ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA

CAMPUS DI CESENA

SCUOLA DI INGEGNERIA E ARCHITETTURA

CORSO DI LAUREA IN INGEGNERIA BIOMEDICA

TITOLO DELL'ELABORATO

Software dispositivo medico: analisi del rischio e integrazione nelle reti IT

ELABORATO IN

Informatica medica e reti di telemedicina

RELATORE

Ing. Giovanni Arcuri

CANDIDATO

Silvia Berta

SESSIONE II

ANNO ACCADEMICO 2013/2014

Indice

Introduzione

> "Risk management is a more realistic term than safety. It implies that hazards are ever-present, that they must be identified, analyzed, evaluated and controlled or rationally accepted."
>
> Jerome Ledere

In questa tesi faremo prima una panoramica sui dispositivi medici e, in particolare, andremo ad approfondire l'aspetto del software come dispositivo medico; successivamente andremo ad analizzare il sistema, definito "nuovo approccio", che regolamenta l'immissione in commercio dei dispositivi medici all'interno del mercato europeo per andare poi ad analizzare la parte sulla gestione del rischio che è fondamentale per raggiungere la conformità soprattutto quando si tratta di dispositivi medici. Nel secondo capitolo, andremo poi ad analizzare il report tecnico IEC 80002-1 del 2009 che fornisce una guida, destinata al software, per l'applicazione dei requisiti contenuti nella normativa CEI UNI EN ISO 14971:2007. Nel terzo capitolo, visto il sempre maggior numero di dispositivi medici dotati di interfaccia di rete andremo a fare una panoramica sul report tecnico IEC 80001 del 2009 per la gestione dei rischi delle reti IT medicali ponendo l'attenzione sulle figure professionali coinvolte.

Capitolo 1 Medical device – normative

Contrariamente ai concetti di "farmaco" e "medicinale" quello di "dispositivo medico" (dall'inglese "medical device") ha avuto una diffusione abbastanza recente. Solo negli anni '20 si era sentito il bisogno di estendere il controllo delle autorità sanitarie anche a quella parte dell' "armamentario" del medico che non era riconducibile ai medicinali; si era pertanto stabilito che dovessero essere sottoposti a una "speciale registrazione" anche i "presidi medici e chirurgici" - nonostante allora non si chiarì esattamente, con una definizione, che cosa dovesse rientrare in tale concetto.

Nel corso degli anni, grazie all'evoluzione tecnologica in ambito sanitario, il significato del termine "dispositivo medico" ha subito una continua evoluzione e rivalutazione che ha portato a importati modifiche dal punto di vista legislativo - le ultime sono presenti nella normativa 2007/47/CE emanata nel settembre del 2007 (e recepita, per quanto riguarda lo stato Italiano, nel 2010 con il Dlgs del 25 gennaio 2010).

1.1 Aspetti generali della normativa 2007/47/CE

La normativa vigente nella comunità europea che riporta i criteri generali da usare nella progettazione e realizzazione di alcune catogorie di dispositi medici (imponendo l'obbligo della marcatura CE per la commercializzazione di tali dispositivi in tutto il mercato europeo) è la direttiva 93/42/CEE (recepita in Italia con il Dlgs 46/97) che venne integrata e modificata, nel 2007, con la normative 2007/47/CE (recepita in italia con il Dlgs 37/2010)

Gli articoli (e allegati) di interesse ai fini della nostra tesi sono la definizione di dispositivo medico, contenuta nell'articolo 1:

Dispositivo medico: "qualunque strumento, apparecchio, impianto, software, sostanza o altro prodotto, utilizzato da solo o in combinazione, compreso il software destinato dal fabbricante ad essere impiegato specificamente con finalità diagnostiche o terapeutiche e necessario al corretto funzionamento del dispositivo, destinato dal fabbricante ad essere impiegato sull'uomo a fini di diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia; di

diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap; di studio, sostituzione o modifica dell'anatomia o di un processo fisiologico; di intervento sul concepimento, il quale prodotto non eserciti l'azione principale, nel o sul corpo umano, cui è destinato, con mezzi farmacologici o immunologici né mediante processo metabolico ma la cui funzione possa essere coadiuvata da tali mezzi.“

Dalla definizione si capisce che si tratta di un vasto numero di prodotti anche molto diversi tra loro; alcuni sono di uso domestico (come i termometri) altri sono per uso personale (cerotti) altri ancora sono destinati solo all’uso in ambienti sanitari.

Proprio per questo sono stati categorizzati secondo regole stabilite dalla Direttiva in una delle classi di rischio (Allegato IX) al fine di attuare le necessarie procedure di valutazione della conformità previste per ogni classe senza imporre ai fabbricanti schemi troppo onerosi in rapporto al rischio del prodotto.

Le classi in cui sono suddivisi i dispositive medici sono quattro:

Classe I (basso rischio)

1) Is – dispositivi di classe I forniti allo stato sterile.
2) Im – dispositivi di classe I che svolgono una funzione di misura.

Classe IIa (medio rischio)

Classe IIb (medio/alto rischio)

Classe III (alto rischio)

Le definizioni e regole per la classificazione dei dispositive medici sono contenute nell’alleato IX.

Nel capitolo 1 sono contenute le definizioni dei termini usati per la classificazione, di particolare interesse abbiamo la definizione di dispositivo medico attivo

Dispositivo medico attivo: “Dispositivo medico dipendente, per il suo funzionamento, da una fonte di energia elettrica o di altro tipo di energia, diversa da quella generata direttamente dal corpo umano o dalla gravità e che agisce convertendo tale energia. Un dispositivo medico destinato a trasmettere,

senza modificazioni di rilievo, l'energia, le sostanze o altri elementi tra un dispositivo medico attivo e il paziente non è considerato un dispositivo medico attivo. Il software indipendente (stand-alone) è considerato un dispositivo medico attivo."

Dispositivo attivo terapeutico: "Dispositivo medico attivo utilizzato da solo o in combinazione con altri dispositive medici, destinato a sostenere, modificare, sostituire o ripristinare le funzioni o le strutture biologiche nel contesto di un trattamento o per alleviare una malattia, una ferita o un handicap."

Dispositivo attivo destinato alla diagnosi: "Dispositivo medico attivo utilizzato da solo o in combinazione con altri dispositivi medici, destinato a fornire informazioni riguardanti la diagnosi, la diagnosi precoce, il controllo o il trattamento di stati fisiologici, di stati di salute, di malattie o di malformazioni congenite."

Il secondo capitolo dell'allegato riporta invece regole generali per la classificazione, vengono riportate le più significative ai fini della tesi.

- "L'applicazione delle regole di classificazione deve basarsi sulla destinazione dei dispositivi."
- "Se un dispositivo è destinato ad essere utilizzato in combinazione con un altro dispositivo, le regole di classificazione devono applicarsi separatamente a ciascun dispositivo. Gli accessori sono classificati separatamente dal dispositivo con cui sono impiegati."
- "Il software destinato a far funzionare un dispositivo o ad influenzarne l'uso rientra automaticamente nella stessa classe del dispositivo.**"**
- "Se ad un dispositivo si applicano più regole, tenuto conto delle prestazioni che gli sono assegnate dal fabbricante, si applicano le regole più rigorose che portano alla classificazione più elevata."

La parte tre dell'allegato riporta invece le regole specifiche di classificazione per i dispositivi medici attivi.

Regola 9: Tutti i dispositivi attivi terapeutici destinati a rilasciare o a scambiare energia rientrano nella classe IIa a meno che le loro caratteristiche siano tali da permettere loro di rilasciare energia al corpo umano o scambiare energia con il corpo umano in forma potenzialmente pericolosa, tenuto conto della natura, della densità e della parte in cui è applicata l'energia, nel qual caso essi rientrano nella classe IIb. Tutti i dispositivi attivi destinati a controllare o a sorvegliare le

prestazioni di dispositivi attivi terapeutici appartenenti alla classe IIb, o destinati ad influenzare direttamente la prestazione di tali dispositivi, rientrano nella classe IIb.

Regola 10: I dispositivi attivi destinati alla diagnosi rientrano nella classe IIa se: - sono destinati a rilasciare energia che sarà assorbita dal corpo umano, ad esclusione dei dispositivi utilizzati per illuminare il corpo del paziente nello spettro visibile; sono destinati a visualizzare in vivo la distribuzione di radio farmaci in vivo; - sono destinati a consentire una diagnosi diretta o un controllo dei processi fisiologici vitali, a meno che siano specificamente destinati a controllare I parametri fisiologici vitali, ove la natura delle variazioni è tale da poter creare un pericolo immediato per il paziente, per esempio le variazioni delle funzioni cardiache, della respirazione o dell'attività del sistema nervoso centrale, nel qual caso essi rientrano nella classe IIb.

I dispositivi attivi destinati ad emettere radiazioni ionizzanti e destinati alla diagnosi, alla radioterapia o alla radiologia d'intervento, compresi i dispositivi che li controllano o che influenzano direttamente la loro prestazione, rientrano nella classe IIb.

Regola 11: Tutti i dispositivi attivi destinati a somministrare e/o a sottrarre medicinali, liquidi corporei o altre sostanze dal corpo rientrano nella classe IIa, a meno che ciò sia effettuato in una forma: - potenzialmente pericolosa, tenuto conto della natura delle sostanze in questione, della parte del corpo interessata e del modo di applicazione, nel qual caso essi rientrano nella classe IIb.

Regola 12: Tutti gli altri dispositivi attivi rientrano nella classe I.

In Figura 1 possiamo vedere uno schema per la classificazione dei dispositivi medici attivi.

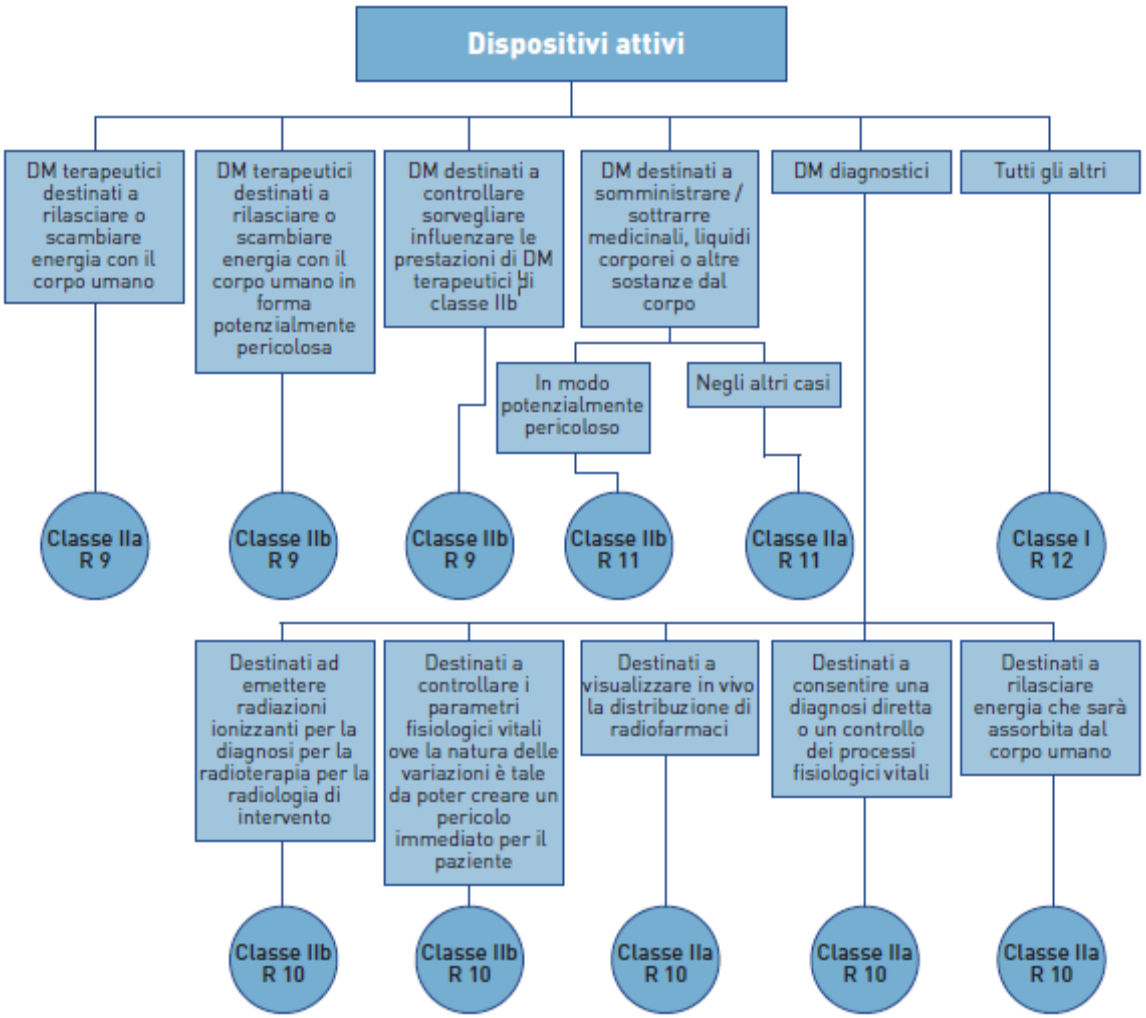

Figura 1 Classificazione dm attivi – tratta da "Dispositivi Medici, aspetti regolatori e operativi"

1.2 Software dispositivi medici

Da questa panoramica iniziale si può notare che anche il software è considerato un dispositivo medico (mentre nella normativa del '93 era compreso solo quello usato all'interno di dispositivi medici "necessari al funzionamento dello stesso"). Il software quindi non è più considerato solo come un "accessorio" di un dispositivo medico ma lo è lui sesso e, come tale, gli verranno applicate le stesse prescrizioni progettuali e dovrà essere certificato come qualsiasi altro dispositivo.

