

**IEC 80001 -  
Anwendung des  
Risiko Managements  
für IT-Netzwerke “mit”  
medizinischen Geräten**

*“Application of Risk Management for IT-networks incorporating  
Medical Devices”*

# Gerhard Weller

Siemens AG  
Healthcare Sector  
Med QT ST  
Henkestraße 127  
91052 Erlangen

Tel. 09131 - 842391

[gerhard.weller@siemens.com](mailto:gerhard.weller@siemens.com)



## **Zuständigkeiten:**

Übergreifende Innovations-Aktivitäten, Technologie Management,  
Standardisierung (DKE 811.3, DKE 811.3.2, IEC 80001), ...

## Historie

### **IEC 80001 hat eine bewegte Historie aufzuweisen**

- Start unter DIN DKE 811 Ende der neunziger Jahre
- Inzwischen ca. 30 Arbeitsgruppen-Sitzungen
- Erster Anlauf zur internationalen Normenzulassung scheitert
- Titel bis 2005: „Sicherheit von medizinisch genutzten Geräten/Systemen/Einrichtungen in der vernetzten Anwendung“
- Anschließend internationale Sondierungsgespräche führen zu einer Titeländerung, Risikomanagement steht nunmehr im Fokus
- Die internationale, gut vorbereitete Abstimmung des NWIP mit dem geänderten Titel verläuft positiv
- Bisher 4 internationale Meetings, jeweils 30...40 Teilnehmer
- Beim letzten internationalen Meeting in Roanoke/USA wird leider die Netzwerk-Klassifizierung A/B/C als unnötig erachtet und gestrichen
- Hersteller, Anwender, Berater, Körperschaften, Zulassungsstellen, Behörden, Universitäten sind in ausgewogenem Verhältnis beteiligt

## IT-Netzwerke und IEC 80001

### IT-Netzwerke „in Krankenhäusern“:

- stark zunehmende Verbreitung (Mobil-/Kleingeräte, WLAN, RFID, ...)
- müssen hohe Ansprüche erfüllen (*patient safety, data security*)
- übertragen vielfältige Daten:
  - Verwaltungsdaten (z.B. von *non-medical devices*)
  - zeitkritische Patienteninformationen (z.B. von *medical devices*)
  - vertrauliche und potentiell riskante Daten (z.B. e-Mails, www)
- nutzen zunehmend gemeinsame Leitungsnetze
- schaffen ggfs. eine Verbindung mit dem Internet
- werden bisher von keinem Standard unterstützt
- Verantwortlichkeit oftmals unklar

### IEC 8000 ist die erste umfassende Norm:

- für IT-Netzwerke in Krankenhäusern (*user facilities*)
- die sich ganz wesentlich auch an die Betreiber richtet

Status 2008-02: CD Entwurf, 30 Seiten (*Committee Draft*)

## Probleme und Risiken mit IT-Netzwerken „in Krankenhäusern“

### **Normung, Regulierung, Zulassung medizinischer Geräte**

Herstellung und Gebrauch medizinischer Geräte unterliegen der:

- Normung
- Regulierung
- Zulassung

### **Normung, Regulierung, Zulassung – nicht für IT-Netzwerke?**

- IT-Netzwerke werden nicht spezifisch für Kliniken zertifiziert/zugelassen
- Klinische IT-Netzwerke verbinden medizinische Geräte miteinander, aber auch mit nicht-medizinischen Geräten/Software
- Die Anbindung medizinischer Geräte an IT-Netzwerke unterliegt bisher keiner Normung
- *Safety, effectiveness* und *data security* für IT-Netzwerke mit medizinischen Geräten sind daher bisher dem Zufallsprinzip überlassen

## Probleme und Risiken von IT-Netzwerken vermeiden

### IEC 80001 hilft Probleme und Risiken zu vermeiden:

- Systematische Prozesse bei Netzwerk-Erstellung und -Betrieb (statt Zufallsprinzip)
- Klar definierte Zuständigkeiten und Verantwortlichkeiten bei Herstellern und Betreibern
- fokussiert auf Risiko. Management Aktivitäten bei der IT-Vernetzung medizintechnischer Geräte (*Medical Devices*) als zentrale Sicherheits-Aktivität

### Die wesentlichen Prozess-Schritte der IEC 80001:

- Planung der (Des-)Integration eines medizinischen Gerätes
- Risiko Management:
  - startet zur Planung, läuft über gesamte Integrations-Lebensdauer
- Hersteller und Anwender kooperieren bei allen notwendigen Aktivitäten
- Ein verantwortlicher Integrations-Manager wird benannt
- Top-Management trifft Entscheidungen, trägt persönliche Verantwortung

## Risiko Management

### Anwendung von Risiko Management bei IEC 80001:

- während der gesamten Integrations-Lebensdauer:
  - Planung
  - Betrieb
  - Änderungen
  - Außerbetriebnahme
- für das Netzwerk und die damit verbundenen medizinischen Geräte
- durch die verantwortlichen Organisation (*responsible organisation*)
- für grundlegende, auszugleichende Eigenschaften\*):
  - Sicherheit (*SAFETY*, für Patienten)
  - Wirksamkeit (*EFFECTIVENESS*)
  - Daten- und Systemsicherheit (*SECURITY*)
  - Interoperabilität (*INTEROPERABILITY*)
- wenn die Verantwortung außerhalb der Kontrolle eines Herstellers liegt
- mit mindestens minimalem Prozeßumfang durchzuführen

\*)Nicht sachgemäßer Ausgleich der auszugleichenden Eigenschaften wird als Gefährdung der Patienten oder der verantwortlichen Organisation interpretiert.

