Hindawi
Scientific Programming
Volume 2022, Article ID 9790327, 1 page
https://doi.org/10.1155/2022/9790327

Retraction

Retracted: Research on Analysis and Classification of Vulnerability of Electromagnetic Pulse with a STM32 Single-Chip Microcomputer

Scientific Programming

Received 7 April 2022; Accepted 7 April 2022; Published 7 June 2022

Scientific Programming has retracted the article titled "Research on Analysis and Classification of Vulnerability of Electromagnetic Pulse with a STM32 Single-Chip Microcomputer" [1], due to concerns with the authenticity of the data. It was found that previous versions of this submission contained a figure unrelated to the topic of the paper and this graph was subsequently identified within several other submissions, all with accompanying text claiming to have generated the graph. A number of these submissions were rejected from the journal; however, 6 were published and have now been retracted from *Security and Communication Networks* and *Scientific Programming* [2–6].

The authors responded to explain that an author from one of the identified submissions had provided copy editing for their manuscript and introduced the graph and accompanying text in error.

The authors were unable to provide copies of correspondence to support their claim or the raw data from their study. The authors' explanation did not satisfy the concerns of the editorial board, and the article is therefore being retracted due to concerns with the reliability of the data.

The authors do not agree to the retraction.

References

[1] L. Keshun, Z. Xijun, and Z. Xing, "Research on Analysis and Classification of Vulnerability of Electromagnetic Pulse with a STM32 Single-Chip Microcomputer," *Scientific Programming*, vol. 2021, Article ID 6836158, 10 pages, 2021.

[2] L. Zhuang, Y. Qi, and F. Zhang, "Braking Control System of Oilfield Minor Repair Machine Based on Wireless Sensor Network," *Security and Communication Networks*, vol. 2021, Article ID 6966041, 14 pages, 2021.

[3] L. Huo, "Intelligent Recognition Method of Vehicle Path with Time Window Based on Genetic Algorithm," *Security and Communication Networks*, vol. 2021, Article ID 3614291, 11 pages, 2021.

[4] L. Fan, M. Xia, P. Huang, and J. Hu, "Research on Educational Information Platform Based on Cloud Computing," *Security and Communication Networks*, vol. 2021, Article ID 3109473, 11 pages, 2021.

[5] L. Yan, "Research on Crude Oil Trade Procurement Model Based on DEA-Malmquist Algorithm," *Scientific Programming*, vol. 2021, Article ID 6360439, 10 pages, 2021.

[6] G. Yin, R. Qi, J. Zhao, X. Zhao, and J. Xu, "Optimization Method of Sports Service Network Node Layout Based on Network Communication," *Security and Communication Networks*, vol. 2021, Article ID 3013135, 8 pages, 2021.

Hindawi
Scientific Programming
Volume 2021, Article ID 6836158, 10 pages
https://doi.org/10.1155/2021/6836158

Research Article

Research on Analysis and Classification of Vulnerability of Electromagnetic Pulse with a STM32 Single-Chip Microcomputer

Liu Keshun, Zhang Xijun, and Zhou Xing

Army Engineering University, Shijiazhuang Campus, National Key Laboratory on Electromagnetic Environment Effects, Shijiazhuang, Hebei 050003, China

Correspondence should be addressed to Zhou Xing; 720414@hebtu.edu.cn

Received 23 June 2021; Revised 27 July 2021; Accepted 2 August 2021; Published 9 August 2021

Academic Editor: Muhammad Usman

With the continuous development of information technology, the performance of the entire traditional electrical system is gradually optimized. Nowadays, the single-chip technology is an important part of the traditional electrical system because it determines the operating quality of the entire traditional system. However, due to the electromagnetic pulse, the single-chip microcomputer system may be interfered with malfunction or damage, which seriously affects its performance. Therefore, to investigate the impact of an electromagnetic pulse on a single-chip microcomputer system, in this research work, we have used a STM32 single-chip microcomputer as the research object by setting up multiple sets of STM32 single-chip microcomputer serial communication systems. Besides, we have conducted an electromagnetic pulse vulnerability experiment using the inductive coupling inject method which has improved the antielectromagnetic pulse capacity of the STM32 single-chip serial communication system. The experimental results show that the damage threshold of the single-chip microcomputer with positive pulse injection is greater than the negative pulse injection, which indicates that the serial communication system of the STM32 single-chip microcomputer is more sensitive to the negative pulse injection. Moreover, this research work is of great significance to evaluate more accurately the viability and anti-interference capability of a single-chip microcomputer system under the action of electromagnetic pulse.

1. Introduction

Modern electronic systems must be highly resistant to a variety of electromagnetic interruptions to avoid faults that could have unintended repercussions if the system's functionality is important to security [1]. As a result, understanding the system's immunity is crucial. An electromagnetic pulse (EMP) is a high-frequency transient burst of electromagnetic energy that generates a significant electric field due to the rapid acceleration of energetic particles, either naturally or artificially produced. Lightning is a natural form of EMP that occurs when the atmosphere is filled with excessively charged particles, whereas an EMP generator is used to produce a constructed or intentional electromagnetic pulse. Electromagnetic pulse energy frequencies range from zero hertz to gigahertz (GHz) [2] and can be communicated by a magnetic field, electrical field, electrical conduction, and electromagnetic conduction, based on the variety of the pulse. On the other hand, STM32 single-chip microcomputer refers to the 32 bit microcomputer developed by STMicroelectronics in recent years. It has been widely used in automatic navigation system, intelligent communication equipment, and other fields by its diversified functional structure, high-cost performance, and easy-to-use operation mode. Electromagnetic pulse is everywhere, with the high integration of single-chip microcomputer systems; electromagnetic pulse has posed a dangerous threat to single-chip microcomputer systems. On the one hand, an electromagnetic pulse can make the chip of a single-chip microcomputer system produce logical chaos, leading to the system abnormal or failure, causing soft damage. On the other hand, an electromagnetic pulse can cause logical chaos in the chip of a single-chip microcomputer system by causing soft damage, while, on the contrary,

