Risikominderung durch konsequentes EMV-Engineering

Sicherheit durch EMV

Ernst Habiger

Technische Prozesse können, falls sie außer Kontrolle geraten, ein hohes Gefahrenpotential für daran beteiligte Menschen, Maschinen, Anlagen und die Umwelt darstellen. Fragen der Sicherheit spielen daher in einer zunehmend technisierten Welt eine immer bedeutsamere Rolle. Im Folgenden wird dieses weit gefächerte Problemfeld zunächst einer kurzen orientierenden Betrachtung unterworfen und daran anschließend gezeigt, welche Beiträge zur Systemsicherheit bzw. Risikominderung ein zielgerichtet EMV-orientiertes Systems-Engineering leistet.

Folgerichtig erhebt sich damit zunächst die Frage:

Was ist eigentlich Sicherheit?

Sichtet man das Fachschrifttum, stößt man auf eine verwirrende Vielfalt von 'Sicherheiten' und Sicherheitsbegriffen, die sich mit sehr unterschiedlicher Relevanz und Häufigkeit im Sicherheits-Fachsprachgebrauch finden (Bild 1).

Dies generiert bei vielen Beteiligten, Nachwuchskräften, Quereinsteigern u. a. Interessierten sofort die verständliche Frage: Was besagt eigentlich der Begriff Sicherheit?

Gebraucht man zur Beantwortung dieser Frage den gesunden ingenieurmäßigen Sachverstand, kommt man, unbeschadet der Tatsache, dass hierzu im einschlägigen Schrifttum eine Vielzahl zweckorientierter, mehr oder weniger scharfer Definitionen existieren (Bild 2), sehr schnell zu dem Ergebnis, dass Sicherheitsprobleme bzw. Sicherheitsbedürfnisse überall dort in Erscheinung treten, wo der in Bild 3 skizzierte elementare Sacherhalt vorliegt [1].
Das heißt, es existiert eine Bedrohungs- bzw. Gefahrenquelle ***Q,*** von der Bedrohungen ausgehen und eine Bedrohungssenke ***S***, d.h. ein Bedrohungsopfer bzw. ein schutzbedürftiges Objekt, das durch diese Bedrohungen einem Risiko ausgesetzt ist. Das heißt, einer mit Ungewissheit behafteten Sachlage, die mit einer mehr oder weniger den jeweiligen Umständen entsprechenden hohen Wahrscheinlichkeit ***W*** erwarten lässt, dass ein unerwünschtes, mit einem mehr oder weniger großen Schaden für das bedrohte Objekt einhergehendes Ereignis eintritt.

Potentielle Bedrohungs- bzw. Gefahrenquellen ***Q*** sind dabei, allgemein gesehen, alle materiellen oder virtuellen Objekte, d. h. alle belebten und unbelebten Bestandteile, Komponenten, Systeme und Phänomene in unserer nahen und fernen Umgebung, die über ein akutes Gefährdungspotential in Form von Materie (Erdmassen, Wassermassen), Energie (in allen Erscheinungsformen), Information (z. B. impliziert in Schadsoftware) oder, sofern es sich um Personen handelt, solche die über unkontrollierte Handlungsoptionen verfügen.

Themenfelder	Auftrittshäufigkeit
Security	957.000.000
Safety	418.000.000
Sicherheit	102.000.000
Datensicherheit	5.900.000
Arbeitssicherheit	2.700.000
Reaktorsicherheit	1.500.000
IT-Sicherheit	1.400.000
Netzwerksicherheit	1.200.000
Internetsicherheit	1.150.000
Betriebsicherheit	791.000
Versorgungssicherheit	569.000
Anlagensicherheit	499.000
Systemsicherheit	440.000
Informationssicherheit	362.000
Computersicherheit	343.000
Funktionssicherheit	154.000
Maschinensicherheit	128.000
Passive Sicherheit	124.000
Gerätesicherheit	83.000
Aktive Sicherheit	83.000

Bild 1: Sicherheitsbezogene Themenfelder und ihre Auftrittshäufigkeiten im Internet (Google-Suchergebnisse, Januar 2007)

Bezüglich der von diesen Gefahrenquellen ausgehenden Bedrohungen ist aus Sicht einer Bedrohungssenke ***S*** (Mensch, Tier, Umwelt, technische Komponente, Gerät, Hardware- oder Softwaresystem oder irgendeine andere Struktureinheit der realen oder virtuellen Welt) zwischen folgenden Bedrohungsklassen zu unterscheiden.

