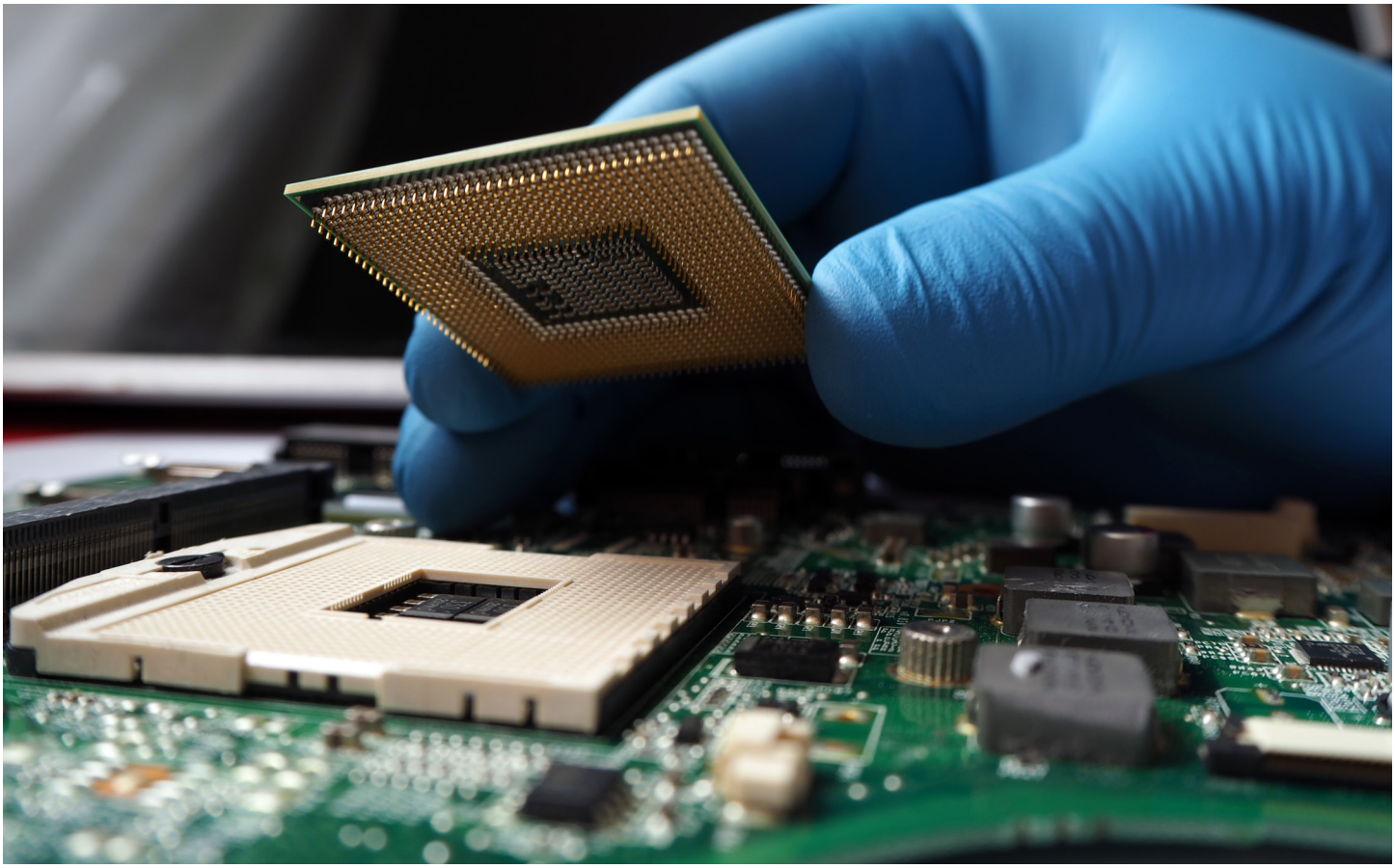
MAXIVOLT
TRANSIENT VOLTAGE SOLUTIONS

TECH NOTES

HOW TRANSIENT OVERVOLTAGE AFFECTS **MICROPROCESSOR LOGIC**



KEY TAKEAWAYS

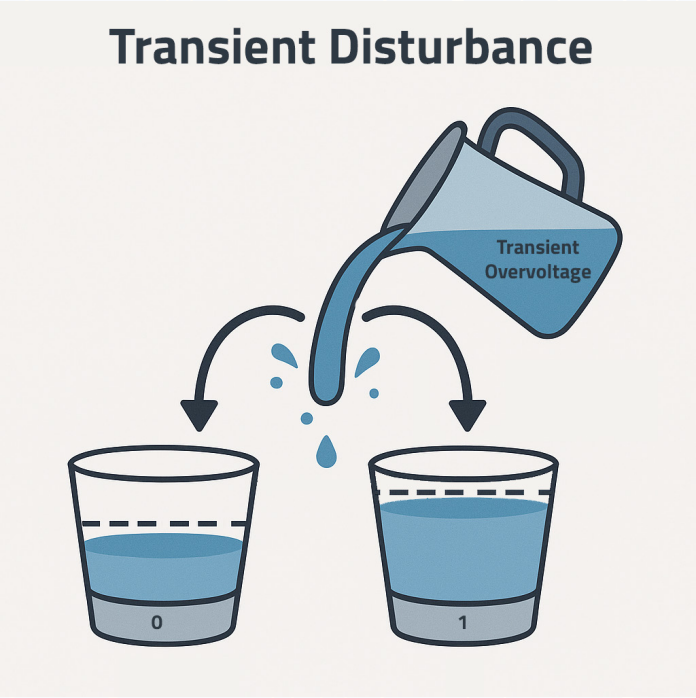
- Transient overvoltage can cause logic faults in microprocessors by flipping bits at critical moments.
- Modern chips are more vulnerable due to lower voltages, smaller geometries, and faster speeds.
- Common faults include bit upsets, latched errors, and I/O disruptions.
- A layered protection strategy is essential for reliable system performance.

INTRODUCTION

Transient overvoltage events—such as lightning, switching surges, or electrostatic discharge (ESD)—introduce brief but disruptive voltage spikes into microprocessors. These transient overvoltages induce logic faults that manifest as unexpected malfunctions or system errors.

HOW TRANSIENT OVERVOLTAGE-INDUCED **LOGIC FAULTS OCCUR**

Microprocessors store each bit of information on tiny circuit nodes whose voltage level encodes the state, a '0' or a '1'. A transient overvoltage event—such as a rapid voltage increase from a lightning flash, a switching transient overvoltage, or an electrostatic discharge (ESD) on a signal line—can momentarily raise or lower the node's voltage by adding (or removing) charge from the capacitance.



If this brief voltage change pushes the node above the logic-high threshold (VIH) or below the logic-low threshold (VIL) exactly when the processor samples it, the stored bit flips unexpectedly, causing a soft error (single-event upset, SEU).

Imagine each logic node as a small cup holding water at a set level: low means '0', high means '1'. Transient overvoltage is like quickly pouring water into the cup (or draining water out as voltage can be both positive and negative). If the water level crosses the 'high' or 'low' mark—even for an instant—the system may misread the bit. That error can then ripple through the processor, leading to corrupted data or erratic behavior.