an electromagnetic pulse can damage or burn the components and microelectronic circuits of a single-chip microcomputer system, causing hardware damage, so it is important to study the subject. Since the beginning of this century, domestic researchers have carried out a lot of work [3–5] on the effect and vulnerability of electromagnetic pulse to single-chip microcomputer systems and analyzed the reasons of various effect phenomena to some extent. However, the existing research is mainly to classify single-chip microcomputer systems whether there is damage or not and does not classify the vulnerability levels for various effect phenomena. Moreover, due to high test costs and limited data, it is impossible to determine the statistical law of vulnerability for various effect phenomena.

Inspired from the work of the above, this paper used the same batch of STM32 single-chip microcomputers with the following contributions:

(i) To conduct an electromagnetic pulse vulnerability experiment by inductive coupling injection.

(ii) To investigate/analyze the level of electromagnetic pulse vulnerability.

(iii) To carry out the electromagnetic pulse vulnerability experiment of STM32 single-chip microcomputer under the condition of pulse current inductive coupling injection.

(iv) To explore the influence of different factors on vulnerability experiments, we have set up a variety of control groups.

(v) To improve the antielectromagnetic pulse capacity of the STM32 single-chip serial communication system, we have used a shielded line as the serial communication line.

(vi) To investigate the sensitivity of the serial communication system of STM32 single-chip microcomputer, either it is more sensitive to the negative pulse injection or not.

The rest of the paper is organized as follows. Section 2 represents materials and methodology that we have adopted during our work, Section 3 shows the experimental work, and Section 4 illustrates the simulation results and experimental analysis. We conclude our paper in Section 5.

2. Materials and Methodology

In this section, we will discuss the materials and methodology employed in our suggested strategy for analyzing and classifying the vulnerability of electromagnetic pulses with an STM32 single-chip microcontroller in this part.

2.1. Materials

2.1.1. Electromagnetic Pulse (EMP). A high-concentration blast of electromagnetic energy created by the rapid speed of charged particles is known as an electromagnetic pulse (EMP). As a result of this huge EM energy, our electrical network, communication networks, and computer systems may be destroyed. A short, high-intensity pulse with a pulse width measured in nanoseconds is referred to as transient electromagnetic energy. Such pulses can be emitted as an electric or magnetic field as a result of natural or man-made causes [6].

2.1.2. Types of Electromagnetic Pulse. An EM pulse is a short-duration pulse of energy, which can be produced by a variety of sources including natural, man-made, and military weaponry. All of these sources produce pulse trains that are recurrent and regular. Types of electromagnetic pulse are shown in Figure 1.

(1) *Natural EM Pulse*. LEMP (lightning electromagnetic pulse) is the most common natural source of EM radiation. LEMP can generate massive currents of a few mega-amps, which can cause injury in man-made electronic circuits and electronic systems [5]. ESD is another natural EM source. Interaction and separation of 2 charged objects cause electrostatic discharge (ESD). By sending a high voltage pulse into an electrical circuit, ESD can cause damage [7, 8].

(2) *Man-Made EM Pulse*. Man-made EM radiation is much more detrimental to our health than natural EM radiation. Cooking appliances, televisions, radios, cell phones, and electrical power connections are all sources of man-made electromagnetic radiation. A train of pulses can be generated by the switching action of digital electronic circuitry as well as the internal electrical contact spinning of electrical motors [9]. Electric power lines carry many kilovolts of power, which is powerful enough to kill electronic devices and circuits that are not safeguarded sufficiently.

(3) *Military EM Pulse*. A nuclear detonation in the atmosphere releases gamma rays from the nuclear reaction with a rising time of nanoseconds, resulting in a nuclear electromagnetic pulse (NEMP) [10–12]. These gamma rays cause a flux of Compton scattering returning electrons in the atmosphere, resulting in an electric current concentration. This pulse or EM radiation can have an impact on our electrical system, as well as the sea and air. Nuclear EMPs are categorized into three parts E1, E2, and E3. E1 is the quickest of all electromagnetic elements, with temporal durations ranging from microseconds to nanoseconds. E1 is a powerful electric field capable of rapidly producing an exceptionally high voltage in electrical conductors, destroying our electrical system, computers, and communication devices. The E2 component of an electromagnetic pulse is slower than the E1 part. E2 elements have properties that are identical to lightning electromagnetic pulses, making them the easiest to defend against. Across all electromagnetic components, the E3 element is the slowest [13–16]. The Sun produces this type of pulse.

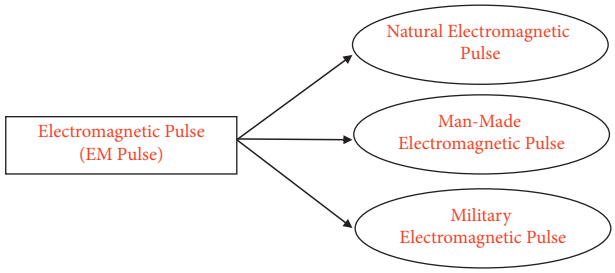


Figure 1: Types of electromagnetic pulse.

2.1.3. Effect of EMP on Electronic Circuits. An EMP (electromagnetic pulse) is a burst of energy that damages electronic circuits. EM weapons can generate a pulse of energy, which can destroy electronic systems. There are two sorts of coupling modes that can occur:

(i) Front door coupling: EMP interacts with a front-end digital equipment such as antennas in this type of coupling and destroys semiconductor devices in transmission lines such as receivers and transmitters [17].

