IEC 80001: Risikomanagement vernetzter medizinischer Systeme

Armin Gärtner

Einleitung

Im Krankenhaus werden immer mehr Medizinprodukte in Netzwerke eingebunden, um Daten (z. B. radiologische Bilddaten) klinikweit dem Nutzer zur Verfügung zu stellen und/oder zentral zu speichern. Zusätzlich werden vermehrt telemedizinische Vernetzungen zwischen räumlich entfernten Krankenhäusern eingerichtet, um die Qualität der Patientenversorgung auch in kleineren Häusern mittels Teleradiologie und/oder Teleneurologie zu verbessern, die keine Radiologie oder Neurologie haben.

Mit dieser zunehmenden Vernetzung von Medizinprodukten nehmen auch Risiken und Zwischenfälle [2] zu, sodass ein Normenprojekt (IEC 80001) initiiert wurde, um vernetzte medizinische Systeme sicherer zu gestalten und Risiken zu beherrschen, die sich bei der Vernetzung ergeben. Die noch nicht abgeschlossene Norm IEC 80001 E soll u. a. das Risikomanagement für medizinische Netzwerke einzuführen. Nachfolgend wird ein erster kurzer Überblick über Inhalte und Umsetzung der zukünftigen Norm aus Sicht der Medizintechnik dargestellt.

Ausgangssituation: Risiken vernetzter Medizinprodukte

Folgende Erfahrungen, Überlegungen und Risiken [2] stellten die Basis für eine Norm dar, mit der die Risiken des Betriebes von Medizinprodukten in Netzwerken beherrscht werden sollen:

Hersteller haben bisher die Vernetzung ihrer Produkte in einem Netzwerk des Betreibers wenig berücksichtigt und dem Betreiber keine Informationen über eine sichere und zuverlässige Integration zur Verfügung gestellt.

Netzwerke sind i. d. Regel historisch gewachsen und nicht aus „einem Guss“ installiert. Die Netzwerke waren auch primär nicht für die Vernetzung von Medizinprodukten und den Datentransfer vorgesehen.

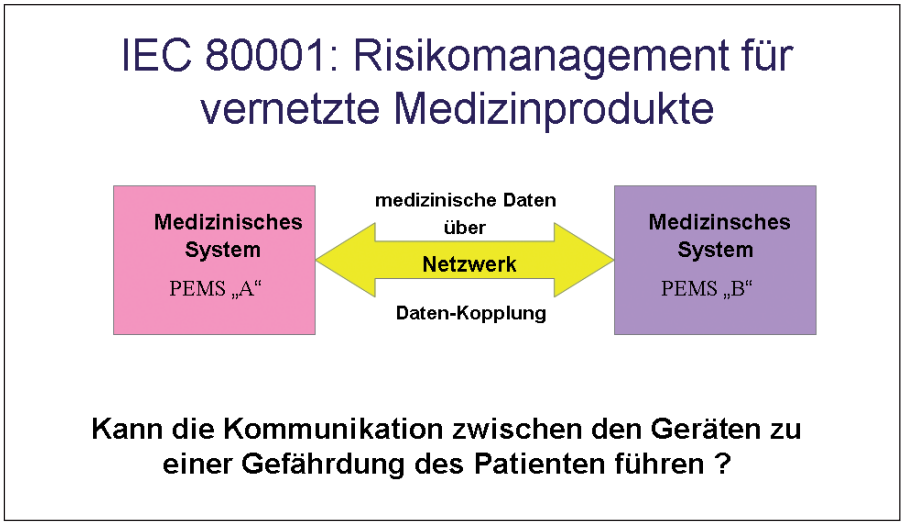

Abbildung 1: *Vernetzte programmierbare medizinische Systeme (PEMS)*

Der Betreiber führt die Vernetzung von Medizinprodukten technisch und organisatorisch häufig ohne Berücksichtigung der sich daraus ergebenden Konsequenzen und Komplikationen durch.

