EHEALTHCOM
Magazin für Health-IT, vernetzte Medizintechnik und Telemedizin

Broadcaststurm im Med. IT-Netzwerk – Teil 2: Risikomanagement

Expertenbeitrag von Armin Gärtner und Mahmoud El-Madani

Der zweite Teil des Artikels über einen Broadcaststurm als Ursache für eine Patientengefährdung beschreibt das Risikomanagement. Dabei liegt der Schwerpunkt des Beitrages darauf, zu zeigen, wie man zum einen das initiale Risikomanagement in eine technische Dokumentation integriert und zum anderen, wie man das Risikomanagement über den Lebenszyklus des Medizinischen IT-Netzwerkes aufrechterhält. Dazu werden die beiden Risikomanagement-Normen DIN EN 80001-1 und DIN EN ISO 14971 herangezogen und angewendet.

Technische Dokumentation als Basis für ein Risikomanagement

Um ein Risikomanagement für eine Patientenüberwachungsanlage durchzuführen, benötigt man viele Informationen über das geplante Medizinische IT-Netzwerk, das Anforderungsprofil der Anwender aber auch über das umzusetzende technische Konzept und das Betriebskonzept. Die dazu benötigten Informationen und Abstimmungen mit den Nutzern werden sinnvollerweise im Vorfeld der Beschaffung geklärt und in einer Projektdokumentation oder technischen Dokumentation (TD) zusammengefasst [1]. Eine solche technische Dokumentation über ein Projekt stellt somit die Grundlage dar, auf der überhaupt erst ein praktikables Risikomanagement durchgeführt werden kann.

Durch die vorherige Abstimmung und Beschreibung insbesondere des technisches Konzeptes und des Betriebskonzeptes können viele der Fragen nach Gefährdungen und Risiken, die im Risikomanagement gestellt werden, bereits beantwortet werden. So kann das technische Konzept z. B. die Beschreibung beinhalten,

- ob und dass ein vom Krankenhaus gelieferter LAN-Switch verwendet wird,
- ob der LAN-Switch Funktionen zur Verhinderung von Broadcast- bzw. Multicast-Stürmen unterstützt oder beinhaltet,
- ob die Software des LAN-Switches Funktionen zur präventiven Warnung vor Broadcast-Stürmen bietet,
- wer den LAN-Switch konfigurieren und testen darf,
- wie der LAN-Switch zu konfigurieren ist,
- wie Tests und Abnahmeprozesse verlaufen,
- wie ein Change Management Prozess definiert und umgesetzt wird
- u. a. Fragestellungen.

Wenn dann im Risikomanagement mögliche, IT-bedingte Gefährdungen als Ursachen für Risiken erkannt werden, können diese unter Verweis auf das technische Konzept und Betriebskonzept im Rahmen der technischen Dokumentation beantwortet werden.

Nachfolgend soll gezeigt werden, welchen Beitrag ein Risikomanagement nach DIN EN 80001-1 [2] bzw. DIN EN ISO 14971 [3] leisten kann, um eine solche, in Teil 1 beschriebene Situation eines Broadcaststurms in einem Medizinisches IT-Netzwerk mit Patientengefährdung zu verhindern bzw. die Auftretenswahrscheinlichkeit zu verringern.

Risikomanagement – Ermittlung von Gefährdungen

In dem vorgenannten Beispiel des Broadcaststurms gab es weder eine technische Dokumentation über die Planung und Installation noch ein Risikomanagement für die Patientenüberwachungsanlage z. B. nach DIN EN 80001-1.

Eine solche Technische Dokumentation dient als Basis für die Durchführung eines Risikomanagements nach DIN EN 80001-1, für das die Begriffe, Verfahren und Beispiele der DIN EN ISO 14971 verwendet werden können.

Diese Norm enthält die Grundlagen für die Anwendung des Risikomanagements auf Medizinprodukte, die in der DIN EN 80001-1 nicht enthalten sind. Dafür beschreibt die Tabelle A.1 der DIN EN 80001-1 den Zusammenhang zwischen beiden Normen, aus dem hervorgeht, dass für ein Risikomanagement die Norm DIN EN ISO 14971 verwendet werden kann.