(ii) Back door coupling: back door coupling occurs when an EMP interacts with back-end electronic apparatus via data, wire, and power connections, causing damage to transmission devices such as power supply, data transmitters, and receivers.

Any electromagnetic pulse's primary target is semiconductor devices. Breakdown happens in BJT devices when the junction is reverse biased as a result of the EM pulse. Thermal damage to the PN junction is another impact of the EM pulse. The EM pulse causes very strong electric fields to gust through the gate dielectric in field-effect transistors devices like MOSFET. The waveform of a mixture of pulses depicts how the electromagnetic field's intensity or current changes over time. Pulses have a strong leading edge and rapidly reach their maximum level [18]. EMP energy passes through the cables and circuitry of electronic equipment. In sophisticated systems with more wiring, energy is gathered more efficiently. In a matter of nanoseconds, the EMP blasts up to 50,000 volts of energy into electrical circuits [19]. This pulse completely melts modern computer CPUs.

2.1.4. STM32 Single-Chip Microcomputer. STM32 is a STMicroelectronics series of 32 bit microcontroller integrated circuits. Each microcontroller has a processing core, static RAM, flash memory, a debugging connection, and different peripherals on the inside [20]. The STM32 microprocessor group comprises 14 series, each of which is based on an ARM Cortex-M7F, Cortex-M4F, Cortex-M33, Cortex-M3, Cortex-M0+, or Cortex-M0 processing core. Abstractly, the Cortex-M4F is a Cortex-M3 with DSP and single-precision floating-point instructions [21, 22].

2.2. Methodology

2.2.1. Hardware Circuit. The power supply component, the main control part, and the communication part are the three main problems of the control system's hardware circuit [18]. Through the USB charger, the main supply component (220v) is connected to the USB port. The suggested system's main control element is in charge of the tiny microcomputer's control signal. STM32F103RCT6 Chip and STM32F103RCT6 Chip are linked via USB ports. Serial port communication is used in the communication component, which connects the USART serial port to RS232.

To conduct an electromagnetic pulse vulnerability experiment, we have selected the same batch of two STM32 microcomputers to build a set of serial communication systems. The microcomputer without an LCD (liquid crystal display) is used as the sending end and its TX pin circularly sends 8 bit binary data 00000000 to 11111111. The microcomputer with an LCD is used as the receiving end, where the data are received by its RX pin. This data will be displayed on the 2.8-inch LCD in a cycle from 0 to 255 decimal data. This system is mainly composed of an STM32-F103MINI microcomputer, STM32F103RCT6 chip, 2.8-inch LCD, USB charger, and data line (serial communication line and ground electrode), as shown in Figure 2.

2.2.2. Vulnerability. Vulnerability is a flaw in a computing device used by an attacker, such as a hacker, to break privilege boundaries. An attacker must have at least one tool or technique, which can connect to a system flaw to exploit the vulnerability. Vulnerabilities are sometimes referred to as security vulnerabilities in this context. Computer security vulnerabilities can broadly be divided into the following 4 categories [23]:

(i) *Network Vulnerabilities.* These are flaws in a network's software or hardware that make it vulnerable to outside infiltration. Examples are Wi-Fi gateways that are not secure and firewalls that are not set up properly.

(ii) *Operating System Vulnerabilities.* These are flaws in a specific operating system that hackers can use to obtain entry to or destroy an asset that the OS is installed on. Examples are default super user accounts, which may exist in some OS installations and hidden backdoor applications.

(iii) *Human Vulnerabilities.* The human factor is the weakest link in so many cyber-security systems. User errors can readily expose sensitive data, provide hackers with exploitable entry points, or cause systems to malfunction.

(iv) *Process Vulnerabilities.* Process design constraints can cause some vulnerability. The usage of weak passwords is an example of this kind of vulnerability.

Major types of vulnerabilities are shown in Figure 3.

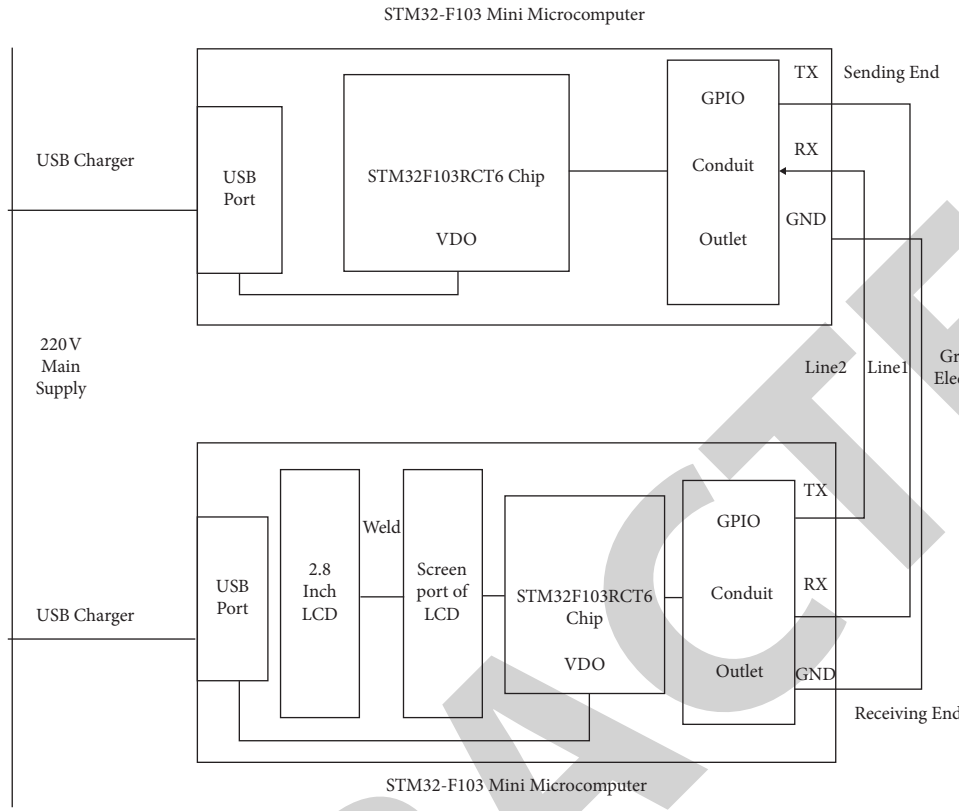


Figure 2: Composition of the serial communication system.