Durch das Aufkommen der Telemedizin werden nicht nur interne Prozesse und Abteilungen/Geräte eines Betreibers vernetzt, sondern zunehmend auch externe Anbindungen und Vernetzungen zwischen Krankenhäusern und anderen Anbietern im Gesundheitswesen durchgeführt, aus denen sich bisher nicht gekannte Probleme, Risiken und Gefährdungspotenziale ergeben.

Welche Risiken können beim Einsatz bzw. Anbindung/Integration von Medizinprodukten in ein Netzwerk eines Krankenhauses entstehen?

- Jedes Krankenhaus weist unterschiedliche gewachsene Netzwerkstrukturen auf (Ausnahme: Neubauten).
- Netze unterliegen einem permanenten Wandel, werden verändert, erweitert, erneuert usw.
- Neue Modalitäten bzw. aktive Medizinprodukte werden angeschlossen.
- Die Funktionalität und Belastung eines Netzes ändert sich.
- Netze wurden bisher nicht für die Bedürfnisse und Anforderungen der zunehmenden medizinischen Daten und Anschluss von Geräten entwickelt. Die Betreuung von Medizinprodukten und Netzwerken liegt historisch bedingt in unterschiedlichen Organisationsstrukturen der klassischen Abteilung Medizintechnik und IT.
- Modalitäten wie CT, MR usw. erfordern mittlerweile grundsätzlich einen Remote Service Anschluss.
- usw.

Folgende Risiken können bestehen:

- Netzwerküberlastung durch Flaschenhälse
- Inkompatibilitäten von Protokollen
- Fehlerhafte aktive Komponenten
- Übertragungsfehler durch Störeinkopplung

Autor: Armin Gärtner
Titel: IEC 80001: Risikomanagement vernetzter medizinischer Systeme
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2009
Seite: 40-44

- doppelte IP-Adressenvergabe
- Zugriffsschutz (Update, Upgrade, Release)
- Netzverfügbarkeit
- heterogene IT-Netzwerktopologien und Änderungen
- usw.

Daraus können sich erhebliche Probleme und Risiken für die Diagnose und Therapie von Patienten ergeben, indem

- Daten nicht oder nur unvollständig zur Verfügung stehen
- Daten nicht rechtzeitig zur Verfügung stehen
- Daten wie Bilder während einer Operation plötzlich nicht mehr zur Verfügung stehen
- Transfer von Vitalparametern und/oder Alarmen nicht möglich ist oder unterbrochen wird
- usw. usw.

Sicherheit (safety), Wirksamkeit (effectiveness), Datenschutz (data security) waren bisher im Gesundheitswesen wie dem Krankenhaus ohne spezifische Normung für IT-Netzwerke mit medizinischen Geräten dem Zufallsprinzip überlassen.

Richtlinie Medical Devices Directive (MDD) 93/42/EWG und Normen

Die Richtlinie MDD 93/42/EWG fordert Sicherheit für Patient, Anwender und Dritte beim Einsatz von Medizinprodukten. Weder die Richtlinie noch ihre nationale Umsetzung in Form des Medizinproduktegesetzes (MPG) beschäftigen sich mit dem Thema der vernetzten Medizinprodukte. Die technischen Details finden sich ansatzweise und vereinzelt in den Normen als Regeln der Technik.

Die Entwicklung und Fertigung von Medizinprodukten erfolgt nach Europäischen Richtlinien und harmonisierten Normen. Medizinprodukte können nur in Verkehr gebracht werden, wenn ein Konformitätsbewertungsverfahren erfolgreich abgeschlossen wurde, mit dem die Konformität mit der zutreffenden Richtlinie nachgewiesen wurde. Dieses Verfahren ist die Grundlage und Voraussetzung für die CE-Kennzeichnung.