Grundlage Risikomanagement
Technische Dokumentation!

Inhalt:
- Anforderungsprofil
- Workflow der Anwender
- Technisches Konzept
- Betriebskonzept

Technische Dokumentation als Grundlage → Risikomanagement

Abbildung 1: Inhalte und Nutzen einer technischen Dokumentation

Risikomanagement Med. IT-Netzwerk

Anwendung DIN EN 80001-1

Begriffe und Verfahren der DIN EN ISO 14971

Drei Schutzziele
1. Safety – Patientensicherheit
2. Security – Daten und Systemsicherheit
3. Effektivität

- Gefährdung
- Ursachen
- Gefährdungssituation
- Risikoanalyse und -Bewertung
- Maßnahmen zur Risikominimierung

Abbildung 2: Zusammenhang zwischen DIN EN 80001-1 und DIN EN ISO 14971

Mit anderen Worten, da die DIN EN 80001-1 auf die Risikoanalyseverfahren der DIN EN ISO 14971 verweist, wird nachfolgend ein vereinfachtes Risikomanagement nach dieser Norm kurz erläutert.

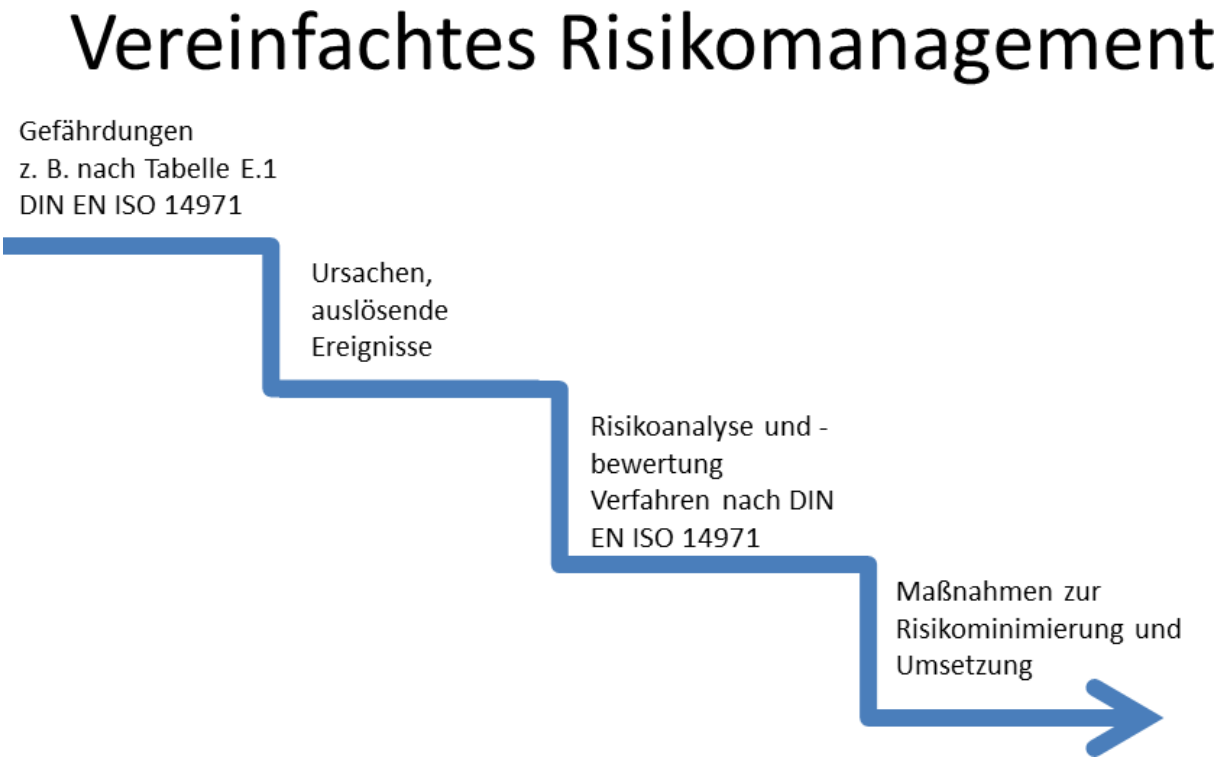

Abbildung 3: Vereinfachtes Risikomanagement nach DIN EN ISO 14971

Gemäß Abbildung 3 besteht ein vereinfachtes Risikomanagement aus den folgenden grundsätzlichen Teilschritten:

- Ermittlung von Gefährdungen
- Ursachen, auslösende Ereignisse und Gefährdungssituationen
- Risikoanalyse mit –Bewertung
- Maßnahmen

Bezogen auf das in Teil 1 geschilderte Vorkommnis mit einem nicht richtig konfigurierten LAN-Switch als Teil eines Medizinischen IT-Netzwerkes bedeutet dies, mögliche Gefährdungen durch eine IT-Netzwerkkomponente wie einem LAN-Switch u. a. zu ermitteln und eine Risikoanalyse sowie –Bewertung durchzuführen.

Um dazu Gefährdungen zu ermitteln, kann man auf den informativen Anhang E der DIN EN ISO 14971 zugreifen, der folgende Tabellen mit Beispielen als Hilfestellung enthält:

- Tabelle E.1 - Beispiele von Gefährdungen
- Tabelle E.2 - Beispiele von auslösenden Ereignissen und Umständen

- Tabelle E.3 – Zusammenhang zwischen Gefährdungen, vorhersehbaren Abfolgen von Ereignissen, Gefährdungssituationen und dem möglicherweise auftretenden Schaden.

Die nachfolgende Tabelle 1 enthält daher die zutreffenden Beispiele aus dem Anhang E.1, die durch einige IT-bedingte Gefährdungen ergänzt wurden. Die beispielhaften Ergänzungen sind kursiv dargestellt und können nach Belieben erweitert werden

Beispiele von Gefährdungen durch den Betrieb des Med. IT-Netzwerkes (Patientenüberwachungsanlage)
Funktion
Unrichtige oder ungeeignete Ausgabe oder Funktionsweise
Unkorrekte Messungen
Fehlerhafte Datenübertragungen
Verlust oder Abbau der Funktion

Beispielhafte Ergänzungen

Organisatorisch nicht geregelte Zuständigkeit
Unzureichende Spezifikation der Überprüfungen vor Gebrauch
Unzureichende Personalausstattung der Anwender
Fehlerhafte Konfigurationen von Netzwerkkomponenten wie eines LAN-Switches als zentrale Komponente eines Med. IT-Netzwerkes
Fehlende Funktionen in einer Software und/oder Hardware
Kauf von alternativer Hardware ohne vorherige Bewertung (Evaluierung) der benötigten Funktionen bzw. ob benötigte Funktionen vorhanden sind
Einsatz eines Switches des Krankenhauses anstelle eines vom Hersteller mitgelieferten Switches für das Med. IT-Netzwerk
Fehlende Kenntnisse der Abteilung Medizintechnik für IT-Netzwerke
Fehlende Kenntnisse der Abteilung IT für Medizinprodukte
Menschliche Faktoren

Beispiele von Gefährdungen durch Information
Kennzeichnung von Produkten und Informationen
Unvollständige Gebrauchsanweisung
Unzureichende Beschreibung der Leistungsmerkmale
Unzureichende Spezifikation der Zweckbestimmung
Unzureichende Information über Gebrauchseinschränkungen

Beispielhafte Ergänzungen

Fehlendes Projektmanagement
Unzureichende Abstimmung zwischen Herstelleranforderungen an Netzwerk-Infrastruktur und Vorgaben einer krankenhauseigenen IT-Abteilung bezüglich Netzwerkkomponenten wie Switches
Fehlende / unzureichende Zusammenarbeit zwischen MT und IT eines Krankenhauses
Fehlende Planung und fehlendes Konzept für ein Med. IT-Netzwerk

Festlegung zu Betrieb und Instandhaltung
Keine Vereinbarung in Form von Service Level Agreements (SLA) zwischen MT und IT eines Krankenhauses

