltage transfer function is totally non-linear. Consequently, the analog behavior of the I/O due to the EFT voltage cannot be accurately monitored by the signal observed on the oscilloscope, and the output voltage of the optocouplers can not be considered as a valid immunity criterion.

After a first EFT injection into the common 3.3 V power supply (powered through the EFT generator), all resistors were removed one by one and a separate power supply was used on J33 for the remaining tests (performed through J8 to J10). Then, all resistors were fitted again in the 3.3 V supplies, and the same operation was repeated for 1.8 V supplies, using V_{DDOUT} as the separate power supply when required.

C. Failure Criteria

As mentioned previously, the only immunity criterion to monitor a failure in the practical EFT tests performed is the μC crash, i.e. the square wave from PA7 being no longer observable on the oscilloscope, due to the embedded software not running properly. Table I shows apparent failure types classified from A to E.

No failure (A) occurs when the supply pin is completely immune to EFT and causes no malfunction in the μC.

Self-recovery (B) is likely to be due to the power-on-reset (POR) or low-voltage detector (LVD) blocks [3]. POR maintains an internal RESET while the core power supply is below a given threshold when the the supply voltage is applied from zero, while LVD maintains the internal RESET when the supply voltage drops below another threshold, until it rises back to its nominal value. In both cases, that automated

TABLE I
SPECIFICATION OF FAILURE MODES

Classification	Failure Type	Description
A	No Failure	The µC does not crash and remains operational during EFT exposure
B	Self-Recovering	The µC crashes and resumes operation as soon as EFT exposure is removed
C	Soft Failure	The µC crashes and is only operational when the EFT exposure is removed and a manual reset is performed
D	Repower Recovering	The µC crashes and is only operation when the EFT exposure is removed and power cycling is performed
E	Damaged	The µC is permanently deteriorated due to EFT exposure

RESET makes it possible for the μC to restart from a well-known state.

Soft failure (C) usually occurs when the state machine of the μC core crashes into an unknown state due to interference, which can be recovered by an explicit (external) RESET of the core.

Repower-recovering (D) implies that the core is unable to restart by itself when reset. This may be due, for example, to a crash in the Flash memory controller or an internal signal maintained at an incorrect level due to latch-up. This can only be resolved by power cycling. Sometimes, a slight increase in DC current may be observed due to that incorrect state.

The E-type failure encompasses "soft" and "hard" damage which, in both cases, prevent the μC from restarting when power is cycled. "Soft" damage refers, for example, to a spurious erasure of a Flash memory block (or a change in Flash contents) due to the interference triggering the state machine of the Flash controller. "Hard" damage reflects a permanent, physical damage in the IC structure; in that case, a significant rise in the DC supply current is often observed.

III. EXPERIMENTAL RESULTS AND DISCUSSION

This section deals with the direct impact of EFT disturbances on the performance of the SAM3 and SAM7 μCs. Each mentioned pin was subjected to a specified range of EFT and the square wave generated through PA7 is monitored in real time. An apparent failure was reported when the μC crashed and a constant high/low logic level was detected. This depends on the current state of the logic level when the μC software stops running. A comparison was drawn depending on the types of failure of each supply pins of both boards and their specific causes will be discussed.

A. Experimental Results

The first practical test involved ramping the EFT signal on the 3.3 V (J33) main supply of SAM3 and SAM7. The lowest value of the EFT signal was 250 V due to the limits of the EFT generator. The maximum value of the EFT signal was intentionally limited to 1.65 kV. The abrupt increase in DC current was the deciding factor to be limited to this voltage not to damage the test boards.

For SAM3, when the EFT signal was injected at 250 V, the square wave instantly began to oscillate and flickers were visible on each rising and falling level. The oscillations increased with constant rise in EFT voltage and maximum

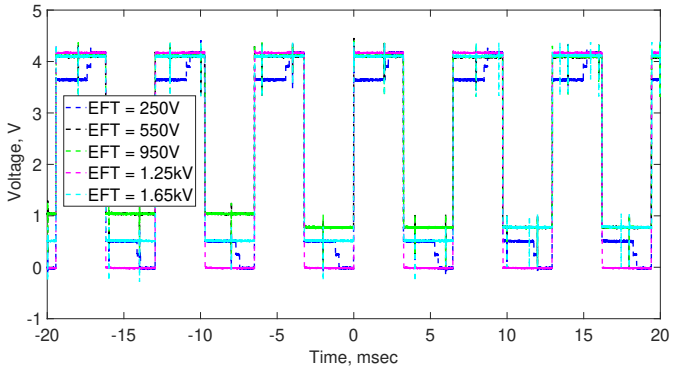


Fig. 5. Output of SAM3 after EFT injection to main supply (Equivalent results with SAM3 V_{DDIO} and V_{DDIN}).