- *natürliche Bedrohungen* aus der unmittelbaren oder fernen Umgebung (beispielsweise galaktisches und atmosphärisches Rauschen, direkter und indirekter Blitzeinschlag, Meteoriteneinschläge, Erdbeben, Erdrutsche, Vulkanausbrüche, Wirbelstürme, Hochwasser, Schlammlawinen, Sturmfluten u.ä. Naturkatastrophen),

- *unbeabsichtigte Bedrohungen* insbesondere durch menschliches Unvermögen, Versagen oder Fehlverhalten (verursacht bzw. begünstigt durch organisatorische Mängel, Missmanagement, Wissenslücken, Fehleinschätzung von Gefahrensituationen, Konzentrationsschwächen, Bedienfehler, Wartungsfehler, fehlerhafte Informationsübermittlung, Missachtung oder Fehlinterpretation von Vorschriften oder Signalen, mangelnde Kontrolltätigkeit, Nachlässigkeit, leichtsinniger Umgang mit gefährlichen Gütern oder gefährdeten Objekten) aber auch durch funktionelles Versagen technischer Betriebsmittel (ausgelöst durch Bauelemente-, Geräte-, Systemstörungen und -ausfälle infolge mangelnder Zuverlässigkeit oder nicht erkannter systemimmanenter systematischer Fehler in Form von Konstruktions-, Schaltungs-, Programmier- und Dimensionierungsfehlern oder mangelnder Immunität gegenüber vor Ort wirkenden Beanspruchungen),

- *absichtliche (böswillige) Bedrohungen* z. B. durch frustrierte Mitarbeiter,

konkurrierende Unternehmen, Verleumder, Hacker, Kriminelle, Geheimdienste,
Terroristen oder andere Übel wollende Angreifer, destruktive Kräfte und organisierte Gewalt.

Jede dieser Bedrohungen versetzt die Bedrohungssenke ***S***, d. h. das bedrohte Objekt in eine Risiko- bzw. Schadenerwartungssituation, die beim Eintreten bestimmter auslösender Ereignisse zu einer Schädigung oder Zerstörung des bedrohten Objektes eskalieren kann. Das heißt, zur Verletzung eines Rechtsgutes wie einem

- Körperschaden (Leben und Gesundheit bei Mensch und Tier), einem
- Sachschaden (Vermögensverlust, Beschädigung oder Zerstörung materieller Güter, Umweltzerstörungen u.ä.), einem
- Leistungsschaden (Produktionsverlust, Lieferverzug, z.B. infolge von Störungen in Betriebsmitteln, Maschinen oder Anlagen) oder zu einem
- ideellen Schaden, z.B. zu einem Ansehens-, Integritäts-, oder Vertrauensverlust, der natürlich auch wirtschaftliche Konsequenzen zur Folge haben kann.

Damit wird die eingangs gestellte Frage »Was ist Sicherheit?« beantwortbar:

Sicherheit = Zustand, der für ein klar abgegrenztes bedrohtes Objekt dann besteht, wenn für dieses Objekt das Risiko im oben erklärten Sinn Schaden zu nehmen, während seiner gesamten Existenzphase einen akzeptierbaren Wert nicht überschreitet.

Dieser Sachverhalt ist beispielsweise in der Sicherheitsnorm DIN EN 61508-4 [2], stark verdichtet, wie folgt, formuliert:
Sicherheit = Freiheit von unvertretbaren Risiken.

Abschließend sei vermerkt, dass im Prinzip jedes Objekt gleichzeitig Gefahrenquelle und Gefahrensenke sein kann. Beispielsweise kann einerseits jemand bei Unachtsamkeit durch ein elektrisches Gerät zu Schaden kommen andererseits aber auch das Gerät selbst z. B. durch Fehlbedienung, Feuer- oder Wassereinwirkung Schaden nehmen.

Damit erhebt sich als Nächstes die praktisch relevante Frage:

Wie wird Sicherheit erreicht?