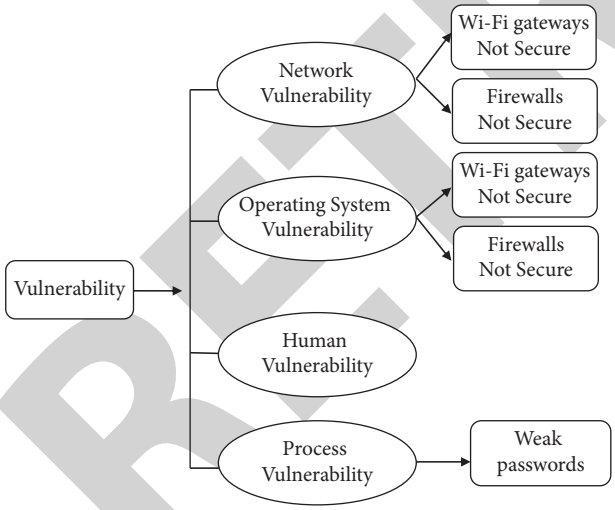


Figure 3: Major types of vulnerabilities.

2.2.3. Levels of Vulnerability. The effect of injection pulse current of different intensities on STM32 microcomputers is varied. We have combined the results of the electromagnetic pulse vulnerability experiment of the STM32 single-chip microcomputer to check whether the working state of the STM32 single-chip microcomputer is normal and serial communication function is changed [24]. This paper divided the experiment phenomena into three vulnerability levels of interference, failure, and damage, as shown in Figure 4 to analyze the vulnerability reasons:

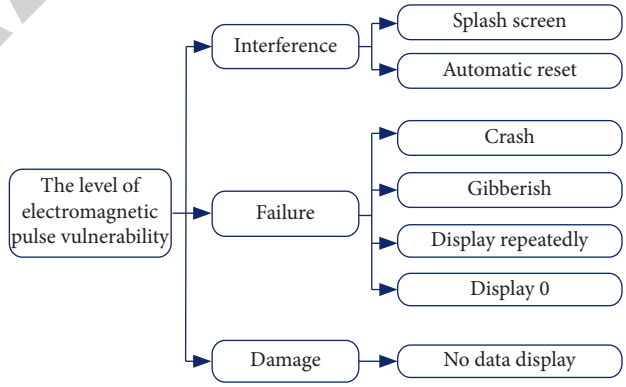


Figure 4: The level of electromagnetic pulse vulnerability.

(1) Interference: under the action of pulse current injection, the serial communication of the STM32 single-chip microcomputer failed to work properly within a short period. However, the serial communication returned to normal by itself after pulse current injection, and such a short-time disorder did not affect the normal working function of serial communication. Therefore, the STM32 single-chip microcomputer is said to be "interference" under the injected energy intensity.

(2) Failure: under the action of pulse current injection, the serial communication of STM32 single-chip microcomputer could not work normally, but the working state could be restored after manual button

reset or repowering; then, the STM32 single-chip microcomputer is said to be "failure" under the injected energy intensity.

(3) Damage: under the action of pulse current injection, the serial communication of STM32 single-chip microcomputer stopped working, and it still stopped working after manual button reset and repowering. Only replacing the new STM32 single-chip microcomputer or serial communication pin can restore its normal working function, and then the STM32 single-chip microcomputer is said to be "damage" under the injected energy intensity [25].

3. Experimental Work and Results

In this section, we discuss our experimental work for our proposed scheme and then explain its results in detail.

3.1. Conditions of the Experiment. The electromagnetic pulse vulnerability experiment of the STM32 single-chip microcomputer is carried out under the condition of pulse current inductive coupling injection. The INS4040 high-frequency noise generator, 9142-1N current injection probe, 9123-1N current monitoring probe, 30 dB pulse attenuator, and Agilent oscilloscope are the major components of the current injection equipment, which can generate square wave pulses with amplitude values of 0.01–4 kV. The square wave pulse is injected into the data line via inductive coupling using calibrated 9142-1N current injection probe, and the 9123-1N current monitoring probe is used to monitor the pulse current on the data line in real-time and is connected to the Agilent oscilloscope through the pulse attenuator, as shown in Figure 5.

In the experiment, when the experiment conditions remain unchanged and the injection pulse amplitudes are all 400 V, the inductive coupling injection is carried out for different data line combinations in turn. The typical pulse waveform observed on the Agilent oscilloscope is shown in Figure 6.

3.2. Results of Experimental Work. According to GJB548B-2005 Test Methods and Procedures for Microelectronic Device [26], the stepwise method was adopted. First, the pulse width was kept unchanged. Then, the single injection was carried out from 0.1 kV with the step value of 0.01 kV in turn. In order to prevent the cumulative effect which could cause errors in the experiment results, the time interval of each injection should be greater than 15 s [27]. Finally, since STM32 single-chip microcomputer has realized serial communication normally, the amplitude of injected pulse was recorded when the experiment phenomena occurred every time and stopped the experiment until the STM32 single-chip microcomputer could not work normally by the ways of manual button reset and repowering. If the serial communication of STM32 microcomputer stopped working when the pulse current was injected for the first time, it was judged that the experimental data were invalid [28]. It was necessary to check whether the STM32 microcomputer was in a normal state and replace the STM32 microcomputer to start the experiment again [29].