Come è facile immaginare in ambiente sanitario sono impiegati moltissime tipologie di software ma non tutte sono considerate dispositivo medico. Sono considerati dispositivo medico solo quei software che hanno finalità medicale. Intuitivamente quindi i software per la gestione del magazzino o quelli che

riguardano l'area amministrativa non rientreranno nella definizione di dispositivo medico mentre i software che forniscono un aiuto a operatori sanitari (come, per esempio, software per l'intepretazione di ECG) rientrano nella categoria di dispositivi medici. E' importante notare però che solo la destinazione d'uso (descritta dal fabbricante) è rilevante per la classificazione e qualificazione di ogni dispositivo.

E' tuttavia necessario chiarire alcuni criteri per la classificazione dei software come dispositivo medico. In Figura 2 è riportato un grafico che ci fornisce qualche indicazione riguardante gli step necessari per la qualifica del software come dispositivo medico.

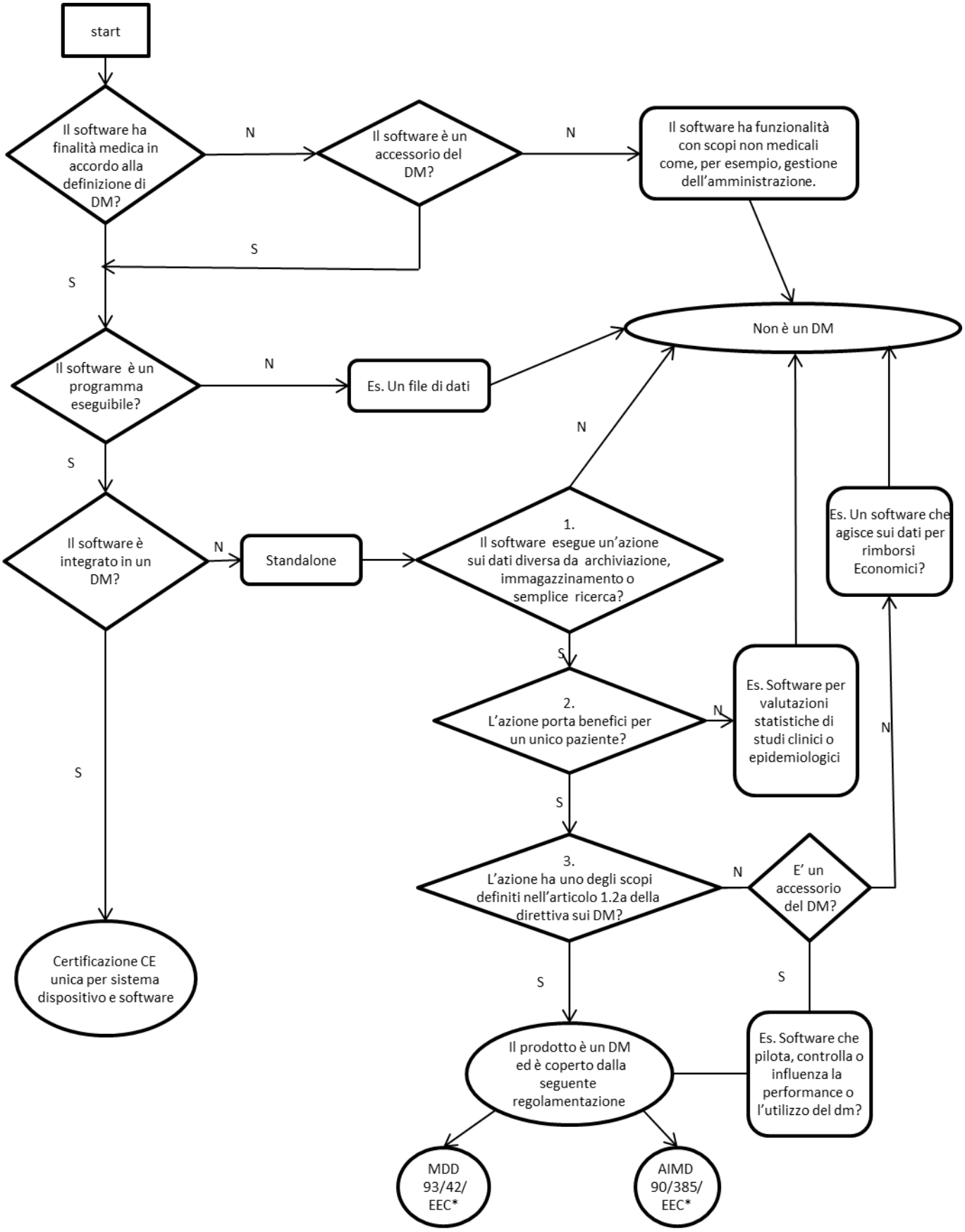

Figura 2: Schema decisionale per la qualificazione del software come dispositivo medico

Un software può essere considerate un dispositivo medico solo se è un programma del computer (come un'applicazione, una macro, uno script) mentre se è un documento digitale (file immagini, registrazioni digitali dell'ECG) non può essere considerate tale.

Se il software è integrato in un dispositivo medico deve essere considerato parte del dispositivo medico stesso e dovrà essere sottoposto a procedure di controllo come parte integrante del dispositivo e dovrà essere classificato nella sua stessa classe se è necessario al suo funzionamento o ne influenza l'utilizzo. Se invece il software è un accessorio di un dispositivo medico (per esempio un software per la presentazione 3D delle immagini ecografiche) deve seguire la normativa sui dispositivi medici ed essere classificato a sua volta. Se invece il software è indipendente (stand-alone) il fabbricante per classificarlo e qualificarlo può avvalersi della linea guida pubblicata dalla Commissione Europea denominata MEDDEV 2.1/6 "Qualification and Classification of standalone software".

Step 1) Il software esegue un'azione sui dati diversa da archiviazione, immagazzinamento o semplice ricerca? Se il software non esegue un'azione sui dati o esegue un'azione limitata all'archiviazione, immagazzinamento, semplice ricerca (intesa come recupero di registrazioni dal confronto dei metadati con dei criteri di ricerca, ad esempio funzioni libreria) o compressione dati senza perdita di informazione non è un dispositivo medico. L'alterazione nella rappresentazione dei dati ai fini di migliorarne la qualità non rende il software un dispositivo medico. In alcuni casi, se il software altera la rappresentazione dei dati per finalità mediche può essere considerato un dispositivo medico. Software destinati a creare o modificare informazioni mediche possono essere considerati dispositive medici se tali alterazioni possono facilitare il personale sanitario durante la revisione delle informazioni.

Step 2) L'azione porta benefici per un unico paziente? Un esempio di software che porta un beneficio individuale al paziente è quel software che è stato destinato a essere usato per la valutazione dei dati del paziente al fine di supportarne e influenzarne la terapia.

Step 3) Se il fabbricante ha specificatamente destinato il software a essere usato per finalità previste dalla definizione di dispositivo medico allora il software può essere considerato un dispositivo medico. Tuttavia, se il fabbricante ha aggiunto anche solo una finalità non medicale (come la gestione del personale) allora non può essere considerato un dispositivo medico.

Il software incorporato nel disposito medico rientra nella classe del dispositivo medico in cui è integrato mentre il software stand alone dispositivo medico deve essere considerato un dispositivo medico attivo e, come tale, classicificato secondo le regole 9,10,11 e 12 dell'allegato IX della normativa – di seguito alcuni esempi di software stand alone:

-) classe I: software usati in ortopedia per misurare la distanza del canale interpeduncolare o il diametro saggittale del canale vertebrale.

-) classe IIa: software per la presentazione del battito cardiaco (o altri parametri fisiologici) durante un controllo di routine.

-) classe IIb: software usati per la presentazione del battito cardiaco (o di altri parametri fisiologici) usati in UTIC.

Software stand alone che guidano un altro dispositivo medico o ne influenzano l'uso ricadono automaticamente nella stessa classe del dispositivo che gestiscono.

Ora che sappiamo identificare e classificare i dispositivi medici, e, in particolare, i dispositivi medici software, non ci resta che capire come è possibile immetterli sul mercato europeo.

1.3 Nuovo Approccio

L'immissione in commercio dei dispositivi medici all'interno del mercato europeo è regolamentata su base comunitaria secondo il medesimo sistema definito "nuovo approccio".

Al fine di rimuovere ostacoli tecnici agli scambi nel mercato interno europeo risultanti dall'esistenza di norme e regolamentazioni tecniche nazionali divergenti tra loro, nel 1985, con la risoluzione del Consiglio EU, è stata adottata una nuova strategia in materia di armonizzazione tecnica e normalizzazione detta "nuovo approccio". Nel 2008, alla luce di venti anni di esperienza, il sistema è stato rivisto e questa revisione ha preso il nome di "New Legal Framework".

Il "nuovo approccio" garantisce che gli stessi requisiti essenziali vengano richiesti ai prodotti nei diversi Paesi Europei e che, di conseguenza, le Autorità Competenti di ciascuno Stato Membro permettano la libera circolazione di

dispositivi fabbricati in altri Sati Membri, avendo la certezza giuridica che tali prodotti siano equivalenti con quelli che rispondono alla normativa applicabile nel loro Paese. La "conformità" ai requisiti imposti dalle normative è dimostrata dalla presenza sul prodotto del marchio CE (Figura 3) e dalla dichiarazione di conformità ovvero quel documento con il quale il fabbricante dichiara che il prodotto soddisfa le disposizioni applicabili della normativa di riferimento.

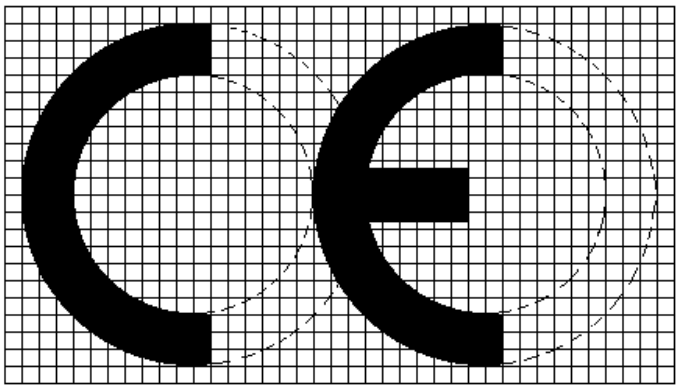

Figura 3 il marchio CE

Per quanto riguarda i dispositivi medici le direttive indicano una serie di requisiti essenziali che i dispositivi medici devono rispettare (per esempio, la sicurezza del paziente e degli utilizzatori e l'efficacia) senza però prescrivere dettagli tecnici per raggiungere l'adempimento di tali requisiti. La scelta di non prevedere specifiche tecniche nei testi delle direttive in quei settori dove l'avanzamento tecnologico porta a una rapida evoluzione delle tecnologie permette che quelle stesse direttive non risultino obsolete ma continuino a essere validamente applicabili nel tempo. Per questa ragione, alle direttive del "nuovo approccio", sono affiancate norme tecniche (norme internazionali Iso o Iec adottate, a volte con eventuali modifiche, in campo euroepo) che vengono frequentemente aggiornate o riscritte e che, pertanto, riflettono lo "stato dell'arte" relativo alle conoscenze in quel determinato settore.

I requisiti essenziali che i dispositivi medici devono soddisfare per poter circolare liberamente nell'UE sono divisi in:

-) requisiti generali (requisiti relativi alla sicurezza e alla prestazione del dispositivo e che sono applicabili a tutti i prodotti) sono:

1) Sicurezza e salute del paziente e degli operatori
2) Garanzia delle prestazioni del dispositivo assegnate dal fabbricante

3) Inalterabilità delle caratterisiche del dispositivo drante l'uso, il trasporto e l'immagazzinamento
4) Minimizzazione dei rischi associati all'uso
5) Analisi dei rischi
6) Valutazione clinica per dimostrare la conformità ai requisiti essenziali (in particolar modo a quelli di efficacia)

-) requisiti relativi alla progettazione e costruzione.

