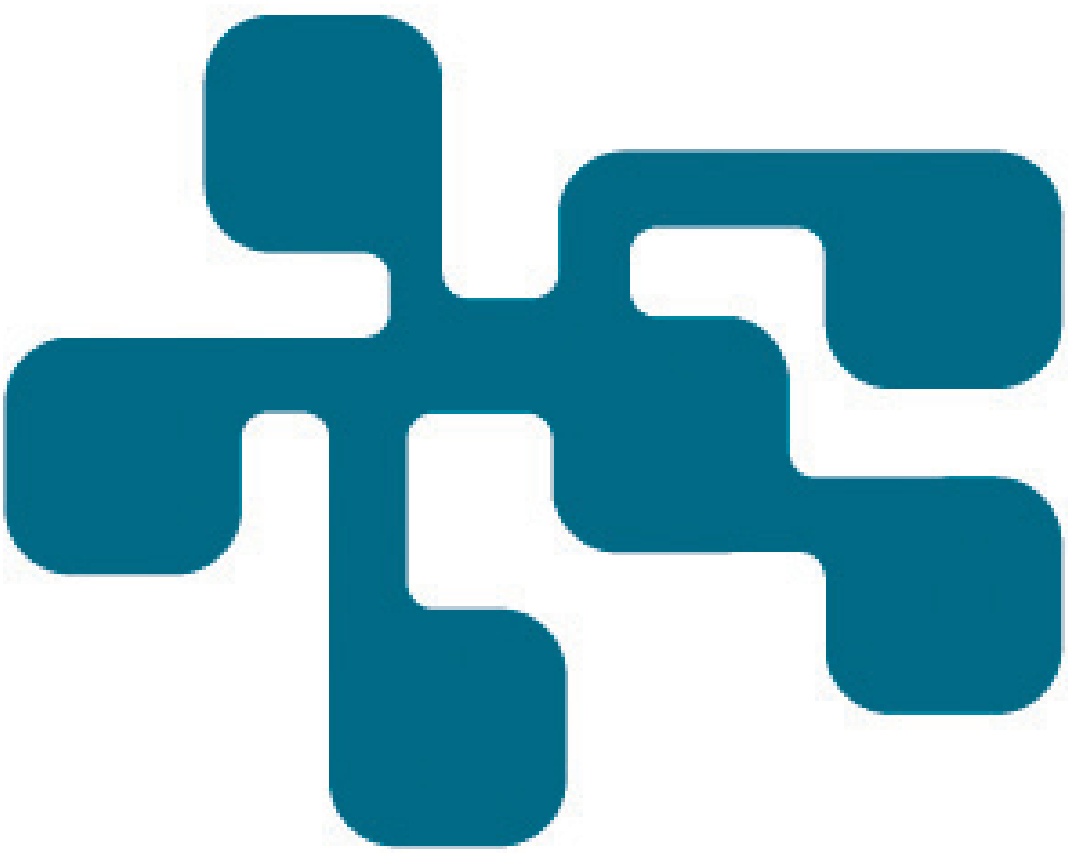
NCS3 - Informations- och styrsystem inom hälso- och sjukvård

En kartläggning av produkter och incidenter

Hannes Holm, Erik Westring

FOI
MSB



FOI-R--4088--SE
MSB 2014-1131
ISSN 1650-1942

Maj 2015

Hannes Holm, Erik Westring

NCS3: Informations- och styrsystem inom hälso- och sjukvård

En kartläggning av produkter och incidenter

Titel	NCS3: Informations- och styrsystem inom hälso- och sjukvård – En kartläggning av produkter och incidenter
Title	NCS3: Information- and control systems within healthcare – A survey of products and incidents
Rapportnr/Report no	FOI-R--4088--SE
Månad/Month	Maj/May
Utgivningsår/Year	2015
Antal sidor/Pages	79
ISSN	1650-1942
Kund/Customer	Myndigheten för samhällsskydd och beredskap (MSB)
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	
Projektnr/Project no	E3239606
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Hälso- och sjukvården i Sverige är en kritisk samhällsfunktion som på en kort tid genomgått en omfattande teknisk modernisering. Tanken med denna modernisering är att minska den administrativa och operativa arbetsbördan och bidra med mer precisa analyser och behandlingar. Den har dock också bidragit till att vanliga IT-relaterade brister såsom mjukvarubuggar numera kan ha en reell effekt på mänskligt liv.

Denna studie undersöker vilka informations- och styrsystem som finns inom hälso- och sjukvård i Sverige och vilka incidenter som förekommit som en följd av datorrelaterade problem med dessa system. Analysen baseras på vetenskaplig litteratur, incidentdatabaser i Sverige och USA, intervjuer och en enkät.

Resultatet visar att det finns över 20 000 olika typer av medicintekniska produkter (MTP) som nyttjas och att allt från laserskrivare till infusionspumpar ses som MTP:er. Intervjuerna visar dock att produkter som ligger närmre administration och drift (t.ex. patientjournalsystem, routrar och nätverkskablar) ses som informationsteknologi (IT), medan produkter som ligger närmre patienter (t.ex. infusionspumpar och pacemakers) ses som ”riktiga” MTP:er.

Analys av incidentdatabasen REIDAR som registrerar svenska MTP-relaterade incidenter visar att cirka 30% av alla incidenter inom Sveriges hälso- och sjukvård har varit datorrelaterade, samt att antalet datorrelaterade incidenter ökar i ungefär samma takt som antalet icke-datorrelaterade incidenter minskar (ett liknande mönster kan ses för USA). Dödsfall orsakas av cirka 1.7% av alla datorrelaterade incidenter, och primärt av lungventilatorer, dialysapparater och defibrillatorer. De allra flesta datorrelaterade incidenter rör dock infusionspumpar. Denna incidentdatabas ses av respondenterna som kritisk för god nationell samverkan – det som händer ett sjukhus händer sannolikt även andra så småningom – men rapporteringsfrekvensen till den har sedan den startades varit lägre än förväntat. Ett sätt att öka den vore att modernisera webbapplikationen som exponerar databasen, särskilt gällande sök- och analysfunktionalitet.

Resultatet visar även att en bättre intern kommunikation behövs mellan IT och medicinteknik/vården. Detta kan exempelvis behandlas genom fysisk samverkan, utbildning eller sammanslagning av medicinteknik och IT (vilket har gjorts inom vissa Landsting i Sverige).

Slutligen så finns det relativt få omfattande IT-säkerhetsrelaterade incidenter, såsom datormaskar, som uppmärksammats i Sverige. Sårbarheten för IT-attacker är dock stor och framtida IT-attacker är en risk som bör tas på stort allvar.

Nyckelord: Hälso- och sjukvård, medicinteknisk produkt, IT-haveri, incidenter, avvikelser, IT-säkerhet, cybersäkerhet

Summary

The Swedish healthcare system is a critical infrastructure service that in a short timespan has undergone comprehensive technological modernization. The rationale behind this modernization is to decrease the administrative and operative burden and help to yield more precise analyses and treatments. It has however also enabled regular IT related issues such as software bugs to have a real effect on human life.

This report presents a study of what information- and control systems that are used within healthcare and what incidents that have occurred due to computer related problems with these systems. The analysis is based on scientific literature, incident databases within Sweden and USA, interviews and a questionnaire.

The results show that there are more than 20 000 different kinds of medical devices which are used and that everything from laser printers to infusion pumps are viewed as medical devices. The interviews however show that products that are closer to administration (e.g., patient journal systems, routers and network cables) are however viewed as IT, while products that are closer to patients (e.g., infusion pumps and pacemakers) are viewed as "true" operative medical devices.

Analysis of the incident database REIDAR that registers Swedish medical device related incidents show that approximately 30% of all such incidents within Swedish healthcare are computer related, and that the number of computer related incidents increase at about the same pace as the number of non-computer related incidents decrease. Deaths are caused by 1.7% of all computer related incidents, primarily by lung ventilators, dialysis devices and defibrillators. Most incidents however involve infusion pumps. This incident database are viewed by the respondents as critical for sound national cooperation – what happens at one hospital is likely to eventually occur for others' – but the reporting frequency to it has since its creation been lower than expected. One means of increasing it would be to modernize the web application that exposes it, in particular regarding search and analysis functionality.

The results also show that a better internal communication is required between IT and medical technicians/healthcare. This can be achieved by greater physical collaboration, education or merging the departments concerning IT and medical devices (which has been done at some locations in Sweden).

Finally, relatively few significant IT security related incidents, such as computer worms, have been observed in Sweden. However, the IT security vulnerability is large and the risk for future IT attacks should be viewed with concern.

Keywords: Healthcare, medical devices, IT failure, incidents, IT security, cyber security

Innehållsförteckning

Förkortningar

AD	Active Directory
COTS	Commercial-off-the-shelf
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
FDA	US Food and Drug Administration
HSA	Hälso- och sjukvårdens adressregister
IP	Internetprotokoll
ISP	Internet Service Provider
IT	Informationsteknologi
IVO	Inspektionen för vård och omsorg
LfMT	Ledningsnätverket för Medicinsk Teknik
MAUDE	Manufacturer and User Facility Device Experience
MREDR	Medical and Radiation Emitting Device Recalls
MSB	Myndigheten för samhällsskydd och beredskap
MT	Medicinteknik
MTP	Medicinteknisk produkt
MTPReg	Register för Medicintekniska produkter
NCS3	Nationellt centrum för säkerhet i industriella informations- och styrsystem för samhällsviktig verksamhet
NLTK	Natural Language Toolkit
OS	Operativsystem
PACS/RIS	Picture Archiving and Communication System/Radiology Information System
REIDAR	Rikstäckande Elektronisk Informationsdatabas för Avvikelser Rörande Medicintekniska Produkter
ROS	Remiss Och Svar
SIEM	Security information and event management
SKL	Sveriges kommuner och landsting
SLL	Stockholms Läns Landsting
SSL	Secure Sockets Layer
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

1 Inledning

Hälso- och sjukvård är en samhällskritisk funktion som innefattar att diagnostisera, behandla och förhindra sjukdomar, skador och andra fysiska och mentala problem hos människor.