Abbildung 2: *Vernetzte Medizinprodukte im Krankenhaus (Quelle G. Weller, Siemens)*

Die Anwendung von Medizinprodukten ist durch die Medizinprodukte-Betreiberverordnung geregelt. Die Einbindung von Medizinprodukten in ein IT-Netzwerk eines Betreibers (Krankenhaus, Arztpraxis) ist weniger an Bestimmungen gebunden und somit weitgehend nicht geregelt. Zwar behandeln entsprechende Normen für die IT allgemeine Themen wie Planung, Entwurf, Wartung u. a. eines Netzwerkes, aber bisher definierte keine Norm, wie Medizinprodukte mit den für allgemeine Daten und Zwecke gedachten IT-Netzwerken verbunden werden können und sollen.

Bereits die 3. Ausgabe der DIN EN 60601-1:2007 beschäftigt sich initial mit der Vernetzung von medizinisch elektrischen Geräten und Systemen, indem der Betreiber als „verantwortliche Institution" definiert und unterstellt wird, dass Betreiber und Hersteller von netzwerkfähigen medizinisch elektrischen Systemen gemeinsam die Sicherheit eines Systems aus Netzwerk und medizinisch elektrischen Geräten sicherstellen. Dies funktioniert [2] in der Praxis häufig nicht.

Die DIN EN 60601-1 enthält in der 3. Ausgabe, gültig seit Juli 2007 zwar wesentlich mehr betreiberbezogene Aspekte und Regelungen bezüglich des Anschlusses von Medizinprodukten an Netzwerke als die frühere 2. Ausgabe, geht aber nicht auf die Beherrschung der daraus entstehenden Risiken ein.

IEC 80001

Die IEC 80001 richtet sich an die Betreiber und Hersteller, die Aufgaben, Zuständigkeiten und Verantwortlichkeiten definieren müssen. Sie schlägt vor, das Verfahren des Risikomanagements einzusetzen, bevor die Einbindung eines Medizinproduktes in das IT-Netzwerk erfolgt. Das Risikomanagement muss über die gesamte Lebensdauer/Nutzung eines Medizinproduktes betrieben werden, um unerwünschte Auswirkungen bei der Einbindung und im Betrieb zu verhindern, die möglicherweise zu einem Schaden für Patienten (und Anwender sowie Dritte) führen können.

Die Aufgabe der Norm besteht darin, durch Herstellerangaben, vertragliche Vereinbarungen zwischen Hersteller und Betreiber, das Risikomanagement und Definition der Position des Risikomanagers (auch als Netzwerkintegrators bezeichnet) beim Betreiber folgende Zielsetzung zu erreichen:

- Sicherheit im Netzwerk
- Effektives Netzwerk
- Daten- und Systemsicherheit
- Vertraulichkeit
- Integrität der Daten
- Verfügbarkeit der Daten
- Interoperabilität
- Sicheres Zusammenschalten von Medizinprodukten und Geräten, die keine

Medizinprodukte sind, in demselben Netzwerk.

Die Norm fordert daher von Herstellern und Betreibern:

- Hersteller müssen konstruktionsbedingt die Einbindung von Medizinprodukten in Netzwerke beim Betreiber berücksichtigen.
- Der Betreiber (als verantwortliche Organisation bezeichnet) muss die Einbindung von Medizinprodukten in Netzwerke durch ein Risikomanagement begleiten.
- Die Einbindung von Medizinprodukten in ein IT-Netzwerk ist eine Aufgabe, die eine Einbindungsgestaltung erforderlich macht, die unabhängig vom Hersteller sein kann und eine Veränderung des Medizinproduktes einschließen darf.
- Der Betreiber als verantwortliche Organisation muss Personen bestimmen, die die in dieser Norm festgelegten Aufgaben und Verantwortlichkeiten übernehmen. Entscheidend ist die Bestellung des Risikomanagers für die medizinische IT-Einbindung.
- Hersteller sind dafür verantwortlich, Informationen und Anweisungen als Begleitpapiere für ein Medizinprodukt zur Verfügung zu stellen, mit dem der Risikomanager des Betreibers ein Medizinprodukt sicher in ein IT-Netzwerk einbinden kann.
- Die Begleitpapiere müssen Informationen enthalten, wie ein Medizinprodukt eingebunden und wie der Datenaustausch mit diesem Medizinprodukt ablaufen soll. Die Begleitpapiere sollten auch die Leistungsmerkmale festlegen und fordern, die das IT-Netzwerk und daran angeschlossene Geräte mindestens erfüllen müssen. Als weitere Informationen müssen die Begleitpapiere auch auf Gefährdungen durch missbräuchliche Anwendung der Netzwerkverbindungen oder der übertragenen Daten hinweisen.
- Der Risikomanager für die medizinische IT-Einbindung muss verantwortlich ein Verfahren sicherstellen, das
  - das Konfigurationsmanagement und die Änderungssteuerung des IT-Netzwerkes beinhaltet,
  - die Planung und Einbindung neuer Medizinprodukte berücksichtigt,
  - das Risikomanagement für die Eingliederung und die Anwendung der übertragenen Informationen vornimmt.

