Adv. Radio Sci., 8, 179–182, 2010
www.adv-radio-sci.net/8/179/2010/
doi:10.5194/ars-8-179-2010

Advances in Radio Science

Untersuchung von Schutzelementen für IT-Systeme gegen HPEM-Bedrohungen

F. Brauer and J. L. ter Haseborg

Institut für Messtechnik und EMV, Technische Universität Hamburg-Harburg, Deutschland

Zusammenfassung. Die Entwicklung von Schutzschaltungen gegen elektromagnetische Störungen ist unverzichtbar, um die Immunität von komplexen elektronischen Systemen zu gewährleisten. In diesem Beitrag wird das Verhalten von nichtlinearen Schutzelementen für IT-Systeme untersucht. Hierzu finden spezielle Testverfahren im passiven und aktiven Zustand des IT-Testsystems Anwendung.

1 Einleitung

Die schnelle und sichere Übertragung von Informationen ist ein wesentliches Ziel unserer Gesellschaft. Fast jedes technische System für zivile oder militärische Anwendungen ist von einer zuverlässigen Datenübertragung abhängig. Mit der wachsenden Anzahl an künstlichen elektromagnetischen Interferenzen (EMI) ist die Störung der Kommunikationssysteme immer wahrscheinlicher, vor allem im Fall von HPEM (High Power Electromagnetics), wie UWB- (Ultra Wideband), DS-(Damped Sinusoids) oder HPM-(High Power Microwave) Quellen. Es sind bereits Szenarien denkbar, wo diese Quellen für terroristische Zwecke zur absichtlichen Störung von elektronischen Systemen benutzt werden könnten. Diese Bedrohung ist unter dem Oberbegriff IEMI (Intentional Electromagnetic Interferences) zusammengefasst worden (Radasky et al., 2004). IT-Netzwerke stellen den größten Teil der gängigen Kommunikationssysteme dar. COTS-IT-Komponenten sind auf dem Markt weit verbreitet und werden für aktuelle Applikationen bereits großflächig eingesetzt. Ein Fehler oder eine kurze Unterbrechung der Datenübertragung kann für einige Applikationen schon äußerst kritisch sein. In Bezug auf Personenbeförderung im zivilen Bereich (z.B. Luftfahrt) oder militärische Anwendungen kann ein Fehler menschliches Leben gefährden. Aus diesem Grund ist die Untersuchung von Schutzelementen zur Härtung dieser Systeme unvermeidlich.

In diesem Beitrag sind für ein beispielhaftes IT-Testnetzwerk im passiven Zustand die in die Datenübertragungskabel eingekoppelten Störspannungen unter UWB-Bedingungen gemessen worden, wobei gleichzeitig Schutzelemente zum Vergleich im jeweiligen Koppelpfad integriert worden sind. Zusätzlich ist das System im aktiven Zustand unter Einfluss von HPEM-Störungen mit und ohne Schutzelemente untersucht worden. Eine spezielle Ethernet-Teststrecke ist hier entwickelt worden, um den Einfluss von zusätzlichen passiven oder aktiven Schutzmaßnahmen auf die Fehlerrate beim Datentransfer zu untersuchen. Die Ergebnisse liefern die Grundlage zur Entwicklung von neuen, angepassten Schutzkonzepten und für die Integration von COTS-Schutzschaltungen in vorhandene IT-Systeme.

2 Empfindlichkeit des Testsystems

Als Testsystem wird ein IT-Netzwerk gewählt, das im zivilen wie auch militärischen Bereich eingesetzt werden könnte. Das System basiert auf dem Ethernet 100 Base TX-Standard, womit Übertragungsraten von 100 Mbit/s möglich sind. Abildung 1 zeigt den schematischen Aufbau. Zwei PCs werden hierbei jeweils mit einem Switch über ein Ethernet-Kabel verbunden. Die beiden Switche sind über Lichtwellenleiter- (LWL-) Kabel verbunden, um Störungen auf diesem Übertragungsweg zu vermeiden. Bei Untersuchungen in Radasky et al. (2004) sind mittels Störfestigkeitsuntersuchungen am aktiven Testsystem (d.h. während der Datenübertragung) mit Hilfe von Netzwerkanalyse-Software sowie Messungen der eingekoppelten Störspannungen bzw. -ströme am passiven Netzwerk kritische Koppelpfade des Systems gegenüber UWB-, DS- und HPM-Pulsen ermittelt worden. Tabelle 1 liefert einen Überblick bei welcher Störungsform auf der jeweiligen Koppelstruktur welche Effekte während einer Datenübertragung am System

