Peter Knipp

Risikomanagement im AAL-Umfeld

TMF-Workshop
AAL meets E-Health
Berlin, 14.10.2014

qcmed®

Quality Consulting Medical GmbH

Zulassung
Qualität
Risiko

Management • Beratung • Training

VQZ Bonn
Zertifiziert
DIN EN ISO 9001

www.qcmed.de

E-Health
Technik

Per Internet ans Krankenbett

Die leitenden Anästhesisten der Asklepios Südpfalzkliniken GmbH können sich von außerhalb auf den „Integrated Care Manager“,

heise Security

News | Hintergrund | Erste Hilfe | Foren | Tool

Security > News > 7-Tage-News > 2010 > KW 42 > Virus legt Krankenhaus lahm

News-Meldung vom 21.10.2010 11:30 « Vorige | Nächste »

Virus legt Krankenhaus lahm

vorlesen / MP3-Download

Ein Virusbefall auf den Servern des Westfriesgasthuis im niederländischen Hoorn hat am Mittwoch
auf Notfälle wu
dessen Name
Mutation eines

Mittlerweile so
wieder herges
Operationssäl
Operationen k
Virus nicht erb

Der Virus sei a
Systeme eing
noch nicht kla
Informationen
gewählter Ker
fehlerhaften A
Mitarbeiter plö
durch den Ang

iX > 7-Tage-News > 2014 > KW 18 > Gravierende Lücken in medizinischen Geräten

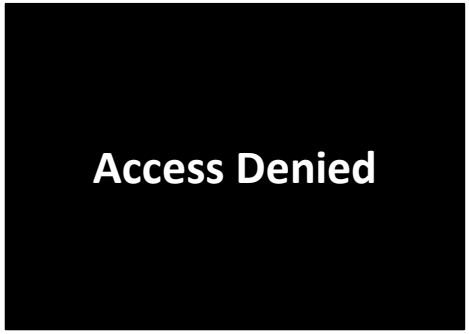
News-Meldung vom 28.04.2014 17:10 Uhr « Vorige | Nächste »

Gravierende Lücken in medizinischen Geräten

vorlesen / MP3-Download

Medizintechnik in US-Krankenhäusern ist mit erschreckend simplen Verfahren angreifbar. Triviale Passwörter und Daten im Klartext gestatten Zugriff auf den OP und das Fernsteuern von lebenswichtigen Systemen.

Medizinische Geräte in US-Krankenhäusern offenbaren gravierende Sicherheitsmängel, berichtet das Magazin *Wired*. Scott Erven, bei einem Gesundheitsdienstleister zuständig für IT-Sicherheit, prüfte sämtliche computer-basierte Medizintechnik in zahlreichen Kliniken. Was er in einem Zeitraum von zwei Jahren fand, gleicht einem Horror-Szenario: ferngesteuerte OP-Roboter,



Eine **Gefährdung** des Patienten?

Und wer hat die **Verantwortung**?

GESETZE etc.

Grundlage §

- **RL 93/42/EWG** Medizinprodukte (MDD)
- **RL 85/374/EWG** Haftung für fehlerhafte Produkte
- Datenschutzrichtlinie
- Datenschutz-Verordnung

- MPG Medizinproduktegesetz
- MPBetreibV Medizinprodukte-Betreiberverordnung
- BDSG Bundesdatenschutzgesetz
- SGB Sozialgesetzbuch
- Konfessionelle Datenschutzgesetze
- Landesdatenschutzgesetze
- TMG TeleMedienGesetz
- Telekommunikationsgesetz
- Gesundheitsdatenschutz…