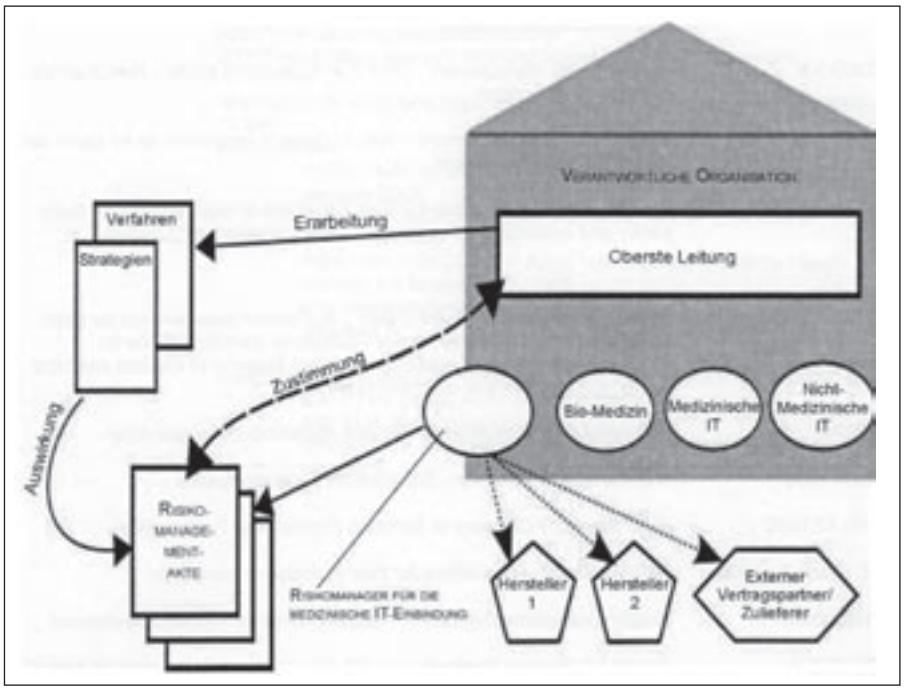

Abbildung 3: *Risikomanagement-Verknüpfungen*

Insbesondere der Betreiber eines Netzwerkes, d. h. normalerweise die Geschäftsführung, muss ein dauerhaftes Risikomanagement einführen, das nicht nur den Status eines Netzwerkes umfasst und beinhaltet sondern auch alle Änderungen in der Konfiguration des Netzwerkes einschließt.

Beispiel: Netzwerkgestützte EKG- und EEG-Analyse

Der Hersteller eines solchen netzwerkgestützten Systems übernimmt bzw. kann keine Verantwortung für das Netzwerk beim Betreiber übernehmen.