## Hersteller

### **Aufgaben des Herstellers gemäß IEC 80001: (*MANUFACTURER*)**

Hersteller medizinischer Geräte müssen die verantwortliche Organisation mit allen notwendigen Informationen versorgen (z.B. technische Anleitungen zur Vernetzung der medizinischen Geräte).

Neu und erstmalig bei IEC 80001:

Aufteilung der Rollen und Verantwortlichkeiten an:

Hersteller (*MANUFACTURER*)

und

Betreiber (in der Regel *RESPONSIBLE ORGANISATION*)

## Hersteller

### **Weitere Aufgaben des Herstellers gemäß IEC 80001:**

- 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 Risiko Managements für das medizinische Gerät, soweit für die Vernetzung erforderlich
  - Weitere, für die Vernetzung hilfreiche Informationen

## IT Technologie Hersteller

### **Aufgaben der IT Technologie Herstellers gemäß IEC 80001:**

- Belieferung der verantwortliche Organisation mit allen notwendigen Dokumentationen über die im Netzwerk eingesetzten Geräte und Software, wie im Kooperationsvertrag angegeben
- Dokumentations-Mindestumfang:
  - Technische Produktbeschreibungen
  - Empfohlene Produktkonfigurationen
  - Produktänderungen und Rückrufe
  - Schutz gegen Internet-Risiken
  - Testbeschreibungen und Testergebnisse

## Verantwortliche Organisation

### **Aufgaben der verantwortlichen Organisation gemäß IEC 80001: (*RESPONSIBLE ORGANISATION*)**

- Start, Durchführung, Verantwortung des Risiko Management Prozesses
- Benennung von Rollen und nachgeordneten Verantwortlichkeiten
- Abschluß einer Verantwortlichkeits-Vereinbarung (*RESPONSIBILITY AGREEMENT*) mit allen am IT Netzwerk Projekt beteiligten Partnern
- hält übergeordnete Projekt-Verantwortlichkeit über die Projekt-Lebensdauer

## Top Management

### **Verantwortlichkeiten und Aufgaben des Top Management gemäß IEC 80001:**

- persönliche Verantwortung und Haftung
- erstellt Richtlinien zur Bestimmung von Risiko-Akzeptanzkriterien
- veranlaßt den Lebensdauer Risikomanagement Prozess
- benennt berechnigte Personen zur Durchführung des Risiko Management Prozesses und stellt die nötigen Ressourcen bereit
- Benennt den qualifizierten medizinischen IT Integrations Risiko Manager
- gibt die IT-Netzwerk Risiko Management Dokumentation frei
- beobachtet die Wirksamkeit von Risikokontrollmaßnahmen und System- und Technologieänderungen
- überprüft regelmäßig die Eignung des Risiko Management Prozesses

Top Management kann eine Einzelperson oder Personengruppe innerhalb der verantwortlichen Organisation sein

## Top Management

### Weitere Aufgaben des Top Management gemäß IEC 80001:

Identifikation des:

- verantwortlichen Management Teams für alle Aktivitäten des Risiko Bewertungs Prozesses
- verantwortlichen Entscheiders zur abschließenden Freigabe der Netzwerk-Verbindungen medizinischer Geräte
- Dokumentationsverantwortlichen (einschließlich der Verantwortungs-Vereinbarung und der IT-Netzwerk Risiko Management Doku)

Während des Risk Management Prozesses die Sicherstellung der Teilnahme des verantwortlichen Managements für:

- IT-Netzwerke mit medizinischen Geräten (medizinische IT Abteilung)
- IT-Abteilung (allgemeine IT Abteilung)
- Medizinische Geräte (Medizintechnik, zuständig für die Betreuung von vernetzten medizinischen Geräten über die gesamte Lebensdauer)

## Top Management

### **Delegation von Aufgaben des Top Management gemäß IEC 80001:**

Das Top Management kann Aufgaben des Risiko Management Prozesses per Vertrag an einen oder mehrere medizinische IT Integrations Risiko Manager delegieren.

Die abschließende Verantwortung der Entscheidung bezüglich eines möglichen Risikos/Vorteils und der Qualität und Sicherheit der Daten und Systeme verbleibt jedoch beim Top Management.

## Medizinischer IT Integrations Risiko Manager

### **Verantwortlichkeiten und Aufgaben des medizinischen IT Integrations Risiko Managers gemäß IEC 80001:**

- Moderation und/oder Durchführung des Risiko Management Prozesses
- Alle relevanten Informationen der medizinischen Geräte einholen
- Integrationsplanung der medizinischen Geräte in Übereinstimmung mit den entsprechenden Angaben der Hersteller-Informationen
- Risikomanagement für das IT-Netzwerk durchführen, auch bei Änderungen, Ergänzungen/Erweiterungen oder Verkleinerungen
- Information der verantwortlichen Organisation über das IT-Netzwerk und mögliche Risiken aufgrund jeglicher Konfigurationsänderungen
- Bericht an das Top Management

Person: Einzelexperte oder Expertengruppe, von der verantwortlichen Organisation, von Extern, oder beides.

Die abschließende Verantwortung kann jedoch nicht vom Top Management auf den Integrations Risiko Manager delegiert werden.

## Übereinstimmung

### **Übereinstimmung eines IT-Netzwerk Projektes mit IEC 80001:**

- wird kontrolliert durch Überprüfung der Dokumentation die gemäß IEC 80001 gefordert ist
- die Überprüfung beinhaltet auch:
  - die Verantwortlichkeits-Vereinbarung
  - die Risiko Management Dokumentation

Andere anwendbare Normen sind ebenfalls zu beachten. Dies betrifft insbesondere:

ISO 14971:2007, *Medical devices – Application of risk management to medical devices*

**Danke für Ihre  
Aufmerksamkeit!**