Idag används olika typer av informationsteknologier (IT) för att stödja ett framgångsrikt arbete med dessa aktiviteter. Exempelvis används dokumentationssystem såsom journalsystem för att minska den administrativa bördan, insulin kan administreras autonomt med pumpsystem[1] och ett hjärta kan stimuleras med en pacemaker[2]. Teknologier som dessa har ökat kvaliteten för vården i stort, för olika behandlingsformer i synnerhet och ibland även möjliggjort behandling av tidigare ej behandlingsbara åkommor. Att de är värdefulla är därmed utan tvivel.

Ett problem med IT-system är dock att det kan förekomma buggar som får dem att bete sig på ett sätt som de inte är konstruerade för. Ibland kan dessa buggar reproduceras av (för systemet) externa aktörer på ett tillförlitligt (repeterbart) sätt som skadar applikationens funktionalitet. I detta fall är buggen en så kallad säkerhetsbugg, eller *sårbarhet* för systemet. Olika sårbarheter har olika konsekvenser för ett system – vissa kan användas för att ge angriparen privilegier på systemet (t.ex. som en administratör) medan andra kan användas för att störa ut kritisk funktionalitet på systemet så att dess faktiska användare inte kan bruka det som det är tänkt.

IT-system som används inom hälso- och sjukvård är inget undantag från denna regel – det förekommer buggar och sårbarheter även i dessa. Exempelvis har sårbarheter hittats i inbyggda system såsom autonom pumputrustning (för insulin, kemoterapi eller antibiotika) och defibrillatorer [11]. Av sårbarheterna som beskrivs i [11] kan sårbarheten i pumputrustningen exploateras för att förändra dosen som administreras till patienten medan sårbarheten i defibrillatorerna möjliggör för en antagonist att styra över administrationen av elchocker till en patients hjärta. I tv-serien Homeland[3] hackas USAs vicepresidents pacemaker med dödligt utfall. Detta må vara fiktivt men faktum är att USAs (verkliga) förra vicepresident Dick Cheney stängde av den trådlösa accessmöjligheten till sin pacemaker för att skydda sig mot just ett sådant IT-angrepp [40].

När det gäller administrativa system såsom journalsystem så är de ofta implementerade i en traditionell IT-miljö med commercial-off-the-shelf (COTS) produkter såsom Windows 7. Detta medför att IT-attacker som rör traditionella IT-system, såsom vanliga datormaskar, också är applicerbara mot dessa system.

[1] http://www.diabetes.co.uk/insulin/Insulin-pumps.html
[2] http://www.bcs.com/pages/Cardiac_Pacemakers.asp
[3] http://www.sho.com/sho/homeland/home

Exempel på attacker som förekommet genom sådana buggar är datormasken Conficker som har angripit IT-system i diverse sjukhus i Sverige [25], och Secure Sockets Layer (SSL)-sårbarheten Heartbleed som nyligen möjliggjorde för antagonister att stjäla journalinformation om 4.5 miljoner amerikanska patienter [5].

I sammanfattning är tanken bakom ”IP-fieringen”[4] att minska den operativa och administrativa bördan för olika aktörer inom hälso- och sjukvård. Den kan dock samtidigt bidra till att öka mängden möjliga fel, varav vissa kan användas för missbruk av illvillig aktörer [32].

1.1 Syfte och definitioner

Nationellt centrum för säkerhet i industriella informations- och styrsystem för samhällsviktig verksamhet (NCS3) drivs av Totalförsvarets forskningsinstitut (FOI) på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) och utgör en del av MSB:s satsning på ett nationellt program för ökad säkerhet i industriella informations- och styrsystem [18]. Verksamheten vid NCS3 syftar till att minska de risker som införandet av nätanslutna industriella informations- och styrsystem för styrning av samhällsviktig infrastruktur medför, speciellt med avseende på avsiktlig störning.

Hälso- och sjukvård är en sektor som hittills inte studerats inom ramen av NCS3. Syftet med denna studie är att få en aktuell bild av hur *informations- och styrsystem* används inom sektorn, hur dessa tekniskt är uppbyggda samt vilka *incidenter* som har förekommit. Studien skall också ge förslag på Centrumets fortsatta hantering av sektorn.

1.1.1 Definitioner

Två centrala definitioner som används i denna rapport rör *informations- och styrsystem* samt *incidenter*. Dessa definieras av följande två stycken.

Produkter som används inom hälso- och sjukvård går under det gemensamma namnet *medicintekniska produkter* (MTP). MTP är formellt definierat av Lag (1993:584) om medicintekniska produkter:

> ”***2 §*** *Med en medicinteknisk produkt avses i lagen en produkt som enligt tillverkarens uppgift ska användas, separat eller i kombination med annat, för att hos människor*
>
> 1. *påvisa, förebygga, övervaka, behandla eller lindra en sjukdom,*

[4] En övergång från analogt till digitalt samt från isolerat till ihopkopplat.

2. *påvisa, övervaka, behandla, lindra eller kompensera en skada eller en funktionsnedsättning,*
3. *undersöka, ändra eller ersätta anatomin eller en fysiologisk process, eller*
4. *kontrollera befruktning.*"

Bestämmelserna i Lag (1993:584) gäller även tillbehör till medicintekniska produkter. Inom vården klassas även dessa som MTP:er. Informations- och styrsystem inom hälso- och sjukvård tolkas i denna studie som MTP:er som innefattar datorkomponenter och i någon mån är kopplade till fysisk interaktion.

Vad en incident (eller avvikelse) inom hälso- och sjukvård rörande en MTP innebär är definierat i Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården [38]:

> "***3 §** Anmälan ska göras vid funktionsfel och försämring av en produkts egenskaper eller prestanda samt vid felaktigheter och brister i märkningen eller bruksanvisningen som kan leda till eller har lett till*
>
> - *en patients, en användares eller någon annan persons död, eller*
> - *en allvarlig försämring av en patients, en användares eller någon annan persons hälsotillstånd.*"

1.1.2 Forskningsfrågor

Mer konkret söker studien svar på följande forskningsfrågor:

1. Vilka MTP:er finns?
2. Vilka incidenter har inträffat inom hälso- och sjukvård?
    a. Vilka är orsakerna till dessa incidenter?
    b. Vilka konsekvenser har dessa incidenter fått?
    c. Vilka åtgärder bör tas för att motverka förekomsten och effektivisera behandlingen av dessa incidenter?
    d. Vilka av dessa incidenter har inträffat på grund av IT-angrepp?

1.2 Avgränsningar

För att hälso- och sjukvård skall fungera på ett effektivt sätt krävs det, på samma sätt som för de flesta andra branscher, att en mängd olika vanliga samhällstjänster, såsom elförsörjning och rent vatten, fungerar. Denna studie fokuserar på de informations- och styrsystem som existerar specifikt inom hälso- och sjukvård vilket innebär att liknande system inom andra stödjande samhällssektorer (såsom

elkraft) inte behandlas i denna rapport. Bakgrunden till detta beslut är att NCS3 tidigare utfört studier av flertalet sådana sektorer, exempelvis elkraft, vattendistribution och spårbunden transport.

En andra större avgränsning som genomförts inom projektet gäller själva produktionen av läkemedel och MTP:er, vilka innefattar diverse informations- och styrsystem. Denna produktion har dock avgränsats bort i studien eftersom sådan tillverkning ofta görs utanför Sverige.

1.3 Disposition

Denna rapport är strukturerad som följande: Kapitel 2 ger en översiktlig beskrivning av hälso- och sjukvård i Sverige. Kapitel 3 beskriver studiens metod. Kapitel 4 beskriver resultaten för forskningsfråga ett och kapitel 5 resultaten för forskningsfråga två. Kapitel 6 diskuterar dessa resultat och ger förslag på NCS3:s fortsatta hantering av hälso- och sjukvårdssektorn.

2 Översiktlig beskrivning av hälso- och sjukvård

I det svenska sjukvårdssystemet är ansvaret för hälso- och sjukvården delat mellan stat, landsting och kommun enligt hälso- och sjukvårdslagen (1982:763). Staten är ansvarig för den övergripande hälso- och sjukvårdspolitiken samt, via Socialstyrelsen, för tillsynen av all hälso- och sjukvård i riket [37]. Staten är även via Läkemedelsverket ansvarig för tillsynen av medicintekniska produkter. Landstingen ansvarar för att organisera vården så att alla medborgare har tillgång till en god vård. Kommunerna ansvarar för vård av äldre samt stöd och service till dem som är färdigbehandlade och utskrivna från sjukhusvård. Kommunerna ansvarar också för boende, sysselsättning och stöd till dem med psykiska funktionsnedsättningar. Vidare finns det tre typer av sjukvård: regionsjukvård, länssjukvård och primärvård. Dessa beskrivs av följande stycken.

Regionsjukvård är i Sverige en beteckning på den sjukvård som har ansvar för särskilt komplicerade eller sällsynta sjukdomar och skador. Denna sjukvård bedrivs vid Sveriges sju regionsjukhus (alla dessa är för övrigt så kallade universitetssjukhus), som har mer högspecialiserad vård än länssjukhus och länsdelssjukhus:

- Karolinska Universitetssjukhuset (Solna och Huddinge)
- Norrlands universitetssjukhus i Umeå
- Universitetssjukhuset i Linköping
- Universitetssjukhuset i Örebro
- Sahlgrenska Universitetssjukhuset
- Skånes universitetssjukhus (Lund och Malmö)
- Akademiska sjukhuset i Uppsala

Länssjukvård omfattar ett tjugotal länssjukhus och ett fyrtiotal länsdelssjukhus. Länssjukhusen har de flesta typer av specialistmottagningar och avancerad medicinsk utrustning som täcker de flesta åkommor. Länsdelssjukhusen är enklare och har ett urval av mottagningar.

Primärvård är en del av den öppna hälso- och sjukvården i Sverige och ger den vård som de flesta patienter har behov av. På vårdcentralerna tas de patienter som inte kräver sjukhusens tekniska och medicinska resurser omhand för medicinsk behandling, rehabilitering, omvårdnad och förebyggande arbete. Patienter med kroniska sjukdomar, exempelvis diabetes, besöker vårdcentralen för regelbundna kontroller. Primärvården sysslar även med hemsjukvård baserad på läkare distriktssköterskor och undersköterskor.