Il fabbricante (cioè colui che "assume la responsabilità delle conformità del prodotto, ma che può non esserne il produttore materiale, potendo egli affidare a terzi la realizzazione dello stesso, o anche solo di una parte del processo produttivo"), per ogni dispositivo, dovrà indicare l'applicabilità o meno dei singoli requisiti essenziali e, in caso di applicabilità, dovrà descrivere le soluzioni adottate per soddisfare tali requisiti e le procedure attuate con riferimenti al fascicolo tecnico predisposto – applicando (integralmente) le norme tecniche (da cui derivano le soluzioni) il fabbricante si assicura la presunzione di conformità del dispositivo ai requisiti essenziali. Per i dispositivi di classe superiore alla I però la sola dichiarazione di conformità da parte del fabbricante non basta per ottenere il marchio CE; ma deve essere valutata da una terza parte, denominata Organismo Notificato (in Italia, per esempio, l'Istituto Superiore di Sanità) che la attesta mediante una certificazione rilasciata al fabbricante.

Poichè l'assoluta assenza di rischio è irraggiungibile, soprattutto quando si tratta di dispositivi medici, un aspetto molto importante per poter giungere a dichiarare la conformità di un dispositivo medico è la parte inerente alla gestione dei rischi. Per gestione dei rischi si intendono quei processi con i quali si analizzano i rischi e la loro entità (intesa come probabilità*gravità di un evento dannoso) e, successivamente, si sviluppano strategie per eliminarli o ricondurli a un livello di rischio accettabile (tanto più grande quanto maggiore sarà il beneficio apportato al paziente).

Nel seguente capitolo andremo ad analizzare la specifica norma tecnica sulla gestione del rischio (la CEI UNI EN ISO 14971) e, in particolare, il report tecnico sulla gestione del rischio dei dispositivi medici software; il rapporto tecnico IEC 80002 del 2009 che fornisce indicazione specifiche su come eseguire la gestione del rischio.

Capitolo 2 Analisi del rischio per software medical device

Come abbiamo detto nel precedente capitolo il software è spesso parte integrante della tecnologia dei dispositivi medici e, quindi, per stabilirne la sicurezza e l'efficacia bisogna essere a conoscenza di ciò che il software è destinato a fare e del fatto che l'implementazione del software soddisfi tali intenzioni senza portare ad alcun rischio inaccettabile. Il software di per sè non è un pericolo ma può contribuire a situazione pericolose per cui la maggior parte delle attività di gestione del rischio per i software consistono nell'identificare quelle serie di eventi che possono contribuire a situazioni pericolose e quei punti in cui la serie può essere interrotta prevenendo un danno o riducendone la probabilità. Le serie di eventi che possono portare a situazioni pericolose possono rientrare in due categorie:

1. Errori nelle specifiche del software
2. Errori nell'implementazione del software

Dal momento che è molto difficile stimare la probabilità di anomalie software che possono contribuire a situazioni pericolose e poichè il software non si danneggia durante l'uso per rottura o usura, il focus sugli aspetti software di analisi del rischio deve essere posto sull'identificazione di potenziali funzionalità del software o anomalie che possono portare a situazioni pericolose.

Da questa piccola premessa si può intuire che se già di per sè l'analisi del rischio è difficile, quando è coinvolto il software lo è ancora di più - fortunatamente però viene in aiuto degli operatori di gestione del rischio e degli ingegneri software il report tecnico 80002-1 del 2009 che fornisce una guida, destinata al software, per l'applicazione dei requisiti contenuti nella normativa CEI UNI EN ISO 14971:2007.

Ma chi è coinvolto nel processo di gestione del rischio?

2.1 Responsabilità

In primo luogo la responsabilità riguardante la gestione del rischio è del fabbricante che deve, tenendo conto delle norme internazionali, definire una

politica per la determinazione di un rischio accettabile, fornire adeguate risorse, avere a disposizione personale qualificato e verificare periodicamente l'efficacia del processo di gestione del rischio.

Apparentemente le attività di gestione del rischio sembreranno interessare solo il produttore ma non è così, infatti la normativa va applicata per tutto il ciclo di vita del dispositivo medico software che comprende quindi anche le fasi di istallazione e collaudo, utilizzo, aggiornamenti e manutenzione del dispositivo all'interno dell'azienda ospedaliera. In queste ultime tre fasi è l'organizzazione responsabile a dover assicurarsi che le indicazioni del produttore siano eseguite correttamente. Sarà quindi compito dell'ingegnere gestire il rischio residuo e fare in modo che tutto proceda correttamente. Inoltre è l'operatore sanitario, consapevole dei rischi e benefici che può comportare l'utilizzo del dispositivo, a decidere se utilizzarlo o meno.

2.2 Piano di gestione del rischio

Le attività di gestione del rischio devono essere pianificate, pertanto, per ogni dispositivo medico il fabbricante deve stabilire e documentare un piano di gestione del rischio, conforme al processo di gestione del rischio, che deve fare parte parte del file di gestione del rischio presente nel fascicolo tecnico allegato a ogni dispositivo medico e deve includere:

1. Scopo e campo di applicazione del piano, identificando e descrivendo il DM e le fasi del ciclo di vita per cui il piano è applicabile.
2. Identificazione delle responsabilità
3. Le attività di verifica
4. Le attività relative alla raccolta e revisione di informazioni di produzione e post-produzione

   Se il software è parte integrante del dispositivo medico bisogna includere anche:
5. Un documento che certifica lo sviluppo del software in accordo con la IEC 62304.
6. Descrizione del dispositivo medico e funzionalità del software
7. Aspetti di sviluppo del software che fanno riferimento alla gestione del rischio.

8. Criteri di accettabilità del rischio (inclusi criteri per l'accettabilità dei rischi quando la probabilità che si verifichi un danno non può essere stimata).
   Poichè per il software dispositivo medico la probabilità che si verifichi un danno non può essere stimata i criteri di accettabilità del rischio si basano sulla gravità del danno, se questa è considerata accettabile non sono necessarie misure di controllo del rischio altrimenti devono essere implementate; tali misure devono essere una combinazione di tutte le misure ragionevolmente praticabili che soddisfano le normative applicabili secondo lo stato dell'arte. Poichè gli standard internazionali non danno indicazioni specifiche è compito del fabbricante scegliere appropriati criteri di accettabilità del rischio.
9. Attività relative alla raccolta e revisione di informazioni di produzione e post produzione.

2.3 Processo di gestione del rischio

Il fabbricante deve stabilire, documentare e mantenere per tutto il ciclo di vita del dispositivo un processo per identificare i pericoli associati al dispositivo medico, stimando e valutando tali rischi e monitorando l'efficacia dei controlli. Il processo deve includere:

1. Analisi del rischio
2. Valutazione del rischio
3. Controllo del rischio
4. Informazioni di produzione e post-produzione.

In Figura 4 troviamo uno schema del processo di gestione del rischio

Nel caso in cui il dispositivo medico contiene un software le attività di gestione del rischio per il software non devono essere eseguite in isolamento dal sistema (che nel nostro caso è l'intero dispositivo medico) a causa dell'interdipendenza tra guasti hardware e software. E' per questa ragione che è opportuno considerare il ruolo del software nella sicurezza del dispositivo medico già durante le prime fasi della sua progettazione. Infatti partecipando alla progettazione del dispositivo medico l'ingegnere del software può contribuire

alle decisioni sulla sicurezza relative ai rischi connessi al software (per esempio la fornitura di adeguate risorse hardware che supportino il software).

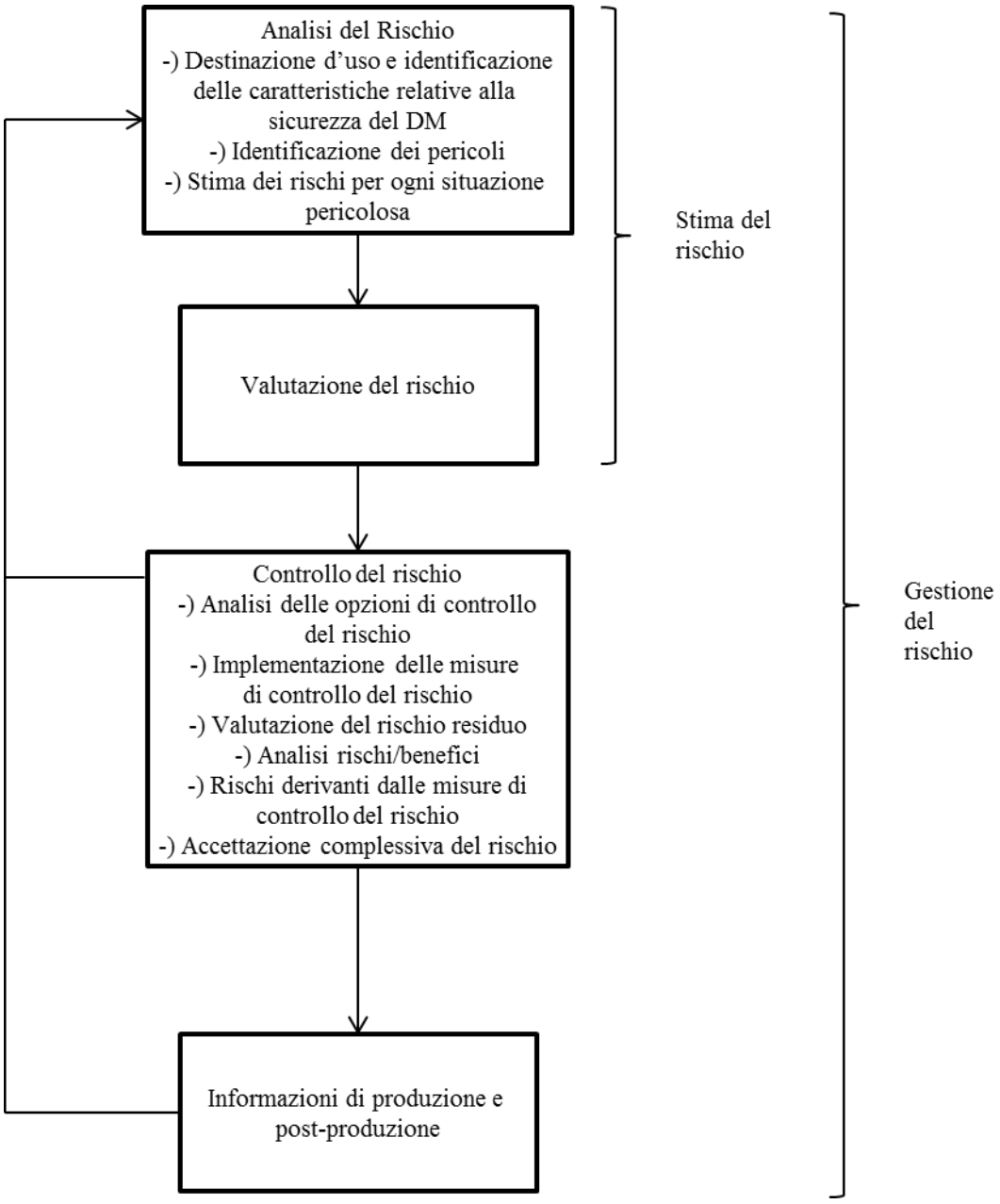

Figura 4 Processo di gestione del rischio – IEC 1836/09

Ma ora andiamo ad analizzare nel dettaglio tutte le varie fasi:

2.3.1 Analisi del rischio

L'analisi del rischio comprende tre diverse attività:

i. *Identificazione della destinazione d'uso e i prevedibili (ed eventuali) usi impropri*:
   In questa fase il fabbricante deve descrivere la destinazione d'uso del dispositivo e qualsiasi ragionevole uso improprio che si potrebbe fare; in più deve elencare tutte le caratteristiche quantitative e qualitative che potrebbero comprometterne la sicurezza.
   Anche se non è un problema software-specifico l'utilizzo del software può portare a un aumento della probabilità di mal utilizzo del dispositivo medico sia perchè il comportamento del dispositivo medico diventa più complesso e quindi più difficile da padroneggiare e comprendere, sia perchè l'operatore può fare troppo affidamento sul software senza capirne i limiti, sia perché l'interfaccia utente potrebbe essere troppo complessa e questo potrebbe generare incomprensioni.
   E' importante quindi prevedere, per quanto possibile, questi mal utilizzi e modificare il progetto affinchè vengano evitati.
   Compito dell'ingegnere del software è quello di identificare quegli aspetti della destinazione d'uso che sono troppo sottili per essere evidenti a livello di sistema in modo che vengano anche essi registrati nel file di gestione del rischio.
   Un altro aspetto molto importante che potrebbe portare a un mal utilizzo è il fatto che l'uso del software in un dispositivo medico rende possibile un range di intecomunicazioni e inteconnessioni tra dispositivi medici e non; se è facile prevedere che questo potrebbe portare a nuovi pericoli non è affatto facile per il fabbricante identificare tutti questi nuovi possibili usi e, di conseguenza, anche abusi se le interconnessioni e intercomunicazioni sono senza restrizioni – si rimanda al capitolo 3 per una trattazione più approfondita di questo aspetto molto importante e molto critico e che interessa particolarmente anche gli ingegneri clinici (delle reti) all'interno delle Aziende Ospedaliere che integrano tali dispositivi medici nelle reti IT
ii. *Identificazione dei pericoli noti o prevedibili (e loro cause):*

L’obiettivo di identificare i pericoli è quello di permettere l’analisi di tutti i rischi prevedibili e la progettazione e attuazione di misure per limitare tali rischi.