Transient-induced logic faults can be classified as follows:

- **Upsets:** Large enough to constitute a logic-level error
- **Latched Errors:** Results in errors stored in first-level latches
- **Module Errors:** Causes errors at the input/output (I/O) nodes of functional units
- **Pin Errors:** Propagates errors at the chip's I/O pins

INCREASED VULNERABILITY OF **MODERN MICROPROCESSORS**

Contemporary processors are susceptible to transient overvoltage-induced faults due to a combination of design trends and performance optimizations that reduce tolerance to transient overvoltage:

- **Lower Operating Voltages (<1 V):** As chip designers achieve better energy efficiency and thermal management, operating voltages have dropped dramatically. These lower voltages reduce the safety buffer between logic threshold levels and actual signal levels, making it easier for transient overvoltage to cause a logic-level error.
- **Reduced Node Capacitances:** Advanced semiconductor fabrication processes rely on ever-smaller transistors and interconnects, which inherently reduce capacitance at each node. Since the stored charge (Q = CV) is lower, even a "small" transient overvoltage event can alter the voltage enough to cross logic thresholds. In other words, less energy is needed to upset the logic state.
- **Higher Operating Speeds:** As operating speeds increase, the timing windows during which the processor samples signals become narrower. This increases the probability a transient overvoltage event coincides with a critical sampling moment, leading to an error. Additionally, less time is available for signals to stabilize after being disturbed.

- **Wider Data Buses and Parallelism:** With more bits being processed in parallel each clock cycle, a single transient overvoltage event has a greater chance of simultaneously disrupting multiple signals or functional units—amplifying the risk of complex, potentially uncorrectable errors.

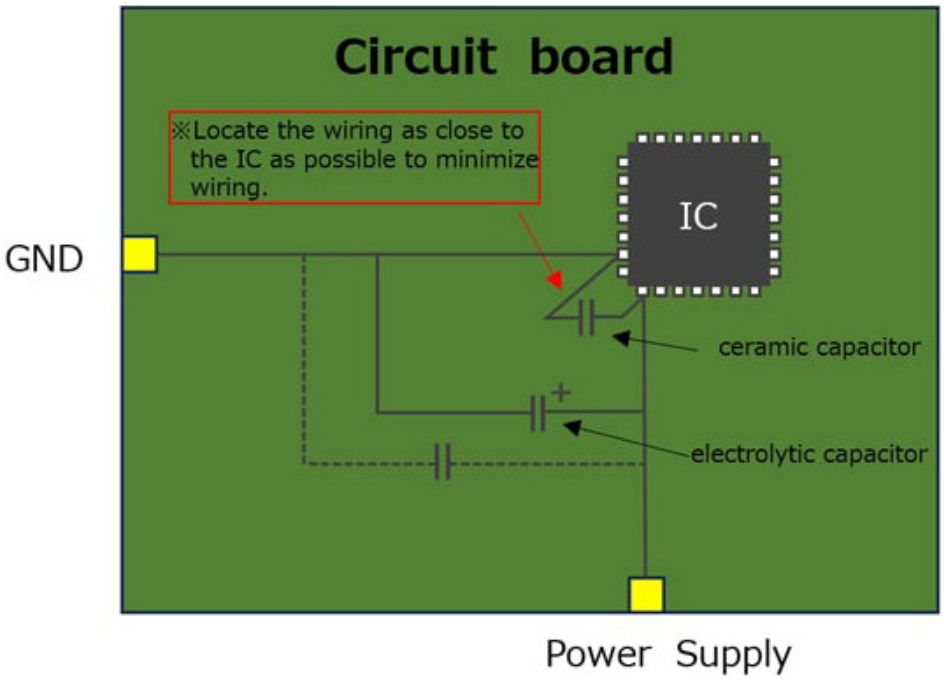
These factors combine to make modern microprocessors highly performant but also inherently more fragile in the presence of transient overvoltage, necessitating more sophisticated protection and fault tolerance strategies.

RECOMMENDED **MITIGATION TECHNIQUES**

Mitigating transient-induced faults requires a multi-layered approach, combining hardware design practices, circuit-level protection, and system-level resilience.

Key circuit board-level techniques include:

- **Local Decoupling Capacitors:** Strategically placed capacitors near sensitive logic nodes or power rails help absorb high-frequency transient energy and stabilize voltage levels during brief disturbances. Tantalum and ceramic capacitors in parallel are often used to target a wider frequency spectrum.