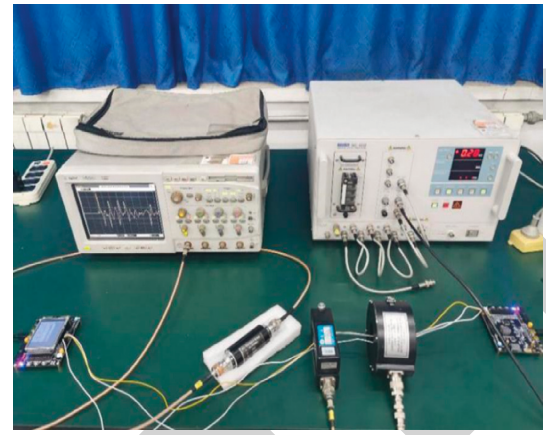


Figure 5: Layout of experiment equipment.

Through the experiment, it could be found that different experiment conditions and different batches of STM32 microcomputer could obtain different experiment phenomena and threshold data which reach these phenomena. The experiment phenomena of electromagnetic pulse vulnerability of STM32 microcomputer were as follows:

(1) After the pulse current was injected, the serial communication could be restored to normal by itself; the LCD screen would cause the phenomena of splash screen and automatic reset.

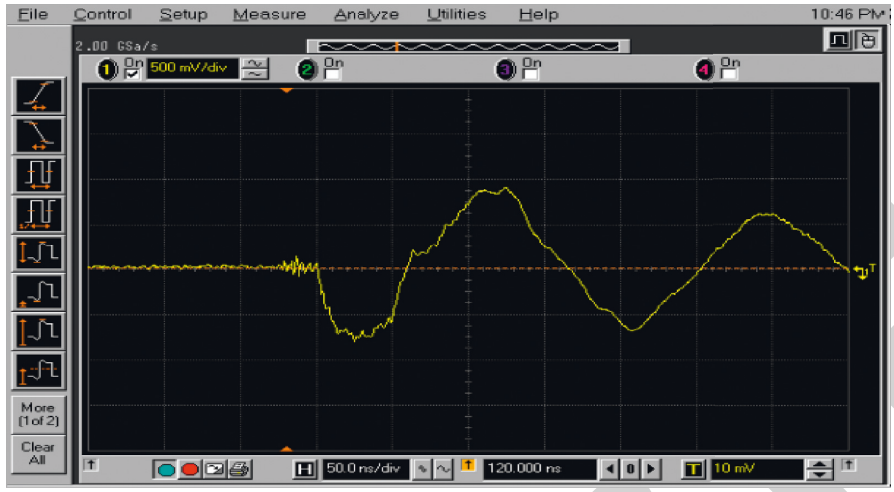
(2) After the pulse current was injected, the serial communication could be restored to normal only by manual button reset or repowering; the LCD screen would cause the phenomena of crash, gibberish, display repeatedly, and display 0.

(3) After the pulse current was injected, the serial communication still stopped working by manual button reset and repowering; the LCD screen would cause the phenomenon of no data display.

Several control groups were set up to explore the influence of injection mode, materials of serial communication lines, and injection location and injection polarity on vulnerability experiment phenomena and threshold data. Under the condition that other factors remained unchanged, the injection mode could be divided into six situations as injecting serial communication line 1, injecting serial communication line 2 and so on; the materials of serial communication lines could be divided into shielded line, unshielded line, and DuPont line; the injection location was respectively set at 25 cm, 50 cm, and 75 cm from the sending end; and the injection polarity could be divided into positive pulse injection and negative pulse injection. Twenty sample sizes were selected for each condition, and the experimental results are shown in Tables 1–4.

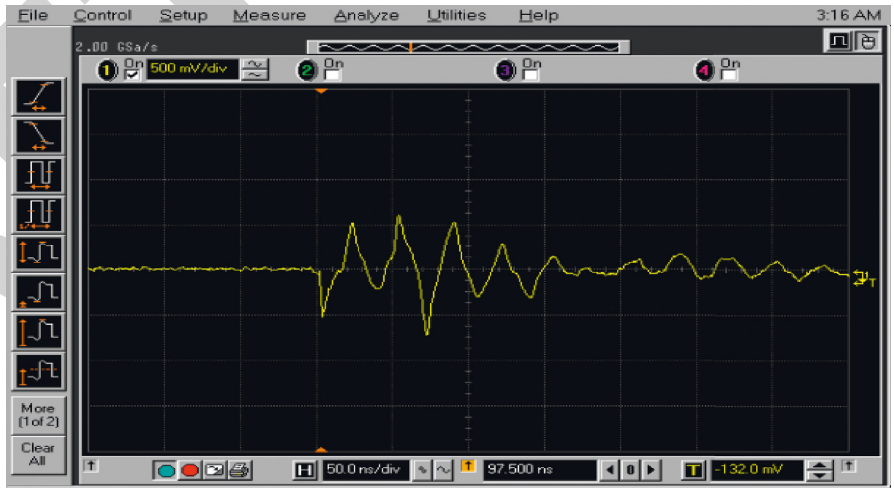
4. Analysis of Vulnerability

Electromagnetic vulnerability refers to the characteristic that the system, equipment, or device degrades the performance or fails to complete the specified task under the influence of