Genauer gesagt, wie lässt sich Sicherheit zielgerichtet verwirklichen, d.h. verlässlich in Geräte, Maschinen und insbesondere in die immer komplexer werdenden technischen Mensch-Maschine-Systeme implementieren und nachhaltig, im gesamten Produktlebenszyklus aufrechterhalten?
Die dazu bestehenden elementaren Möglichkeiten lassen sich unmittelbar aus Bild 3 ablesen. Sie bestehen darin,

- *Meyers Großes Universal-Lexikon:* **Zustand des Unbedrohtseins**, der sich objektiv im Vorhandensein von Schutz[einrichtungen] bzw. im Fehlen von Gefahr[renquellen] darstellt und subjektiv als **Gewissheit von Individuen oder sozialen Gebilden über die Zuverlässigkeit von Sicherungs- und Schutzeinrichtungen empfunden wird.**
- *MIL-Std 882A:* Bei Fehlen dieser **Bedingung** (Sicherheit) werden Tod, Verletzungen, Berufskrankheiten oder Zerstörung bzw. Verlust von Anlagen oder Vermögen herbeigeführt.
- *DIN 44 300. Teil 1:* **Sachlage**, bei der Daten unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigung oder Mißbrauch (Verlust, Zerstörung, Verfälschung) bewahrt sind.
- *DIN 31004:* **Sachlage**, bei der das Risiko kleiner als das Grenzrisiko ist.
- *DIN EN 61508-4:* **Freiheit** von unvertretbaren Risiken.

Bild 2: Beispiele für bereichsspezifische Sicherheitsdefinitionen

- Bedrohungsquellen, sofern dies möglich ist (Naturkatastrophen beispielsweise sind unabwendbare Ereignisse), zu eliminieren bzw. das von ihnen ausgehende Bedrohungspotential soweit wie möglich zu reduzieren.

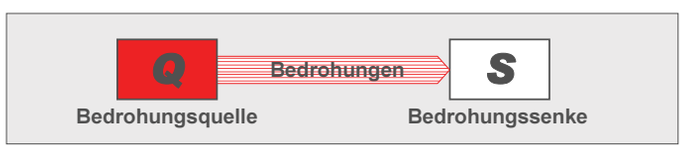

Bild 3: Elementares Bedrohungsszenario

- Das Wirksamwerden von Bedrohungen weitestgehend zu unterbinden, d.h. die Eintrittswahrscheinlichkeit ***W*** eines Schaden auslösenden Ereignisses soweit wie möglich zu vermindern, d. h. das damit verbundene Risiko mittels geeigneter Maßnahmen unterhalb eines vertretbaren Grenzrisikos zu senken (Bild 4). Zu diesen Maßnahmen zählen im Rahmen einer sicherheitsgerichteten konstruktiven bzw. anlagentechnischen Konzipierung und Ausführung u. a. die Umsetzung bewährter Sicherheitsprinzipien (Überdimensionierung, Redundanz, Hardwarediversität u. a.), der Einsatz sicherheitsbewährter Bauteile sowie die zielgerichtete Systemausstattung mit Beobachtungs-, Überwachungs- und Sicherheitsfunktionen, um sich anbahnende, Schaden auslösende Ereignisse möglichst frühzeitig zu erkennen und durch geeignete Maßnahmen (Alarme, automatische Gegenmaßnahmen) zu unterbinden.
- Bei Eintritt eines Schadens möglich rasch vorbedachte, gründlich vorbereitete Schadensbegrenzungsmaßen und -funktionen zu aktivieren und das geschädigte Objekt möglichst rasch wieder in den schadfreien Zustand zu versetzen.

Ein strukturiertes reales System kann somit dann als sicher gelten, wenn diese Überlegungen in der Konzipierungs- und Ausführungsphase umgesetzt sind und dafür Sorge getragen ist, dass alle Sicherheitsvorkehrungen durch ein leistungsfähiges Sicherheits-Management über den gesamten System-Lebenszyklus aufrechterhalten werden.