Source: Toshiba

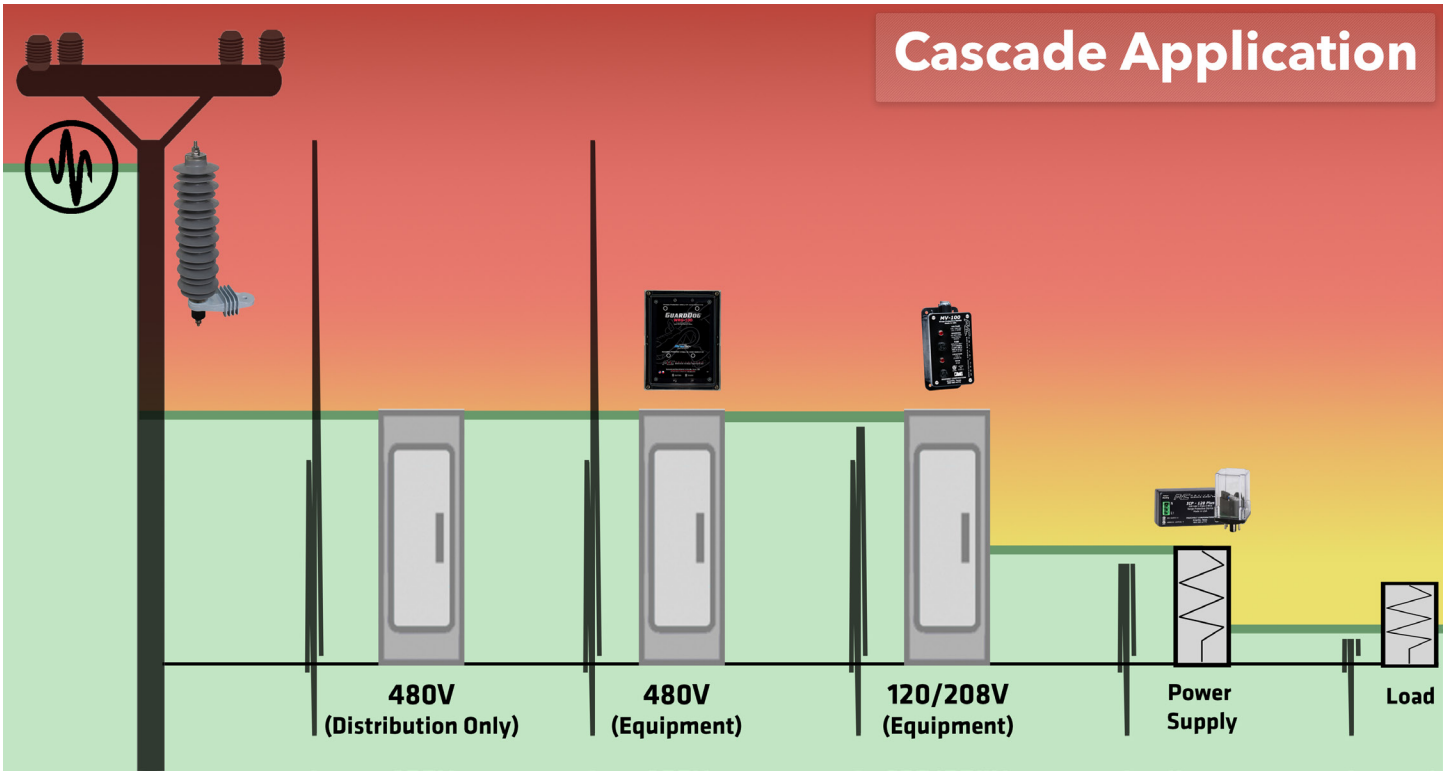
- **Filtering and Series Impedance:** Incorporating passive components such as ferrite beads, inductors, and low-pass filters into power and signal lines slows the rise time of transients, reducing their peak voltage and impact on sensitive circuitry.