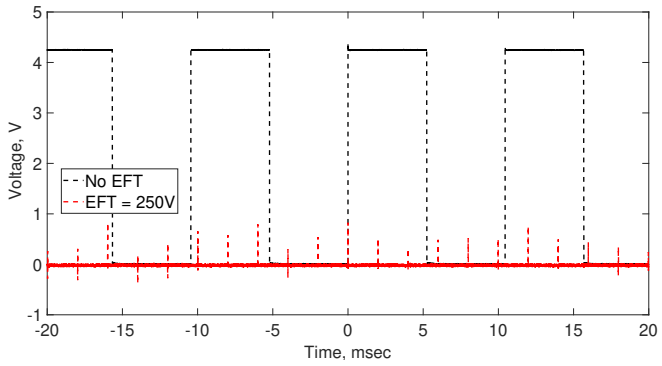


Fig. 6. Output of SAM7 after EFT injection to main supply (Comparable results with SAM7 $V_{DDFLASH}$).

amplitude levels at the optocoupler output were reduced by 21% (3.4 V) compared to the original signal; it should be remembered that this reduction in amplitude is due to a reduction in the optocoupler input current and, therefore, can not be considered a significant immunity criterion. There was no failure observed on the main supply of SAM3. Similar to the main supply, V_{DDIO} and V_{DDIN} were immune to EFT up to 1.65 kV (Fig. 5).

Different results were obtained for SAM7. The μC crashed for an EFT voltage as low as 250 V on the global 3.3 V supply, delivering a low logic level at the optocoupler output (i.e. high on the PA7 pin), as shown in Fig. 6. A D-type failure was observed, and the signal was recovered after power cycling. When EFT was injected into $V_{DDFLASH}$, the SAM7 crashed for the same injection level (250 V).

Prominently displayed in Fig. 7, the V_{DDIO} of SAM7 crashed at 450 V, resulting in a soft failure (C). The DC current experienced an abrupt rise from 21 mA to 289 mA. Interestingly, that increase did not seem to come from permanent damage to the chip, since the current returned to its nominal value after resetting the chip.

The V_{DDIN} of SAM7 was immune to a higher EFT voltage level, with increasing harmonics and oscillations. However, at exactly 1.05 kV, the DC supply current drastically increased from 37 mA to 854 mA. This time, the DC current remained

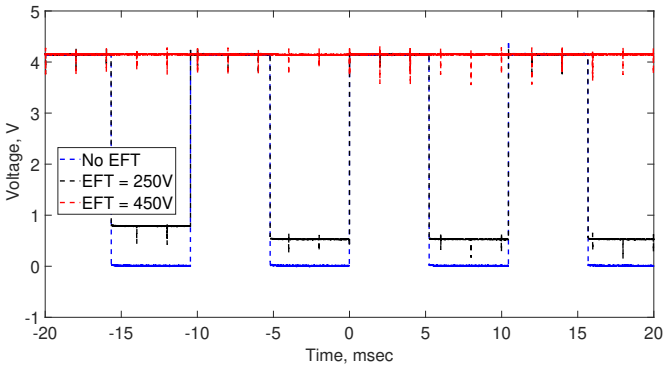


Fig. 7. Output of SAM7 after EFT injection to V_{DDIO}.

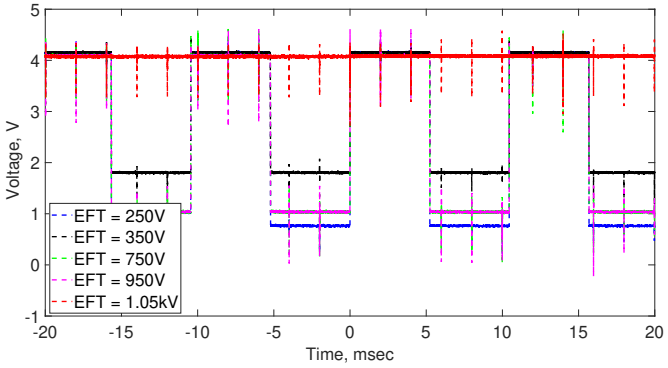


Fig. 8. Output of SAM7 after EFT injection to V_{DDIN}.