MPBetreibV

Grundlage §

§ 2 Allgemeine Anforderungen

(1) Medizinprodukte dürfen nur ihrer Zweckbestimmung entsprechend und nach den Vorschriften dieser Verordnung, den allgemein anerkannten Regeln der Technik sowie den Arbeitsschutz- und Unfallverhütungsvorschriften errichtet, betrieben, angewendet und in Stand gehalten werden.
(2) Medizinprodukte dürfen nur von Personen errichtet, betrieben, angewendet und in Stand gehalten werden, die dafür die erforderliche Ausbildung oder Kenntnis und Erfahrung besitzen.
(3) Miteinander verbundene Medizinprodukte sowie mit Zubehör einschließlich Software oder mit anderen Gegenständen verbundene

(3) Miteinander verbundene Medizinprodukte sowie mit Zubehör einschließlich Software oder mit anderen Gegenständen verbundene Medizinprodukte dürfen nur betrieben und angewendet werden, wenn sie dazu unter Berücksichtigung der **Zweckbestimmung** und der **Sicherheit** der Patienten, Anwender, beschäftigten oder Dritten **geeignet** sind.

mit dem Medizinprodukt zur Anwendung miteinander verbundenen Medizinprodukte sowie Zubehör einschließlich Software und anderen Gegenständen.
(6) Medizinprodukte der Anlage 2 dürfen nur betrieben und angewendet

MPBetreibV

Grundlage §

§ 2 Allgemeine Anforderungen

(1) Medizinprodukte dürfen nur ihrer Zweckbestimmung entsprechend und nach den Vorschriften dieser Verordnung, den allgemein anerkannten Regeln der Technik sowie den Arbeitsschutz- und Unfallverhütungsvorschriften errichtet, betrieben, angewendet und in Stand gehalten werden.
(2) Medizinprodukte dürfen nur von Personen errichtet, betrieben,

(1) Medizinprodukte dürfen nur zu ihrer **Zweckbestimmung** entsprechend und nach den Vorschriften dieser Verordnung, den **allgemein anerkannten Regeln der Technik** sowie den **Arbeitsschutz- und Unfallverhütungsvorschriften** errichtet, betrieben, angewendet und in Stand gehalten werden.

von Medizinprodukten beauftragen, die die in Absatz 2 genannten Voraussetzungen erfüllen.
(5) Der Anwender hat sich vor der Anwendung eines Medizinproduktes von der Funktionsfähigkeit und dem ordnungsgemäßen Zustand des Medizinproduktes zu überzeugen und die Gebrauchsanweisung sowie die sonstigen beigefügten sicherheitsbezogenen Informationen und Instandhaltungshinweise zu beachten. Satz 1 gilt entsprechend für die mit dem Medizinprodukt zur Anwendung miteinander verbundenen Medizinprodukte sowie Zubehör einschließlich Software und anderen Gegenständen.
(6) Medizinprodukte der Anlage 2 dürfen nur betrieben und angewendet

Stand der Technik

DEUTSCHE NORM November 2011

DIN EN 80001-1 (VDE 0756-1)

DIN

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation" bekannt gegeben worden.