Er muss aber im Rahmen seines Konformitätsbewertungsverfahrens die sichere Funktionsfähigkeit der Datenübertragung mit einem anderem Netzwerk (Netzwerk X) überprüfen und validieren, d. h. er muss die Schnittstellen und das Systemverhalten testen sowie sicherstellen, dass bei einem Ausfall der Netzwerkübertragung Daten nicht verloren gehen. Dies bedeutet, dass ein netzwerkgestütztes System prüfen muss, ob Daten vollständig übertragen wurden, bzw. muss sicherstellen, dass im Fall einer Unterbrechung eine Wiederholung des Datentransfers an einen Server so lange erfolgt, bis der Server bzw. die Datenbank auf dem Server den vollständigen Abschluss der Übertragung an den sendenden PC im Netzwerk übermittelt. Dies bedeutet, dass der Hersteller dem Betreiber Informationen über den bestimmungsgemäßen und sicheren Betrieb seines Produktes in einer vernetzten Umgebung zur Verfügung stellen muss.

Ein Teil der Risikobetrachtung bei netzwerkgestützten Systemen muss eine weitere, unvermeidliche Prozessauswirkung berücksichtigen, die Belegung von Ressourcen in IT-Systemen. Durch ungünstige Wechselwirkungen zwischen den Ressourcenbedürfnissen unterschiedlicher Prozesse, etwa Bandbreitenbedarf in einem Netzsegment, kann zufällig oder vorsätzlich ein „weniger sicherheitskritischer" Prozess einen sehr sicherheitsbedürftigen Prozess mit den entsprechenden Folgen beeinträchtigen.

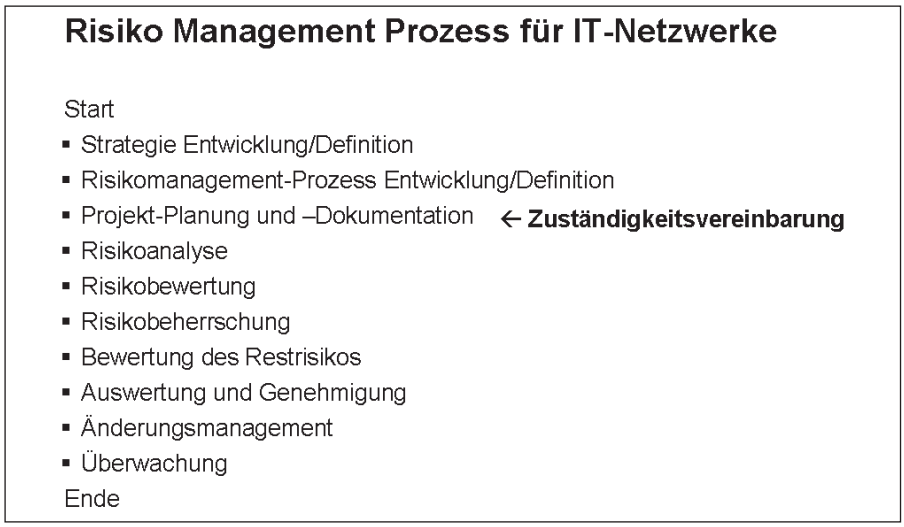

Abbildung 4: *Grundsätzliche Inhalte des Risikomanagement-Prozess für IT-Netzwerke*

Telemedizin

Die gleichen Überlegungen und Maßnahmen gelten auch für telemedizinische Verbindungen. Der Betreiber muss ein Risikomanagementverfahren auch für telemedizinische Anbindungen und Verbindungen aufbauen.

Mögliche Umsetzung in der Praxis

Die IEC 80001 definiert die Aufgaben und Positionen bei der verantwortlichen Organisation, die Aufgaben und Pflichten der Hersteller und beschreibt das Risikomanagement.

Die oberste Leitung (i. d. R. die Geschäftsführung eines Krankenhauses) muss folgende Aufgaben übernehmen:

- eine Strategie für die Bestimmung der Risiko-Akzeptanzkriterien aufstellen
- einen Prozess für die Anwendung des Risikomanagement über die gesamte Lebensdauer einführen
- Personen mit entsprechenden Befugnissen beauftragen, den Risikomanagementprozess auszuführen,
- die notwendigen Ressourcen zur Verfügung stellen
- die Risikomanagementakte für das IT-Netzwerk bestätigen,
- die Wirksamkeit der Maßnahmen zur Risikobeherrschung und die System- und Technologieänderungen überwachen und
- in regelmäßigen Abständen den Risikomanagementprozess einer Eignungsprüfung unterziehen.