2.1 Huvudsakliga aktörer och incidenthantering

Åtta huvudsakliga aktörer identifierades rörande medicinteknik (MT): patienter, vårdpersonal, MT-tekniker, IT, leverantörer, Inspektionen för vård och omsorg (IVO), Socialstyrelsen och Läkemedelsverket. Dessa beskrivs nedan.

- *Patienter* är ibland direkta brukare av MTP:er (t.ex. en patient som har en respirator i hemmet) och ibland indirekta brukare av MTP:er som hanteras av vårdpersonal (t.ex. insulinpumpar på sjukhus).
- *Vårdpersonal* (t.ex. läkare, verksamhetschefer, sjuksköterskor och läkarassistenter) är användare av MTP:er och de som ofta först uppmärksammar problem med MTP:er.
- *MT-tekniker* är ingenjörer vars huvudsakliga uppgift är att vara ett direkt stöd för vårdpersonalen rörande operativa MTP:er (t.ex. infusionspumpar och defibrillatorer). MT-tekniker befinner sig generellt ute i vårdens operativa miljöer och har personlig samverkan med vårdpersonalen.
- *IT* är ansvariga för att den huvudsakliga systemarkitekturen (t.ex. nätverk, datalagring och intrångsdetektion) fungerar som det är tänkt. IT är även ansvariga för hälso- och sjukvårdens vanliga kontorssystem och administrativa system, såsom journalsystemet.
- *Leverantörer* är ansvariga för distributionen av MTP:er. I många fall är leverantören också *tillverkare* av produkten. För att en MTP ska få användas så måste den uppfylla gällande produktregelverk i EU[5]. I Europa är det tillverkarnas uppgift att visa att de uppfyller de legala kraven (i USA är det myndigheten som godkänner att produkter uppfyller legala krav). Därefter utfärdas CE-certifikat av särskilda organisationer (anmälda organ). Detta gör utveckling och driftandet av MTP:er till reliabla men långsamma processer. Det medför också att leverantörerna själva till stor del blir ansvariga för installation och drift (t.ex. mjukvaruuppdateringar) av MTP:er.
- *Inspektionen för vård och omsorg (IVO)* bedriver tillsyn av hälso- och sjukvård för att identifiera brister och förbättringsområden. IVO är också ansvariga för att ta emot händelser som har medfört eller hade kunnat medföra en allvarlig vårdskada – så kallade lex Maria anmälningar[6].
- *Socialstyrelsen* var innan IVO startades ansvarig för de aktiviteter som nu bedrivs där[7]. Deras nuvarande ansvarsområden involverar exempelvis att

[5] Direktiv 90/385/EEC om aktiva implanterbara produkter, Direktiv 93/42/EEC om övriga medicintekniska produkter och Direktiv 98/79/EEC om in-Vitrodiagnostiska produkter.
[6] http://www.ivo.se/anmala-och-rapportera/anmal-vardskada-lex-maria/Sidor/default.aspx
[7] http://www.socialstyrelsen.se/nyheter/2013maj/nubildasinspektionenforvardochomsorg

utfärda föreskrifter och vägledningar, att utföra utvärderingar samt ansvara för ett antal register såsom patientregistret och dödsorsaksregistret.

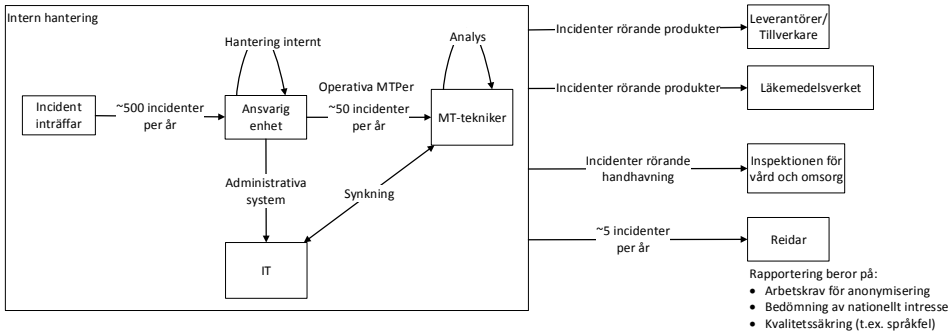
- *Läkemedelsverket* har ansvar för tillsynen av MTP:er och deras tillverkare. Läkemedelsverket utfärdar föreskrifter om MTP:er, exempelvis rörande omfattning och regler för avvikelserapportering[8].

En översikt av incidenthanteringsprocessen rörande MTP:er för det fallstuderade universitetssjukhuset (se avsnitt 3.2) kan ses i Figur 1. Denna process skiljer sig sannolikt något åt mellan olika universitetssjukhus, eller om det istället handlar om länssjukvård eller primärvård. Om en MTP-incident (också vanligen benämnd som avvikelse) inträffar uppmärksammas den i regel först av sin brukare (den ansvariga vårdpersonalen). På det studerade universitetssjukhuset beräknas cirka 500 sådana incidenter inträffa per år. Oftast är incidenterna så små att de kan hanteras internt på de ansvariga enheterna, exempelvis om ingen skada har skett eller bedöms kunna ske i framtiden, och en enkel rutinmanöver behöver ses över. I cirka 10% av alla fall så kan incidenten inte hanteras helt av den ansvariga enheten utan behöver expertstöd.

Om incidenten rör IT:s ansvarsområden (t.ex. journalsystemet eller nätverkskommunikation) meddelas IT; om det rör operativa MTP:er (t.ex. infusionspumpar) meddelas MT-tekniker. Ofta är det svårt för vårdpersonalen att avgöra denna skillnad. I dessa fall kontaktas generellt MT-tekniker, sannolikt på grund av deras närvaro på vårdavdelningarna. Vid behov koordinerar MT-tekniker och IT sedan internt för att avgöra hur problemet bäst kan lösas. Enligt svensk lagstiftning rapporteras incidenter som rör problem med MTP:er till Läkemedelsverket och leverantörerna, och problem som rör handhavandefel till IVO. I praktiken behöver ofta alla tre aktörer kontaktas.

Det finns en publik nationell databas kallad REIDAR[9] (Rikstäckande Elektronisk InformationsDatabas för Avvikelser Rörande MTP:er) vilken är tänkt att logga alla MTP-relaterade incidenter inom hälso- och sjukvård på en plats som möjliggör enkel kommunikation av problem och lösningar mellan olika aktörer, samt mer omfattande analyser. För det studerade universitetssjukhuset rapporteras cirka 1% av alla uppkomna incidenter till REIDAR. Anledningen till den låga rapporteringssiffran för fallstudieobjektet tros vara att: (i) MT-enheten är ansvarig för rapportering, och får endast in 10% av alla incidenter som inträffar, (ii) det tar arbetstid (som inte finns tilldelad) att anonymisera och kvalitetsgranska incidenter, och (iii) alla incidenter bedöms inte vara av nationellt intresse. REIDAR beskrivs mer utförligt i avsnitt 3.3.2.

[8] http://www.lakemedelsverket.se/malgrupp/Halso---sjukvard/Rapportera-medicintekniska-olyckor-och-tillbud/
[9] http://www.reidar.se/



Figur 1. Översikt av incidenthanteringsprocessen inom hälso- och sjukvård.

3 Metod

Projektet innefattade fyra huvudsakliga metodval: litteraturstudie, fallstudie, studier av sekundärdata och en enkätstudie. Dessa metodval beskrivs i avsnitt 3.1 till 3.4.

3.1 Litteraturstudie

En litteraturstudie användes för att erhålla en grundläggande förståelse för området avseende de fem forskningsfrågorna (se avsnitt 1.1). Litteraturstudien byggde delvis på vetenskapliga bidrag identifierade i databaserna IEEE, ACM, Scopus, Emerald och Google Scholar och delvis på populärvetenskapliga bidrag identifierade via Google.

Litteraturstudien syftade till att identifiera dels hur forskare tidigare adresserat de fem forskningsfrågorna i avsnitt 1.1 och dels hur hälso- och sjukvård i Sverige är uppbyggt. Resultatet av litteraturstudien beskrivs i kapitel 4-5. Det användes dels för att direkt svara på forskningsfrågorna, dels för att skapa intervjumallar för fallstudien (se avsnitt 3.2), dels för att behandla sekundärdata (se avsnitt 3.3) och dels för skapandet av enkäten (se avsnitt 3.4). Att kombinera kvalitativa och kvantitativa datainsamlingsmetoder är en effektiv forskningsstrategi för att nå både djupgående och generaliserbar kunskap [17].

3.2 Fallstudie

En fallstudie är en metod för att nå djupgående kunskap om en egenskap [22]. För denna studie genomfördes en fallstudie i syfte att skapa en förståelse för vilka problem som hälso- och sjukvård har rörande medicintekniska produkter. Målet med fallstudien var dels att direkt svara på forskningsfrågorna (se avsnitt 1.1), och dels att ge input till studierna av sekundärdata (se avsnitt 3.3) och enkätstudien (se avsnitt 3.4).

3.2.1 Intervjufrågor

Grunden för intervjufrågorna som användes under denna studie baseras på ett frågebatteri som togs fram för studier av IT-säkerheten inom industriella informations- och styrsystem i allmänhet[10]. Frågebatteriet består av 407 frågor rörande 14 huvudsakliga områden (t.ex. användare, noder och nätverk) och har tidigare testats av en fallstudie rörande spårbunden trafik (se fotnot 10). Dessa områden och frågor anpassades efter de särskilda omständigheter som

[10] FOI-R--4029--SE, NCS3- Informations- och styrsystem inom spårbunden trafik.

identifierades av litteraturstudien, med ett övergripande intervjuformulär som resultat. Detta övergripande intervjuformulär anpassades sedan inför (och förädlades efter) varje studietillfälle.