Tabelle 1.: Beispiele von Gefährdungen nach DIN EN ISO 14971 Anhang E.1 (ohne Anspruch auf Vollständigkeit)

Risikomanagement nach DIN EN 80001-1

Wie im vorigen Abschnitt und in Abbildung 2 gezeigt, können bei einem Risikomanagement nach DIN EN 80001-1 die Begriffe und Verfahren der DIN EN ISO 14971 verwendet werden.
Die DIN EN 80001-1 definiert drei Schutzziele für ein Med. IT-Netzwerk wie einer Patientenüberwachungsanlage:

- Safety – Patientensicherheit
- Security – Daten und Systemsicherheit
- Effektivität

Mit Hilfe der Verfahren der DIN EN ISO 14971 kann herausgearbeitet werden, welche Risiken die Einhaltung dieser Schutzziele gefährden und wie man solche Risiken minimieren kann. In dem Beispiel der Patientengefährdung in Teil 1 durch einen Broadcaststurm soll nachfolgend nur das Schutzziel der Patientengefährdung nach DIN EN 80001-1 betrachtet werden.

Die Betrachtung der beiden anderen Schutzziele der Norm würde den Rahmen dieses Beitrages sprengen.

Zur Vorbereitung der Gefährdungs- und Risikoanalyse kann man die Tabelle E.3 der DIN EN ISO 14971 verwenden, um sich einen Überblick und mögliche Auswirkungen von Gefährdungen zu verschaffen.

Die Tabelle E.3 betrachtet beispielhaft den Zusammenhang zwischen Gefährdungen, vorhersehbaren Abfolgen von Ereignissen, Gefährdungssituationen und dem möglicherweise auftretenden Schaden, der in diesem Beispiel durch einen Broadcaststurm auf Grund eines fehlerhaften bzw. nicht richtig konfigurierten LAN-Switches entstanden ist.

Schutzziel Patientensicherheit

Gefährdung	Ursache - Vorhersehbare Abfolge von Ereignissen	Gefährdungs-situation	Schaden
Nicht vollständige bzw. fehlerhafte Konfiguration eines LAN-Switches – Keine technische Dokumen-tation vorhanden.	Ein Anwender erzeugt im Med. IT-Netzwerk einen Loop, der zu einem Broadcaststurm führt. Die Situation entsteht, indem ein herunterhängendes Netzwerkkabel versehentlich in eine Netzwerkdose gesteckt wird, das auf der anderen Seite bereits in einer Netzwerkdose steckt.	Monitore und -Zentrale stellen Überwachungs-funktion ein. Kritisch kranke Patienten werden auf Grund zu geringer Personalausstattung nicht überwacht. Wiederherstellung der Betriebsbereitschaft der Monitore verzögert sich.	z. B. Tod bei Auftreten einer Asystolie, die durch fehlende Alarmierung und zu geringer Personal-ausstattung nicht therapiert wird.
w. v.	Medizintechnik verfügt über keine IT-Kenntnisse – kann Ursache nicht erklären und nicht beheben	w. v. Wiederherstellung der Betriebsbereitschaft der Monitore verzögert sich.	w. v.
w. v	IT verfügt über keine Medizintechnik-Kenntnisse und kann/will keine Fehlersuche durchführen	w. v.	w. v.
w. v	Keine Rufbereitschaft der technischen Abteilung Anwender bekommen nachts und am Wochenende keine Hilfestellung durch MT oder IT	w. v.	w. v.
	Anwendung durch unausgebildetes/ungeübte s Personal	w. v.	w. v.

Tabelle 2: Tabelle E.3 DIN EN ISO 14971 (ohne Anspruch auf Vollständigkeit)

Die ermittelten Gefährdungen, die zu einem nicht akzeptablen Schaden führen können, können dann in einem nächsten Schritt in Form einer Risikoanalyse und Risikobewertung betrachtet werden. Dabei gilt es insbesondere zu ermitteln, ob es sich um inakzeptable Risiken handelt und mit welchen Maßnahmen solche Risiken möglichst minimiert oder sogar vermieden werden können.