TABLE II
MAXIMUM APPLIED EFT VOLTAGE (FAILURE TYPE)

Pin No.	SAM 3	SAM 7
Main supply	1.65 kV (A)	250 V (D)
V_{DDIO}	1.65 kV (A)	450 V (C)
V_{DDIN}	1.65 kV (A)	1.05 kV (E)
$V_{DDFLASH}$	Not Applicable	250 V (D)
V_{DDCORE}	250 V (B)	250 V (B)
V_{DDPLL}	550 V (C)	1.45 kV (C)

at the same value after power cycling. The SAM7 was permanently degraded (E), as shown in Fig. 8, and had to be replaced by a new IC for subsequent tests, since it was not even possible to reprogram its Flash memory.

The sole matching results for both μCs were obtained when EFT was injected into the V_{DDCORE}. In that context:

- the DC power supply connected to the EFT generator was adjusted so that the V_{DDCORE} pin was supplied with 1.8 V
- the internal 1.8 V regulator was powered from the secondary power supply channel connected to all 3.3 V pins, and its output was connected to the V_{DDPLL} pin

This pin was susceptible to EFT on both SAM3 and SAM7. As displayed in Fig. 9, a self-recovering (B) failure was encountered by both μCs at 250 V, with no sudden change in current.

The V_{DDPLL} pins were tested using a similar procedure as

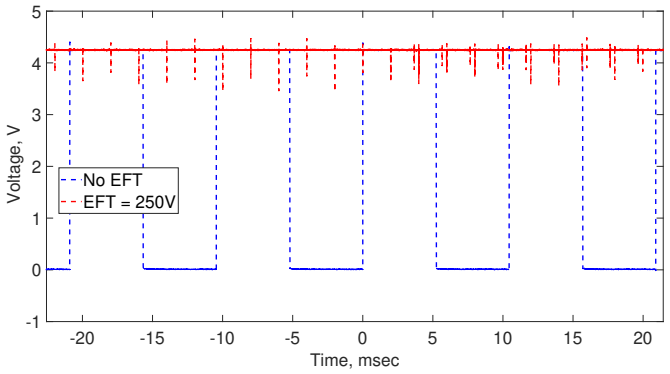
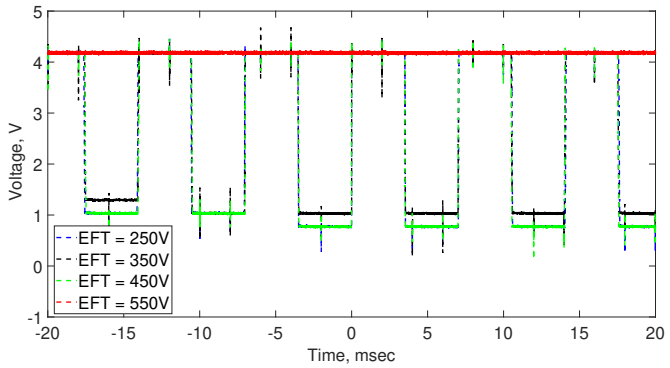
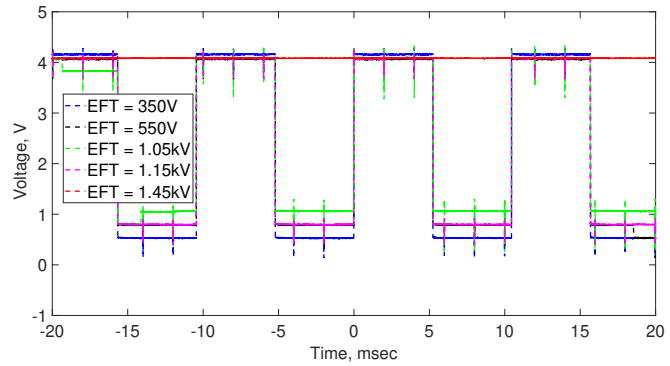


Fig. 9. Output of SAM3 after EFT injection to V_{DDCORE} (Matching results with the SAM7 V_{DDCORE}).



(a)



(b)

Fig. 10. EFT applied to V_{DDPLL} : (a) SAM3 ; (b) SAM7.

above. The SAM7 PLL was more immune (1.45 kV) to EFT than that of SAM3 (550 V). Those results are compared in Fig. 10.

All the mentioned experimental EFT failure voltages and their respective pins are summarized in Table II. To sum up, the SAM3 μC is generally more immune to EFT than the SAM7, except on the V_{DDPLL} pin where a significantly lower EFT voltage triggers a recoverable failure (550 V compared to 1.45 kV). note that all those results were verified to be repeatable, even when SAM7 was changed due to permanent damage after V_{DDIN} injection.