VDE

ICS 11.040; 35.110; 35.240.80

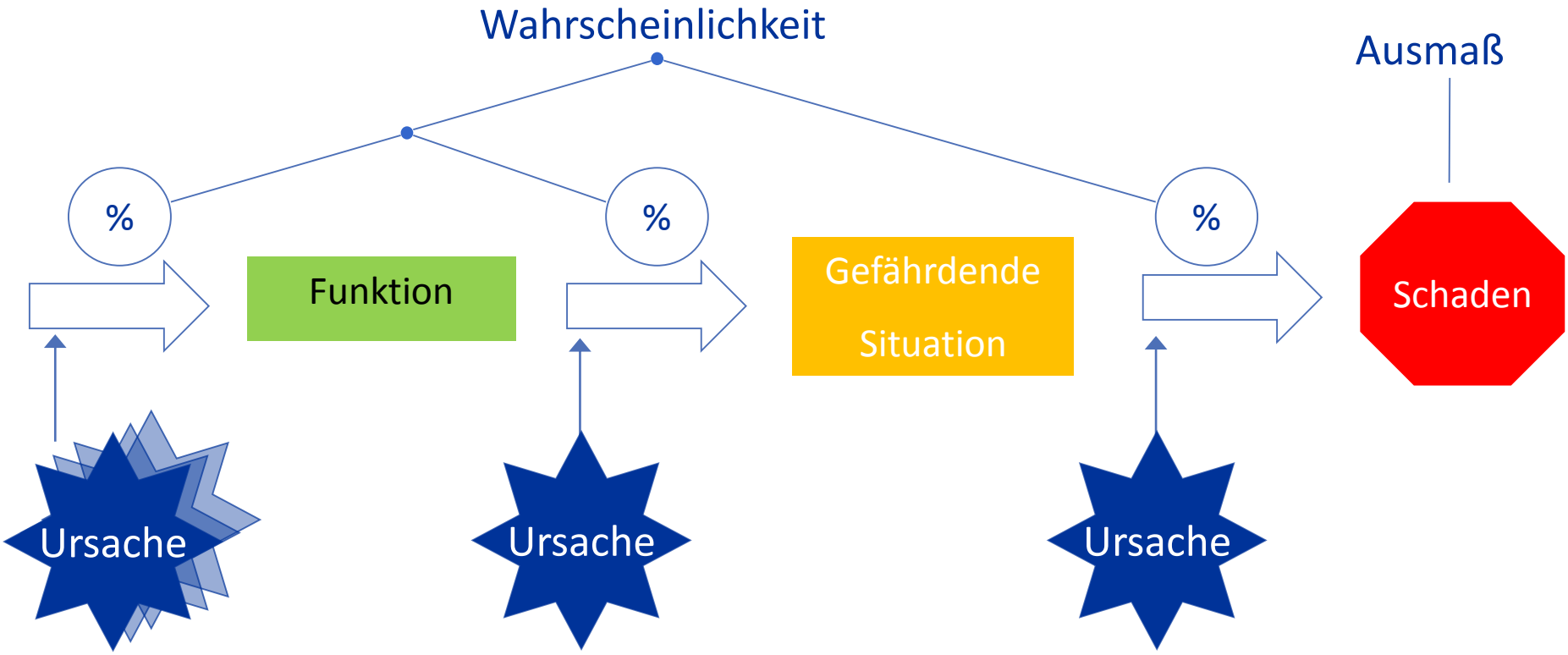
**Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten –
Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten
(IEC 80001-1:2010);
Deutsche Fassung EN 80001-1:2011**