Der Vollständigkeit halber sei darauf hingewiesen, dass auch bei einem sorgfältig durchgeführten umfassenden Risikomanagement Restrisiken verbleiben. Solche Restrisiken bestehen darin, dass neue, bisher unbekannte Gefährdungen auftreten. Zum anderen bestehen sie darin, dass sich z. B. Anwender nicht an die festgelegten

Prozesse und Dienstanweisungen beim Einsatz von Verteilten Alarmsystemen halten, wodurch Situationen entstehen, in denen Patienten mit einer Asystolie nicht (rechtzeitig) therapiert werden können.

Durchführung eines Risikomanagements vor der Planung bzw. Installation

Wie sich bei der Ursachenanalyse des in Teil 1 geschilderten Zwischenfalls zeigte, war während des Entwurfs, der Planung und Installation der Patientenüberwachungsanlage keine technische Dokumentation erstellt worden. In einer solchen Dokumentation sollte die Verwendung eines von der Krankenhaus-IT vorgegebenen, alternativen LAN-Switches anstelle des vom Hersteller der Patientenüberwachungsanlage vorgesehenen LAN-Switches im technischen Konzept und Betriebskonzept beschrieben sein. Dadurch lassen sich im Vorfeld folgende Fragestellungen beantworten:

- Entspricht der von der Krankenhaus-IT geforderte LAN-Switch in seinen netzwerktechnischen Funktionen dem Original-LAN-Switch des Herstellers der Patientenüberwachungsanlage?
- Verfügt der von der Krankenhaus-IT geforderte LAN-Switch über die gleichen Eigenschaften und Leistungsparameter wie der Original-LAN-Switch des Herstellers der Patientenüberwachungsanlage?
- Wer ist für die Überwachung und den Service des von der Krankenhaus-IT bereitgestellten LAN-Switches verantwortlich und wer führt es durch?
- Wer prüft und validiert, ob die vom Hersteller der Patientenüberwachungsanlage vorgegebenen Anforderungen an einen LAN-Switch eingehalten werden bzw. umgesetzt wurden?
- Wer prüft und testet, ob der LAN-Switch nach Einspielen von Firmware-Upgrades ordnungsgemäß funktioniert, Konfigurationen und Netzwerkprotokolle wie das Spanning-Tree-Protokoll oder andere technische Maßnahmen zur Vermeidung eines Broadcaststurms [4] korrekt funktionieren?
- U. a. Fragen.

Wenn diese Fragestellungen bereits während der Planung und Installation geklärt werden, können diese Fragestellungen im Risikomanagement unter Verweis auf die Beschreibung der technischen Dokumentation beantwortet werden.

Fortschreibung des Risikomanagements über den Lebenszyklus einer Patientenüberwachungsanlage - Informationen aus dem laufenden Betrieb

Beide in diesem Beitrag referenzierten Normen beschreiben die Notwendigkeit einer Fortschreibung des Risikomanagements über den Lebenszyklus eines Medizinproduktes bzw. Medizinproduktesystems. Diese Anforderung gilt somit nicht nur für Hersteller sondern auch für Betreiber.

Im sog. „informativen Anhang“ A.2.9 betont die DIN EN ISO 14971 sehr deutlich, dass ein Risikomanagement niemals als beendet anzusehen ist, wenn ein Medizinprodukt bzw. ein Medizinproduktesystem in Betrieb gehen.

Die weitere Fortführung des Risikomanagements ergibt sich auch aus Kapitel 4 der Norm 80001-1, die vom Betreiber verlangt, dass er die Schutzziele für ein Medizinisches IT-Netzwerk während des gesamten Lebenszyklus einhält. Dies bedeutet in der Praxis, dass nach Errichtung und Inbetriebnahme eines solchen Medizinischen IT-Netzwerkes in der Technischen Dokumentation festgelegt werden muss, in welchen Zeiträumen (z. B. nach einem Jahr) der Risikomanager oder die Risikomanagementgruppe (gemäß dem Vorschlag der Norm 80001-1) die betreffende Risikomanagementakte für ein solches Medizinisches IT-Netzwerk erneut überprüft und erforderlichenfalls aktualisiert.