Correspondence to: F. Brauer
(f.brauer@tuhh.de)

Published by Copernicus Publications on behalf of the URSI Landesausschuss in der Bundesrepublik Deutschland e.V.

Tabelle 1. Übersicht über die verschiedenen HPEM-Bedrohungsformen und die auftretenden Effekte am Testsystem (Brauer et al., 2010).

Koppelstruktur	Störungsform/Effekte		
	UWB	DS	HPM
Ethernetkabel (CAT5, Schirm aufgelegt)	kein Effekt	vereinzelte Fehler	kein Effekt
Ethernetkabel (Schirm nicht aufgelegt)	Fehler/Totalausfall	Ausfall	kein Effekt
Kaltgerätekabel	kein Effekt	Totalausfall	kein Effekt
Gehäusestruktur	kein Effekt	kein Effekt	Totalausfall

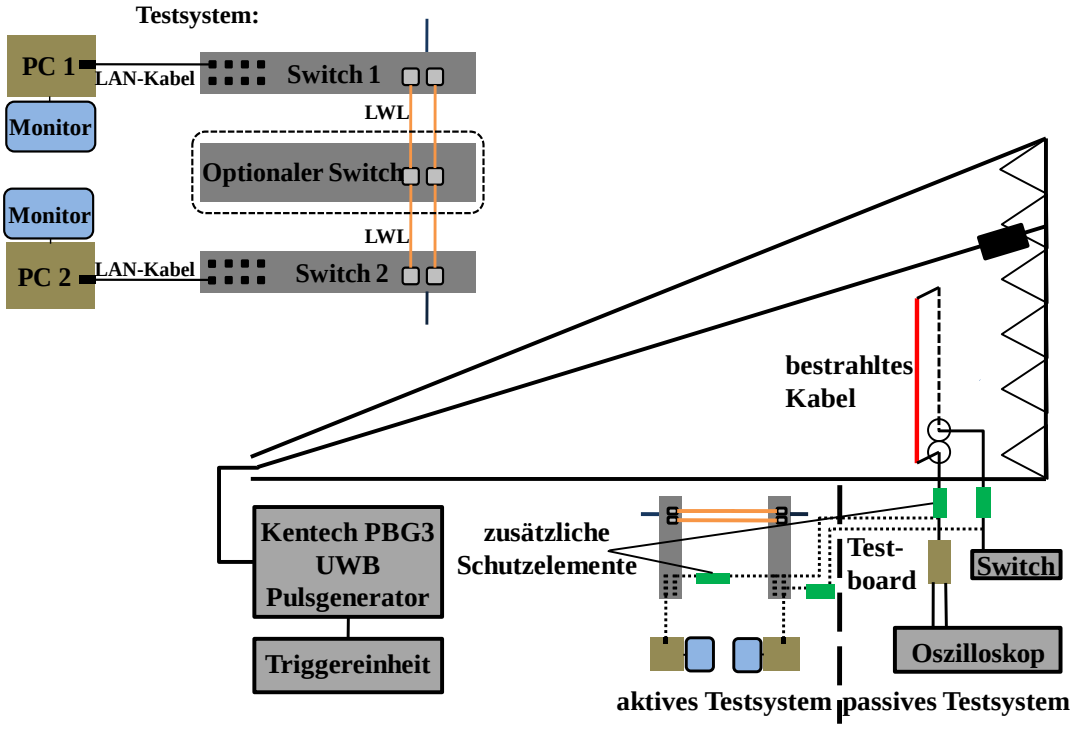


Abb. 1. Testsystem und Messaufbau.