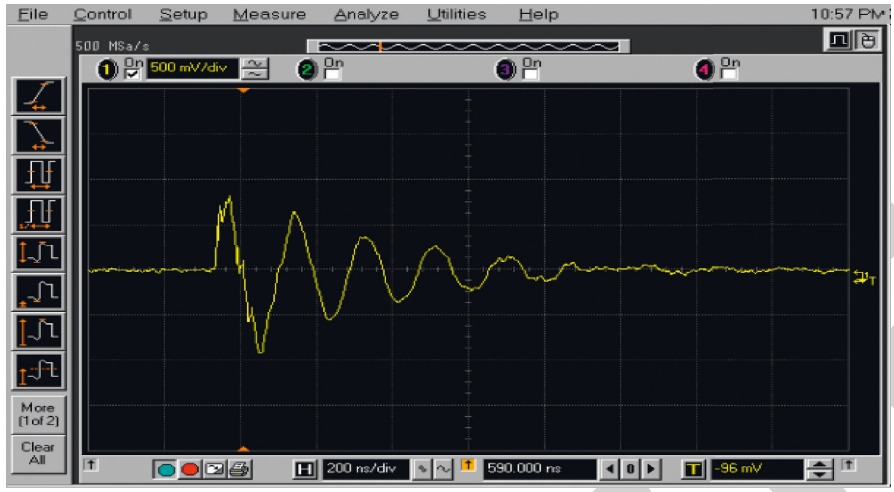
(a)

(b)



(c)

Figure 6: Continued.



(d)

Figure 6: Typical pulse waveform after inductive coupling injection. (a) Injection of single serial communication line. (b) Injection of two serial communication lines. (c) Injection of single serial communication line and ground electrode. (d) Injection of two serial communication lines and ground electrode.

Table 1: Influence of injection mode on experiment results (kV).

Experiment phenomena	Line 1	Line 2	Lines 1 and 2	Line 1 and ground	Line 2 and ground	Lines 1 and 2 and ground
No	0.10–0.31	0.10–0.28	0.10–0.18	0.10–0.20	0.10–0.15	0.10–2.00
Splash	0.32–0.79	0.29–0.46	0.19–0.31	0.21–0.45	0.16–0.30	*
Reset	*	*	0.32–0.42	*	0.31–0.40	*
Repeat	*	*	0.43–0.62	*	0.41–0.53	2.01–2.67
Display 0	0.80–1.26	*	0.63–0.73	0.46–0.78	0.54–0.63	2.68–3.32
Gibberish	*	0.47–0.53	*	*	*	*
No display	1.27	0.54	0.74	0.79	0.64	3.33

Table 2: Influence of the materials of serial communication lines on experiment results (kV).

Experiment phenomena	Shielded line	Unshielded line	DuPont line
No	*	0.10–1.69	0.10–2.00
Repeat	*	*	2.01–2.67
Display 0	*	1.70–2.59	2.68–3.32
Gibberish	*	2.60–3.20	*
No display	*	3.21	3.33

Table 3: Influence of injection location on experiment results (kV).

Experiment phenomena	25 cm	50 cm	75 cm
No	0.10–0.57	0.10–0.41	0.10–0.42
Repeat	*	0.42–0.79	*
Display 0	*	*	0.43–0.78
Gibberish	0.58–0.78	*	*
Crash	0.79–0.83	0.80–0.83	0.79–0.82
No display	0.84	0.84	0.83

electromagnetic interference [30]. The vulnerability process of an electromagnetic pulse to an STM32 microcomputer can be divided into three stages: penetration, transmission, and damage. Electromagnetic pulse penetrates STM32 microcomputer through the long-distance by using serial communication cable. Its energy becomes large currents and

Table 4: Influence of injection polarity on experiment results (kV).

Injection mode	Line 1	Line 2	Lines 1 and 2	Line 1 and ground	Line 2 and ground	Lines 1 and 2 and ground
Positive	1.32–1.37	1.03–1.09	0.81–0.85	1.02–1.07	0.82–0.86	3.92–3.97
Negative	1.27–1.29	0.52–0.55	0.70–0.78	0.76–0.79	0.46–0.54	3.31–3.34

voltages that vary with time and space and then in the form of large current, large voltage transmission to the chip, integrated circuit, connection points, and other fragile parts inside STM32 microcomputer, making these parts damage due to high energy density.

Through the experiment, it could be found that except for the serial communication pins of the STM32F103RCT6 chip were damaged; other pins or devices were not damaged. Because the STM32F103RCT6 chip had five groups of serial communication pins, as long as a set of serial communication pins was replaced, serial communication could be continued after burning the program. However, if all of them have been damaged, a new set of STM32 microcomputer serial communication systems should be built for the experiment. Combined with the results of the electromagnetic pulse vulnerability experiment of STM32 single-chip microcomputer, the reasons for vulnerability caused by various experimental phenomena were analyzed:

(1) Splash screen: the coupling current entered into the chip through the GPIO conduit outlet and then reached the 2.8-inch LCD through the screen port of LCD. As a result, the power supply voltage of the 2.8-inch LCD changed instantaneously, which caused the splash screen phenomenon to occur on the 2.8-inch LCD. After the pulse current, the 2.8-inch LCD automatically returned to normal.

(2) Automatic reset: the coupling current entered into the chip through the GPIO conduit outlet, electromagnetic interference appeared on the chip reset pin (NRST), and the interference signal was mistaken for the reset signal, which caused the automatic reset phenomenon to occur on the 2.8-inch LCD. After the pulse current, the 2.8-inch LCD automatically returned to normal.

(3) Crash: the serial data register (USART-DR) was confused by the coupling current and decided to enter into the chip through the GPIO conduit outlet. This caused the last half of the previous data to be executed as the same bit of data as the first half of the next data, resulting in a dead cycle [31], which caused the crash phenomenon on the 2.8-inch LCD. After manually pushing the reset or repowering the device, it would return to normal.

(4) Gibberish: the coupling current entered into the chip through the GPIO conduit outlet and the data contents in the serial data register (USART-DR) would be flipped over so the data become disordered and cause the gibberish phenomenon to occur on the 2.8-inch LCD. It would be restored to normal after manually pressing the button to reset or repowering.