Im praktisch konkreten Fall werden bei

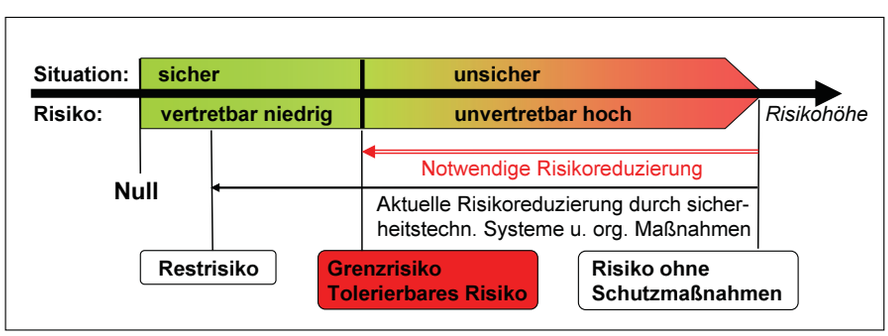

Bild 4: Risikobehandlung im Zuge einer sicherheitsgerichteten Systemgestaltung

Probability **W** Schadenseintritt-Wahrscheinlichkeit (Ereignisse / Stunde)	Schadensausmaß **S** Negligible (unbedeutend)	Marginal (gering)	Critical (kritisch)	Catastrophic (katastrophal)
$>10^{-4}$ bis $<10^{-3}$ Frequently (häufig)	ALARP Region	Not Acceptable	Not Acceptable	Not Acceptable
$>10^{-5}$ bis $<10^{-4}$ Probable (wahrsch.)	ALARP Region	ALARP Region	Not Acceptable	Not Acceptable
$>10^{-6}$ bis $<10^{-5}$ Occasional (geleg.)	ALARP Region	ALARP Region	ALARP Region	Not Acceptable
$>10^{-7}$ bis $<10^{-6}$ Remote (gering)	Acceptable	ALARP Region	ALARP Region	ALARP Region
$>10^{-8}$ bis $<10^{-7}$ Improbable (unw.)	Acceptable	Acceptable	ALARP Region	ALARP Region
$>10^{-9}$ bis $<10^{-8}$ Incredible (sehr unw.)	Acceptable	Acceptable	Acceptable	Acceptable

Bild 5: Risikobewertung $R = f(W,S)$ nach DIN EN 61508 [2]

der Konzipierung sicherer Systeme im Zuge eines Risikomanagements, d.h. durch die systematische Anwendung von Managementgrundsätzen, -verfahren und -praktiken während des Entwicklungs-, bzw. Projektierungsprozesses die zu erwartenden Risiken analysiert, bewertet und im Sinne einer Zurückdrängung auf ein vertretbares Maß kontrolliert (Bild 4). Für die allgemeine Bewertung der Risikohöhe spielen dabei Kriterien wie Eintrittswahrscheinlichkeit eines unerwünschten Ereignisses, Schadensausmaß, geografische Ausbreitung und zeitliche Ausdehnung des Schadens, mögliche Behebbarkeit des Schadens, Verzögerung zwischen Ereigniseintritt und späteren Folgen sowie gesellschaftliche Reaktionen, die bei Verletzung von individuellen, sozialen oder kulturellen Interessen oder Werten möglich sind, eine Rolle.

Im Übrigen erfordern diese Arbeiten große Erfahrung und werden in der Regel von einem Expertenteam durchgeführt. Die Ergebnisse repräsentieren gewissermaßen die quantifizierte Meinung der Experten und sind genau so gut wie diese aber in jedem Falle subjektiv und oftmals von Einzel- oder Gruppeninteressen geprägt, da eine durchgängig objektiv formale Risikobewertung nun mal nicht möglich ist, d.h. stets ein bestimmter Entscheidungsspielraum bleibt, der Interessen getrieben ausgeschöpft wird.

Da es aus wissenschaftstheoretischer Erkenntnis aber auch aus wirtschaftlichen Erwägungen heraus eine absolute Sicherheit im Sinne einer Freiheit von jeglichen Risiken nicht geben kann, verbleibt in allen Fällen ein Restrisiko (Bild 4), mit dem man sich arrangieren bzw. abfinden muss.

In technischen Systemen wird das Risiko in vielen Fällen als Funktion der Schadenseintritt-Wahrscheinlichkeit und der Schwere des möglichen Schadens beschrieben. Das heißt, vereinfacht betrachtet, gilt:

Risikohöhe $R = W \cdot S$,
wobei
W = Eintrittswahrscheinlichkeit des Schadens, [$W = 0...1$],
S = Schadenshöhe/Schadensausmaß, ausgedrückt in passenden Verlusteinheiten [Währungseinheiten, Verletzte, Tote u.ä.].