B. Discussion

Both SAM3 main supplies (V_{DDIO} and V_{DDIN}) were immune to EFT up to the limit (1.65 kV) determined by a change in DC current. However, this was not the case for SAM7. With only global injection results, that failure could be attributed to almost any block of the SAM7.

It was later verified that the main supply failure (D) was due to $V_{DDFLASH}$, since equivalent results were obtained for the same voltage when that pin was subjected to EFT, while all other power pins were susceptible to higher voltages. As mentioned earlier, only the SAM7 Flash memory is susceptible to such a level. This can be corroborated by the type of failure, which suggests a defect in the operation of the Flash controller.

The V_{DDIO} of SAM7 was shown to be more susceptible to EFT when compared to that of SAM3. The root cause (still to be confirmed) may be a defect in the port controller or the buffers themselves. It can be noted that V_{DDIO} is a dual-range (1.65 V to 1.95 V, or 3.0 V to 3.6 V) power supply, which might make the port architecture more complex and, possibly, less immune than the wide-range (1.62 V to 3.6 V) supply used in the SAM3. As far as V_{DDIN} is concerned, the probable cause for the SAM7 failure could be due to the internal regulator or the input clamp being destroyed, leading to a permanent high current and an unusable chip.

The B-type failures noticed for the V_{DDCORE} of both SAM3 and SAM7 are likely due to the brown-out detector (BOD) block, which monitors only V_{DDCORE}, being triggered and holding the cores under RESET until the disturbance stops (that would explain how two different cores have the same behavior despite different internal architectures). This could be confirmed by examining, by software, registers containing the latest RESET source of the μC, making it also possible to design specific defensive software capable of recovering from soft failures.

Finally, it can be observed that the PLL of the SAM3 is less immune than that of the SAM7. In both cases, a C-type failure is triggered. It can be noted that the cores enter an idle state when a clock failure is monitored, from which is it possible to exit through a hardware RESET. This is consistent with the observed type of failure. As mentioned in Section II-A, a visible difference between both μCs is the inclusion of the PLL loop filter in the SAM3. This might explain the difference in immunity, since the EFT disturbance could be attenuated by the package parasitics of the loop filter pin driving the external RC filter of the SAM7.

IV. EMC Risk Assessment

From the above obtained results, it can be concluded that replacing a SAM7 μC by a pin-compatible SAM3 μC can result in a better EFT immunity, except for the PLL. This highlights the need for a detailed EMC study when dealing with obsolescence, since a more recent IC does not necessarily mean a higher immunity. It can be noted, as expected, that very simple EMC measurements in the linear operating region of the IC do not provide significant hints about the expected EMC behavior of an IC to transient disturbances. For example,

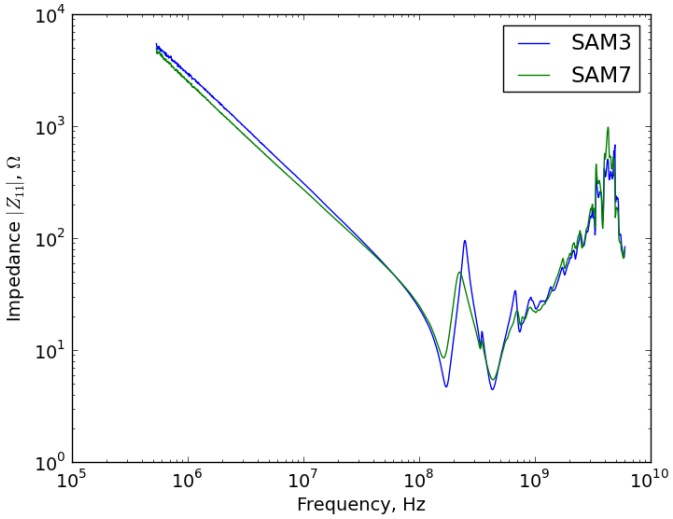


Fig. 11. Input impedance Z_{11} of V_{DDPLL} for SAM3 and SAM7.

Fig. 11 plots the magnitude of the input impedance (Z_{11}) of both V_{DDPLL} pins, extracted from S-parameter measurements with a vector network analyzer. It can be seen that impedance profiles are very comparable, whereas immunity levels are not. This calls for the implementation of extensive EMC testing and/or modeling to verify the compliance of possible replacement ICs compared to existing ones; this has already been corroborated in [13] for memories subject to CW injection.