gültige Fassung

Schutzziele IEC 80001-1

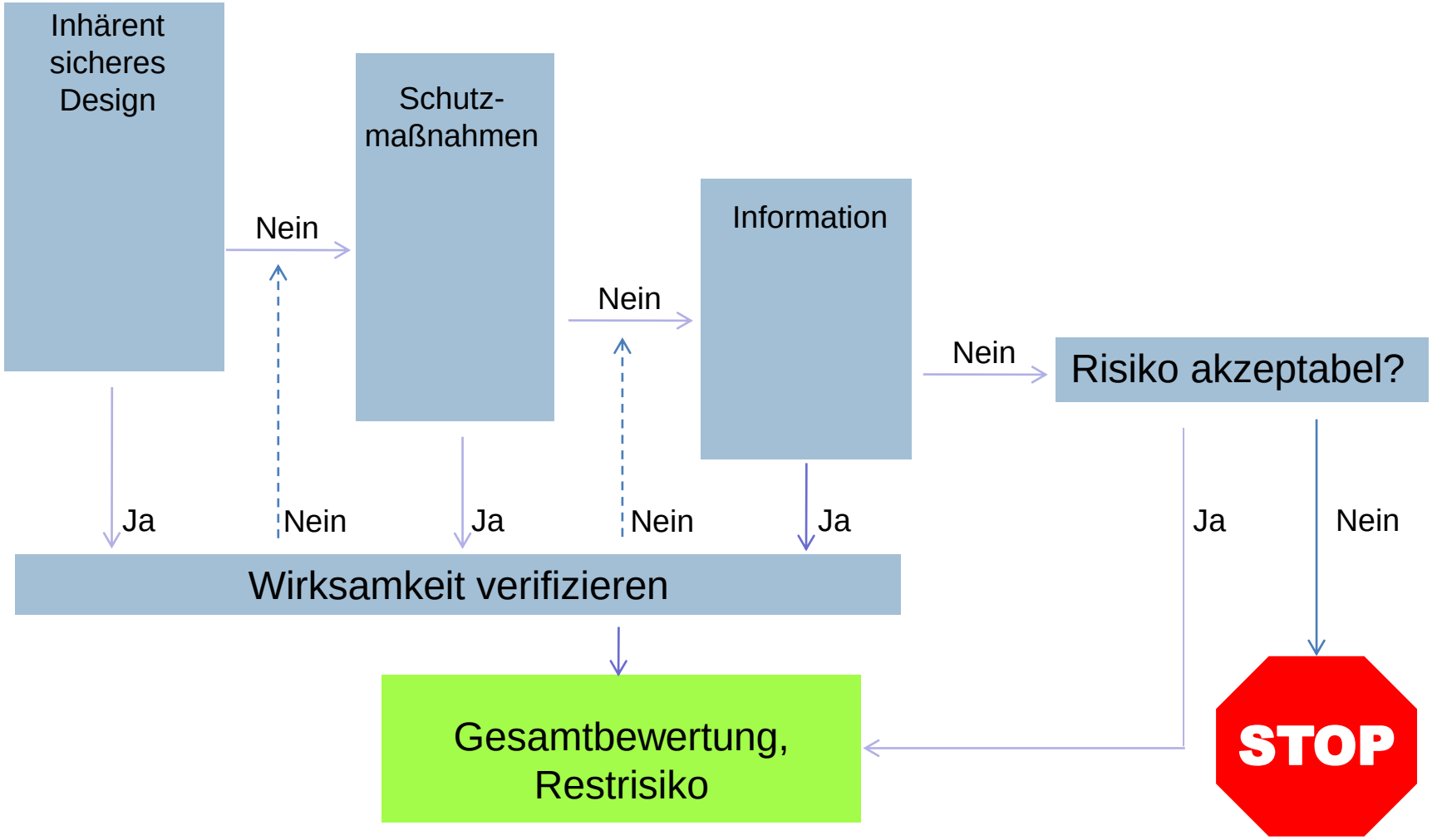
ANALYSE

Risiko

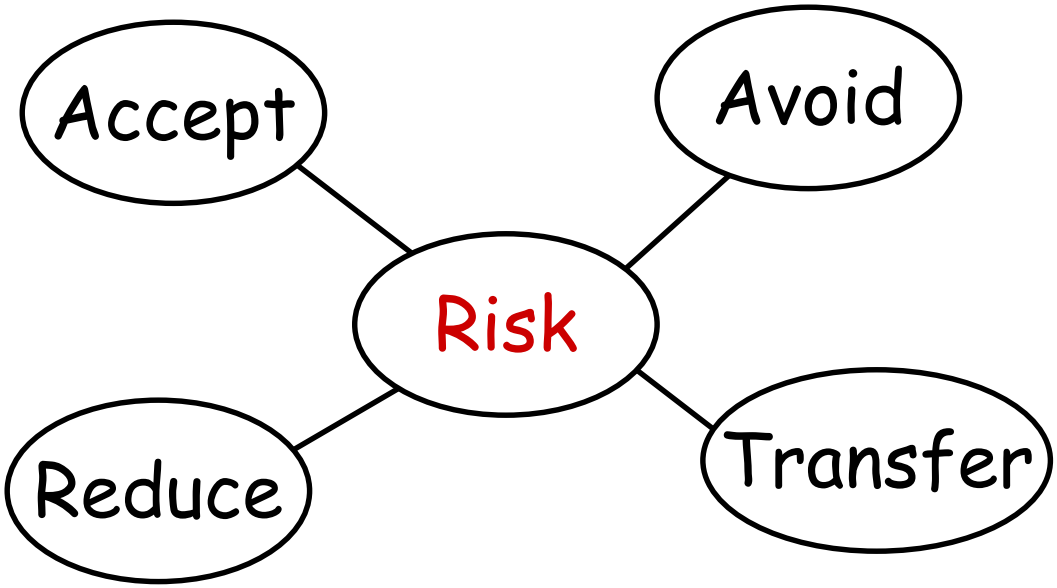


RISIKO NEU, DURCH VERNETZUNG

PRINZIP DER RISIKOBEHERRSCHUNG



STRATEGIE

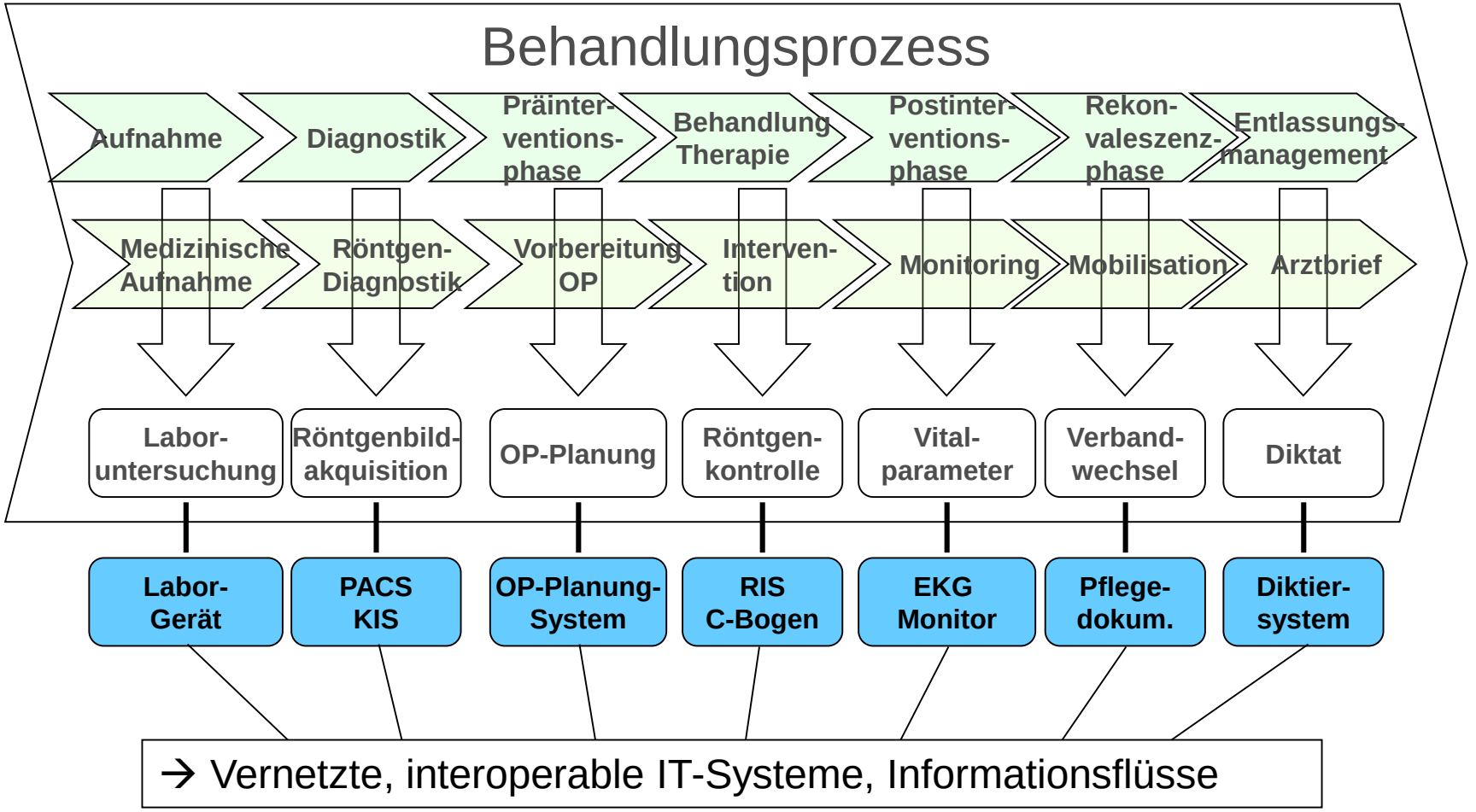


ZENTRALER PROZESS

Risikomanagement

- Planungsphase
- Anwender, Patient, Ziel/Zweck, Kontext erfassen
- Systeme, Prozesse, Infrastruktur erfassen
- Verantwortlichkeitsvereinbarung § mit allen Beteiligten
- Risiko-Analyse
- Risiko-Beherrschung, Systembetrieb, Änderungen

