SVENSK STANDARD SS-EN 80001-1

Fastställd	Utgåva	Sida	Ansvarig kommitté
2011-09-07	1	1 (1+39)	SEK TK 62

Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter – Del 1: Roller, ansvar och aktiviteter

Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities

Som svensk standard gäller europastandarden EN 80001-1:2011. Den svenska standarden innehåller den officiella svenska språkversionen av EN 80001-1:2011.

Nationellt förord

Europastandarden EN 80001-1:2011

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC
– **IEC 80001-1, First edition, 2010 - Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities**

utarbetad inom International Electrotechnical Commission, IEC.

ICS 11.040.01; 35.240.80

Denna standard är fastställd av, SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. *Telefax*: 08 - 444 14 30
E-post: sek@elstandard.se. *Internet*: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard
Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

EUROPASTANDARD **EN 80001-1**
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM **Mars 2011**

ICS 11.040.01; 35.240.80

Svensk språkversion

Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter – Del 1: Roller, ansvar och aktiviteter (IEC 80001-1:2010)

Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux – Partie 1: Fonctions, responsabilités et activités (CEI 80001-1:2010)

Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities (IEC 80001-1:2010)

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

Denna svenska standard utgör den svenska språkversionen av europastandarden EN 80001-1. Den har översatts av SEK. Europastandarden antogs av CENELEC 2011-02-01. CENELEC-medlemmarna är förpliktigade att följa fordringarna i CEN/CENELECs Internal Regulations som anger på vilka villkor europastandarden i oförändrat skick ska ges status som nationell standard.

Aktuella förteckningar och bibliografiska referenser som upplyser om nationella standarder kan på begäran erhållas från CENELECs centralsekretariat eller från någon av CENELECs medlemmar.

Europastandarden finns i tre officiella versioner (engelsk, fransk och tysk). En version på något annat språk, översatt under ansvar av en CENELEC-medlem till sitt eget språk och anmäld till CENELECs centralsekretariat, har samma status som de officiella språkversionerna.

CENELECs medlemmar är nationalkommittéerna i Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Island, Italien, Krotatien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Norge, Polen, Portugal, Rumänien, Schweiz, Slovakien, Slovenien, Spanien, Storbritannien, Sverige, Tjeckien, Tyskland, Ungern och Österrike.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B, B-1000 Brussels

Ref. Nr. EN 80001-1:2011 Sv

Förord

Texten i dokument 62A/703/FDIS, avsedd att blir utgåva 1 av IEC 80001-1 och utarbetad av SC 62A, Common aspects of electrical equipment used in medical practice, i IEC TC 62, Electrical equipment inmedical practice, var föremål för parallell röstning i IEC och CENELEC och fastställdes av CENELEC som EN 80001-1 den 1 februari 2011.

Lägg märke till att vissa delar av detta dokument kan omfattas av patenträttigheter. CEN och CENELEC kan inte ansvara för att sådana patenträttigheter identifieras.

Följande datum fastställdes:

– Senaste datum för överföring av EN till nationell nivå genom utgivning av motsvarande nationell standard eller genom ikraftsättning	(dop)	2011-11-01
– senaste datum för upphävande av motstridig nationell standard	(dow)	2014-02-01

Termer som är definierade i avsnitt 2 i denna standard är skrivna med KAPITÄLER.

För användning i denna standard

– betyder ”ska” att överensstämmelse krävs för att uppfylla fordringen i standarden
– betyder ”bör” att överensstämmelse rekommenderas men inte krävs för att uppfylla fordringen i standarden
– används ”kan” för att beskriva ett tillåtet sätt uppfylla fordringen i standarden
– betyder ”upprätta” och ”fastställa” att definiera, dokumentera och införa.

---

kraftsättningsmeddelande

Texten i den internationella standarden IEC 80001-1:2010 har av CENELEC fastställts som europastandard utan någon avvikelse.