Für diese Aufgaben muss die oberste Leitung folgende Funktionen definieren und Personen benennen:

- die Personen der Leitung, die die Informationserfassung, Auswertung und Bewertung durchführen und die gesamte Bereitstellung des Prozesses der Risikobewertung übernehmen
- den ausführenden Entscheidungsträger, der verantwortlich ist für die endgültige Anbindungsfreigabe von in ein IT-Netzwerk eingebundenen Medizinprodukten und
- den Eigentümer der Dokumentation hinsichtlich des Risikomanagementprozesses für das IT-Netzwerk mit Medizinprodukten, einschließlich den zugehörigen Zuständigkeitsvereinbarungen (Verträge) und der Risikomanagementakte für das IT-Netzwerk.

Die Geschäftsführung eines Krankenhauses kann die personelle Verantwortung und Haftung nicht auf den Risikomanager für die medizinische IT-Einbindung übertragen.

Der Risikomanager übernimmt folgende Aufgaben:

- Sammeln aller Informationen über Medizinprodukte
- Planung der Einbindung der Medizinprodukte entsprechend der von den verschiedenen Herstellern bereitgestellten Anweisungen
- Anwendung des Risikomanagement für IT-Netzwerke mit Medizinprodukten bei jeder Änderung, Ergänzung oder Erweiterung
- Information an die verantwortliche Organisation, d. h. an den Betreiber über das IT-Netzwerk mit Medizinprodukten und die möglichen Gefährdungen infolge von Änderungen in der Konfiguration.

Der Risikomanager hat eine Schnittstellenfunktion und muss daher mit internen und externen Beteiligten kommunizieren, am Risikomanagementprozess mitarbeiten und letztendlich an die Geschäftsführung als die oberste Leitung berichten.

Hersteller von Medizinprodukten übernehmen dabei folgende Aufgaben:

- Abschluss eines Kooperationsvertrages mit der verantwortlichen Organisation
- Information und Dokumentation bereitstellen:
  - Beabsichtigter Gebrauch des medizinischen, vernetzten Gerätes
  - Erforderliche Eigenschaften des IT-Netzwerkes
  - Erforderliche Konfiguration des IT-Netzwerkes
  - Beschränkung der Erweiterungsmöglichkeit des IT-Netzwerkes
  - Spezifikation des medizinischen Gerätes, einschließlich funktionale Sicherheitskonfiguration
  - Informationsfluss in und um das IT-Netzwerk
  - Zusammenfassung des Hersteller-Risikomanagements für das medizinische Gerät, soweit für die Vernetzung erforderlich
  - Weitere, für die Vernetzung hilfreiche Informationen.

Hersteller von IT-Technologie übernehmen ebenfalls wichtige Aufgaben: Sie müssen die verantwortliche Organisation mit allen notwendigen Dokumentationen über die im Netzwerk eingesetzten Geräte und Software versorgen, wie es in dem ab-

zuschließenden Kooperationsvertrag vereinbart werden muss.

Der Dokumentationsumfang muss mindestens folgende Aspekte umfassen:

- Technische Produktbeschreibungen
- Empfohlene Produktkonfigurationen
- Produktänderungen und Rückrufe
- Schutz gegen Internet-Risiken
- Testbeschreibungen und Testergebnisse.

Das Lebenszyklus-Risikomanagement für in IT-Netzwerke eingebundene Medizinprodukte umfasst u. a. folgende Aufgaben und Themen:

- Netzwerkplanung für medizinische Aufgaben
- Katalogisierung aller Modalitäten, Software, Versionszustände, Sammeln aller Informationen der Hersteller bezüglich der Einbindung der Produkte in Netzwerke
- Durchführen des Risikomanagementprozesses für alle Maßnahmen gemäß Bild 4.

Die Verfahrensschritte des Risikomanagementprozesses orientieren sich an der DIN EN 14971.