Come abbiamo già anticipato il software (contrariamente a energia elettrica o masse sospese) non è di per sè un pericolo ma può contribuire a situazioni pericolose. Guasti software infatti facilitano la trasformazione di un pericolo in una situazione pericolosa.

L’identificazione dei pericoli deve considerare danni che possono derivare dalla natura stessa del dispositivo medico e da pericoli relativi all’uso del software (per esempio un’errata identificazione del paziente nel caso in cui il dispositivo ne memorizza i dati o le prescrizioni).

I pericoli identificati devono poi includere sia quelli relativi al software che funzionano correttamente sia quelli relativi ad anomalie software.

Alcuni di questi aspetti comportano il fatto che, se in assenza di software il controllo del rischio era responsabilità solamente del professionista che usava il dispositivo adesso si è spostata sulla gestione del rischio da parte del fabbricante. Si faccia l’esempio del bisturi – se intendiamo il bisturi comune le responsabilità erano tutte dell’operatore che lo utilizzava mentre, se consideriamo un bisturi incorporato in un apparecchio gestito da un software che viene controllato da remoto sempre dallo stesso operatore questa volta la responsabilità di un possibile danno arrecato al paziente non è più solo responsabilità dell’operatore ma anche del fabbricante.

Poichè i software sono molto complessi l’individuazione dei possibili pericoli deve essere fatta a livello di sistema (e non in modo isolato) da personale qualificato e multidisciplinare (comprendente quindi sia esperti clinici che ingegneri del software).

iii. *Stima dei rischi per ogni situazione pericolosa:*

E’ utile avere una stima della probabilità del verificarsi di situazioni pericolose e del loro evolversi. La stima dei rischi si basa sulla probabilità che il danno si verichi e sulla gravità di ogni situazione pericolosa identificata. Siccome non sempre è possibile stimare la probabilità che si verifichi un guasto va considerato il caso peggiore e quindi tale probabilità dovrebbe essere posta a 1 per cui il rischio dovrà essere valutato solo sulla base della gravità del danno derivante da situazioni pericolese. E’ opportuno che il fabbricante prediliga una stima della probabilità di tipo quantitativo, anche se una stima qualitativa è

accettabile ed è da preferire nel caso in cui la stima quantitativa non fosse attendibile.

Per stimare i rischi relativi al software è prima necessario identificare le situazioni pericolose che includono il software; il software può essere sia la causa iniziale della sequenza di eventi che portano a situazioni pericolose oppure può essere all'interno di tale sequenza (come nel caso di sofwtare destinati a rilevare mal funzionamenti hardware).

Per identificare il ruolo potenziale del software in situazioni pericolose ci sono varie tecniche disponibili, come, ad esempio:

i. Fault Tree Analysis (FTA) – metodo top-down in quanto parte da un'analisi "generale" e complessiva del tipo di guasto arriva a identificare i guasti sui componenti. E' un metodo di tipo deduttivo usato per analizzare l'affidabilità dei sistemi evidenziando principalmente le relazioni di causa-effetto (mettendo in relazione il guasto sul sistema con i guasti sui componenti) e l'organizzazione del sistema. Partendo da una conseguenza indesiderata identifico tutte le possibili cause e così via fino ad arrivare alla sorgente del guasto.

   Questo tipo di analisi consente un approccio sistematico ma anche flessibile per permettere l'analisi di vari fattori (incluse le interazioni umane). Questo tipo di analisi è usato principalmente per fornire una stima delle probabilità di guasto.

ii. Failure Modes And Effect Analysis – approccio bottom-up (parte dal singolo componente o sottosistema e procede verso livelli superiori) di tipo induttivo e qualitativo mediante il quale vengono sistematicamente identificate e valutate le conseguenze di una modalità di guasto di un singolo componente.

   Questa tecnica può essere usata per gestire l'errore umano.

   Gli svantaggi invece sono dovuti alle difficioltà di gestire le ridondanze e l'incorporazione di azioni di riparazione o manutenzione preventiva oltre al fatto che si utilizza in condizioni di singolo guasto.

   Entrambi i metodi vanno eseguiti preventivamente e quindi si basano su considerazioni teoriche.

Anche se è difficile prevedere esattamente ciò che può fallire in un componente software è possibile identificare delle categorie di difetti ognuna delle quali ha

delle misure di controllo del rischio note (per esempio la corruzione dei dati è un tipo di difetto che può essere rilevato e impedito mediante una procedura di checksum).

In sintesi la stima dei rischi software dovrebbe concentrarsi sulla gravità e sulla relativa probabilità del danno se dovesse capitare un guasto piuttosto che sul tentativo di stimare la probabilità di accadimento di ogni possibile guasto software.

2.3.2 Valutazione del rischio

In questa fase il fabbricante, noti i rischi possibili, deve decidere, usando i criteri definiti nel piano di gestione del rischio, se è necessaria o meno la riduzione del rischio. Come abbiamo già detto lo standard internazionale non dà indicazioni precise su come definire un rischio accettabile ma contiene delle linee guida; questa stima è soggettiva e viene decisa caso per caso. I metodi per determinare se un rischio è accettabile possono essere:
-) impiegare le norme applicabili che specificano i requisiti che, se implementati, indicano il raggiungimento dell'accettabilità riguardante particolati tipi di dispositivi o rischi.
-) seguire le linee guida appropriate.
-) confrontare i livelli di rischio evidenti per i dispositivi medici già in uso.
I rischi possono essere divisi in tre aree distinte (usando un "traffic light model", di cui abbiamo un esempio in Figura 5, che va personalizzato per ogni dispositivo preso in considerazione) in funzione di probabilità e gravità (in ordine crescente) del danno. Se il rischio ricade nell'area verde allora è considerato accettabile e non sono necessari ulteriori interventi. Se il rischio ricade nell'area gialla (denominata ALARP, acronimo di As Low As Reasonably Praticable) i benefici potrebbero valere il rischio ma si deve comunque cercare di ridurre il rischio al minimo per quanto ragionevolmente praticabile – la praticabilità è la capacità del fabbricante di ridurre il rischio ed è composta da due componenti:
-)la praticabilità tecnica (cioè quella di ridurre il rischio indipendentemente dal costo)
-)la praticabilità economica (cioè la capacità di ridurre il rischio senza portare il costo del prodotto a un livello fuori mercato).
Se invece il rischio ricade nell'area rossa è da considerarsi non tollerabile.

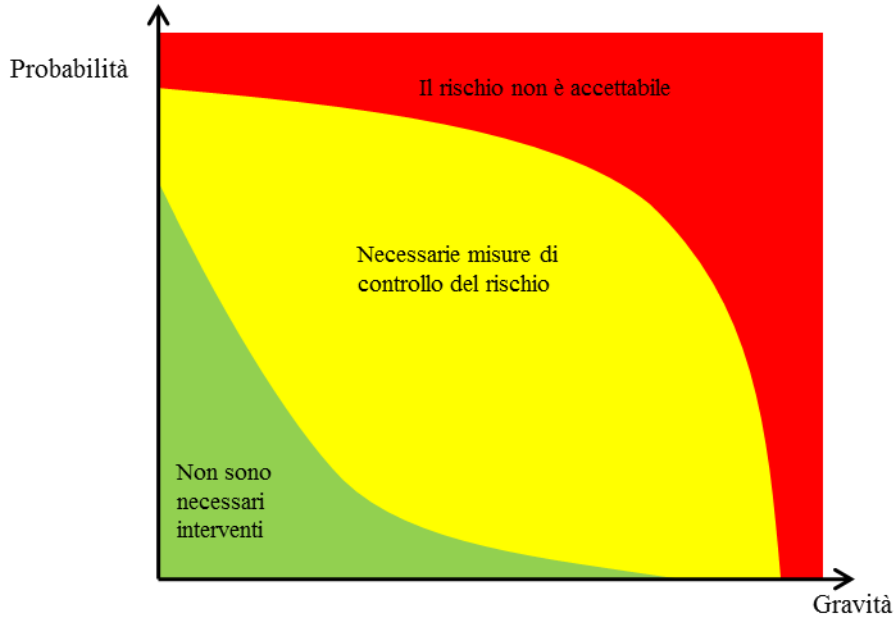

Figura 5 Esempio di diagramma del rischio a semaforo.

2.3.3 Controllo del rischio

Quando è richiesta una riduzione del rischio devono essere eseguite attività di controllo del rischio.

2.3.3.1 Scegliere le misure di controllo del rischio per sistemi complessi

Il fabbricante deve quindi scegliere delle misure di controllo del rischio appropriate per ridurre il rischio a un livello accettabile o, addirittura, eliminarlo. Andremo ad analizzare tre tipi di misure di controllo del rischio che possono essere implementate nel software in ordine di priorità:

i. Sicurezza intrinseca derivante dalla progettazione
   Siccome nei sistemi software si è sempre tentati di includere ogni possibile desiderio del cliente senza discriminazioni questo può portare a un eccessivo numero di modi con cui i componenti possono interagire tra loro portando a situazioni pericolose inaspettate. Applicando una gestione del rischio già dalle prime fasi di sviluppo del dispositivo medico e del suo software è possibile, pur soddisfacendo le esigenze della maggior parte dei clienti, evitare tali situazioni. La sicurezza intrinseca derivante dalla progettazione per il software comporterà:
   -) un'eliminazione di funzionalità non sicure,
   -) modifiche nell'architettura del software per evitare sequenze di eventi che porterebbero a situazioni pericolose,

-) semplificazioni dell'interfaccia utente per ridurre le probabilità di errori umani durante l'utilizzo,

-) definizione di regole di progettazione software per evitare anomalie (per esempio usare solo allocazione statica in memoria e non dinamica oppure usare una versione ristretta di un linguaggio di programmazione limitandosi all'uso di librerie che sono state certificate per applicazioni safety-critical).

ii. Misure protettive (o nel dispositivo medico stesso o durante il processo di produzione)

Le misure protettive per un dispositivo medico che utilizza un software possono essere implementate sia nella parte hardware che nella parte software. Il progetto di tali misure deve dimostrare che le misure protettive sono indipendenti dalla funzione a cui sono applicate – questa cosa è facilmente realizzabile se una misura protettiva per il software è applicata all'hardware o viceversa. Nella scelta di misure protettive che sono sia implementate che applicate al software bisogna evitare la possibilità di più guasti derivanti da una stessa causa – se una misura protettiva individua e/o previene una situazione pericolosa il fabbricante deve dimostrare un'adeguata separazione tra la misura protettiva e la funzione del software che fornisce una performance essenziale (per esempio un software che esegue un trattamento per un paziente può essere eseguito da un processore mentre il software che implementa le misure protettive deve essere eseguito su un altro processore)

iii. Informazioni per la sicurezza

L'uso del software in un dispositivo medico può far apparire più complesso all'utente il comportamento del dispositivo. Migliorandone l'interfaccia utente però posso renderlo più semplice e intuitivo e, di conseguenza, diminuire la complessità e la mole del manuale utente.

Ma quali eventi necessitano l'applicazione di queste misure di controllo del rischio?

Molte sequenze di eventi potrebbero portare a situazioni pericolose ma non per questo è sempre necessario (o possibile) applicare le misure di controllo del rischio a ogni evento di tali sequenze ma è sufficiente applicarle a un numero attentamente selezionato di eventi per ricondurre la complessiva probabilità di danno a un livello accettabile.