3.2.2 Population, urval och datainsamlingsmetod

Populationen för fallstudien var personal inom regionsjukvård, länssjukvård och primärsjukvård beskrivna i avsnitt 2 och aktörerna beskrivna i avsnitt 2.1. Ett urval gjordes till interna verksamhetsaktörer, d.v.s. vårdpersonal, MT-tekniker och IT. En mer omfattande fortsättningsstudie skulle även kunna involvera leverantörer, tillverkare och myndigheter. En annan urvalsparameter som gjordes var att fokusera på universitetssjukhus. Detta urval gjordes då de intressanta aktörerna förmodades vara bättre representerade och användningen av MTP:er större och bredare där än inom länssjukvård och primärvård.

Först utfördes en förstudie med två telefonintervjuer om cirka 30 minuter vardera. Den ena intervjun involverade en IT-koordinator på ett länssjukhus och den andra en MT-ingenjör på ett universitetssjukhus. Dessa intervjuer hjälpte till att förstå problemområdet som helhet och forma projektets huvudsakliga fallstudie.

Tabell 1. Översikt av utförd fallstudie.

Roll	Tidpunkt	Minuter	Metod
MT-säkerhetsansvarig	20140910	120	Personlig intervju
Fem IT-ansvariga (ledning och objektförvaltare)	20140922	140	Workshop
Tre IT-ansvariga (teknisk personal)	20141010	200	Workshop
Fem ur vårdpersonal och MT-tekniker	20141105	180	Personliga intervjuer samt observationer på sjukhuset

Fallstudien involverade ett universitetssjukhus och 14 personer (se Tabell 1), och utfördes på grund av sekretess- och resursanledningar enbart i form av (tre) intervjuer och (två) workshops (exempelvis utfördes inga aktiva nätverkskartläggningar). Fallstudien följde de riktlinjer för utförande av fallstudier som beskrivs av Runeson och Höst [35]. Ett undantag gjordes dock för användning av inspelningsverktyg, vilket rekommenderas av Runeson och Höst då det förbättrar kvaliteten för det insamlade datamaterialet. Inspelningsutrustning

användes inte under denna studie på grund av sekretesskäl och baserat på forskarnas erfarenhet av att många respondenter vid delgivning av känslig information (såsom säkerhetsincidenter) blir mindre öppna om inspelningsutrustning används. För att säkerställa datakvalitet tilläts istället alla respondenter att kommentera de renskrivna intervjuanteckningarna, samt utkastet till denna rapport.

3.3 Studier av sekundärdata

3.3.1 Amerikanska databaser

Litteraturstudien identifierade ett antal publikt tillgängliga databaser med information rörande projektets forskningsfrågor som driftas av US Food and Drug Administration (FDA)[11]. Dessa databaser är relevanta att studera då erfarenheter av FDA (d.v.s. USA) möjligen är tillämpbara även för Sverige.

En av dessa databaser innefattar information kring vilka typer av utrustning som är godkända av FDA[12]. Denna databas innehåller 1700 produkttyper grupperade inom 16 medicinska specialområden. Varje utrustning klassificeras inom en av tre kategorier som motsvarar vilken typ av granskning som utrustningen behöver gå igenom för att godkännas:

1. Generella kontroller
2. Generella kontroller och särskilda kontroller
3. Generella kontroller och godkännande innan distribution[13]

En översiktlig tolkning av dessa kategorier är att utrustning som rör mer känsliga användningsområden kräver mer granskning (= en högre klassning) för att godkännas av FDA.

Det finns också en databas som beskriver avvikelser som inträffat på grund av felaktig utrustning (t.ex. ofarliga fel, skador och dödsfall) kallad Manufacturer and User Facility Device Experience (MAUDE)[14], samt en databas som beskriver återkallade typer av utrustning (t.ex. för att genomföra mjukvaruuppdateringar) kallad Medical and Radiation Emitting Device Recalls (MREDR)[15].

[11] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Databases/default.htm
[12] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051530.htm
[13] Från engelskans ”Premarket approval”.
[14] http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm
[15] http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm

MAUDE och MREDR har studerats av forskare vid ett flertal tidigare tillfällen (se avsnitt 4.1). I synnerhet har Alemzadeh m.fl. [2] använt dem för att analysera incidenter som rör problem med datorhårdvara och datormjukvara. Föreliggande projekt jämför resultatet från Alemzadeh m.fl. [2] med underlag från svenska databaser i syfte att identifiera likheter och skillnader.

Det finns ännu ingen forskning rörande MAUDE och MREDR med fokus på datorintrång. Detta projekt ämnade därför identifiera datorintrång beskrivna i MAUDE och MREDR. Informationen i MAUDE tankades ned som ett kommaseparerat dokument för att förenkla databehandlingen (de sökformulär som finns för databaserna på deras respektive hemsidor är mycket begränsade). MREDR kan inte tankas ned i sin helhet utan enbart användas genom att söka i genom formuläret som exponeras på FDAs hemsida. Vid tillfället då MAUDE tankades ned (den 27e augusti 2014) fanns det 937 341 incidenter beskrivna i databasen. Sökverktyget för MREDR beskriver inte det totala antalet poster i databasen, eller det totala antalet träffar som ges för en sökning. Det listar dessutom endast de 500 mest relevanta träffarna som ges av en sökning.

Det finns inga nyckelord för datorintrång beskrivna i MAUDE eller MREDR (något som forskare tidigare påtalat som ett problem [15][16]). För att identifiera datorintrång användes därför en kombination av fördefinierade nyckelord[16] (kompilerade av författarna till denna rapport) och de öppna textfälten beskrivna i MAUDE och MREDR (de allra flesta incidenter och återkallelser har långa, ostrukturerade beskrivningar).

3.3.2 Svenska databaser

I Sverige för Ledningsnätverket för Medicinsk Teknik (LfMT) ett register kallat MTPReg[17] som beskriver vilka medicintekniska produkter som används inom Sverige (dock inte deras antal) och ett annat register kallat REIDAR som beskriver svenska incidenter som inträffat rörande medicintekniska produkter. Dessa databaser identifierades under projektets fallstudie (se avsnitt 3.2).

De allra flesta entiteter som hanterar MTP:er (såsom sjukhus) rapporterar till REIDAR, vilket innebär att den har en bred variation kring uppkomna incidenter. En enkätstudie utförd av LfMT kring REIDAR från 2013 visar dock att rapporteringsfrekvensen av incidenter till REIDAR är relativt låg [7], något som projekts fallstudie bekräftar (se avsnitt 2.1). Med andra ord, studier av REIDAR är inte nödvändigtvis valida för uttalanden om svenska incidenter rörande MTP:er i

[16] Sökningar utfördes med sökorden (”malware” or ”malicious software” or ”malicious code” or ”intrusive software” or ”virus” or ”computer attack” or ”computer intrusion” or ”cyber intrusion” or ”cyber attack” or ”security breach” or “security compromise” or “cyber compromise” or “cyber security”).

[17] http://www.mtpreg.se, användarnamn: mtc01, lösenord: mtc01

allmänhet. Andra svenska regionala incidentdatabaser, såsom Västra Götalands Regions incidentdatabas har långt fler dataposter. Dessa avgränsades från på grund av att de inte är nationellt delade och för att de inte nödvändigtvis är valida för hälso- och sjukvård som helhet, utan begränsade mot regionerna som de behandlar. Framtida studier bör dock studera incidenter även i sådana databaser.

Trots denna potentiella brist påtalades REIDAR under fallstudien ett flertal gånger som ett område projektet borde innefatta. Dels för att det idag inte finns några publikt tillgängliga (eller för projektgruppen kända) analyser utförda på REIDAR och dels för att respondenterna ansåg att en analys skulle kunna hjälpa till att öka intresset för REIDAR, och därmed öka rapporteringsfrekvensen, vilket ansågs kunna gynna den svenska vården som helhet. Det bör även poängteras att Sverige och REIDAR inte är unika i att ha en bristfällig rapportering: Alemzadeh m.fl. [2] beskriver följande kring FDAs incidentdatabaser:

> ”[…] *our observation is similar to other studies that found inaccuracies and underreporting in the MAUDE database and inconsistencies between the FDA MAUDE and Recalls databases*.”

MTPReg tillhandahåller en möjlighet att tanka ner en kopia av REIDAR via dess webbformulär. Detta genomfördes den 23 september 2014. Vid detta tillfälle fanns 20 539 olika produkttyper beskrivna i MTPReg. En beskrivning av dessa produkter ges i avsnitt 4.2.

REIDAR har ett webbformulär som kan användas för att söka efter incidenter. Detta sökformulär är dock mycket begränsat och det finns inte heller någon möjlighet att tanka ned en kopia av databasen via denna webbsida. Efter godkännande från de ansvariga för REIDAR skapades en lokal version av databasen med hjälp av en webbcrawler[18] utvecklad med hjälp av Ruby-biblioteket Nokogiri[19]. Denna webbcrawler användes den 23 september 2014 för att ladda hem all tillgänglig information kring alla incidenter registrerade i REIDAR. Vid detta tillfälle fanns 2867 incidenter beskrivna i REIDAR.

Varje incident i REIDAR beskrivs med ett urval av 33 olika egenskaper. Tabell 2 beskriver dessa egenskaper och hur ofta incidenter innefattar information om dem. De flesta fält (19 av 33) är listbaserade, men det finns även öppna textfält (11 av 33). Flera av dessa öppna fält matas dock med mycket strukturerad information, exempelvis nr 5 (produktmodell), där olika rapporter använder samma nomenklatur. Ett exempel är ”Terumo stc-503” (en typ av infusionspump) som återges 30 gånger.

[18] Ett mjukvaruverktyg som automatiskt söker efter och behandlar information på webbsidor.
[19] http://nokogiri.org/

Tabell 2. Incidentegenskaper i REIDAR.

