Understanding ESD, EFT, and Surge in RS-422 and RS-485 Networks

RS-422 and RS-485 networks are foundational to various industrial, commercial, and residential applications. For these networks to operate reliably, understanding overvoltage transients is crucial. This tutorial provides insight into the types, effects, and management of overvoltage transients affecting RS-422 and RS-485 networks.

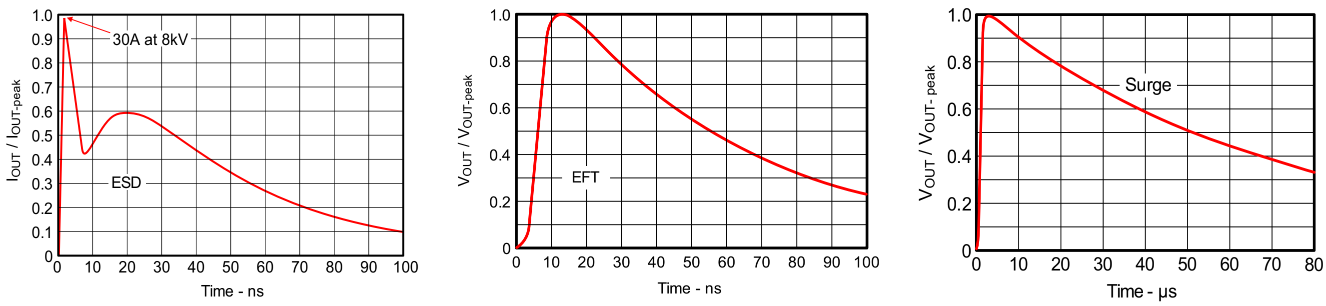

Figure 1. Difference between ESD, EFT, and Surge Transients and Duration

Contents

1. Types of Overvoltage Transients

1.1 Electrostatic Discharge (ESD)

1.1.1 Origin and Causes

In RS-422 and RS-485 networks, ESD events usually originate from ungrounded objects or humans encountering the system. The most common sources include the discharge of built-up static electricity from human operators or from non-conductive surfaces like insulating mats or packaging materials.

1.1.2 Effects and Consequences

ESD can lead to a range of issues from temporary data corruption to a complete operational halt. ESD events can also lead to the degradation of the semiconductor material, reducing its effective lifespan.

1.1.3 How to Identify

Oscilloscopes with fast sampling rates can be used to capture and analyze ESD events. Anomalies in signal integrity or unexpected system behaviors often indicate recent ESD events.

1.2 Electrical Fast Transient (EFT)

1.2.1 Origin and Causes

EFTs are mainly caused by the rapid switching of inductive loads such as relays, contactors, and transformers. When these components switch, they can introduce fast transients into the RS-422 and RS-485 data lines.

1.2.2 Effects and Consequences

EFT can introduce high-frequency noise into the system, leading to data packet losses, system reboots, or even CPU crashes. Continuous exposure to EFTs can degrade signal quality and reduce component lifespan.

1.2.3 How to Identify

High-frequency oscilloscopes coupled with specialized EFT detection algorithms can be used for real-time monitoring of EFT events. Symptoms often include erratic system behavior, frequent reboots, or data transmission errors.

1.3 Voltage Surge

1.3.1 Origin and Causes

Voltage surges in RS-422 and RS-485 systems commonly result from natural events such as lightning strikes or the sudden switching of large inductive or capacitive loads in the electrical network.

1.3.2 Effects and Consequences

Voltage surges can cause catastrophic damage, such as the melting of semiconductor junctions or the breakdown of insulation barriers. This can lead to immediate or delayed system failure.

1.3.3 How to Identify

Voltage surge detection systems, often integrated into industrial monitoring solutions, can be used to identify these occurrences. They usually provide alerts or shut down parts of the network to prevent damage.

2. Countermeasures from Overvoltage Transients

To combat ESD, industry-standard practices recommend the incorporation of ESD diodes in these interfaces, acting as a sink for ESD-induced excess voltage. For quicker response times, Transient Voltage Suppression (TVS) diodes are often used. Also, proper system grounding is essential because it provides an alternative path for ESD-related currents and results in safeguarding sensitive components.

When dealing with EFT, twisted-pair cables are commonly advised because their inherent geometry nullifies EFT-induced noise. Adding ferrite beads or chokes on data lines can attenuate the high-frequency noise produced during EFT events. To further shield the system, surge protectors are often installed on power supply lines leading to RS-422 and RS-485 devices, effectively diverting transient currents away from the system.

For countering Voltage Surges, Gas Discharge Tubes (GDTs) are recommended. These tubes contain a specialized gas that becomes conductive under high-voltage conditions, channeling the excess energy safely to the ground. Metal-Oxide Varistors (MOVs) are another viable option; these devices offer a resistive barrier to surges, dynamically adjusting their resistance levels in response to varying voltage conditions. Finally, maintaining a physical distance between RS-422 and RS-485 networks and high-voltage equipment can minimize the impact of surge events.

Revision History

Revision	Date	Description
1.00	Dec 4, 2023	Initial release.

IMPORTANT NOTICE AND DISCLAIMER

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Contact Information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/