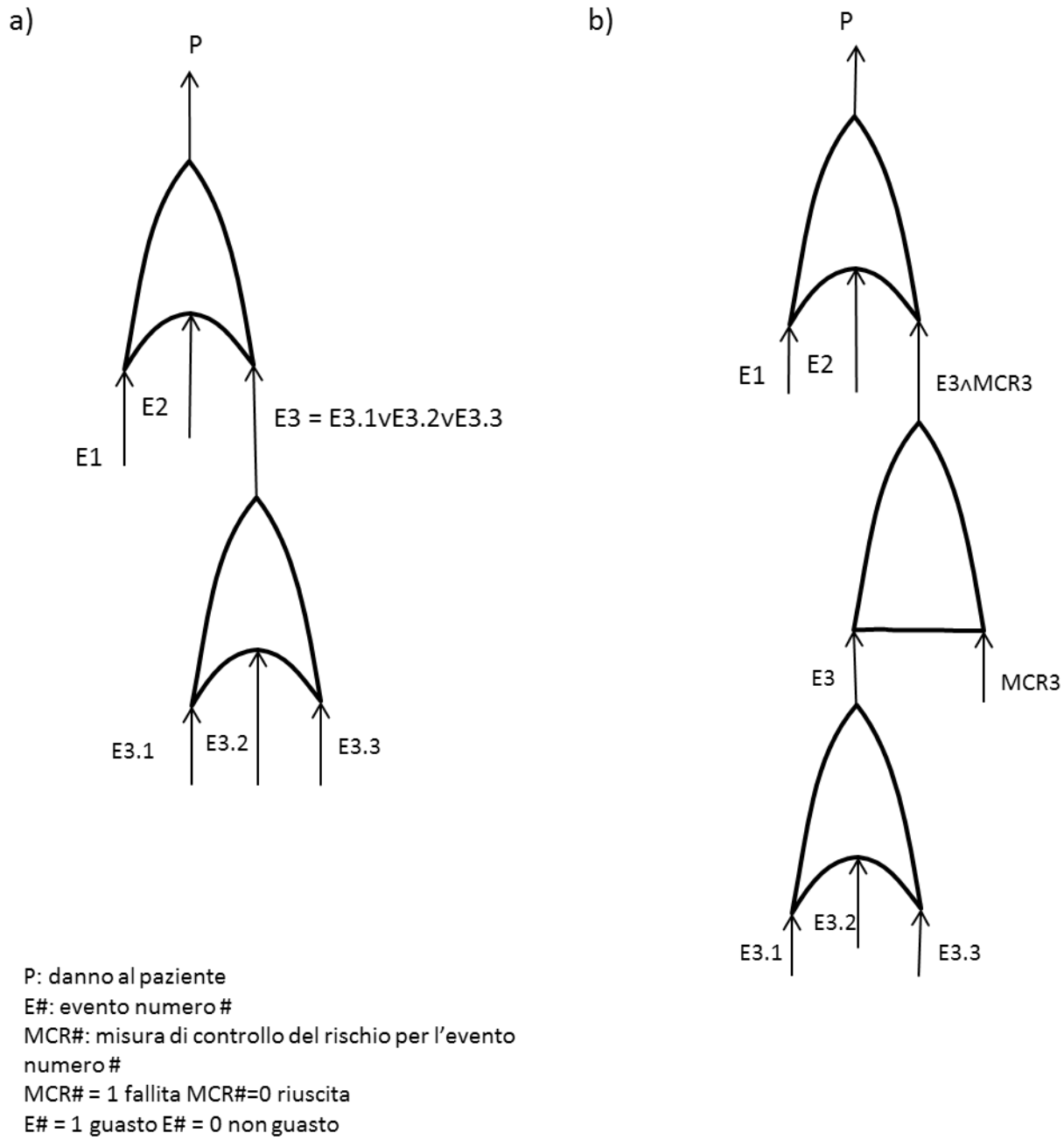

Figura 6 Esempio di grafico FTA per l'identificazione di sequenze dannose.

Prendiamo come esempio la Figura 6. Il punto a) mostra come, in caso del fallimento o dell'evento 3.1 o dell'evento 3.2 o dell'evento 3.3 risulta una comune causa di pericolo E3 per il paziente per cui, come si vede in figura b) può essere più conveniente applicare una sola misura di controllo del rischio direttamente all'evento 3 ponendoli entrambi in ingresso a una porta AND, in questo modo, se la misura di controllo del rischio non fallisce riesco a evitare un possibile danno al paziente – la stessa procedura può essere applicata ricorsivamente a tutti i rami. Questa procedura sebbene semplifichi il controllo

del rischio non identifica la sequenza di eventi per cui è più difficile capire a che livello intervenire per correggere il problema.

Punti in cui possono essere applicate misure di controllo del rischio includono:

-) Input: limitando il range di input al software prevengo output non sicuri e, inoltre, posso ridurre la probabilità che un input determini un danno dovuto a un'anomalia software, questo poichè riduce la probabilità che il software operi in modi che possono non essere stati testati. Esempi di tali misure possono essere:

- misure di controllo del rischio di tipo software che controllano gli input e rifiutano i valori non corretti o incoerenti
- misure di controllo del rischio di tipo hardware come, banalmente, una stanza chiusa a chiave per evitare inserimento di dati da persone non autorizzate.

-) Output: applicando misure di controllo del rischio agli output posso controllare che tali valori siano all'interno di un range di valori sicuro e coerente in modo da prevenire danni. Esempi di tali misure possono essere:

- misure di controllo del rischio di tipo software che controllano i valori in output in modo che non si discontino da un range di sicurezza
- misure di controllo del rischio di tipo hardware che limitano l'energia applicata al paziente
- la combinazione di un'etichetta di warning e un interruttore. Questo tipo di misura di controllo presuppone la presenza di un operatore in grado di identificare una situazione pericolosa per il paziente.

-) Interfacce interne tra moduli software.

Le misure di controllo del rischio possono anche essere applicate anche a input o output di componenti software.

Poichè a volte può non essere possibile identificare un singolo range per i parametri nel quale il dispositivo operi in sicurezza si può però specificare un "safe operating envelope" – per esempio il software potrebbe combinare la temperatura di una parte applicata con il tempo di esposizione per verificare se c'è il rischio di bruciare il paziente. Altre volte invece gli input e gli output sono conosciuti solo dal medico e quindi non è possibile anticipare, durante la fase di

progetto, un range di valori di sicurezza per cui le misure di controllo del rischio software o hardware possono solo limitarsi a trovare incongruenze tra input e output.

2.3.3.2 Metodi di controllo del rischio

Al fine di implementare efficaci misure di controllo del rischio per il software bisogna considerare attentamente lo sviluppo del prodotto e il ciclo di vita del software – per esempio, alcune misure di controllo sono meno costose e più semplici da implementare nelle prime fasi della progettazione piuttosto che più tardi.

Può anche essere utile classificare i componenti software e assegnare classi di sicurezza ai vari componenti software per distinguere quelli più critici da quelli meno critici. Assegnare classi di sicurezza può servire come base per un maggior rigore e attenzione ai componenti software più critici. E' possibile che componenti software prima classificati in un modo, dopo l'implementazione di opportune misure di controllo del rischio e particolari scelte di progettazione, possano essere trattati come meno critici.

Andiamo quindi ad analizzare con maggior dettaglio alcune misure di controllo del rischio.

- Misure di controllo del rischio e progettazione dell'architettura del software

Alcune scelte progettuali riguardanti l'architettura del sistema possono intrinsecamente evitare danni, dal punto di vista della parte hardware questo fatto è facilmente intuibile (basti pensare che usando una batteria al posto della corrente alternata riesco a evitare che il paziente venga folgorato) vale la stessa cosa per la parte software (per evitare la corruzione dei dati posso usare memorie statiche invece che dinamiche). Se il componente software ha un ruolo nella sicurezza durante la valutazione del rischio dovrei pormi le seguenti domande:

-) una funzione di sicurezza può accedere al processore quando necessario?
-) il processore concede abbastanza tempo per svolgere una funzione di sicurezza?

-) è possibile dimostrare che altri componenti software non interferiscano con l'esecuzione della funzione di sicurezza?

I metodi di sviluppo dovrebbero essere scelti in modo tale che tutti i problemi sopracitati siano chiari al designer.

- Struttura Faul-Tolerant

Soprattutto nell'ambito dei dispositivi medici è importante che alcune funzioni continuino ad operare anche in presenza di guasto. Per rendere il mio dispositivo fault-tolerant posso ricorrere alla *ridondanza* – duplicando un componente vitale o aggiungendo dei componenti che rilevano il guasto e cambiano il modo con cui viene svolta la funzione; se la ridondanza non dovesse bastare posso avvalermi della *diversificazione* – posso cioè usare un software aggiuntivo per rilevare l'errore e per eseguire un programma di recupero. In casi ancora più critici posso utilizzare due o più componenti software indipendenti (sia dal punto di vista della progettazione che dell'implementazione) per svolgere la stessa funzione – in questo caso si parla di "*programmazione diversificata*". Anche se il dispositivo continua a funzionare è importante che, in caso di errore, questo venga comunque segnalato all'operatore.

- Segregazione del codice

Il produttore deve fare in modo che i componenti software non relativi alla sicurezza non interferiscano con le funzioni dei componenti software relativi alla sicurezza. Le interazioni possono avvenire a molti livelli, per esempio i componenti software possono interagire per contendersi le risorse hardware condivise (accesso ai processori) oppure a seguito della condivisioni di alcune variabili. Per evitare che questo accada il modo migliore sarebbe far girare su processori diversi i componenti software che non devono interagire. Il produttore deve inoltre dimostrare l'efficacia della segregazione dimostrando che, per esempio, in normali condizioni di funzionamento, componenti software non relativi alla sicurezza non possano modificare dati relativi alla sicurezza.

- Misure protettive

Siccome non è sempre possibile o pratica una progettazione che prevede l'eliminazone intrinseca di ogni causa di rischio o che introduca tolleranza a tutti i possibili mal funzionamenti. Nei casi in cui queste misure preventive non possono essere applicate si ricorre alle misure protettive per gestire i potenziali

rischi – tali misure possono sia agire automaticamente per eliminare o almeno limitare i danni oppure possono generare un allarme per far si che intervenga il personale. In certi casi la sicurezza può essere ottenuta a spese dell'operatività, in architetture fail-safe un malfunzionamento del sistema o di un componente può portare a una perdita di funzione che però preserva la sicurezza di paziente e operatore mentre nei sistemi fail-operational il sistema può continuare a operare sicuramente ma con performance ridotte.

Particolare attenzione va posta anche alla frequenza con cui eseguire misure di controllo del rischio per fare in modo che il periodo che intercorre tra un controllo e il successivo non sia sufficiente a fare in modo che un mal funzionamento si evolva fino a causare un danno al paziente.

I software pongono un ulteriore complicazione alla progettazione delle misure di controllo del rischio in quanto possono presentare anomalie difficilmente prevedibili anche con un attento design – le misure di controllo del rischio possono ridurre la probabilità di un danno derivante da anomalie software. Ciò è reso più pratico se tali misure vengono applicate in punti dell'architettura software in cui la probabilità di danno può essere ridotta indipendentemente dalla natura degli eventi che avrebbero potuto causarlo – in questo modo si garantisce la sicurezza anche senza avere conoscenza completa di tutte le possibili anomalie.

Per quelle anomalie che generano sequenze di eventi che portano a un danno che non può essere evitato con le misure di controllo del rischio è importante ridurre la probabilità dell'anomalia stessa. Quei software per cui il produttore garantisce sicurezza e affidabilità della funzionalità e che operano in totale assenza di errori possono essere trattati come componenti ad alta integrità. Il processo di sviluppo di tali componenti può essere usato per ridurre la probabilità di anomalie software. Per ottenere un componente ad alta integrità è opportuno definire un rigoroso processo di sviluppo del software seguendo, per esempio, le indicazioni descritte nella direttiva IEC 62304, avvalendosi di personale qualificato, garantendo l'adeguatezza delle specifiche, del design, del testing, operando revisioni rigorose e formali e usando strumenti di qualità.

2.3.3.3 Implementazione delle misure di controllo del rischio

Una volta che ho identificato le misure di controllo del rischio non mi resta che implementarle e verificarne l'efficacia. Gli aspetti chiave da considerare includono:

-) tracciabilità per assicurarmi che tutti i componenti software sono stati identificati e che tutte le funzionalità relative alla sicurezza sono state specificate, implementate e testate in tutte le possibili versioni e varianti del software

-) che i test siano stati eseguiti in modo rigoroso e utilizzando un ampio range di condizioni

-) focus sulle misure di controllo del rischio di test di regressione e funzionalità legate alla sicurezza quando vengono apportate modifiche (anche quando tali cambiamenti non sembrano destinati a compromettere la sicurezza).

Poichè l'applicazione di misure di controllo del rischio potrebbe creare nuovi pericoli o situazioni pericolose è necessario che siano soggette a nuove valutazioni del rischio subito dopo averle specificate. Queste revisioni dovrebbero essere ripetute sia dopo la progettazione software sia dopo i test del sistema software.

Dopo aver applicato le misure di controllo del rischio bisogna valutare il rischio residuo complessivo usando i criteri definiti nel piano di gestione del rischio. Se il rischio residuo non è considerato accettabile e non sono praticabili ulteriori controlli del rischio il fabbricante può raccogliere e esaminare dati clinici e letteratura per determinare se i benefici superano la gravità del rischio residuo, in caso affermativo il fabbricante deve decidere quali informazioni per la sicurezza è necessario includere nel rischio residuo altrimenti rimane inaccettabile. I risultati delle attività di test dovrebbero essere valutati con l'aiuto dei criteri di accettabilità. Tutte le restanti anomalie software devono essere documentate nel file di gestione del rischio e valutate per assicurarsi che non contribuiscano a un rischio inaccettabile. Dove necessario tale valutazione deve essere effettuata tramite controlli interdisciplinari. Dove necessario è possibile includere tali informazioni anche nel documento di accompagnamento.

2.3.4 Informazioni di produzione e post produzione

Sebbene le stime dei rischi possano essere rese più accurate con la realizzazione di un prototipo funzionante tuttavia nessuna attività di modellazione può sostituire un dispositivo effettivo nelle mani dell'utilizzatore poichè è proprio in questa fase che tutti i pericoli divengono reali.E' per questo motivo che i fabbricanti dovrebbero monitorare le informazioni posteriori alla commercializzazione sugli aspetti che possono riguardare la stima dei rischi e le decisioni in materia. Come abbiamo quindi accennato all'inizio le attività di gestione del rischio devono continuare per tutto il ciclo di vita del dispositivo e sarà l'ingegnere clinico e l'organizzazione responsabile (cioè i dirigenti dell'azienda) a doversi occupare della gestione del rischio clinico.