Nr	Kategori	Tillstånd	Förekomst	Andel
1	ID	Kod	2867	100%
2	Datum	Datum	2867	100%
3	Produkt: benämning	Öppen text	2791	97%
4	Produkt: fabrikat	Öppen text	2699	94%
5	Produkt: typ/modell	Öppen text	2719	95%
6	Produkt: CE-märkning	Lista	1671	58%
7	Produkt: CE-alternativ	Öppen text	114	4%
8	Leverantör: kommentar	Öppen text	275	10%
9	Händelsebeskrivning: rubrik	Öppen text	2841	99%
10	Händelsebeskrivning: kommentar	Öppen text	2849	99%
11	Händelsebeskrivning: vårdgivare	Lista	1726	60%
12	Händelsebeskrivning: plats	Lista	1724	60%
13	Händelsebeskrivning: typ av verksamhet	Lista	1662	58%
14	Händelsebeskrivning: specialitet	Lista	1322	46%
15	Händelsebeskrivning: typ av vård	Lista	1608	56%
16	Händelsebeskrivning: vem skötte produkten?	Lista	1639	57%
17	Händelsebeskrivning: situation	Lista	1661	58%
18	Certifierad rapportörs orsaksbeskrivning	Öppen text	1750	61%
19	Konsekvens: patient	Lista	2861	100%
20	Konsekvens: personal	Lista	2861	100%
21	Konsekvens: produkt	Lista	2861	100%
22	Orsak: människa	Lista	529	18%
23	Orsak: lokal teknisk verksamhet	Lista	242	8%
24	Orsak: leverantörer/tillverkare	Lista	1056	37%
25	Orsak: organisation	Lista	268	9%
26	Riskbedömning: bedömning	Lista	1229	43%
27	Riskbedömning: typ av avvikelse	Lista	1738	61%
28	Riskbedömning: aggregering	Lista	623	22%
29	Certifierad rapportörs åtgärdsbeskrivning	Öppen text	482	17%
30	Certifierad rapportörs föreslagna åtgärder	Lista	1556	54%
31	Uppföljning	Öppen text	62	2%
32	Kommentar från socialstyrelsen och läkemedelsverket	Öppen text	161	6%
33	Bifogade filer	Bilagor	224	8%
	Totalt antal incidenter	*Summa*	*2867*	*100%*

På ett liknande sätt som för MAUDE finns det i REIDAR intressanta felorsaker rörande medicintekniska produkter (såsom om felorsaken rör datorhårdvara eller datormjukvara) som inte beskrivs på ett strukturerat sätt. Denna typ av information

är istället tänkt att beskrivas i något av de öppna textfälten. De primära fält som nyttjas för detta ändamål är nr 10 (kommentarsfält rörande händelsebeskrivningen), nr 18 (certifierade rapportörers orsaksbeskrivningar) och nr 29 (certifierad rapportörers åtgärdsbeskrivningar). Utmaningen ligger här i att klassificera incidenterna i REIDAR med hjälp av textmassorna givna i dessa tre fält. För detta ändamål nyttjades metoden beskriven i Figur 2, vilken är snarlik den metod som användes av Alemzadeh m.fl. [2]. Denna metod innefattar identifiering av vilka incidenter som är datorrelaterade, och om de bakomliggande felorsakerna för dessa incidenter är hård- eller mjukvarurelaterade, med hjälp av öppna textfält.

Python-biblioteket Natural Language Toolkit[20] (NLTK) användes för att identifiera vilka unika ord som användes i de öppna textfälten i REIDAR samt hur frekventa dessa ord var. NLTK är värdefullt då det (exempelvis) kan identifiera olika böjningar och synonymer av ord, så som ”dator”, ”datorn”, och ”datorerna”, och på det sättet minska antalet ord som måste behandlas manuellt[21]. Den slutliga ordlistan processades sedan manuellt för att identifiera nyckelord som kunde anses röra antingen batterier, datorhårdvara eller datormjukvara (utan att för den delen råka täcka in sådant som varken rör datorhårdvara eller datormjukvara).

De identifierade nyckelorden användes för att klassificera alla incidenter i kategorierna ej datorrelaterad, datorhårdvara, datormjukvara eller batteri[22]. Batteri är en subkategori till datorhårdvara som är extra vanlig och separerades från hårdvara även av Alemzadeh m.fl. [2]. Klassningsmetodens reliabilitet studerades genom att 60[23] slumpmässigt utvalda incidenter manuellt undersöktes av forskarna. Av dessa 60 incidenter ansågs 38 vara korrekt klassificerade, 12 felaktigt klassificerade och för 10 gick det ej att säkerställa vilken/vilka kategorier som var relevanta. En datakorrekthet på 63% (38/60) kan anses som ok utifrån förutsättningarna, men betyder ändock att resultatet bör tas med en nypa salt.

Den manuella granskningen resulterade i en mindre justering av kategoriseringsmodellen. Exempelvis var nyckelordet ”server” ursprungligen kategoriserat som hårdvara men visade sig förekomma ofta även i anknytning till

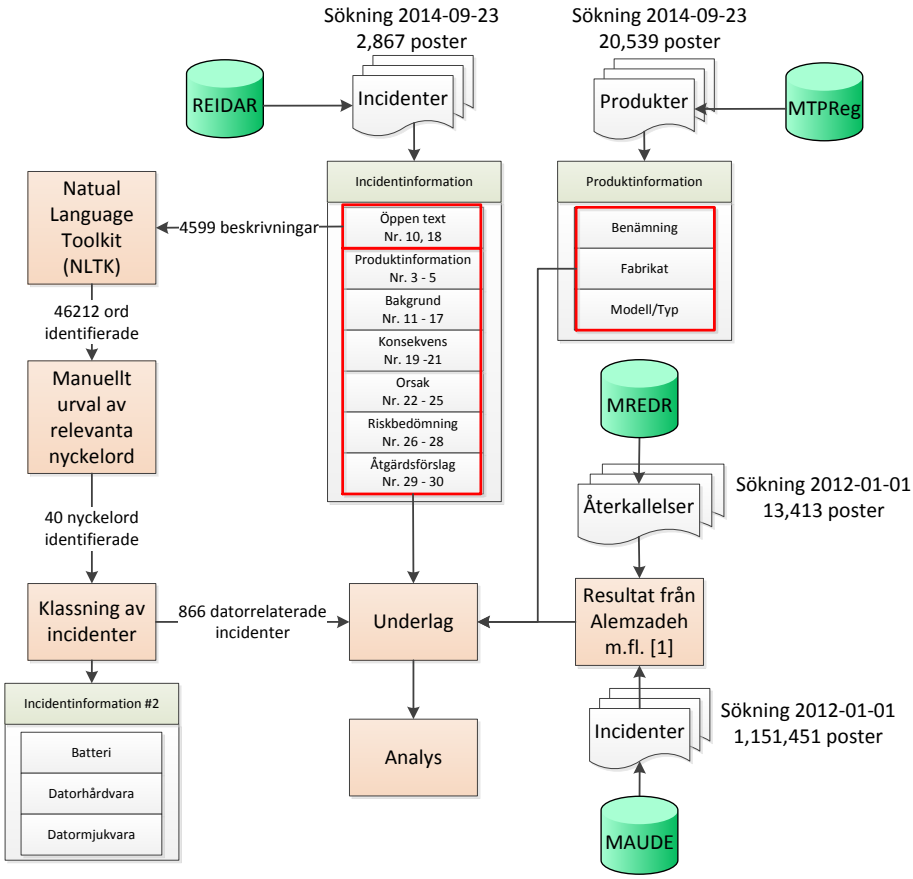
[20] Ett bibiliotek är samling extern programkod som skapats för något specifikt syfte. NLTK (http://www.nltk.org/) är ett sådant bibliotek för programmeringsspråket Python.

[21] Det bör poängteras att NLTK har begränsat med stöd för det svenska språket. Det vill säga, det har fel oftare än det har när det rör engelskspråkig text. Detta till trots förenklar det den manuella ordbehandlingen mycket.

[22] Förutom dessa kategorier har Alemzadeh m.fl. även kategorierna *I/O* (t.ex. nyckelorden ”sensor”, ”screen” eller ”speaker”) och *annat* (t.ex. nyckelorden ”system”, ”robotic” och”document”). Det är oklart för denna studie varför Alemzadeh m.fl. nyttjar dessa två kategorier då de är klart korrelerade med mjukvara och hårdvara. Av denna anledning är de avgränsade från studiens omfång.

[23] 20 klassade som datorhårdvara, 20 klassade som datormjukvara och 20 som klassades som varken datorhårdvara eller datormjukvara

mjukvarufel. Av denna anledning klassades serverrelaterade incidenter både som hårdvara och mjukvara.



Figur 2. Analys av rapporterade incidenter.

De nya kategorierna tillsammans med all annan strukturerad information i REIDAR gav underlaget rörande incidenter i Sverige. Detta underlag kompletterades med information från MTPReg (vilka produkter som används i Sverige) och information från Alemzadeh m.fl. [2] (incidenter och återkallelser av MTP:er i USA). Sökningar efter antagonistiska angrepp gjordes på datamassan med samma förfarande som med MAUDE[24] (se avsnitt 3.3.1).

[24] Med nyckelorden ”IT-säkerhet” eller ”IT säkerhet” eller ”cybersäkerhet” eller ”cyber säkerhet” eller ”intrång” eller ”virus” eller ”skadlig kod” eller ”uppdatering” (gällande säkerhetsuppdateringar).

3.4 Enkätstudie

Informationen från litteraturstudien, fallstudien och studierna av sekundärdata gav input till utformningen av enkätfrågor. Hela enkäten återges i bilaga A.

3.4.1 Population och urval

Populationen för enkäten är densamma som populationen som beskrivs i avsnitt 3.2.2. Ett bekvämlighetsurval gjordes av medlemmarna i LfMT. LfMT är ett ledningsnätverk för medicinsk teknik och sjukvårdshuvudmännens gemensamma forum för samverkan, erfarenhetsutbyte och utveckling inom det medicintekniska området. LfMT är även remissinstans för Sveriges kommuner och landsting (SKL) i medicintekniska frågor. Detta gör att LfMT:s medlemmar ansågs synnerligen lämpliga för en enkät om problem med MTP:er. Det är även sannolikt att medlemmarna har värdefulla kontaktnät som erbjuder möjligheter att indirekt sprida enkäten till ytterligare kompetenta respondenter. Av denna anledning ombads varje respondent att sprida enkäten till relevanta kollegor. Det är dock oklart hur många svarande som var ursprungliga mottagare av enkäten och hur många som refererades till den av kollegor.