Weitere Entwicklungen

Die als Entwurf beim Beuth- oder VDE-Verlag erhältliche erste Fassung der Norm wird zur Zeit auf internationaler Ebene als 2. Committee-Draft überarbeitet. Diese zweite internationale Fassung wird vrsl. im November 2008 an die nationalen Normen-Kommitees verteilt. Da die Unterschiede zwischen der ersten und zweiten Fassung signifikant sind, wird es gegebenenfalls auch einen zweiten Entwurf in deutscher Sprache geben. Aus heutiger Sicht wird das Normenprojekt IEC 80001 nicht vor 2010 fertig werden.

Die IEC 80001 wird möglicherweise die Basis- oder Grundnorm für eine Reihe von weiteren Normen sein, die sich ähnlich entwickeln können wie die DIN EN 60601-1 mit den Zusatznormen und den Normen mit besonderen Anforderungen der Reihe DIN EN 60601-2-X.

Die Umsetzung der Anforderungen der Norm IEC 80001 wird auch in Deutschland mit dazu beitragen, dass Krankenhäuser Risikomanagementprozesse einführen werden. Die Norm wird auch zu einer weiteren Integration und Zusammenarbeit der Bereiche IT und MT zu MIT führen.

Literatur und Quellenangaben

1 DIN IEC 80001; VDE 0756-1:2008-03 Norm-Entwurf, 2008-03 Anwendung des Risikomanagements für IT-Netzwerke mit Medizinprodukten (IEC 62A/591/CD:2007)

2 Stettin, J.; Hintergründe zur Norm IEC 8001, 8. Würzburger Medizintechnik Kongress, Kongressband ISBN 978-3-937988-06-1, S. 137 – 138

3 Rose, I.; Ross, P.; Erwartungen der Betreiber an die Norm 80001, 8. Würzburger Medizintechnik Kongress, Kongressband ISBN 978-3-937988-06-1, S. 139 -140

4 Pauli, N.; IEC 80001 – Eine Herausforderung für die Medizinprodukte-Industrie, 8. Würzburger Medizintechnik Kongress, Kongressband ISBN 978-3-937988-06-1, S. 141 – 142

5 Sefkovicz, H.; IT-Praxis für Medizintechniker – Sicherheitsaspekte in der vernetzten IT-Welt, 8. Würzburger Medizintechnik Kongress, Kongressband ISBN 978-3-937988-06-1, S. 143 - 145

6 Hüsken, V.; Erste Hilfe: IT-Sicherheit, EHEALTHCOMPASS aus EHEALTHCOM Nr. 5, September/Oktober 2007, S. 4 – 9

7 Maus, T.; Zur Inventarisierung und Bewertung von IT-Risiken – MEDNET, Arbeitsbuch für die integrierte Gesundheitsversorgung 2005/5, Edition Timmen, ISBN 3-86108-056-7

8 Kaiser, J.; Absicherung vernetzter Medizinprodukte, Vortrag Würzburger Medizintechnik Kongress 2008

9 Stettin, J.; IEC 80001: Risikomanagement im Krankenhaus, Vortrag Würzburger Medizintechnik Kongress 2008

10 Weller, G.; Verantwortlichkeits-Vereinbarungen zwischen Herstellern und Betreibern zur IEC 8001, Vortrag Würzburger Medizintechnik Kongress 2008

11 Gärtner, A.; Band 3 Telemedizin und computerunterstützte Medizin, Reihe Medizintechnik und Informationstechnologie, TÜV Media Verlag Köln 2006, ISBN 978-3-8249-1004-7

Kontakt
Armin Gärtner
Dipl.-Ing. Medizintechnik
ö. b. u. v. Sachverständiger für Medizintechnik und Telemedizin der IHK Wuppertal Remscheid Solingen
Ingenieurbüro für Medizintechnik
Edith-Stein-Weg 8
40699 Erkrath
Tel.: +49 (0) 21 04 / 3 55 19
Armin.gaertner@t-online.de

DGTelemed