I bibliografin ska följande anmärkningar läggas till för de angivna standarderna:

[1] IEC 60601-1:2005	ANM –	Harmoniserad som EN 60601-1:2006 (utan ändring).
[2] IEC 61907:2009	ANM –	Harmoniserad som EN 61907:2010 (utan ändring).
[3] IEC 62304:2006	ANM –	Harmoniserad som EN 62304:2006 (utan ändring).
[4] ISO 14971:2007	ANM –	Harmoniserad som EN ISO 14971:2009 (utan ändring).
[7] ISO 16484-2:2004	ANM –	Harmoniserad som EN ISO 16484-2:2004 (utan ändring).
[8] ISO 9000:2005	ANM –	Harmoniserad som EN ISO 9000:2005 (utan ändring).

Innehåll

Inledning 5
1 Omfattning 7
2 Termer och definitioner 7
3 Roller och ansvar 11
3.1 Allmänt 11
3.2 ansvarig VÅRDGIVARE 11
3.3 HÖGSTA LEDNINGENS ansvar 12
3.4 RISKHANTERINGSANSVARIG FÖR MEDICINTEKNISKT IT-NÄTVERK 13
3.5 Tillverkare av MEDICINTEKNISKA PRODUKTER 14
3.6 Leverantörer av annan informationsteknologi 15
4 RISKHANTERING för hela livscykeln för MEDICINTEKNISKA IT-NÄTVERK 16
4.1 Översikt 16
4.2 Den ANSVARIGA VÅRDGIVARENS RISKHANTERING 17
4.2.1 Policy för RISKHANTERING vid anslutning av en MEDICINTEKNISK PRODUKT 17
4.2.2 RISKHANTERINGSPROCESS 18
4.3 Planering och dokumentation av det MEDICINTEKNISKA IT-NÄTVERKETS RISKHANTERING 18
4.3.1 Översikt 18
4.3.2 RISK-relevant beskrivning av tillgångarna 18
4.3.3 Det MEDICINTEKNISKA IT-NÄTVERKETS dokumentation 19
4.3.4 ANSVARSÖVERENSKOMMELSE 19
4.3.5 RISKHANTERINGsplan för det MEDICINTEKNISKA IT-NÄTVERKET 20
4.4 RISKHANTERING av MEDICINTEKNISKA IT-NÄTVERK 21
4.4.1 Översikt 21
4.4.2 RISKANALYS 21
4.4.3 RISKVÄRDERING 21
4.4.4 RISKSTYRNING 22
4.4.5 Värdering och rapportering av KVARVARANDE RISKER 23
4.5 ÄNDRINGS- OCH FRISLÄPPNINGSHANTERING och KONFIGURATIONSHANTERING 24
4.5.1 ÄNDRINGS- OCH FRISLÄPPNINGSHANTERINGSPROCESSER 24
4.5.2 Beslut om hur man tillämpar RISKHANTERING 24
4.5.3 Driftsättning 25
4.6 Det operationella nätverkets RISKHANTERING 26
4.6.1 Övervakning 26
4.6.2 HÄNDELSEHANTERING 26
5 Dokumentkontroll 26
5.1 Dokumentkontrollförfarande 26
5.2 Det MEDICINTEKNISKA IT-NÄTVERKETS RISKHANTERINGSDOKUMENTATION 26
Bilaga A (informativ) Bakgrund och överväganden 28
Bilaga B (informativ) Översikt av riskhanteringsrelationer 32
Bilaga C (informativ) Vägledning över användningsområde 33

Bilaga D (informativ) Förhållande med ISO/IEC 20000-2:2005, Informationsteknologi – Ledningssystem för tjänster – Del 2: Vägledning 35

Bibliografi 39

Inledning

Ett ökande antal av MEDICINTEKNISKA PRODUKTER är utformade för att utbyta information elektroniskt med annan utrustning i användarmiljön, inklusive andra MEDICINTEKNISKA PRODUKTER. Sådan information utbyts ofta genom ett informationsnätverk (IT-NÄTVERK) som även överför data av mer allmän karaktär.