Enkäten distribuerades till alla utvalda respondenter (totalt 75 stycken) den sjunde oktober 2014. Varje email innefattade både en bakgrundsbeskrivning av studien samt motivatorer för deltagande. Av dessa 75 utskick studsade två på grund av att mailadresserna inte längre existerade. En påminnelse distribuerades den 21e oktober. Enkäten stängdes ned den 25:e oktober. Totalt svarade 36 respondenter (48%) på enkäten, vilket kan ses som en hög svarsfrekvens för en webbenkät [44].

En översikt av respondenterna i enkätstudien presenteras i Tabell 3. De allra flesta hade en befattning som antingen medicinteknisk chef eller medicinteknisk ingenjör. De övriga var främst verksamhetsansvariga såsom verksamhetschefer eller kvalitetssamordnare. Antal års erfarenhet med MTP:s är i snitt mycket lång (från 2 till 42 år).

Tabell 3. Respondenter i enkätstudie. Erfarenhet är medelvärdet för antal års erfarenhet med medicintekniska produkter.

Roll	Antal	Erfarenhet
Medicinteknisk chef	18	24.9
Medicinteknisk ingenjör	11	17.2
Andra	7	28.0

3.4.2 Enkätutformning

Enkäten distribuerades online via Google Forms[25]. Enkätstrukturen och dess frågor formulerades med hjälp av riktlinjerna för god enkätkonstruktion som beskrivs av McColl m.fl. [28] och Fanning [12]. Enkäten bestod av tre huvudsakliga avsnitt och innefattade 26 skattningsfrågor med 5-gradiga Likertskalor och 16 öppna frågor.

I enkätens första avsnitt introducerades respondenterna till syftet med enkäten och gavs information om varför det var viktigt att delta. Respondenterna ombads ange sin organisationsroll och antalet års erfarenhet av att arbeta med MTP:er.

I enkätens andra avsnitt ombads respondenterna att återge de tre mest problematiska MTP:erna i sina respektive verksamheter, vilka problem dessa skapade och vilka orsaker som förelåg dessa problem (frågorna använde egenskaperna i databasen REIDAR, se avsnitt 3.3). Syftet med detta avsnitt var att komplettera den bild av vilka problem med MTP:er som ges av databasen REIDAR.

I enkätens tredje avsnitt ombads respondenterna beskriva förekomsten av undermåliga riktlinjer, behov av kompetensutveckling och bristande kommunikation med olika aktörer som hanterar MTP:er (både vid inträffande av en incident samt vid daglig drift). Dessa frågeställningar identifierades som potentiella problemområden under projektets fallstudie (se avsnitt 3.2).

Enkätens reliabilitet och validitet studerades på två sätt[26]:

- Enkätens sista avsnitt innefattade en fråga för att studera dess validitet (huruvida den täckte in allt av vikt) och en fråga för att mäta dess reliabilitet (om det fanns problem med enkätverktyget i sig). Totalt 19 respondenter svarade på frågan gällande enkätens validitet. Av dessa ansåg två att allt av vikt täckts in. Av de resterande 17 var spridningen i förslag mycket stor: allt ifrån utbildning till standardisering och kopplingen mellan tillverkare och leverantörer diskuterades. Totalt 15 respondenter svarade på frågan gällande enkätens reliabilitet. Av dessa ansåg tre att enkäten var bra utan problem. De allra flesta av de resterande 12 ansåg att enkätens frågeställningar var för omfattande/komplexa. Det ansågs särskilt svårt att identifiera de tre mest problematiska MTP:erna då det ansågs finnas otaliga typer av MTP:er med diverse komplexa problem.

[25] www.google.com/forms. En alternativ metod som diskuterades men avgränsades från var att distribuera enkäten via en specialskräddad webbapplikation.

[26] Ett vanligt sätt att mäta en enkäts reliabilitet (dess interna konsistens) är genom det statistiska måttet Chronbach's alpha [8]. Denna metod nyttjades ej på grund av dess krav på extra enkätfrågor (och därmed risk för en lägre svarsfrekvens).

- Innan enkätens utskick testades dess reliabilitet och validitet med hjälp av en telefonintervju med en respondent som ansågs representativ för urvalet (se avsnitt 3.4.1). Denna respondent svarade på enkäten under samma förutsättningar som i skarpt läge (d.v.s. utan hjälp från forskarna), men med skillnaden att forskarna deltog över telefon. Denna metod medförde flera förändringar av enkäten. Exempelvis fanns det ursprungligen enbart en enda enkätfråga om kommunikation i enkäten – efter telefonintervjun delades denna upp i fem frågor.

4 Industriella informations- och styrsystem inom hälso- och sjukvård

Detta kapitel besvarar forskningsfråga 1: *Vilka MTP:er finns?*

4.1 Litteratur

Det finns ännu inga forskningsrapporter som beskriver vilka MTP:er som används i Sverige. Det finns dock flera forskningsrapporter som studerar MTP:er i USA, primärt genom att korrelera resultat från MAUDE och MREDR (se avsnitt 3.3.1 för beskrivningar av dessa) för att analysera vilka fel (t.ex. mjukvarubuggar) som finns för olika produkter (t.ex. pacemakers) som föranleder olika konsekvenser (t.ex. dödsfall) [2][6][34][42].

Alemzadeh m.fl. [2] har kartlagt vilka typer av utrustning involverande inbyggda datorer av olika slag som återkallas. Författarna fann att 1210 av 5294 återkallelser (23%) av produkttyper rörde datorbuggar korresponderande till totalt 12 024 836 inbyggda medicinska system världen över. Av dessa 1210 återkallelser rörde 81% system använda inom radiologi, kardiologi, anestesiologi, allmän sjukvård (t.ex. autonoma pumpar), samt allmän kirurgi (t.ex. elektrokirurgiska system). Cirka hälften av de säkerhetskritiska återkallelserna kunde vidare härledas till någon av sju olika produkttyper: (i) bildhanteringssystem (t.ex. felaktig presentation av data), (ii) röntgensystem (t.ex. felaktig detektion eller dosering), (iii) externa defibrillatorer (t.ex. felaktiga elchocker), (iv) inopererade defibrillatorer (t.ex. avstängning av funktion), (v) inopererade pacemakers (t.ex. avstängning av funktion), (vi) fysiologiska patientmonitorer (t.ex. felaktiga larm), (vii) infusionspumpar (t.ex. felaktig dosering). Av dessa var externa defibrillatorer vanligast att fela överlag (415 537 återkallade system) och inopererade defibrillatorer vanligast att orsaka dödsfall (293).

MSB:s ”Vägledning till ökad säkerhet i industriella informations- och styrsystem” [10] innehåller rekommendationer för att höja säkerheten i systemen. Den beskriver med andra ord inte hur det ser ut inom dagens kritiska samhällssektorer, men utan hur det bör se ut. Den riktar sig främst till områden som innehåller kritisk infrastruktur såsom kärnkraft, elkraft, transport, hälso- och sjukvård och vatten och avlopp, men är tillämpbar för alla som jobbar med nätverksuppkopplade styrsystem. Flera av rekommendationerna är specifika, exempelvis gällande säkerhetsfrämjande nätverksarkitektur:

- ”*Inventera organisationens tillgångar och identifiera de som är kritiska genom att tillämpa ett riskbaserat synsätt*”,
- ”*Dela upp de industriella informations- och styrsystemen i olika zoner med skyddsnivåer som anpassats efter hur kritiska de olika systemen är.*

Beroende på bland annat system- och informationsklassificering kan även så kallade subzoner behöva skapas",

- "*Dela upp nätverket utifrån funktionell klassificering*",
- "*Datatrafik över zongränser bör hanteras extra restriktivt och även övervakas och loggas. För vissa typer av it-miljöer kan det vara bra att använda datadioder och dataslussar*" och
- "*Placera osäkra tjänster och andra externa anslutningar i demilitariserade zoner (DMZ)*".

4.2 Resultat och analys

Fallstudien visade att det finns en stor mängd olika MTP:er ("tusentals"), men också att det råder skilda meningar kring vad en MTP är beroende på vilken aktör som tillfrågas. Inom vården och MT ser man på MTP:er enligt Läkemedelsverkets beskrivning (se avsnitt 1.1); inom IT ser man inte det som man själv driftar som MTP:er (t.ex. patientjournalsystemet). I allmänhet kan dock dessa komponenter klassas in i olika delområden. Denna rapport beskriver resultatet rörande den första forskningsfrågan från fyra olika perspektiv: produkter och mjukvara (avsnitt 4.2.1), nätverksarkitektur (avsnitt 4.2.2), fjärråtkomst (avsnitt 4.2.3) och behörighetskontroll (avsnitt 4.2.4).

4.2.1 Produkter och mjukvara

Studien av MTPReg identifierade 20 539 olika MTP:er av 1057 olika typer och 2784 olika leverantörer. De tio vanligaste typerna av MTP:er (med flest olika modeller) beskrivs i Tabell 4. Även om denna bild inte innefattar hur många faktiskt MTP:er som finns ute i vården säger den något om spridningen som finns i produkter – en MTP kan vara allt från en elektronisk våg till en laserskrivare.

Fallstudien bekräftar denna spridning: alla produkter inom vården är per definition MTP:er. Det finns dock enligt respondenterna två primära kategorier av MTP:er som baseras på vilka som sköter driften. Den första kategorin är den *administrativa datormiljön* med vanliga operativsystem (OS) såsom Windows 7, vilken sköts av landstingets IT-enhet. Den andra kategorin är *operativa MTP:er* med deras inbäddade operativsystem och mjukvara, samt tillhörande datorer som stödjer användning av MTP:er (t.ex. för styrning, datainsamling och datapresentation). Dessa system driftas av MT-personal ute på plats i vården samt av deras leverantörer.

Tabell 4. De tio medicintekniska produkterna med flest produktmodeller i svensk hälso- och sjukvård.