The use of non-linear transient immunity models such as ICIM-CPI (Integrated Circuit Immunity Model - Conducted Pulse Immunity) [14] can be a valuable help to the simulation of EMC risk assessment for whole PCBs and/or systems. However, at the time being, they still do not take into account the evolution of immunity parameters as functions of ageing and/or obsolescence.

V. Conclusion

A comparative study was conducted between two pin-compatible SAM3 and SAM7 μCs, the former being a more recent version suitable for upgrade, to investigate the EFT immunity of their individual voltage supply pins. The μC crash was considered as the immunity criterion to monitor the failure due to the injected EFT bursts with respect to the IEC 61000-4-4 standard. A customized optoisolation board was used to avoid reinjection of high-voltage EFT signals into the oscilloscope. Results show that, except for the PLL supply pin, SAM3 had higher EFT immunity compared to SAM7 on all the considered supply pins. The core supply pin was found to be the least immune to EFT injection in both μCs (except for the Flash supply pin which is present only on SAM7). Moreover, regardless of the failure type, the obtained results were verified to be entirely reproducible. These results clearly demonstrated that a more modern version of a μC does not necessarily ensure a higher EFT immunity and further EMC analyses are to be performed, particularly when dealing with obsolescence. Non-linear transient immunity models as functions of ageing and/or obsolescence (such as ICIM-CPI) can be put into perspective. Moreover, an improvement of a μC robustness may also be achieved through specific software designed to recover from soft failures.

Acknowledgment

The authors would like to cordially thank J.-L. Levant from Microchip France for the fruitful discussions.

References

[1] Deutschmann. Bernd, Winkler. Gunter, and Bauer. Susanne, "Prediction of the robustness of integrated circuits against EFT/BURST," *IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pp. 45-49, 2015.

[2] M. Ramdani, E. Sicard, A. Boyer, J.J. Whalen, T.H. Hubing, M. Coenen, and O. Wada, "The electromagnetic compatibility of integrated circuits — Past, present, and future", *IEEE Trans. Electromagnetic Compatibility*, vol. 51, no. 1, pp. 78-100, 2009.

[3] IEC 61000-4-4, Electromagnetic Compatibility (EMC)-Part 4-4: Testing and measurement techniques - electrical fast transient/burst immunity test. standard, International Electro-technical Commission, 2012.

[4] J. Wu, Y. Li, H. Zhang, H. Li, A. Zhang and P. Wang, "Impulse immunity of interfaces between intelligent media processors and DDR3 SDRAM memory," 2019 *12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo)*, Hangzhou, China, pp. 150-152, 2019.

[5] B. Li, et al., "Investigations on the EFT immunity of microcontrollers with different architectures", *Microelectronics and reliability.*, vol. 76, pp. 708-713, 2017.

[6] C. Li, et al., "Microcontroller susceptibility variations to EFT burst during accelerated aging," *Microelectronics and reliability.*, vol. 64, pp. 210-214, 2016.

[7] L. Jiancheng, W. Jianfei, W. Chunming, "Investigation of reproducibility and repeatability issue on EFT test at IC Level to microcontrollers," *Computer Engineering Technology 17th National Conf.*, NCCET 2013, Xining, China, July 20-22, 2013. Revised Selected Papers, First edition., vol. 396, pp. 171-179, 2013.

[8] C. Leveugle and T. Weyl "Implementation methodology of industrial and automotive ESD, EFT and surge generator models which predict EMC robustness on ICs and systems," *Electrical Overstress/Electrostatic Discharge Symposium proceedings*, 2017.

[9] Microchip AT91SAM7S256 datasheet. [Online] Available: https://www.microchip.com/www.products/en/AT91sam7s256

[10] Microchip ATSAM3S4B datasheet. [Online] Available: http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-6500-32-bit-Cortex-M3-Microcontroller-SAM3S4-SAM3S2-SAM3S1_Datasheet.pdf

[11] IEC 62132-2: Integrated circuits, measurement of electromagnetic immunity, 150 kHz to 1 GHz, Measurement of radiated immunity - TEM cell and wideband TEM cell method, 2010.

[12] User Manual IMU4000. [Online] http://www.eltest.hu/pdf/IMU4000.pdf.

[13] M. Amellal, M. Ramdani, R. Perdriau, M. Medina, M. Drissi and A. Ahaitouf, "The conducted immunity of SPI EEPROM memories," *2013 International Symposium on Electromagnetic Compatibility*, Brugge, pp. 926-930, 2013.

[14] P. Fernandez-Lopez, Ch. Marot, "Introducing ICIM-CPI model the IC immunity to conducted pulses," *EMC Europe*, 2017. [Online] https://hal.archives-ouvertes.fr/hal-01598946.