Samtidigt blir IT-NÄTVERK allt viktigare för den kliniska miljön och de måste föra en alltmer skiftande trafik, allt från livskritiska patientdata som kräver omedelbar leverans och respons, till allmänna data och e-post med potentiellt skadligt innehåll (t ex virus).

För många jurisdiktioner omfattas konstruktion och produktion av MEDICINTEKNISKA PRODUKTER av myndigheters regelverk och av standarder som erkänts av myndigheterna. Traditionellt riktar sig tillsynsmyndigheterna till tillverkare av MEDICINTEKNISKA PRODUKTER genom att kräva särskilda produktegenskaper och en dokumenterad PROCESS för konstruktion och tillverkning. MEDICINTEKNISKA PRODUKTER kan inte släppas ut på marknaden i dessa jurisdiktioner utan bevis för att dessa krav har blivit uppfyllda.

Också klinisk personals användning av MEDICINTEKNISKA PRODUKTER är föremål för reglering. Den kliniska personalen måste vara lämpligt utbildad och kvalificerad och blir alltmer föremål för definierade PROCESSER som tillkommit för att skydda patienter från oacceptabel RISK.

Däremot är införlivandet av MEDICINTEKNISKA PRODUKTER i IT-NÄTVERK i den kliniska miljön ett mindre reglerat område. Enligt IEC 60601-1:2005 [1] [1] ska tillverkare av MEDICINTEKNISKA PRODUKTER inkludera en del information i de MEDFÖLJANDE DOKUMENTEN, om den MEDICINTEKNISKA PRODUKTEN är avsedd att anslutas till ett IT-NÄTVERK. Standarder omfattar också gemensamma informationstekniska aktiviteter som planering, konstruktion och underhåll av IT-NÄTVERK, t ex ISO 20000-1:2005 [9]. Men innan publiceringen av denna standard fanns ingen standard som tog upp hur MEDICINTEKNISKA PRODUKTER kan kopplas till IT-NÄTVERK, inklusive allmänna IT-NÄTVERK, för att uppnå interoperabilitet utan att äventyra organisationen och vården i termer av SÄKERHET, EFFEKTIVITET och DATA- OCH SYSTEMSÄKERHET.

Det återstår ett antal potentiella problem associerade med införlivandet av MEDICINTEKNISKA PRODUKTER i IT-NÄTVERK, till exempel:

– brist på hänsyn till RISK p g a användning av IT-NÄTVERK under utvärdering av klinisk RISK
– brist på stöd från tillverkare av MEDICINTEKNISKA PRODUKTER då man kopplar deras produkter till IT-NÄTVERK (t ex avsaknaden av eller bristfällig information från tillverkaren till IT-NÄTVERKETS OPERATÖR)
– felaktig användning eller sämre prestanda (t ex inkompatibilitet eller felaktig konfiguration) till följd av en kombination av MEDICINTEKNISKA PRODUKTER och annan utrustning på samma IT-NÄTVERK
– felaktigt handhavande till följd av en kombination av MEDICINTEKNISK MJUKVARA och andra mjukvaruapplikationer i samma IT-NÄTVERK
– avsaknad av säkerhetskontroller på flera MEDICINTEKNISKA PRODUKTER, och
– konflikten mellan behovet av strikta kontroller vid förändringar av MEDICINTEKNISKA PRODUKTER och behovet av snabba insatser vid hot om cyberattack.

När dessa problem visar sig, uppstår ofta oavsiktliga konsekvenser.

Den här standarden riktar sig till VÅRDGIVARE, tillverkare av MEDICINTEKNISKA PRODUKTER och till andra leverantörer av informationsteknik.

[1] Siffrorna inom parentes hänvisar till bibliografin.

I denna standard gäller följande principer som en grund för dess normativa och informativa avsnitt:

– Installation eller borttagande av en MEDICINTEKNISK PRODUKT eller andra komponenter i ett IT-NÄTVERK kräver planerade åtgärder och kan vara utom kontroll för tillverkaren av den MEDICINTEKNISKA PRODUKTEN.