Medicinteknisk produkt	Modeller
Våg lab elektronisk	525
Bildskärm, färg	508
Dator, stationär	428
Centrifug, laboratorie, allmän användning	376
Ultraljudsprob bildgivande extrakorporeal handhållen	335
Laserskrivare	321
Mikroskop med ljuskälla	304
Träningsapparat	265
Patientmonitor multiparameter	263
Omrörare, lab	261

Vanliga mjukvaror i den administrativa datormiljön är journalsystemet Cosmic, Microsoft Office, Remiss och Svar (ROS), Synergi (ett incidenthanteringssystem för IT) och Medusa (ett incidenthanteringssystem för MT-tekniker). Uppdateringar sker till stor grad automatiserat via en egen intern uppdateringsserver, vilket ger en god kontroll över mjukvaran som rullas ut samt att system blir uppgraderade som det är tänkt. En intern uppdateringsserver medför att få externa kopplingar behövs för uppdateringar. De är även skyddade med traditionella IT-säkerhetsmekanismer såsom antivirus. Ibland utförs intrångstester av olika komponenter i den administrativa IT-miljön (i synnerhet av webbapplikationer). Detta är dock en aktivitet som enligt IT-enheten utförs alldeles för sällan.

Operativa MTP:er använder istället typiskt gamla OS såsom inbäddade Windows XP, äldre Linux-distributioner eller helt egenutvecklade varianter. Driftlängden på ett MTP-system är längre än för en vanlig standarddator (cirka 7 år). Mjukvarukonfigurationerna för dessa system är väl beprövade och skapade för att vara robusta. Patchning sker enbart efter verifiering av leverantörer, vilket i praktiken innebär att det utförs mycket sällan (det kan ta månader till år mellan uppdateringar). De patchas dessutom sällan av säkerhetshänsyn utan snarare om det rör driftsäkerhet, såsom en förbättring av ett gränssnitt eller en vanlig[27] bugg. Systemen testas om möjligt innan implementation i en testmiljö på sjukhusen där det finns goda möjligheter att kontrollera funktionalitet. Omgivande hjälpdatorer i MTP-miljön innehåller oftast Windows XP eller Windows 7. Inte heller dessa patchas regelbundet.

[27] En mjukvarubugg som påverkar driftsäkerheten men inte är en IT-säkerhetssårbarhet.

Ett problem som är svårt att behandla är att operativa MTP:er oftast måste vara fysiskt nära patienter. Diverse incidenter kan inträffa som en följd av detta, såsom störning av komponenter genom radiovågor i form av vanlig trådlös datortrafik och telefoni [13] och spridning av skadlig kod via USB. USB är för övrigt en av de vanligaste spridningsvektorerna för skadlig kod då protokollet kringgår vanliga IT-säkerhetsmekanismer såsom brandväggar och operativsystem automatiskt exekverar diverser olika rutiner som finns lagrade på dem [33].

De tio produktutvecklare med flest MTP:er i MTPReg beskrivs i Tabell 5. Siemens, Philips, Olympus, Hewlett Packard (HP) och General Electrics (GE) har alla över 500 olika operativa typer av produkter inom den svenska hälso- och sjukvården.

Tabell 5. De tio produktutvecklare som har flest medicintekniska produkter i svensk hälso- och sjukvård.

Utvecklare	Modeller
Siemens	645
Philips	626
Olympus	580
HP	570
GE Healthcare	508
Storz	333
Mettler	222
Dell	211
Zeiss	181
Fluke Biomedical	163

De tio produkttyper med flest datorrelaterade incidenter enligt REIDAR beskrivs i Tabell 6 och utvalda produkter visualiseras i Figur 3 till Figur 7. En beskrivning av hur dessa identifierades finns i avsnitt 3.3.2; en analys av de bakomliggande orsakerna till dessa incidenter görs i avsnitt 5.2.

- *Infusionspump*: Används för att tillföra mediciner, näring eller andra lösningar till en patient (Figur 3).
- *Ventilator (respirator)*: Används för att underlätta eller ersätta en patients andning (Figur 4).
- *Patientövervakningscentral*: Grundövervakningsenheten mäter parametrar som puls, blodtryck, EKG och andra relevanta mätvärden som varierar beroende på vårdinsats. Den kan även byggas på med en utökad funktionalitet och de delarna benämns tillsatsenhet för övervakning av patient.

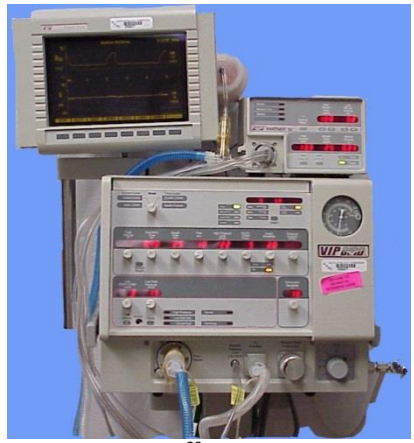
- *Mobil anestesiapparat*: Används för olika former av bedövning och sövning av patienter (Figur 5).
- *Dialysapparat*: Används för att rena vätskor från oönskade partiklar. Metoden är diffusion genom ett membran. Den hjälper t.ex. njuren när den har för svag funktion (Figur 6).
- *Extern hjärtstimulator (extern pacemaker)*: Ger elektriska impulser för att hjärtat skall fungera normalt.
- *Defibrillator*: Ger starka elektriska elstötar för att få ett hjärta som har stannat (hjärtstillestånd) att åter slå. En semiautomatisk defibrillator fungerar efter utvalda algoritmer till skillnad från en manuell där en person med hög kunskap behöver göra adekvata inställningar (Figur 7).

Tabell 6. De tio produkttyperna med flest datorrelaterade incidenter.

Medicinteknisk produkt	**Modeller**
Infusionspump	65
Ventilator (för lungor)	125
Grundenhet för övervakning av patient	*
Mobil anestesiapparat	46
Dialysapparat hemo	38
Extern hjärtstimulator	18
Defibrillator	59
Övervakningscentral grundenhet	78
Manuell defibrillator	84
Tillsatsenhet för övervakning av patient	*

*Ingen information

Figur 3. Infusionspump[28].



Figur 4. Ventilator[29].

Figur 5. Mobil anestesiapparat[30].

Figur 6. Dialysapparat[31].

[28] http://en.wikipedia.org/wiki/File:Infusionspumpe.JPG
[29] upload.wikimedia.org/wikipedia/commons/9/94/VIP_Bird2.jpg
[30] http://upload.wikimedia.org/wikipedia/commons/5/53/Maquet_Flow-I_anesthesia_machine.jpg
[31] http://upload.wikimedia.org/wikipedia/commons/f/fc/Hemodialysismachine.jpg

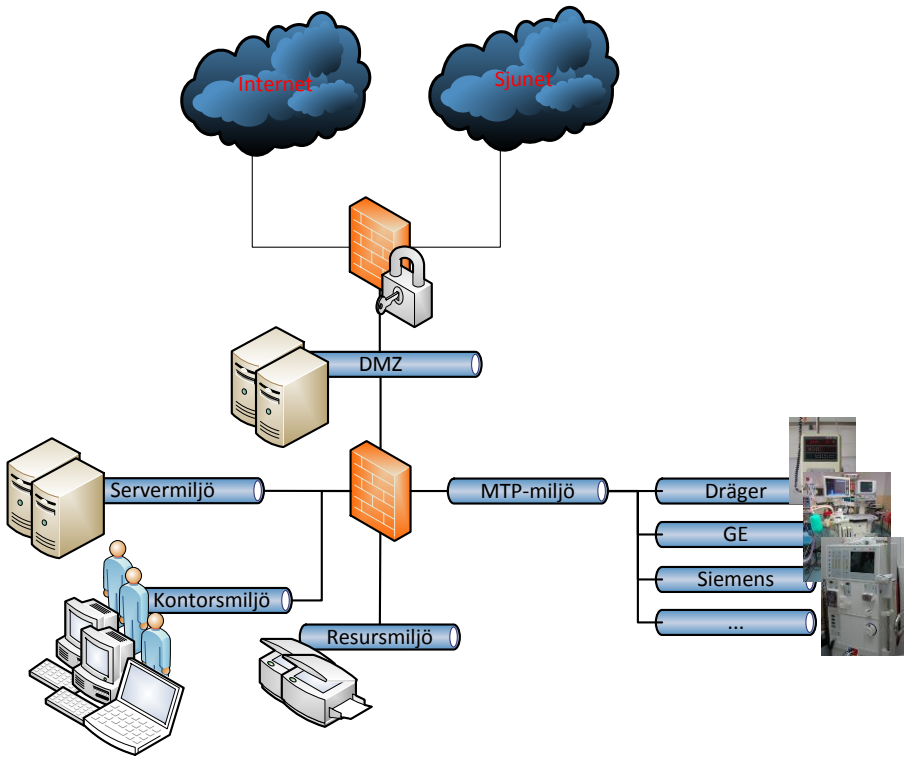
Figur 7. Semi-automatisk defibrillator[32].

4.2.2 Nätverksarkitektur

En mycket förenklad skiss av nätverkstopologin för det fallstuderade universitetssjukhuset beskrivs av Figur 8. Det finns två huvudsakliga externa nätverkskopplingar. Den ena kopplingen är via en av landstinget utvald Internet Service Provider (ISP). Denna koppling har landstinget god kontroll över. Den andra kopplingen är mot ett nätverk kallat Sjunet där diverse sjukhus, leverantörer och andra godkända aktörer ingår. Denna koppling känner landstingets IT-enhet lågt förtroende över; framförallt har de en mycket begränsad kontroll över den (t.ex. rörande passerande datortrafik).

Nätverksadresser administreras primärt automatiskt med hjälp av DHCP-servrar för de olika segmenten. Kopplingar mellan domännamn och IP-adresser administreras av interna DNS-serverar. Tjänster som behöver vara exponerade mot Internet (t.ex. webbservrar, terminalservrar och mailservrar) ligger som virtuella maskiner[33] i ett särskilt nätverkssegment. Internt är nätverksarkitekturen i det studerade landstinget väl segmenterad i många olika delnätverk. Nätverkssegmentering utförs med hjälp av en blandning av fysiska och logiska (VLAN) resurser, vilket skapar både redundans[34] och kontroll. Exempelvis sitter kontorsdatorer, servrar (administration), hjälpprodukter (t.ex. skrivare) och operativa MTP:er (t.ex. operationsrobotar) alla på olika dedikerade VLAN. Konceptet demilitarized zone (DMZ), som förordas av MSB:s riktlinjer kring arbete med IT-säkerhet i industriella informations- och styrsystem [10], nyttjas till hög grad.