beobachtet worden sind (vgl. Brauer et al., 2010). Hieraus ist ersichtlich, dass das Ethernet-Kabel (Schirm nicht aufgelegt), das Kaltgerätekabel und das Switchgehäuse je nach Bedrohungsform die empfindlichen Koppelpfade darstellen. Bei UWB-Störungen mit ansteigenden Pulswiederholraten (max. 1 kHz) sind hierbei Fehler in Form von Retransmissions, kurzzeitige Ausfälle bis hin zu Totalausfällen (Reset ist erforderlich) aufgetreten, womit ein sehr großer Einfluss auf die Ethernet-Datenübertragung gegeben ist.

3 Untersuchung von Schutzelementen

3.1 Messaufbau

Zum Schutz gegen die in Abschnitt 2 beschriebenen Effekte bei Beaufschlagung mit UWB-Pulsen sollen nun Untersuchungen von speziellen Schutzelementen vorgestellt werden. Abbildung 2 liefert einen Überblick über die untersuchten Schutzelemente. Zum einen kommen hier passive Ethernet-Schutzelemente mit schnellen Suppressordioden der Firma Semtech in Betracht und zum anderen ein aktives Ethernet-Schutzelement der Firma Akros Silicon. Die passiven Elemente werden auf Platinen mit zwei RJ45-Buchsen implementiert. Diese sind mit dem Ethernet-Standard konform, um Störungen durch die zusätzlichen in den Übertragungsweg geschalteten Elemente zu vermeiden. Die Störbeaufschlagung findet in einer GTEM-Zelle statt, an die der UWB-Pulsgenerator PBG3 der Firma Kentech angeschlossen wird (siehe auch Abb. 1). Als Koppelpfad kann eine definierte Länge der Ethernetleitung in die GTEM-Zelle eingebracht werden. Die Kabelenden werden über spezielle Ethernetdurchführungen nach außen geführt wo die Schutzelemente implementiert werden können. Die aktiven Schutzelemente werden auf einer selbst entwickelten

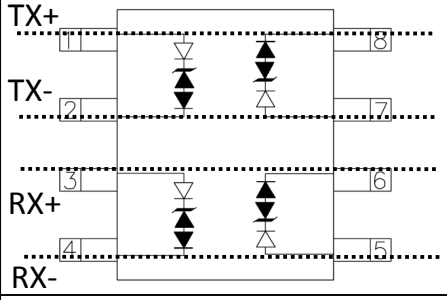
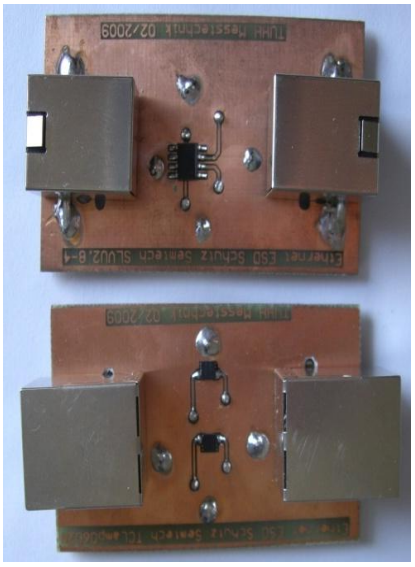
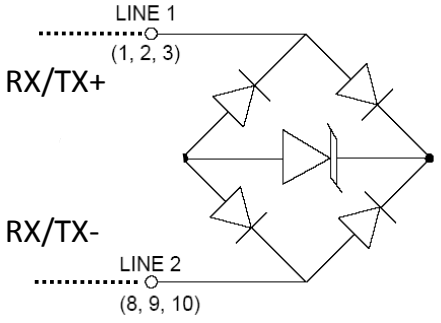
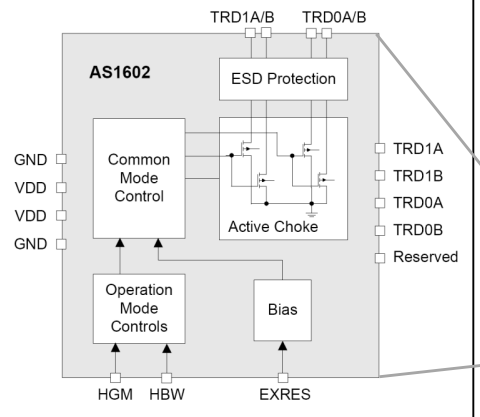
Schutzelement	**clamping voltage**	**Ersatzschaltbild**	**Foto**
Semtech SLVU2.8-4	12 V @ 20 A (I_{PP}) t_r= 8µs t_d= 20µs		
Semtech TClamp0602N	9 V @ 20 A (I_{PP}) t_r= 2µs t_d= 10µs		
Akros Silicon AS 1602 (aktiv)	3,47 V		