- **Error Detection and Correction (EDAC):** Memory systems often use parity bits or more advanced ECC (Error-Correcting Codes) to identify and correct single-bit or multi-bit errors caused by transient overvoltage. EDAC circuits help prevent such faults from propagating into software-level failures.
- **Redundant Logic and Voting Schemes:** Triple Modular Redundancy (TMR) involves three identical logic paths with a majority-voting mechanism to ensure the correct output, even if one path experiences a fault. This method is commonly used in aerospace and safety-critical applications.
- **Supervisory Circuits and Watchdogs:** These components monitor system activity and can reset or reinitialize the processor when anomalous behavior is detected, such as a fault-induced lockup or logic error. Watchdog timers are particularly useful for automatically recovering from transient-induced faults.
- **Surge Protective Components:** Surge protective components should be placed at vulnerable interfaces (e.g., power inputs, communication ports) to absorb excess voltage and limit voltage excursions.
- **Shielding and Grounding:** Proper PCB layout, including ground planes and shielding of sensitive traces, minimizes the coupling of external transient overvoltage into critical circuitry. (This also applies to incoming power distribution, before it reaches the processor.)

While board-level techniques are critical for minimizing the effects of transient overvoltage once it reaches the microprocessor, the most effective defense often starts before the disturbance ever reaches the circuit board. Broader strategies help protect all downstream equipment—not just individual components—by addressing the root causes and entry points of transient overvoltage.

Broader mitigation techniques include:

- **Facility-Level Surge Protection:** Install Transient Voltage Surge Suppressors (TVSS)—also known as surge protective devices (SPDs)—at the main service entrance, subpanels, key branch circuits, and upstream of all integrated circuits (IC). TVSS/SPDs redirect high-energy transients (such as lightning or utility switching events) before they propagate through the electrical system, causing damage, degradation, malfunction, or failure.
- **Proper Grounding and Bonding:** Ensure all systems adhere to proper grounding practices. Poor or inconsistent grounding allows voltage differentials to develop between equipment, increasing



susceptibility to transient overvoltage-induced errors. Bonding all grounds to a common reference point mitigates potential voltage differences.

- **Cascaded Protection:** Use a layered or cascaded surge protection scheme across multiple levels (service entrance distribution panel point-of-use). Each stage handles a portion of the surge energy, increasing overall effectiveness and protecting sensitive downstream loads.
- **Environmental Hardening:** Enclosures rated for industrial or harsh environments protect against transient-inducing conditions, such as dust, moisture, or radiation.
- **Maintenance and Monitoring:** Regularly inspect surge protection devices, grounding systems, and filter components. Over time, SPDs can degrade due to cumulative exposure to minor surges, and grounding connections may loosen or corrode—reducing their effectiveness.

CONCLUSION

Transient overvoltage impacts microprocessor reliability by inducing unintended logic state changes. Understanding these faults and implementing robust protection strategies ensures stable performance in all environments.

ABOUT **MAXIVOLT**

Established almost four decades ago, Maxivolt is a pioneer in the power quality industry with over a century of combined experience. Maxivolt manufactures specialized technology and provides value-added services custom-tailored to extend the life and protect the operational integrity of electrical and electronic equipment.

For more information, contact Maxivolt:

800-583-4773

info@maxivolt.com

www.maxilovt.com

REFERENCES

1. Electric Power Research Institute (EPRI), “Protecting Sensitive Electronics from Voltage Surges and Transient Events,” Technical Report 3002020764, Palo Alto, CA, 2019.
2. Baumann, R. C., “Radiation-induced soft errors in advanced semiconductor technologies,” IEEE Transactions on Device and Materials Reliability, vol. 5, no. 3, Sept. 2005.
3. JEDEC Standard JESD89A, “Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices,” JEDEC Solid State Technology Association, 2006.
4. NASA Technical Memorandum, “Fault Injection and Error Classification Techniques,” NASA TM-102647, 1990. [Online]. Available: https://ntrs.nasa.gov/api/citations/19900008317/downloads/19900008317.pdf