Il fabbricante offre all'Azienda Ospedaliera un dispositivo sicuro ed efficace ma, poichè come abbiamo già accennato, un sempre maggior numero di dispositivi è in grado di scambiare informazioni con altri dispositivi medicali e non attraverso una rete IT (che è un ambiente in costante cambiamento) questo porta al fatto che il produttore non può prevedere tutti i possibili cambiamenti e non ha modo di potersi assicurare che il dispositivo funzionerà correttamente in tutti i casi possibili. E' quindi compito dell'Azienda Ospedaliera dotarsi di una struttura adeguata e di una gestione del rischio in grado di tener conto sia delle modifiche associate all'evoluzione della rete sia del loro impatto della gestione dei dispositivi sia dell'incorporazioni di altri dispositivi all'interno della rete.

Capitolo 3 Gestione medical it-network

Il fabbricante di dispositivi medici è stato per lungo tempo l'unico responsabile per i rischi associati alla progettazione e produzione dei dispositivi. Dal momento che ormai molti dispositivi medici sono dotati di interfaccia di rete e quindi si connettono alla rete IT dell'ospedale, lo scopo di molte attività di gestione del rischio da parte del fabbricante è reso vano. Siccome il fabbricante non può decidere la progettazione della rete o le operazioni della rete stessa è l'ospedale che deve diventare l'entità che si occupa della gestione del rischio (da qui il termine di organizzazione responsabile). Se, come abbiamo visto, la parte riguardante i dispositivi medici è un'area attentamente regolamentata quella che riguarda l'incorporazione dei dispositivi medici in rete non lo è ancora. A parte lo standard IEC 60601-1 del 2005 che richiede al fabbricante del dispositivo medico di fornire informazioni, nel documento di accompagnamento, nel caso in cui il dispositivo debba essere connesso a una rete; bisogna aspettare il 2009, con il report tecnico IEC 80001-1, per avere uno standard che affronti *come* il dispositivo medico possa essere connesso a una rete IT. In questo capitolo andremo dunque ad analizzare lo standard IEC 80001-1:2009 che definisce le funzioni, le responsabilità e le attività necessarie alla gestione dei rischi delle reti IT incorporanti dispositivi medici ai fini di sicurezza, efficienza e sicurezza dei dati e del sistema.

I principi base di questa normativa sono:

- L'incorporazione o rimozione di un dispositivo medico o altri componenti in una rete IT è un compito che richiede un piano d'azione che potrebbe essere fuori dal controllo del fabbricante del dispositivo medico
- La gestione del rischio deve essere effettuata prima che il dispositivo medico venga incorporato in una rete IT e durante l'intero ciclo di vita della rete IT che incorpora il dispositivo onde evitare rischi inaccettabili che potrebbero derivare dall'incorporazione del dispositivo nella rete.
- Il fabbricante del dispositivo medico è responsabile per l'analisi del rischio del dispositivo durante la sua progettazione, implementazione e produzione.
- Il fabbricante di un dispositivo medico destinato a essere incorporato in una rete IT deve fornire le informazioni necessarie (che vanno incluse nel

documento di accompagnamento) per consentire all'Organizzazione Responsabile di gestire il rischio in accordo con questo standard.

- Il documento di accompagnamento deve quindi contenere le istruzioni su come incorporare il dispositivo nella rete IT, sul modo in cui il dispositivo trasferisce informazioni attraverso la rete e sulle caratteristiche minime che la rete IT deve avere affinchè il dispositivo funzioni correttamente oltre alle avvertenze sui pericoli associati a un mal utilizzo della rete IT.
- Possono essere stabiliti uno o più accordi di responsabilità in grado di stabilire ruoli e responsabilità tra le varie parti interessate. Un accordo di responsabilità può riguardare uno o più progetti o il mantenimento di una o più reti IT medicali e deve identificare le responsabilità per tutti gli aspetti del ciclo di vita della rete IT medicale e tutte le attività che ne fanno parte. L'accordo di responsabilità deve quindi contenere, come minimo: il nome della persona responsabile per le attività di gestione del rischio contemplate nell'accordo di responsabilità; una lista di dispositivi medici e altri dispositivi che devono essere incorporati o modificati nella rete IT insieme con i nomi dei fabbricanti dei dispositivi medici; una lista di documenti che deve essere fornita dal fabbricante o dal fornitore di rete IT che contengono le istruzioni necessarie per connettere o disconnettere i dispositivi alla rete e le informazioni tecniche necessarie per effettuare l'analisi dei rischi per le reti IT.
- L'organizzazione responsabile è tenuta a scegliere il personale per ruoli specifici per l'attuazione di questo standard come, per esempio, il manager per la gestione del rischio delle reti IT medicali.
- Il manager per la gestione del rischio delle reti IT medicali deve assicurarsi che la gestione del rischio si svolga sia durante il periodo di pianificazione e progettazione di nuove incorporazioni di dispositivi medici o di cambiamenti di tali incorporazioni, sia durante la messa in uso e conseguente utilizzo della rete IT includendo anche la gestione change-release della rete IT per l'intero ciclo di vita.

La gestione del rischio deve garantire le segueni proprietà chiave:

- **Sicurezza** intesa come l'assenza di rischi non accettabili per il paziente (ma anche agli operatori o a terze parti) o danni alla proprietà o all'ambiente che possono essere causati da un malfunzionamento dei dispositivi medici; da guasti o errate configurazioni degli interfacciamenti o da interazioni indesiderate tra il dispositivo medico e la rete informatica.

- **Efficacia** intesa come la capacità di produrre il risultato atteso per il paziente e l'organizzazione responsabile.
- **Sicurezza del sistema e dei dati**; è un obbligo di legge garantire che le risorse informatiche siano protette da accessi non voluti, integrità e disponibilità dei dati.

E' importante notare che questo standard riconosce una responsabilità condivisa tra fabbricante e aziende ospedaliere che devono collaborare per effettuare una corretta gestione del rischio.

3.1 Ruoli e responsabilità

Andiamo adesso a definire le responsabilità per l'incorporazione, le modifiche e la gestione di software o apparecchiature all'interno di una rete IT medicale.

Organizzazione responsabile è quell'ente responsabile dell'uso e della manutenzione di un apparecchio o di un sistema elettromedicale, della rete IT e del software dispositivo medico – nel nostro caso l'organizzazione responsabile sono le aziende ospedaliere. L'azienda ospedaliera sarà quindi la responsabile di tutto il processo di gestione del rischio per le reti IT medicali e si dovrà quindi occupare di tutto ciò che le riguarda; dalla progettazzione, all'istallazione fino, eventualmente, alla disattivazione. Compiti dell'azienda ospedaliera sono:

1. Fornire una descrizione delle risorse che possono comportare dei rischi e stabilire una lista di risorse della rete IT che si interfacciano con i dispositivi medici. Le risorse possono includere informazioni di configuration management; dati sulla configurazione di software e hardware; dati personali di uno specifico paziente; componenti specifici della rete IT e di tutti i dispositivi medici collegati e altri strumenti dell'infrastruttura IT.
2. Fornire una documentazione della rete IT necessaria per sostenere la gestione del rischio della rete per le interfacce tra i dispositivi medici e tutte le altre risorse di rete. Questa documentazione deve includere la configurazione della rete fisica e della rete logica; gli standard applicati e la dichiarazione di conformità, la struttura client/server; la sicurezza, affidabilità e integrità dei dati; futuri cambiamenti/aggiornamenti/miglioramenti pianificati o ragionevolmente prevedibili.

3. Stabilire e mantenere un *piano di gestione dei rischi* per ogni rete IT medicale che deve contenere:
    - una descrizione della rete IT medicale che include:
      -) un'identificazione delle parti coinvolte all'interno dell'organizzazione responsabile che devono essere informate sui pericoli in modo da essere consapevoli dei rischi.
      -) la ragione per l'incorporazione dei dispositivi medici nella reti IT.
      -) l'impatto sulla destinazione d'uso definita dal fabbricante di ogni dispositivo medico che dovrà essere incorporato in una rete IT
    - Fornire una descrizione delle attività, ruoli e responsabilità per tutte le parti coinvolte nella gestione e nel mantenimento delle reti IT, includendo anche l'dentificazione di noti e possibili nuovi pericoli.
    - Stabilire e mantenere un processo di monitoraggio per ogni rete IT medicale istallata.
    - Fornire criteri di accettabilità del rischio anche quando la probabilità che si verifichi un danno non può essere stimata.

Il piano di gestione del rischio deve essere aggiornato quando un progetto introduce dei cambiamenti a una rete IT già esistente.

Per assicurarsi che tutto venga eseguito correttamente l'organizzazione responsabile deve allocare adeguate risorse allo scopo. Per assicurarsi che tutto sia svolto correttamente la normativa nomina "una persona o un gruppo di persone che dirige e controlla l'organizzazione responsabile ai più alti livelli" nota come **Top Management** e richiede ad essi di creare politiche per stabilire le attività di gestione del rischio.

Il top management, come riassunto anche in Figura 7, deve:

1. Stabilire una politica per la gestione del rischio
2. Definire una polica per la determinazione del rischio accettabile, tenendo conto degli stanard internazionali.
3. Garantire la fornitura di adeguate risorse.

4. Esaminare i risultati delle attività per la gestione del rischio a intervalli regolari per assicurare l'adeguatezza e l'efficacia dei processi di gestione del rischio.
5. Assicurarsi che le attività svolte durante tutto il ciclo di vita delle reti IT siano effettuate in base al piano di gestione del rischio e che tutte le parti in gioco siano adeguatamente informate sulle loro responsabilità secondo questo standard, incluse le responsabilità per il mantenimento e l'efficacia del controllo del rischio.
6. Nominare un **manager per la gestione del rischio** che abbia le competenze, qualifiche, esperienze e conoscenze necessarie per la gestione del rischio applicata alle reti IT medicali e scegliere personale adeguato che collabori con il manager di gestione del rischio. Il manager per la gestione del rischio è anche il ruolo più importante nell'ambito della gestione del rischio.

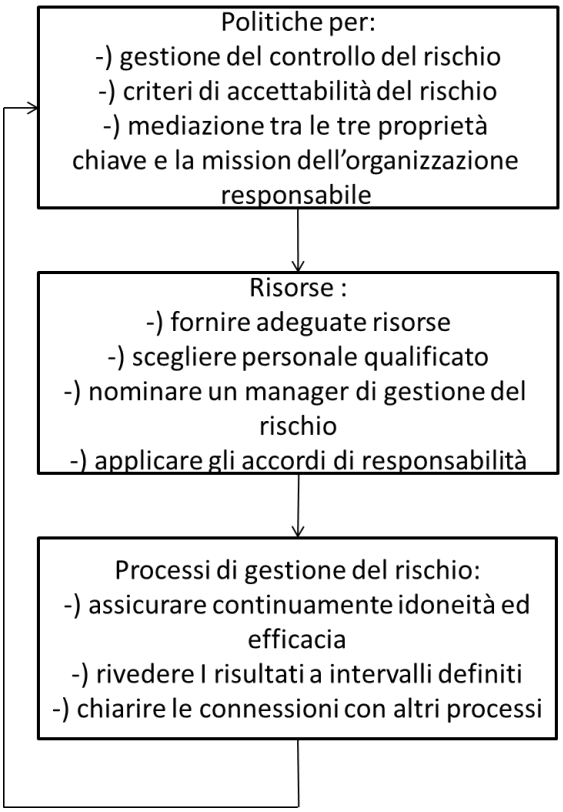

Figura 7 Responsabilità del top-management – TR IEC 80001-1: 2009

Il Manager della gestione del rischio delle rete IT è la persona responsabile per la gestione e l'esecuzione dei processi di gestione del rischio della rete IT medicale; deve quindi avere le competenze e l'esperienza necessaria in merito alle tecnologie medicali e alle reti IT (l'ingegnere clinico?).

Il manager per la gestione del rischio deve gestire complessivamente i processi di controllo del rischio; tenere informato il top management e coordinare i rapporti tra le parti coinvolte nella gestione del rischio sia interni (come lo staff dei clinici, il dipartimento di ingegneria clinica e quello delle reti IT) che esterni (ovvero il fabbricane del dispositivo medico e i fornitori di reti IT).
Il manager di gestione del rischio è quindi responsabile per la progettazione, mantenimento e performance dei processi di gestione del rischio e deve assicurarsi che tali processi siano inclusi durante:

-) la pianificazione e progettazione di nuove incorporazioni di dispositivi medici in accordo con le istruzioni fornite dai vari fabbricante.
-) la pianificazione e progettazione di cambiamenti nelle incorporazioni.
-) la messa in funzione della rete IT medicale e conseguente uso.
-) la gestione change-release della rete IT durante l'intero ciclo di vita del dispositivo.