(5) Display repeatedly: the coupling current entered into the chip through the GPIO conduit outlet, the transmission completion bit (TC) of the serial status register (USART-SR) was changed from 1 to 0, and the serial communication program was always in the state of waiting for the completion of transmission, resulting in the interruption of data sending and receiving and causing the display repeated phenomenon to occur on the 2.8-inch LCD. It would be restored to normal after manually pressing the button to reset or repowering.

(6) Display 0: the coupling current entered into the chip through the GPIO conduit outlet, the send break (SBK) of the serial control register (USART-CR1) was changed from 0 to 1, and then the disconnected character was sent. This character was 8 bit low level 00000000, which deemed to receive all zeros in one cycle. Therefore, the display 0 phenomenon occurred on the 2.8-inch LCD. It would be restored to normal after manually pressing the button to reset or repowering.

(7) No data display: the coupling current reached the metal pin of the chip through the GPIO conduit outlet; the metal itself would produce joule heat, especially when the metal was relatively narrow and the temperature was higher. When the temperature rose above the melting point of the metal, the metal pin would overheat and burn out [32] and cause the open circuit between the serial communication pin and the internal lead. Therefore, the serial communication stopped working, and the no-data-display phenomenon occurred on the 2.8-inch LCD. It still stopped working after manually pressing the button to reset and repowering.

According to the three vulnerability levels of interference, failure, and damage, combined with the vulnerability experiment results of the STM32 single-chip microcomputer in Tables 1–4, the threshold range of each vulnerability level is given in these tables. We adopted the Bayesian statistical method and OpenBUGS software based on the Markov chain Monte Carlo method to carry out Gibbs sampling and fitting analysis on the threshold data, and posterior mean value and posterior standard deviation of each vulnerability level were obtained, as shown in Table 5.

Finally, we have obtained the probability of each vulnerability level of STM32 single-chip microcomputer under the action of certain injected energy by using Origin software; the results are shown as in Figure 7.

Table 5: Parameter estimation results of vulnerability level.

Vulnerability level	Range of threshold	Posterior mean value	Posterior standard deviation
Interference	0.16–0.79 kV	0.79	0.35
Failure	0.41–1.26 kV	1.26	0.45
Damage	0.54 kV	1.57	0.54

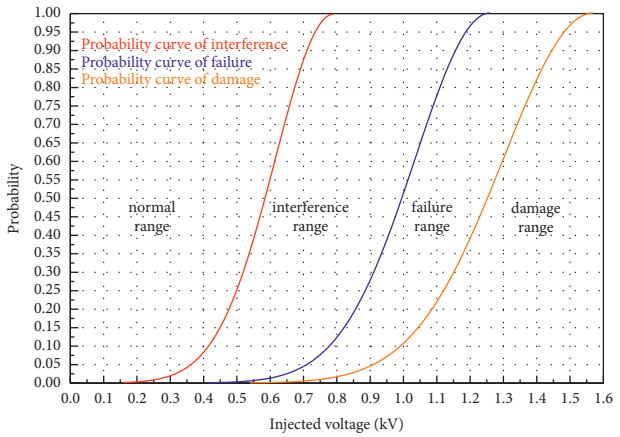


Figure 7: Probability curve of vulnerability level.

5. Conclusions

This research study has investigated the impact of an electromagnetic pulse on a single-chip microcomputer system using the STM32 single-chip microcomputer as the research object. Besides, this work has conducted an electromagnetic pulse vulnerability experiment by using the pulse current injection device of the author's work unit and the inductive coupling injection method, where a variety of control groups were set up to explore the influence of different factors on vulnerability experiment. The results showed that the threshold data of serial communication line 1 were greater than serial communication line 2 and the threshold data of common-mode injection were greater than differential mode injection, which indicated that serial communication line 2 and differential mode injection were more sensitive to pulse current. To improve the anti-electromagnetic pulse capability of the STM32 single-chip microcomputer during serial communication system, the shielded line should be used as the serial communication line. The damage threshold of the single-chip microcomputer with positive pulse injection was greater than the negative pulse injection, which indicated that the serial communication system of the STM32 single-chip microcomputer was more sensitive to the negative pulse injection.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by a project named Inversion of Cloud Flash Discharge Current and Research on Temporal and Spatial Distribution of Electromagnetic Field. Project source is the National Natural Science Foundation of China (Project no. 51707203).

References

[1] X. Li, Q. Wang, X. Zhou, and S. Qin, "The research of electromagnetic conducted coupling in transmission-line networks," in *Proceedings of the 2011 International Conference on Electronics and Optoelectronics*, Dalian, China, July 2011.

[2] S. Q. Zheng, D. Y. Hou, D. D. Wang, and F. Deng, "Electromagnetic pulse protection requirements and test methods for systems," in *Proceedings of the 2012 10th International Symposium on Antennas, Propagation & EM Theory (ISAPE 2012)*, pp. 857–860, Xi'an, China, October 2012.

[3] X. Du, "Study on single-chip microcomputer system under the irradiation effect of strong electromagnetic pulse," *China Science & Technology Panorama Magazine*, vol. 5, no. 17, p. 182, 2011.

[4] M. Hou and J. Wen, "Electromagnetic pulse effect and protection of electronic system," *Space Electronic Countermeasure*, vol. 23, no. 3, pp. 15–17, 2007.

[5] M. Chen, Y. Cheng, W. Wu, J. Li, and B. Li, "Study on simulation experiment of electromagnetic pulse effect on 80C196KC single-chip microcomputer," *Nuclear Electronics & Detection Technology*, vol. 26, no. 3, pp. 364–366, 2006.