Abb. 2. Untersuchte Schutzelemente.

Ethernet-Schnittstelle implementiert. Mit zwei dieser Platinen ist eine direkte PC-gesteuerte Datenübertragung zwischen den Schnittstellen möglich. Um die eingekoppelten Störsignale und Restpulse hinter den Schutzelementen durch Messungen einschätzen zu können, werden passive Messplatinen eingesetzt, die den 100-Ω-Abschlusswiderstand an den 50-Ω-Widerstand der SMA-Messleitung anpassen (Brauer et al., 2009). Um den Einfluss der Schutzelemente auf den Datenverkehr zu untersuchen wird das System im aktiven Zustand betrachtet, d.h. das komplette System wird angeschlossen und es findet eine Datenübertragung statt.

3.2 Ergebnisse

Die eingekoppelten UWB-Störpulse werden in Abb. 3 für die Schutzschaltungen SLVU und TClamp von Semtech präsentiert. Die Messergebnisse zeigen deutlich, dass eine Schutzwirkung durch eine Begrenzung der Störspannung gegeben ist. Beide Schutzelemente zeigen eine sehr ähnliche Schutzwirkung, wobei gerade am Anfang des eingekoppelten Störsignales ein schlechteres Ansprechverhalten der Schutzelemente zu bemerken ist, was mit der relativ langsamen Ansprechzeit der Schutzdioden zusammenhängt.