I processi di gestione del rischio includono:

-) la pianificazione dell'incorporazione del dispositivo medico in accordo con le istruzioni fornite dai diversi fabbricanti dei dispositivi
-) l'esecuzione dei processi di gestione del rischio ogni volta che si aggiunge un dispositivo medico alla rete e ogni volta che un dispositivo medico incorporato o la rete IT stessa subisce delle modifiche.
-) informare l'organizzazione responsabile su tutti i rischi inaccettabili legati alla rete IT e sui pericoli associati derivanti da qualunque cambio di configurazione.
-) la raccolta di tutte le informazioni sui dispositivi medici.

Come abbiamo già detto tra le responsabilità del manager della gestione del rischio per le reti IT medicali c'è quella di raccogliere, analizzare, valutare e memorizzare i dati provenienti da tre sorgenti principali ovvero l'organizzazione sanitaria stessa; il fabbricante del dispositivo medico e il fornitore di tecnologie informatiche.

Ogni **fabbricante** di un dispositivo medico che dovrà essere integrato in una rete IT deve descrivere, nel documento di accompagnamento, oltre alla destinazione d'uso del dispositivo e le istruzioni necessarie per un utilizzo sicuro ed efficace anche istruzioni per l'implementazione di tali connessioni come, per esempio, le caratteristiche che la rete IT deve avere per incorporare il

dispositivo; la configurazione della rete IT che incorpora il dispositivo medico; le specifiche tecniche della connessione di rete del dispositivo medico incluse specifiche riguardanti la sicurezza, restrizioni e incompatibilità note.

I **fornitori di tecnologie informatiche** che possono fornire componenti dell'infrastruttura, server, software applicativi, dispositivi client che non sono dispositivi medici, middleware, possono fornire, all'organizzazione responsabile, ulteriori informazioni per sostenere le attività di gestione del rischio.

In Figura 8 abbiamo una panoramica dei ruoli e delle responsabilità.

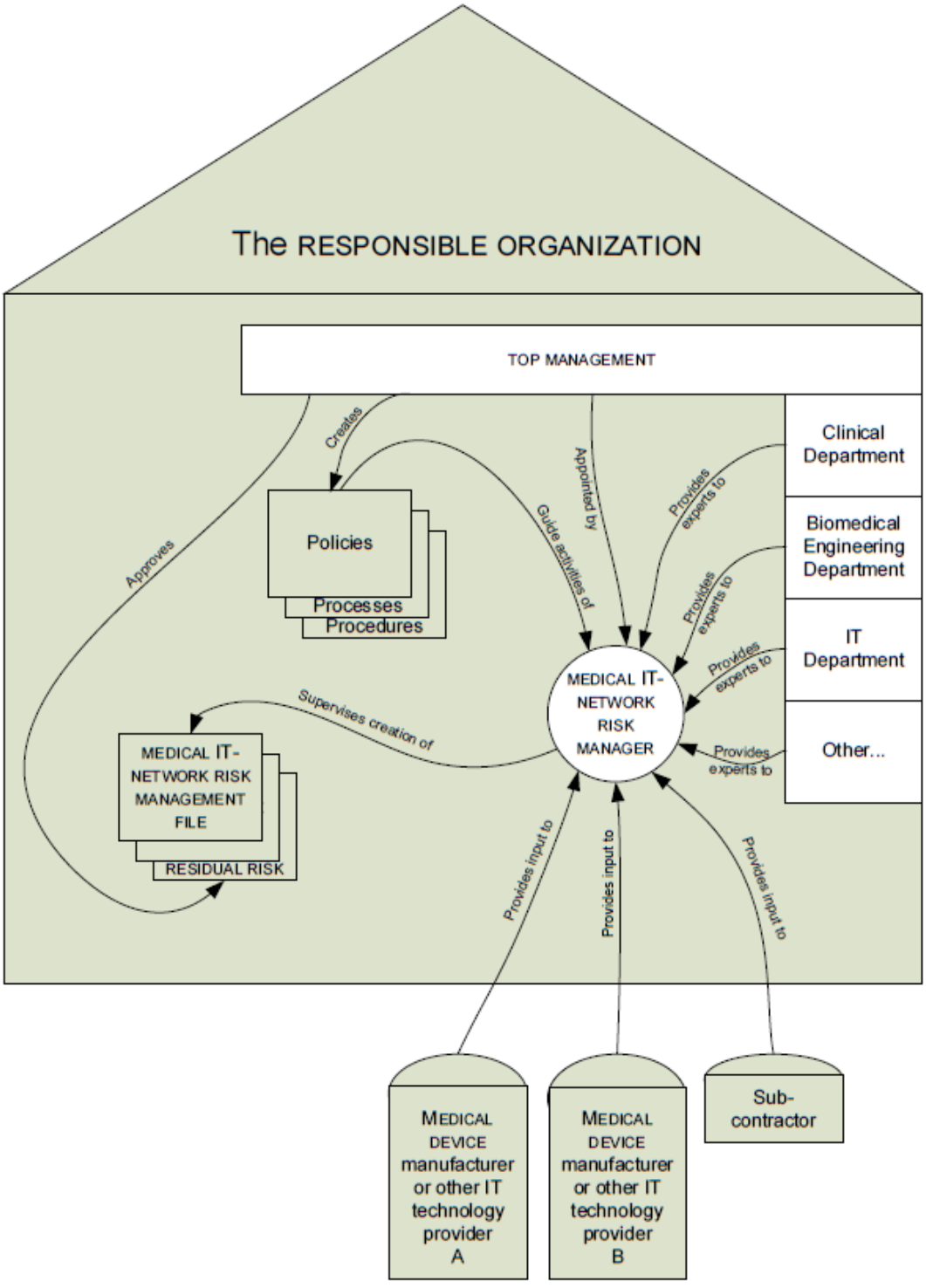

Figura 8 Panoramica dei ruoli e delle responsabilità. 80001-1 IEC 2009

3.2 Ciclo di vita della gestione del rischio per una rete IT

L'organizzazione responsabile deve mantenere le proprierà chiave della rete IT durante tutto il ciclo di vita. Uno schema della gestione del rischio durante l'intero ciclo di vita della rete IT medicale è mostrato in Figura 9

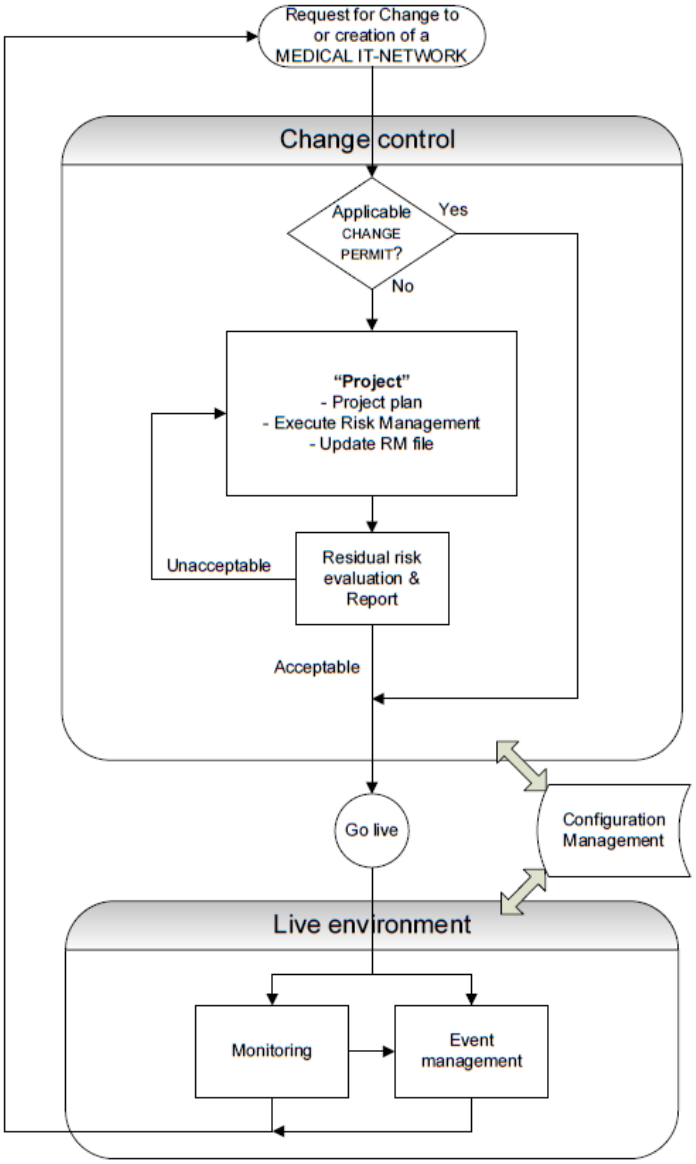

Figura 9 Panoramica del ciclo di vita della gestione del rischio per una rete IT. 80001-1 IEC 2009

Come abbiamo già detto il top management deve definire e documentare una politica di gestione del rischio per l'incorporazione di dispositivi medici all'interno delle reti IT. Le politiche di gestione del rischio dovrebbero includere:

- Una mediazione tra le tre proprietà chiave e la mission dell'organizzazione responsabile (cioè fornire un servizio di alta qualità, e garantire la sicurezza e la privacy dei dati del paziente)
- Criteri per stabilire l'accettabilità del rischio per ogni proprietà chiave (sicurezza, efficienza e sicurezza dei dati e del sistema)
- Una descrizione o un riferimento ai processi che si applicano alle reti IT medicali tra cui event-management, change-release management, configuration management e monitoraggio.

Una volta che si hanno a disposizione tutte le informazioni necessarie dal fabbricante e dallo staff dell'organizzazione responsabile possono iniziare i processi di gestione del rischio.

3.3 Gestione del rischio per le reti IT medicali

La gestione del rischio per le reti IT medicali comprende tre fasi, l'analisi del rischio, la valutazione del rischio, il controllo del rischio e la valutazione del rischio residuo. Tutte queste fasi devono essere documentate; questa documentazione può essere integrata al piano di gestione del rischio oppure può essere contenuta in un documento separato all'interno del file di gestione del rischio associato alla rete IT.

Ma andiamo ad analizzare gli step di gestione del controllo del rischio per reti IT medicali

3.3.1 Analisi del rischio

L'organizzazione responsabile deve identificare i pericoli che possono essere causati dalla rete IT medicale; per ogni pericolo identificato si dovrà stimare il rischio associato usando le informazioni e i dati disponibili. Se non fosse possibile stimare la probabilità che un danno si verifichi allora devono essere elencate le possibili conseguenze.

3.3.2 Valutazione del rischio

Per ogni pericolo identificato, l'organizzazione responsabile, usando i criteri definiti nel piano di gestione del rischio, deve decidere:

- Se i rischi stimati sono così bassi che non è necessario proseguire con le attività di riduzione del rischio. In questo caso bisogna motivare la scelta e documentarla nel file di gestione del rischio.
- se il rischio stimato non può essere considerato accettabile allora si passa all'implementazione delle misure di controllo del rischio.

3.3.3 Controllo del rischio

L'organizzazione responsabile deve individuare e documentare le misure di controllo del rischio per ogni rischio inaccettabile fino a quando il rischio residuo non venga considerato accettabile. Le opzioni di controllo del rischio, che sono già state approfondite nel capitolo precedente, includono, in ordine di importanza: controllo durante la progettazione (per esempio isolando fisicamente una rete da minacce esterne); misure protettive (come, per esempio, allarmi in caso di pericolo) e informazioni per garantire le proprietà chiave (per esempio avvertimenti, documentazione utente e corsi di formazione). Se durante il controllo del rischio l'organizzazione responsabile determina che non sono praticabili misure per la riduzione del rischio deve effettuare un'analisi rischi/benefici del rischio residuo.

Quando è selezionata una specifica misura di controllo del rischio devono essere seguiti e documentati all'interno del file di gestione del rischio della rete IT i processi di gestione change-release. La gestione change-release è un processo di approvazione centralizzato che assicura che tutti i cambiamenti siano valutati, approvati, implementati e rivisti in maniera controllata. I risultati della gestione del rischio devono approvare l'accettabilità della revisione della gestione change-release.

Una volta individuate le misure di controllo del rischio queste devono essere implementate e il rischio residuo deve essere documentato. Una volta implementate bisogna valutarne l'efficacia e documentare la verifica nel file di gestione del rischio. Le misure di controllo del rischio e il sistema operativo devono poi essere riesaminati per identificare potenziali nuovi rischi derivanti dal controllo del rischio.