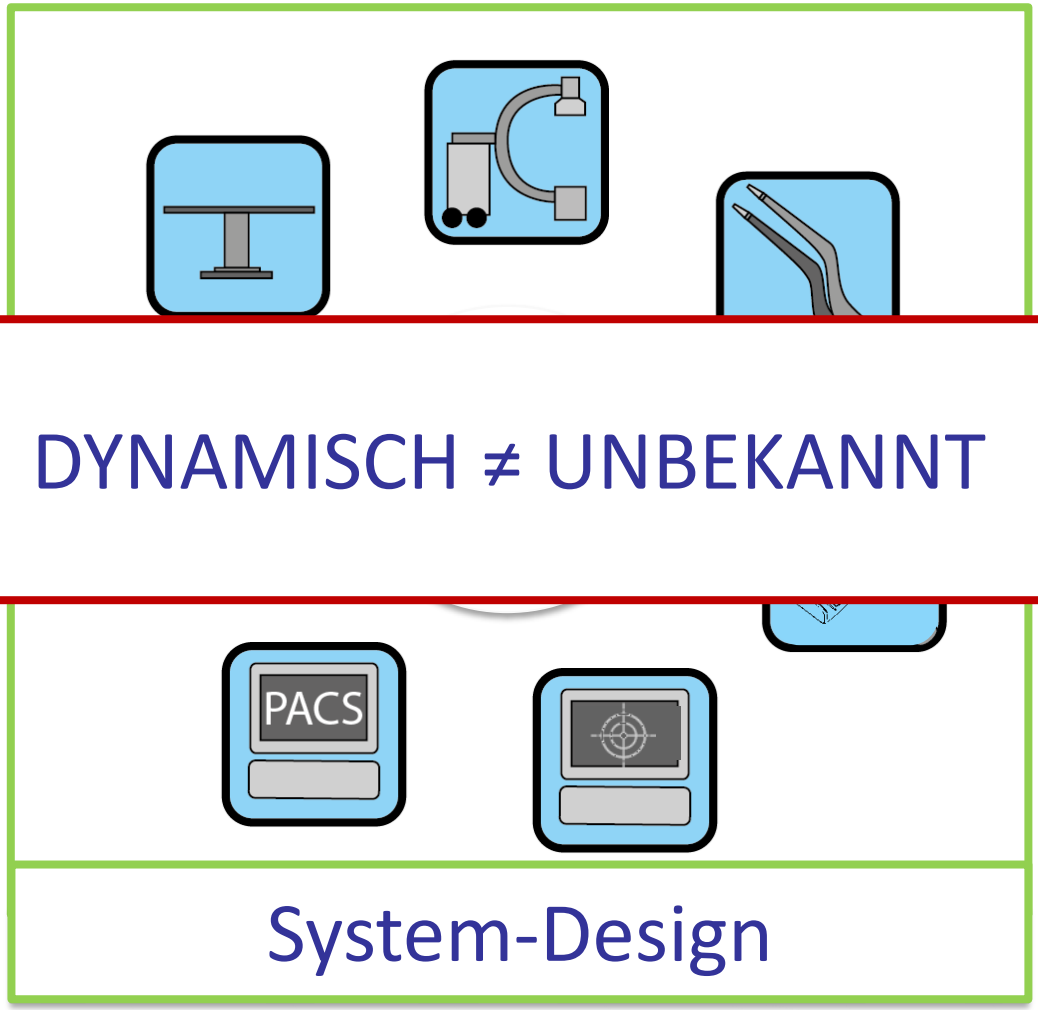
System und Prozess



Zusammen erfolgreich?

Wie in einem großen Orchester braucht man:

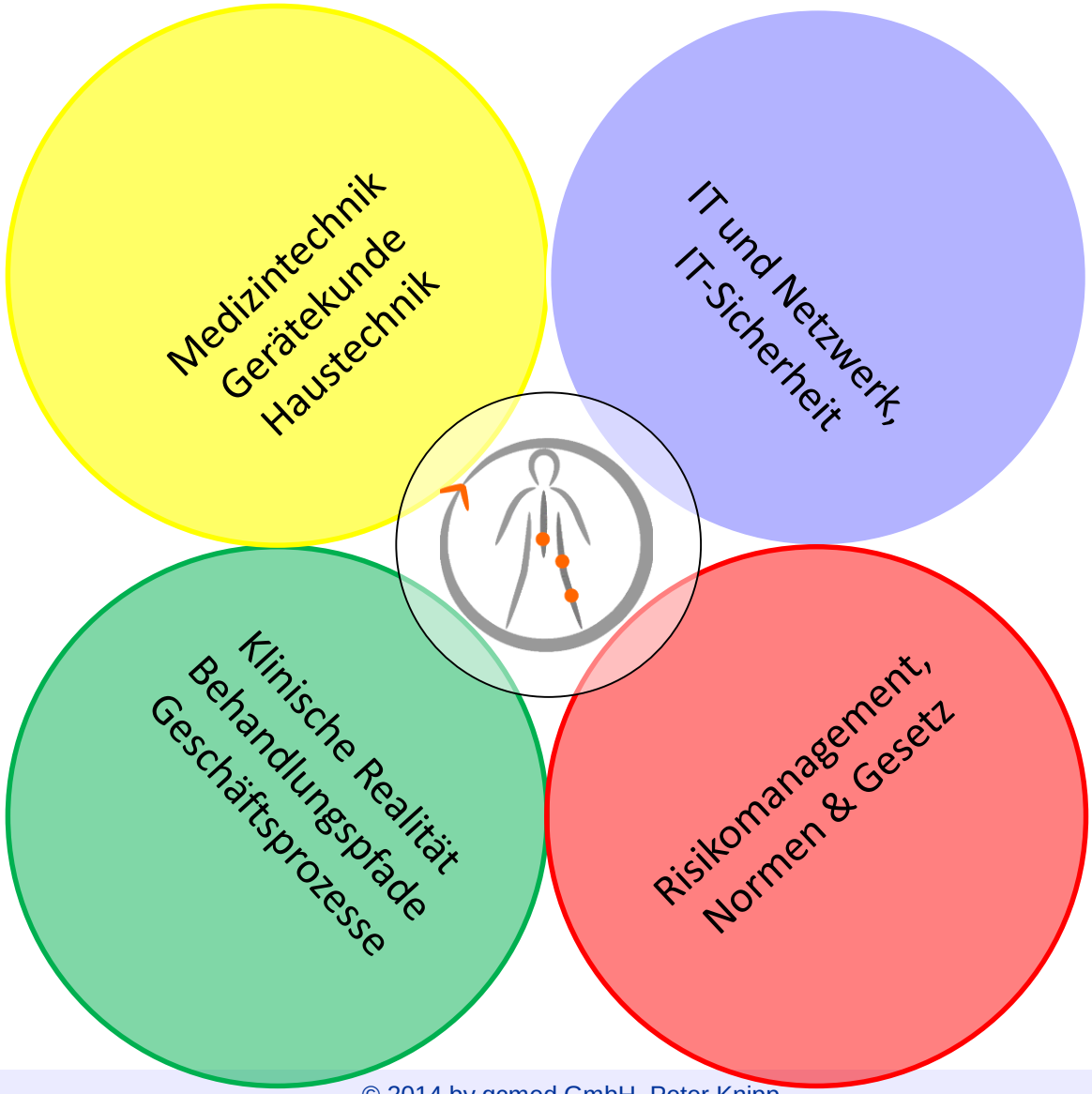
→ Fähigkeit, Architektur, Ablauf



DYNAMISCH ≠ UNBEKANNT

System-Design

RISIKOMANAGER



orthoMIT
Minimal-invasive Orthopädische Therapie

Bundesministerium
für Bildung
und Forschung

Hilfen?

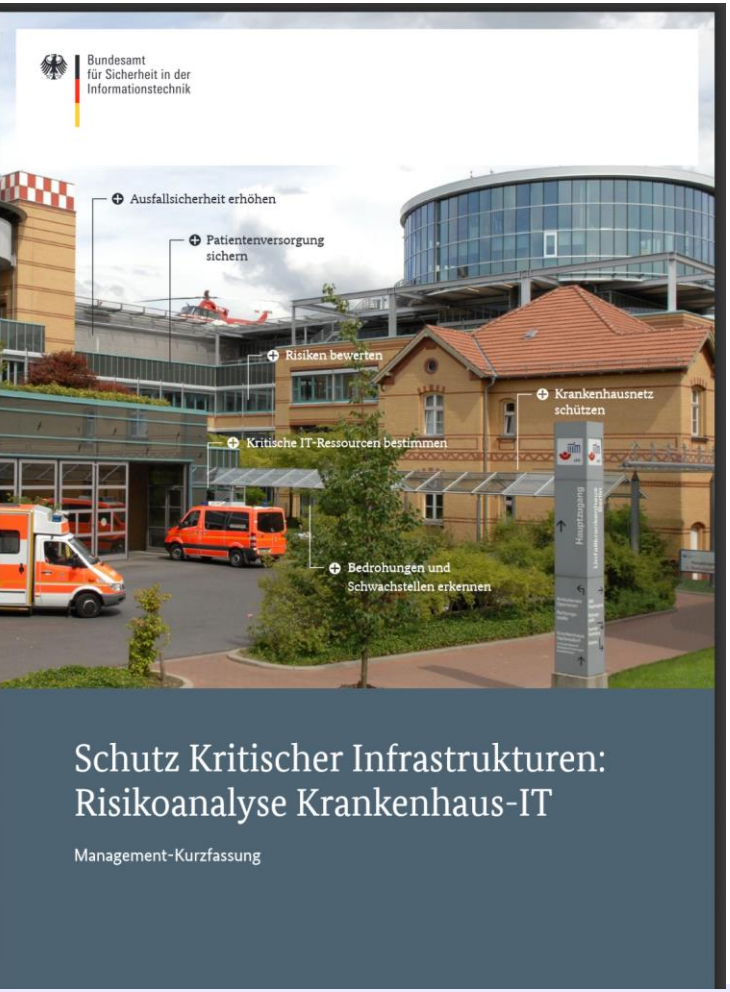
Bundesamt
für Sicherheit in der
Informationstechnik

DIN ISO/IEC 27001:2008-09

Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2005)

Quelle:
http://www.iso27001-it-sicherheit.de/ISMS_ISO_IEC_27001_Einfuehrung.htm

Erfahrungen & Hilfen?



Arbeitshilfe der DKG

Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten (DIN EN 80001-1:2011)

Danke!

www.qcmed.de