– RISKHANTERING bör användas innan installation av en MEDICINTEKNISK PRODUKT äger rum i ett IT-NÄTVERK och för varje förändring under hela livscykeln i det resulterande MEDICINTEKNISKA IT-NÄTVERKET, för att undvika oacceptabla RISKER, inklusive möjlig RISK FÖR SKADA för patienter, till följd av installationen av den MEDICINTEKNISKA PRODUKTEN i ett IT-NÄTVERK. Många frågor är en del av ett RISK-beslut, såsom ansvar, kostnad eller påverkan på uppdrag. Dessa bör beaktas för att fastställa acceptabla RISKER utöver de fordringar som beskrivs i denna standard.

– Aspekter vid flyttning, underhåll, förändring eller modifiering av utrustning, föremål eller komponenter bör beaktas på lämpligt sätt vid installation av en MEDICINTEKNISK PRODUKT.

– Tillverkaren av en MEDICINTEKNISK PRODUKT är ansvarig för RISKHANTERING av den MEDICINTEKNISKA PRODUKTEN under konstruktion, genomförande och tillverkning av den MEDICINTEKNISKA PRODUKTEN. Denna standard omfattar inte RISKHANTERINGSPROCESSEN för den MEDICINTEKNISKA PRODUKTEN.

– Tillverkaren av en MEDICINTEKNISK PRODUKT avsedd att ingå i ett IT-NÄTVERK kan behöva delge den information om den MEDICINTEKNISKA PRODUKTEN som behövs för att VÅRDGIVAREN ska kunna hantera RISKER i enlighet med denna standard. Denna information kan, som en del av MEDFÖLJANDE DOKUMENT, omfatta instruktioner speciellt riktade till den person som kommer att installera den MEDICINTEKNISKA PRODUKTEN i IT-NÄTVERKET.

– Sådana MEDFÖLJANDE DOKUMENT bör förmedla instruktioner om hur man installerar den MEDICINTEKNISKA PRODUKTEN i ett IT-NÄTVERK, hur den MEDICINTEKNISKA PRODUKTEN överför information över IT-NÄTVERKET och de egenskaper IT-NÄTVERKET behöver ha för att möjliggöra den MEDICINTEKNISKA PRODUKTENS AVSEDDA ANVÄNDNING när den installeras i ett IT-NÄTVERK. De MEDFÖLJANDE DOKUMENTEN bör varna för eventuellt farofyllda situationer i samband med fel eller störningar i IT-NÄTVERKET och missbruk av anslutning till IT-NÄTVERKET eller av den information som överförs via IT-NÄTVERKET.

– ANSVARSÖVERENSKOMMELSER kan fastställa roller och ansvar bland dem som är inblandade i installationen av den MEDICINTEKNISKA PRODUKTEN i ett IT-NÄTVERK samt alla aspekter under det resulterande MEDICINTEKNISKA IT-NÄTVERKETS hela livscykel och de aktiviteter som ingår i denna.

– VÅRDGIVAREN är skyldig att utse personer till vissa roller som definieras i denna standard. Denna standard definierar ansvaret för dessa roller. Den viktigaste av dessa roller är det MEDICINTEKNISKA IT-NÄTVERKETS RISKHANTERINGSANSVARIGE. Denna roll kan tilldelas någon inom VÅRDGIVARENS organisation eller en extern entreprenör.

– Det MEDICINTEKNISKA IT-NÄTVERKETS RISKHANTERINGSANSVARIGE ansvarar för att RISKHANTERINGEN ingår i dessa PROCESSER:
  – Planering och utformning vid installation av MEDICINTEKNISKA PRODUKTER eller ändringar av sådana installationer
  – Att ta det MEDICINTEKNISKA IT-NÄTVERKET i bruk och den därav följande användningen av det MEDICINTEKNISKA IT-NÄTVERKET, och
  – ÄNDRINGS- OCH FRISLÄPPNINGSHANTERING samt hantering av förändringar av IT-NÄTVERKET under IT-NÄTVERKETS hela livscykel.