Für die Bewertung eines vorliegenden Risikos kann die in Bild 5 dargestellte Matrix herangezogen werden. Sie lässt erkennen, welcher Wert der Schadenseintritt-Wahrscheinlichkeit W bei einem zu erwartenden Schadensausmaß S als zumutbar gelten kann. Im Grenzbereich zwischen den eindeutig akzeptierbaren (acceptable) und nicht akzeptierbaren (not acceptable) W-S- Paaren existiert ein Ermessens-Spielraum (**ALARP**-Region), in dem fallspezifisch das sogenannte **ALARP**-Prinzip angewandt wird.
ALARP: **A**s **L**ow **A**s **R**easonable **P**ossible = (Risiko) so niedrig wie vernünftiger Weise möglich.
Der obere Bereich dieses Spielraums wird in Anspruch genommen, wenn keine Risikominderung möglich ist oder die Kosten für eine solche ein vertretbares Maß übersteigen und der untere Bereich dann, wenn die erzielbare Verbesserung die Kosten für die Risikoreduktion überwiegt.

Für die Gefahrenanalyse, die Risikoermittlung und Bewertung sowie die sicherheitsgerechte Gestaltung technischer Objekte existiert im Übrigen ein außerordentlich umfangreiches Vorschriftenwerk. Siehe z.B. [2] bis [5].

Bleibt abschließend die Frage zu klären:

Welche Rolle spielt dabei die EMV?

Sichtet man das komplexe, rasant evol-

Bild 6: Technisches Umfeld moderner Industriegesellschaften

vierende, hoch technisierte Umfeld moderner Industriegesellschaften, so finden sich darin bekanntermaßen eine Vielzahl an elektrisch/elektronisch gestützten Techniken und Technologien (Bild 6).

Eng miteinander verflochten und mit allen Bereichen privaten und öffentlichen Lebens und Wirtschaftens untrennbar verknüpft sind sie für die moderne Menschheit die unverzichtbare materielle Existenzgrundlage und Voraussetzung für gehobene Lebensqualität. Ihr Betrieb impliziert jedoch eine Fülle an sich ständig vermehrenden Risiken. Damit werden die Gewährleistung ihrer gefahrlosen Nutzung sowie die Aufrechterhaltung ihrer funktionalen Stabilität und Betriebssicherheit zu einer Frage von höchstem Gewicht.

Aus technischer Sicht entscheidend dafür sind u.a. die folgenden sicherheitsfördernden bzw. risikomindernden Faktoren (Bild 7):

Die Zuverlässigkeit aller beteiligten Komponenten, Geräte, Maschinen und Anlagen, d.h. der Schutz vor Hardwareausfällen und dadurch bedingtem funktionellem Versagen und ggfs. daraus resultierender Sicherheitsrisiken. Die Qualität und Versorgungssicherheit der zu ihrem Betrieb erforderlichen Energien. Die funktionale und informationstechnische Sicherheit sowie in speziellen Fällen die Eigensicherheit aller implizierten elektrischen und elektronischen Betriebsmittel (Antriebs-, Steuerungs-, Regelungs-, Überwachungs-, Prozessleit-, Kommunikations-, Computersysteme und Netze), ihr Schutz vor missbräuchlichen und böswilligen Zugriffen sowie die Gewährleistung eines nachhaltigen Arbeits- und Gesundheitsschutzes, unter anderem des Schutzes gegen gesundheitliche Risiken in elektromagnetischen Feldern.

Erkundet man den Einfluss elektromagnetischer Phänomene auf diese Faktoren [6] bis [8] wird sehr schnell klar, dass in allen Fällen eine EMV-gerechte Produktgestaltung sowie der Einsatz von EMV-Technologien und EMV-Schutzkonzepten, d.h. ein konsequentes EMV-Systems-Engineering einen ganz entscheidenden, unverzichtbaren Beitrag zur Realisierung eines angemessenen Sicherheitsniveaus im gesamten technischen Zivilisationsumfeld leistet. Bild 7 verdeutlicht diesen Sachverhalt. Künftig wird die in Entwicklung befindliche Norm IEC 61000-1-2, die z. Z. im 2. Entwurf vorliegt [9], die damit im Zusammenhang stehenden Arbeiten zielgerichtet unterstützen.