Weitere Erfahrungen, die im Rahmen einer erneuten Überarbeitung einer Risikomanagementakte betrachtet werden sollten, können beispielsweise aus den Meldungen eines Ticketsystems einer Krankenhaus IT-Abteilung oder aber der Gerätebuchdokumentation der Medizintechnik stammen. Aber auch Literaturhinweise, Hinweise des Bundesinstitutes für Arzneimittel und Medizinprodukte (BfArM), Fachzeitschriften sowie Hinweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sollten gesammelt und als mögliche Gefährdungen in die Risikomanagementakte aufgenommen und analysiert werden.

Zusammenfassung und Empfehlungen

Das vorgestellte, anonymisierte Beispiel eines Broadcaststurms im Netzwerk einer Patientenüberwachungsanlage (siehe Teil 1) zeigt sehr deutlich, wie eine IT-bedingte Gefährdung durch einen nicht korrekt konfigurierten LAN-Switch zu Risiken für Patienten geführt hat.

Das Beispiel zeigt warum man das Risikomanagement **nach** DIN EN 80001-1 und DIN EN ISO 14971 als vorausschauende und prophylaktische Maßnahme einsetzen sollte, um derartige Gefährdungen und Risiken für Patienten zu reduzieren oder sogar zu vermeiden. Dies gilt umso mehr, wenn ein Krankenhaus Konzeption, Planung und Installation eines Medizinischen IT-Netzwerkes in Form einer technischen Dokumentation zusammenfasst und diese als Basis für ein Risikomanagement nutzt.

Mit einer solchen Vorgehensweise erfüllt ein Krankenhaus seine Sorgfaltspflichten gegenüber seinen Patienten sowie die rechtlichen Anforderungen der Medizinprodukte-Betreiberverordnung.

Die Einrichtung eines Risikomanagements für vernetzte Medizinprodukte über den Lebenszyklus hilft also einerseits, die Patientensicherheit zu verbessern. Zum anderen versetzt es eine Krankenhausorganisation in die Lage, zu lernen, wie sie mit neuen Bedrohungen und Gefährdungen nicht nur für Medizinische IT-Netzwerke umgehen kann.

Literatur und Quellenangaben

1. Gärtner, A.; Verteilte Alarmsysteme, TÜV Media GmbH Köln, 2016, ISBN 978-3-8249-1990-1
2. DIN EN 80001-1:2011-11; VDE 0756-1:2011-11 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten
3. DIN EN ISO 14971:2013-04 Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte (ISO 14971:2007, korrigierte Fassung 2007-10-01); Deutsche Fassung EN ISO 14971:2012
4. Schreiner, Rüdiger; Computer-Netzwerke, Hanser Verlag 2012, ISBN 978-3-446-43117-1

Diese Publikation ist ein Auszug aus dem gleichnamigen Beitrag des Fortsetzungswerkes Medizintechnik und Informationstechnologie digital -
MIT - Konzepte, Technologien, Anforderungen - TÜV Media GmbH, Köln
Die vollständige Fassung erscheint in der 23 Ergänzungslieferung des Fortsetzungswerkes im März 2017.

Autoren

Armin Gärtner
Ingenieurbüro für Medizintechnik
Ö. b. u. v. Sachverständiger für Medizintechnik
Edith-Stein-Weg 8
40699 Erkrath
Tel.: 49 (0) 2104-8333706
E-Mail: armin.gaertner@t-online.de

Mahmoud El-Madani
Vertex Activity e.U.

Allgemein beeidigter u. gerichtlich zertifizierter Sachverständiger

TÜV Zertifizierter Risikomanager f. medizinische IT-Netzwerke
TÜV Zertifizierter ISMS ISO 27001 Auditor
A-1150 Wien Henriettenplatz 3/1/16
https://www.vertex-activity.com
E-Mail: maelmadani@vertex-activity.com
Tel.: +43 680 315 73 23

Stand 13.11.2016