– RISKHANTERING bör tillämpas för att lösa följande NYCKELEGENSKAPER lämpliga för IT-NÄTVERK som innehåller MEDICINTEKNISK PRODUKT:
  – SÄKERHET (frihet från oacceptabel RISK för fysisk skada eller skada på människors hälsa eller skada på egendom eller miljö)
  – EFFEKTIVITET (förmåga att producera patientens och VÅRDGIVARENS förväntade resultat), och
  – DATA- OCH SYSTEMSÄKERHET (ett driftläge hos ett MEDICINTEKNISKT IT-NÄTVERK där informationstillgångar (data och system) är rimligt skyddade från försämring vad gäller sekretess, integritet och tillgänglighet).

1 Omfattning

Eftersom medicintekniska produkter ofta ingår i IT-NÄTVERK för att uppnå önskvärda fördelar (t ex INTEROPERABILITET), anger denna internationella standard roller, ansvarsområden och aktiviteter som är nödvändiga för RISKHANTERING av IT-NÄTVERK som innehåller MEDICINTEKNISKA PRODUKTER och behandlar SÄKERHET, EFFEKTIVITET och DATA- OCH SYSTEMSÄKERHET (NYCKELEGENSKAPERNA). Denna internationella standard specificerar inte acceptabla RISKnivåer.

ANM 1 – RISKHANTERINGSverksamhet som beskrivs i denna standard härrör från ISO 14971[4]. Förhållandet mellan ISO 14971 och denna standard beskrivs i bilaga A.

Denna standard gäller sedan en medicinteknisk produkt har förvärvats av en VÅRDGIVARE och är tänkt att ingå i ett IT-NÄTVERK.

ANM 2 – Denna standard omfattar inte RISKHANTERING innan produkten är släppt på marknaden.

Denna standard gäller hela livscykeln för det IT-NÄTVERK som innehåller MEDICINTEKNISKA PRODUKTER.

ANM 3 – Den livscykelhantering som beskrivs i denna standard är mycket lik den i ISO/IEC 20000-2 [10]. Förhållandet mellan ISO/IEC 20000-2 och denna standard beskrivs i bilaga D.

Denna standard gäller när det inte finns någon enskild tillverkare av en MEDICINTEKNISK PRODUKT som tar ansvar för att tillgodose NYCKELEGENSKAPERNA hos det IT-NÄTVERK som innehåller en MEDICINTEKNISK PRODUKT.

ANM 4 – Om en tillverkare specificerar en komplett MEDICINTEKNISK PRODUKT som innehåller ett nätverk, omfattas inte installation eller montering av den MEDICINTEKNISKA PRODUKTEN enligt tillverkarens MEDFÖLJANDE DOKUMENT av fordringarna i denna standard, oavsett vem som installerar eller monterar den MEDICINTEKNISKA PRODUKTEN.

ANM 5 – Om en tillverkare specificerar en komplett MEDICINTEKNISK PRODUKT som innehåller ett nätverk, omfattas tillägg till den MEDICINTEKNISKA PRODUKTEN eller ändring av konfigurationen av den MEDICINTEKNISKA PRODUKTEN, utöver vad som anges av tillverkaren, av fordringarna i denna standard.

Denna standard gäller för VÅRDGIVARE, tillverkare av MEDICINTEKNISKA PRODUKTER och andra leverantörer av IT i syfte att hantera risker i ett IT-NÄTVERK som innehåller MEDICINTEKNISK PRODUKT.

Denna standard gäller inte för tillämpningar vid personligt bruk där patient, OPERATÖR och VÅRDGIVARE är en och samma person.

ANM 6 – I de fall där en MEDICINTEKNISK PRODUKT används hemma under uppsikt eller efter instruktion av leverantören, anses leverantören vara den ANSVARIGA VÅRDGIVAREN. Personliga bruk där patienten förvärvar och använder en MEDICINTEKNISK PRODUKT utan övervakning eller instruktion av en leverantör är utanför ramen för denna standard.

Denna standard behandlar inte reglerande eller juridiska krav.