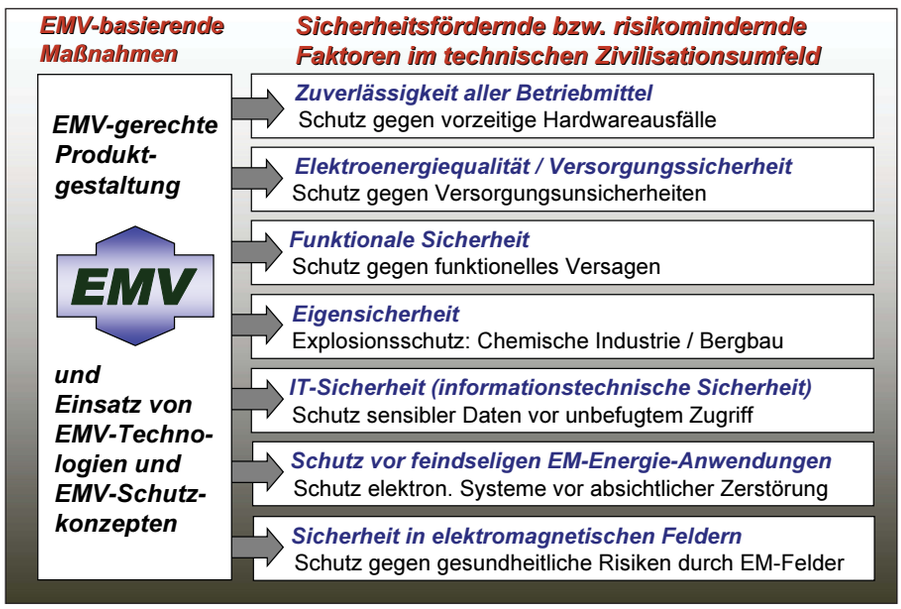

Bild 7: Risikominderung durch EMV-gerechtes Systems-Engineering

Zusammenfassung

Sicherheit ist in einer hoch technisierten Welt ein Thema von höchster Brisanz. Der vorliegende Beitrag gibt einen kurzen Überblick über damit im Zusammenhang stehende elementare Fragen und beleuchtet den Bezug zur EMV. Sicherheitsbelange müssen, wie jede andere gewünschte Systemeigenschaft von Anbeginn im Zuge des Systems-Engineering, d.h. der Konzipierung, Konstruktion, Entwicklung, Projektierung, Realisierung, Pflege und Wartung bis hin zur Entsorgung von Geräten, Maschinen und Anlagen berücksichtigt werden. Die Integration und Beherrschung der EMV-Aspekte ist dabei in Verbindung mit allen elektrisch/elektronisch gestützt arbeitenden Objekten und Systemen ein unverzichtbares, risikominderndes, d.h. die Systemsicherheit unterstützendes Erfordernis.

Literatur & Links

[1] Habiger, E.: Ganz sicher! Safety und Security – unverzichtbare Dimensionen im Gefüge moderner Industriegesellschaften. S&I-KOMPENDIUM 2006, S.16-20. Publish-industry Verlag 2006. www.sui24.net suche > SIK06000

[2] DIN EN 61508 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme. www.rams.de/beratung/safety/61508/index.html

[3] Stein, M.: Sicherheit an Maschinen in: Safety & Automation. 3. Auflage. CEDES AG 2005 www.cedes.com/english/Produkte/SafetyAutomation/Normen/PDF/Normen.pdf

[4] DIN EN 62061 Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

[5] N.N.: VDE-Bestimmungen – Auswahl zur funktionalen Sicherheit. VDE Verlag 2007-01 www.vde-verlag.de/normen/fs.pdf

[6] Habiger, E.: Elektromagnetische Verträglichkeit – Grundzüge ihrer Sicherstellung in der Geräte- und Anlagentechnik. 3. Auflage. Hüthig Verlag 1998

[7] Habiger, E. u.a.: Handbuch Elektromagnetische Verträglichkeit. Grundlagen, Maßnahmen, Systemgestaltung. 2. Auflage. Verlag Technik 1992

[8] Habiger, E.: EMV-Lexikon 2007. 2. Auflage. WEKA-Verlag 2007

[9] IEC 61000-1-2 Ed. 2: Electromagnetic Compatibility – General – Methodology for the achievement of the functional safety of electrical an electronic equipment with regard to electromagnetic phenomena

Prof. Dr.-Ing. habil. Ernst Habiger
Technische Universität Dresden
Institut für Automatisierungstechnik

E-mail:
ernst.habiger@mailbox.tu-dresden.de