3.3.4 Valutazione del rischio residuo

Il rischio residuo deve essere valutato sulla base di una valutazione provvisoria dell'efficacia delle misure di controllo del rischio implementate. Il rischio

residuo deve poi essere esaminato per valutarne l'accettabilità. Nel caso in cui il rischio residuo non sia considerato accettabile si dovranno applicare ulteriori misure di controllo del rischio

Per ogni nuova rete IT medicale o per ogni cambiamento a una rete già esistente bisogna avviare un processo di gestione change-release. Se l'organizzazione responsabile decide, a seguito delle attività di gestione del rischio, che uno specifico tipo di cambio di routine può essere effettuato con rischio accettabile sotto determinate condizioni, allora l'organizzazione responsabile può definire un permesso di modifica che consente tali cambiamenti e specifica le limitazioni. Un permesso di modifica, per esempio, potrebbe consentire la connessione di un altro dispositivo medico di un determinato tipo a una rete IT fino a un numero massimo di dispositivi. Un permesso di modifica deve specificare quali registri di gestione della configurazione sono da mantenere per ciascun cambiamento permesso. I permessi di modifica devono poi essere conservati nel file di gestione del rischio della rete IT.

3.4 Progettazioni di reti IT medicali

L'organizzazione responsabile deve inoltre stabilire e mantenere un piano di progetto per l'incorporazione di nuovi dispositivi medici in una rete IT, per i cambiamenti alla rete IT e per le modifiche al dispositivo medico connesso alla rete, per la disattivazione del dispositivo medico o della rete IT o per ogni altra attività che può introdurre un nuovo rischio. Il piano di progetto deve fornire:

- Requisiti per le attività di gestione del rischio che includono sia un piano per soddisfare i requisiti contenuti nel piano di gestione del rischio della rete IT medicale interessata, sia attività per stabilire o aggiornare i documenti del file di gestione del rischio necessari a seguito del progetto, sia attività per la verifica delle misure di controllo del rischio.
- Una descrizione del progetto che include l'identificazione della rete IT sviluppata o interessata dal progetto; la specifica dei requisiti per il progetto; indicazione di un insieme minimo di documenti richiesti per il progetto della rete IT.
- La portata delle modifiche pianificate per la rete IT deve includere la configurazione fisica e logica della rete IT prima e dopo i cambiamenti pianificati; il flusso di informazioni prima e dopo i cambiamenti previsti; i

componenti che devono essere aggiunti o rimossi; le specifiche di componenti di reti non medicali (dove previsti) e i vincoli di estendibilità della rete IT esistente.

Il piano di progetto deve essere rivisto, ove necessario, per tenere conto delle modifiche apportate e deve essere conservato nel file di gestione del rischio della rete IT medicale.

La messa in funzione della rete IT è l'obiettivo di tutte le iniziative di progetto o di cambiamento. Prima della messa in funzione l'organizzazione responsabile deve esaminare il rischio residuo della rete IT medicale. Il manager di gestione del rischio deve esaminare tutti i sommari di cambiamento o di progetto del rischio residuo per determinare l'accettabilità del rischio associato alle interazioni con i progetti o i cambianti recenti o in sospeso (per esempio l'incorporazione del dispositivo medico in una rete operativa in evoluzione). Il manager di gestione del rischio deve inoltre sovrintendere alla raccolta dei documenti di controllo del rischio per la rete IT medicale.

Quando la rete IT è messa in funzione bisogna stabilire e mantenere un processo per il monitoraggio di ogni rete IT istallata per far emergere nuovi potenziali rischi, l'efficacia delle misure di controllo del rischio e l'accuratezza con cui sono stati stimati i livelli di rischio. I criteri del monitoraggio devono anche essi essere stabiliti nel piano di gestione del rischio della rete IT medicale. Esempi di criteri per il monitoraggio sono:

- Cambiamenti di ambiente.
- Feedback sulla performance/operatività come, per esempio, feedback utente, problemi di velocità, alti tassi di errore, fallimenti, ...
- Informazioni sui componenti incorporati dal fabbricante del dispositivo medico.
- Informazioni su reti IT medicali simili.
- Relazioni sulle esposizioni ai pericoli.
- Revisione di misure di controllo del rischio non tecniche come le politiche organizzative.

Se il monitoraggio indica un effettivo o potenziale aumento del rischio associato alla rete IT medicale o ai suoi componenti devo iniziare un processo di event management e i risultati significativi devono essere segnalati all'organizzazione

responsabile. L'event management deve essere stabilito per raccogliere e documentare gli eventi negativi; risolvere (tali) eventi e proporre cambiamenti in modo appropriato attraverso la gestione change-release; tenere traccia di tutte le azioni preventive e correttive che portano alla chiusura e segnalare le scoperte al manager di gestione del rischio e/o ad altri soggetti all'interno dell'organizzazione responsabile.

Il file per la gestione del rischio delle reti IT dovrà dunque fornire la tracciabilità per ogni pericolo indentificato per l'analisi del rischio, la valutazione del rischio, l'attuazione e la verifica delle misure di controllo, la valutazione dell'accettabilità di ogni rischio residuo.

Tutti i documenti relativi all'intero ciclo di vita della rete IT medicale devono essere rivisti, modificati, revisionati e approvati in conformità con una procedura formale di controllo dei documenti.

Poichè non tutte le reti IT fanno riferimento a questo standard in Figura 10 sono riportati, a titolo di esempio, sia alcuni esempi di reti IT all'interno del campo di applicazione dello standard IEC 80001-1 sia alcuni esempi al di fuori di esso.

Configurazione di sistema		Descrizione dello scenario	Componenti network	Network	Responsabilità della rete	Standard
1	a	Dispositivi medici di un unico fabbricante o dispositivo non medicale incorporato dallo stesso fabbricante del dispositivo medico e istallato come richiesto dal fabbricante del dispositivo medico su una rete IT isolata.	Dispositivi medicali e non da un unico fabbricante	Fisicamente isolata	Fabbricante del dispositivo medico	14971
	b	Dispositivi medici di più fabbricanti e dispositivi non medicali incorporati da un unico fabbricante e istallati come richiesto dal fabbricante del dispositivo medico su una rete isolata	Dispositivi medici e non di più fabbricanti	Fisicamente isolata	Fabbricante del dispositivo medico	14971
2	a	Dispositivi medicali e non incorporati da un unico fabbricante e dispositivi medicali e non medicali incorporati da altri fabbricanti di dispositivi medici e non interconnessi su una stessa rete IT da una terza parte (per esempio l'ospedale)	Dispositivi medicali e non da più fabbricanti di dispositivi medici	Condivisa	Organizzazione responsabile	80001-1
	b	Dispositivi medicali e non medicali incorporati da uno stesso fabbricante e dispositivi medicali e non incorporati da altri fabbricanti di dispositivi medicali, non medicali e di applicazioni interconnessi su una rete condivisa da una terza parte.	Dispositivi medicali e non medicali da più fabbricanti di dispositivi medici oltre a molteplici fabbricanti di dispositivi non medicali.	Condivisa	Organizzazione responsabile	80001-1
3		Impianti con dispositivi non medicali da più fabbricanti usando la rete IT per la trasmissione di informazioni elettroniche protette sulla salute (ePHI)	Più fabbricanti di dispositivi non medicali	Condivisa	Organizzazione responsabile	Fuori dal campo di applicazione della 80001-1

Figura 10 scenari di rete IT che si possono incontrare in ambiente clinico

Per comprendere meglio i vari tipi di rete di cui sopra prendiamo in considerazione degli esempi:

- Configurazione 1a - dispositivi di monitoraggio del paziente sulla propria rete isolata o sullo stesso dispositivo con un gateway alla rete IT dell'ospedale per usi non medicali.
- Configurazione 1b – dispositivi di monitoraggio del paziente da un fornitore A in combinazione con una rete collegata a dispositivi di infusione fornita da un fornitore B come soluzione integrata controllata da un singolo fornitore (A,B o C).
- Configurazione 2a – più dispositivi medici forniti da fabbricanti diversi posti su una rete comune da parte dell'ospedale.
- Configurazione 2b – dispositivi di infusione su una rete condivisa con altre applicazioni ospedaliere e/o dispositivi di monitoraggio paziente su una rete isolata con un gateway alla rete IT dell'ospedale per usi medicali e report di allarmi.
- Configurazione 3 – sistemi ospedalieri che comunicano dati anagrafici del paziente e varie informazioni relative alla salute del paziente.

Applicando questo standard è possibile quindi ridurre il numero e la gravità dei rischi e migliorare la sicurezza e l'efficacia della rete IT che incorpora i dispositivi medici. Questi miglioramenti contribuiranno positivamente ai costi e bilanceranno quelli iniziali per la messa in atto dello standard. Inoltre il miglioramento in sicurezza e efficacia porterà a un miglior flusso di lavoro che andrà ad influire positivamente sulla salute del paziente e sull'efficenza operativa.

Come abbiamo visto quindi la cultura del risk management, in ambito sanitario, permette di ridurre gli eventi avversi e pericolosi, il costo sanitario dei danni al cittadino/paziente e il contenzioso legale permettendo quindi alla tecnologia di potersi esprimere al meglio e in tutto il suo potenziale.

Ma come influisce il fatto che si stia arrivando sempre più a una convergenza tra dispositivi medici e sistemi informatici sul ruolo dell'ingegnere clinico?

Conclusioni

A causa dell'aumento e dell'importanza di apparecchiature mediche sempre più complesse e di problemi legati alla sicurezza (come la sicureza elettrica) a partire dagli anni '70 negli USA si è sviluppata la figura dell'ingegnere clinico. L'ingegnere clinico all'inizio aveva solo i compiti di istallazione, mantenimento e riparazione e, per questa ragione, era associato ai dipartimenti di impiantistica e mantenimento delle apparecchiature. Oggi il compito dell'ingegnere clinico spazia in ambiti più vasti e meno tecnici come la valutazione di tecnologie sanitarie e sistemi sanitari con le metodologie del HTA ("Health Technology Assessment" ovvero la metodica che valuta in termini di costi ed efficacia l'impatto dell'introduzione di una nuova tecnologia sanitaria); il project management & system planning; la pianificazione degli acquisti; la formazione del personale sanitario e la gestione del parco tecnologico.
Come abbiamo visto però, con la normativa CE 47/2007 il software è diventato un dispositivo medico e questo ha aumentato il livello di difficoltà gestionale del rischio; inoltre la presenza e il sempre maggiore sviluppo di dispositivi medici dotati di un'interfaccia di rete ha cambiato profondamente la loro gestione e l'interazione e interoperabilità con altri elementi che costituiscono il parco tecnologico delle aziende sanitarie e, se da una parte ha portato a una diminuzione dei costi e a un aumento dell'efficacia delle cure del paziente dall'altra ne ha aumentato i rischi per la sicurezza, l'efficacia e la protezione del dispositivo, della rete e dei dati. L'interoperabilità dei dispositivi medici ha portato quindi al concetto di gestione del rischio anche per il vasto mondo dell'IT.
Come abbiamo approfondito nel terzo capitolo lo standard IEC 80001-1 per la gestione del rischio per le reti IT medicali è rivolto alle aziende sanitarie; viene quindi spontaneo chiedersi se e come questo standard influisca sul ruolo dell'ingegnere clinico.
E' chiaro che la sempre maggiore convergenza di dispositivi medici e reti IT dovrà portare a una collaborazione sempre più stretta tra l'amminastrazione di alto livello (la dirigenza sanitaria), il dipartimento dell'IT e quello dell'ingegneria clinica. Il dipartimento dell'IT e quello dell'ingegneria clinica dovranno dunque imparare a lavorare insieme per gestire in anticipo i rischi e per attuare i necessari compromessi. Sia gli ingegneri clinici che il dipartimento dell'Information Technology avranno molto da imparare da questa

cooperazione; in particolar modo questi ultimi dovranno imparare ad affrontare problemi legati all'etica e a nuovi aspetti legali che prima non li toccavano mentre le competenze dell'ingegnere clinico dovranno essere sempre più multidisciplinari e spaziare dalla meccanica all'informatica; dalle telecomunicazioni alla fisiologia; dall'elettronica ai principi fisici di funzionamento dei dispositivi medici.
Poichè l'utilizzo della rete in ambito sanitario avrà sempre una maggiore importanza, basti pensare alle possibilità che ci forniscono l'uso di tablet e smartphone in termini di mobile-healt o dello sviluppo di tecnologie medicali a domicilio come dialisi e monitoraggio elettrofisiologico, forse con il tempo ci sarà bisogno di una nuova figura che affiancherà l'ingegnere clinico cioè quello dell'ingegnere delle reti a cui spetteranno i compiti legati gestione delle reti IT che incorporano dispositivi medicali.

BIBLIOGRAFIA

Ministero della Salute: Dispositivi medici – Aspetti regolatori e operativi

Legislazione applicabile

Direttiva 2007/47/CE del Parlamento Europeo e del Consiglio

Direttiva 93/42/CEE

Guide e norme specifiche

UNI CEI EN ISO 14971
Dispositivi medici – applicazione della gestione dei rischi ai dispositivi medici

IEC/TR 80002-1:2009
Software dispositivo medico – Part 1: Guida all'applicazione della ISO 14971 per i dispositivi medici software

IEC/TR 80001-1:2010
Applicazione della gestione del rischio per le reti IT medicali che incorporano dispositivi medici

Guide alla legislazione applicabile

MEDDEV 2.1/6 "Qualification and Classification of standalone software"