[6] D. Wang, Y. Li, P. Dehghanian, and S. Wang, "Power grid resilience to electromagnetic pulse (EMP) disturbances: a literature review," in *Proceedings of the 2019 North American Power Symposium (NAPS)*, Wichita, KS, USA, October 2019.

[7] J.-Y. Lin, W.-J. Dong, C.-M. Zhou, C.-x. Zhang, and J.-F. Ma, "Investigation ofInjury effects to strong electromagnetic pulse onTypical flying control system," in *Proceedings of the 2012 Second International Conference on Instrumentation, Measurement, Computer,Communication and Control (IMCCC)*, Hangzhou, China, December 2012.

[8] Z. L. Tan, Z. Y. Xiang, B. Xu, and P. H. Xie, "Investigation on ESD EMP damage effects of electronic components," in *Proceedings of the 5th Asia Pacific Conference on Environmental Electromagnetics (CEEM 2009)*, pp. 89–92, Xi'an, China, September 2009.

[9] P. H. Ron, "Configurations of intense pulse power systems for generation of intense electromagnetic pulses," in *Proceedings of the International Conference on Electromagnetic Interference and Compatibility'99*, New Delhi, India, December 1999.

[10] S.-q. Zheng, D.-y. Hou, Q.-F. Liu, and F. Deng, "Electromagnetic pulse threats to electronic information system and corresponding protection measures," in *Proceedings of the 2011 IEEE 4th International Symposium on Microwave, Antenna, Propagation, and EMC Technologies for Wireless Communications (MAPE)*, Beijing, China, November 2011.

[11] K.-A. Lee, Y.-M. Cho, and K.-C. Ko, "Circuit models for band pass filter of RF front-end system damaged by high power electromagnetic pulse," in *Proceedings of the 2015 IEEEInternational Conference on Plasma Sciences (ICOPS)*, Antalya, Turkey, May 2015.

[12] A. S. Podgorski, "Composite electromagnetic pulse threat," in *Proceedings of the 1990 IEEE International Symposium on Electromagnetic Compatibility*, Washington, DC, USA, August 1990.

[13] R. Hoad and W. A. Radasky, "Progress in high-altitude electromagnetic pulse (HEMP) standardization," *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 532–538, 2013.

[14] F. Sabath and S. Potthast, "Tolerance values and the confidence level for high-altitude electromagnetic pulse (HEMP) field tests," *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 518–525, 2013.

[15] J. Paasi, J. Smallwood, and H. Salmela, "New methods for the assessment of ESD threats to electronic components," in *Proceedings of the Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD'03)*, Las Vegas, NV, USA, September 2003.

[16] M. Ianoz, "Comparison between high altitudeEMP and high power electromagnetic effects on equipment and systems," in *Proceedings of the 2007 International Symposium on Electromagnetic Compatibility (EMC 2007)*, Qingdao, China, October 2007.

[17] X. Meng, B. Zhou, H. He, and B. Yang, "Experiment study about coupling effect of single chip system under different electromagnetic pulse," in *Proceedings of the 8th International Symposium on Antennas, Propagation and EM Theory (ISAPE 2008)*, Kunming, China, November 2008.

[18] W.-Z. Zhou, J.-X. Wang, X.-X. Liu, and J.-F. Xue, "Implement of electromagnetic pulse effects evaluation of radar system function module," in *Proceedings of the 2010 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR)*, Qingdao, China, July 2010.

[19] X. Chen, Y. Hu, J. Zhang, Y. Huang, and L. He, "The simulation of electromagnetic pulse coupling with computer box," in *Proceedings of the 3rd International Conference on Computational Electromagnetics and its Applications*, Beijing, China, November 2004.

[20] STM32, "STM32 32-bit arm Cortex MCUs," *STMicroelectronics*, 2021, https://www.st.com/en/microcontrollers-microprocessors/stm32-32-bit-arm-cortex-mcus.html.

[21] STM32, "STM32 32-bit arm Cortex MCUs," 2021, https://www.st.com/en/microcontrollers-microprocessors/stm32-32-bit-arm-cortex-mcus.html.

[22] Arm Ltd., "Artificial intelligence enhanced computing," 2021, https://www.arm.com/.

[23] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, "IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges," *IEEE Access*, vol. 8, Article ID 168825, 2020.

[24] L. Hui, "Principle analysis and hardware circuit design of STM32 single-chip microcomputer," *Electronics Test*, vol. 6, no. 14, pp. 26–31, 2018.

[25] H. Gou and G. Liu, "The minimum system based on STM32 and the implementation of serial communication," *Industrial Control Computer*, vol. 25, no. 9, pp. 26–29, 2012.

[26] Gjb548B-2005, *Test Methods and Procedures for Microelectronic Device*, The General Reserve Department of PLA, London, UK, 2005.

[27] Y. Zhou, M. Du, and L. Shi, "Electromagnetic pulse damage threshold and protective measures of EtherCAT equipment port," *High Voltage Technology*, vol. 43, no. 4, pp. 1370–1377, 2017.

[28] X. Chen, B. Sun, S. Liu, and A. Zhai, "Acquisition of electromagnetic pulse damage function of sensitive unit," *Journal of Radio Science*, vol. 25, pp. 154–156, 2010.

[29] F. C., "[iwar] t," 2021, http://all.net/iwar/archive/2002Q2/0233.html.

[30] S. Tang, Y. Zhang, H. Wan et al., *Electromagnetic Environmental Effect Engineering*, National Defense Industry Press, Beijing, China, 2017.

[31] M. Hou and Yu Tian, "Study on the crash failure of computer under electromagnetic pulse," *Space Electronic Countermeasure*, vol. 25, no. 6, pp. 47–49, 2009.

[32] N. Baowei, *Damage Correlation between Different strong Electromagnetic Pulse Parameters and Integrated Circuits*, University of Electronic Science and Technology, Xi'an, China, 2019.