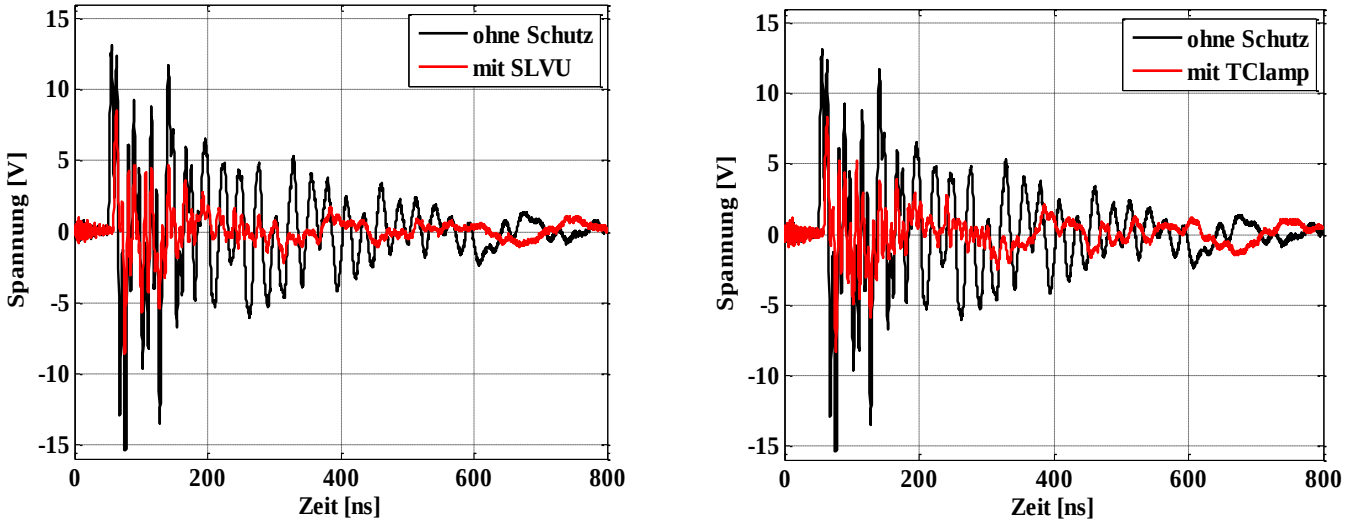


Abb. 3. Messergebnisse im passiven Zustand des Testsystems.

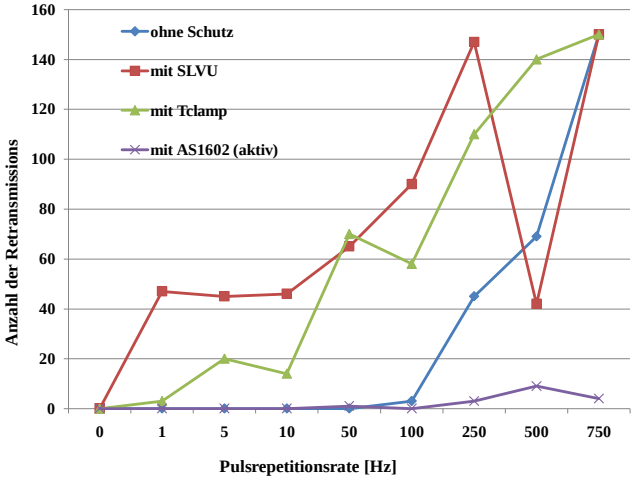


Abb. 4. Messergebnisse im aktiven Zustand des Testsystems.

Im aktiven Zustand des Testsystems ergeben sich die Resultate aus Abb. 4. Hier werden die fehlerhaften Datenpakete bei externer Implementierung der genannten Schutzelemente über der Pulswiederholrate des UWB-Pulsgenerators aufgetragen. Lediglich das aktive Schutzelement zeigt eine durchgehend positive Störunterdrückung auch bei hohen Repetitionsraten, da das Gleichtaktstörsignal hier aktiv gefiltert wird und die Leitungen dabei im Störfall nicht gegeneinander oder gegen Masse kurzgeschlossen werden, wie es bei den passiven Elementen der Fall ist. Bei noch höheren Pulswiederholraten ist festgestellt worden, dass alle Schutzelemente einen kompletten Zusammenbruch des Datenverkehrs oder gar der Datenverbindung verhindern können.

4 Zusammenfassung

Im Rahmen dieses Beitrages sind verschiedene Schutzmaßnahmen für IT-Systeme hinsichtlich ihrer Wirksamkeit gegen UWB-Pulse mit hohen Pulswiederholraten untersucht worden. Hierbei haben insbesondere aktive Schutzkomponenten gute Ergebnisse erzielt. Passive Schutzelemente, die überwiegend für den ESD- Schutz von Ethernet-Datenleitungen eingesetzt werden, zeigen zwar, dass sie das auftretende Störsignal effektiv unterdrücken, allerdings während des Ansprechens im Störungsfall die Datenübertragung erheblich beeinträchtigen.

Literatur

Radasky, W. A., Baum, C. E., and Wik, M. W.: Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI), IEEE Transactions on Electromagnetic Compatibility, 46(3), 314–321, 2004.

Brauer, F., Sabath, F., and ter Haseborg, J. L..: Susceptibility of IT Network Systems to Interferences by HPEM, IEEE EMC Symposium, Austin, Texas, USA, 17.–21. August 2009.

Brauer, F., Kanyou Nana, R., ter Haseborg, J. L., and Dickmann, S.: Ermittlung von Transferfunktionen zur Abschätzung der HPEM-Empfindlichkeit eines IT-Testsystems, EMV Düsseldorf 2010.