[32] http://upload.wikimedia.org/wikipedia/commons/f/f3/Defibrillateur_1.jpg
[33] En virtuell maskin har ett logiskt operativsystem med samma funktionalitet som en vanlig fysisk dator.
[34] Nätverket innehåller nästan fullständig fysisk redundans, vilket innebär att om nätverkskommunikationen är bruten mellan två punkter så finns ändå en alternativ rutt för IP-trafiken att ta sig till ändpunkten.



Figur 8. Översiktlig nätverkstopologi för fallstuderat universitetssjukhus.

Kommunikation mellan segmenten sker via brandväggar med uppdaterade regelverk. Exempelvis, vid en utskrift så har en kontorsdator rätt att nå en skrivare genom brandväggen. En skrivare har dock aldrig rätt att öppna en ny nätverkskoppling tillbaka till kontorsmiljön. Ett särskilt administrationssegment har större rättigheter och används bland annat för uppdateringar av programvara och konfigurationer på vanliga datorer och nätverksuppkopplingar, inklusive routerkonfigurationer.

Varje större leverantör av operativa MTP:er har ett eget platt VLAN-segment så att de kommer åt sin egen utrustning (men inte andras). Mindre leverantörer får samsas. Som beskrivs i avsnitt 4.2.1 patchas MTP:er sällan, vilket gör dem sårbara mot IT-attacker. VLAN-separering hjälper mot utbrott av skadlig kod då det begränsar möjligheten för datormaskar att sprida sig utanför det angripna nätverkssegmentet (den drabbade leverantören). Att segmentera hårt är därmed ett

bra beslut och det bör göras i den mån det är möjligt[35]. Exempelvis kunde problemen med datormasken Conficker som infekterade över 10 000 datorer i Malmö landsting under 2009 [4] sannolikt[36] ha begränsats via god nätverkssegmentering. Det bör dock poängteras att verkligheten inte alltid är så enkel. Ett bra exempel är PACS/RIS system som har delkomponenter både i den operativa MTP-miljön (t.ex. för bildvisning) och servermiljön (t.ex. för datalagring).

Router- och switcharkitekturen bygger på CISCO-produkter och uppdateras mjukvarumässigt av lokal personal. CISCO godkänner vad som skall uppdateras och har ett servicekontrakt vilket innefattar att de är involverade i systemen mer än som enbart leverantör (t.ex. med expertkunskap). Ett centralt verktyg för konfigurering av routerarkitektur används för att kunna implementera uppdateringar och förändringar enkelt och konsekvent.

Det finns ett Security information and event management (SIEM) system, vilket är ett verktyg som används för att upptäcka intrång genom att korrelera larm från olika säkerhetsdetektionsmekanismer. Det finns dock ännu inte personalresurser för att använda lösningen på ett bra sätt. Den dagliga driften tar stora resurser och ingen dedikerad personal är satt för att övervaka det.

Det används primärt brandväggar från Checkpoint. Dessa har en inbyggd funktion för att detektera och förhindra skadlig kod som färdas via dem. Denna funktion är god från ett IT-säkerhetsperspektiv eftersom skadlig kod kan blockeras. Den är dock också en tillgänglighetsrisk då vanlig trafik ibland misstas för skadlig kod, vilket resulterar i blockering av legitim trafik. Under fallstudien framkom att detta ibland händer, men de intervjuade personerna hade inga siffror på hur ofta det var fallet. Inom akademisk forskning har systemet som landstingets intrångsdetektionssystem baserats på testats med upp emot 96% falska larm [39], vilket är en indikation på att det sannolikt förekommer i praktiken (men i mycket mindre omfattning eftersom Landstinget konfigurerar varje intrångspreventionssystem efter de unika förutsättningarna som det hanterar). Ett alternativ är att låta intrångspreventionssystemen enbart detektera och rapportera skadlig kod istället för att blockera den. Detta skulle minska IT-säkerheten men öka driftsäkerheten.

[35] Nätverkssegmentering ökar komplexiteten i en nätverksarkitektur och kan därmed ha en negativ effekt på driftsäkerheten i ett nätverk.

[36] Spridningsmekanismen för denna datormask är främst en sårbarhet i NetBIOS (MS08-067, samma sårbarhet som Stuxnet exploaterade), delade nätverksmappar och USB-minnen. God segmentering hade begränsat möjligheten att spridas via NetBIOS och delade mappar.

4.2.3 Fjärråtkomst

Att logga in i det fallstuderade universitetssjukhusets nätverk från en extern plats är väl reglerat. I första hand tillåts en hårt nedlåst virtuell maskin genom en Citrix-baserad lösning. Inloggning sker med ett SecureID, vilket är en separat kryptodosa (som även ofta används vid bankinloggning). Tvåfaktorautentisering och avskalade virtuella maskiner är säkerhetsfrämjande lösningar. Dosorna är personliga men det händer trots allt ibland att flera personer använder samma dosa. Citrixmaskinen har enbart rätt till ett nätverkssegment för att kunna utföra uppgifter som uppdatering och kontroll av loggar och mjukvara.

Om Citrix inte är möjlig eller tillräcklig så kan en vanlig VPN-uppkoppling upprättas. Det sker bara i undantagsfall och efter en kontroll att behovet verkligen finns. Primärt sker även denna uppkoppling till en virtuell maskin (dock ej Citrix). Endast i nödfall tillåts åtkomst av ett nätverkssegment genom en direkt VPN-uppkoppling mot måldatorn.

4.2.4 Behörighetskontroll

Rättigheter och åtkomst till de olika vårdsystemen i det fallstuderade universitetssjukhuset (t.ex. journalsystemet Cosmic) genomförs i flera steg. Först läggs personen in i hälso- och sjukvårdens adressregister (HSA). IT använder en managementmodul som automatiserat överför HSA-data till det lokala Active Directory:t[37] (AD). Det finns flera färdiga profiler med olika sorters behörighet på maskinerna beroende på vilken roll användaren har i organisationen. Ute på enheterna i vården finns en IT-ansvarig som tilldelar personalen rätt accesskategori. Först när hela kedjan har gåtts igenom kan den nye användaren logga in på systemet. IT-avdelningen sköter allt fram till det sista steget då rättighetskategorin delas ut. Systemet är till stora delar automatiserat vilket ger säkerhet och kontroll över vilka som läggs till och vilken tillgång de kommer få till systemets olika delar.

IT är ansvariga för att de ute i vården har tillgång till att sätta accessrättigheter till sin personal. Vårdpersonalen (IT-ansvariga som är vanlig vårdpersonal) ute på enheterna är ansvariga för att rätt privilegier tillsätts.

[37] Ett Active Directory är en tjänst för att lägga till och ta bort datoranvändare samt rättigheter för dessa datoranvändare rörande exempelvis mappar, filer, programvara och exekvering.

5 Incidenter – orsaker, konsekvenser och åtgärder

Detta kapitel besvarar forskningsfråga 2: *Vilka incidenter har inträffat inom hälso- och sjukvård?* Utöver detta söks det svar på följande frågor:

- *Vilka är de primära orsakerna till dessa incidenter?*
- *Vilka konsekvenser har dessa incidenter fått?*
- *Vilka åtgärder bör tas för att motverka förekomsten och effektivisera behandlingen av dessa incidenter?*
- *Vilka av dessa incidenter har inträffat på grund av IT-angrepp?*

5.1 Litteratur

Det har genomförts vetenskapliga studier för att kartlägga hur ofta säkerhetskritiska IT-fel uppstår i inbyggda system för medicinsk utrustning. Säkerhet behöver i denna bemärkelse inte röra faktiska angrepp, utan mer problem i allmänhet. Alemzadeh m.fl. [2] studerade fel inom medicinsk utrustning som beskrivs i MAUDE och MREDR mellan 2006 och 2011. Under denna period registrerades 1 154 451 negativa händelser orsakade av medicinska inbyggda system (kartlagda genom MAUDE) och 5294 återkallade felaktiga typer av medicinska inbyggda system (kartlagda genom MREDR). De negativa händelserna rörde tre olika fall: (i) en funktionsstörning utan konsekvens för patienten, (ii) en funktionsstörning som gav uppgav till patientskada, eller (iii) en funktionsstörning som gav uppgång till dödsfall. Återkallelse utförs på begäran av de ansvariga för felaktiga inbyggda system, såsom utvecklare och distributörer. Av de 5294 återkallelserna rörde 1210 datorbuggar korresponderande till totalt 12 024 836 inbyggda system världen över.

FDA klassar alla återkallelser baserat på hur säkerhetskritiska de är på en skala från 1-3. *Klass 1* innebär att det finns en rimlig sannolikhet att systemet kommer ge kritiska hälsoproblem eller dödsfall. *Klass 2* innebär att systemet kan ge tillfälliga eller reverserbara hälsoproblem eller en liten risk för kritiska hälsoproblem. *Klass 3* innebär system som bryter mot FDAs regelverk men sannolikt inte ger kritiska hälsoproblem. Alemzadeh m.fl. [2] fann att de allra flesta typer av återkallelser rör klass 2-fel och mjukvara (718 av 1210 återkallade produkttyper), medan de flesta produkter återkallas på grund av hårdvarufel (4.2 miljoner av 12 miljoner återkallade produkter).

Författarna fann även att de datorrelaterade återkallelserna rörde felkonsekvenser av sex olika slag: (i) alarm eller meddelandefel (t.ex. missade alarm), (ii) fysiska risker (t.ex. elchocker), (iii) bildfel (t.ex. felaktig information), (iv)

behandlingsavbrott (t.ex. infusionsavbrott), (v) systemoperationsfel (t.ex. att systemet ej startar upp), samt (vi) beräknings- och presentationsfel (t.ex. att patientinformationen är korrupt). Av dessa felkonsekvenser var de flesta återkallelserna kopplade till beräknings- och presentationsfel (335 återkallelser), och behandlingsavbrott kopplat till flest återkallelser av klass 1 (18 återkallelser).

Alemzadeh m.fl. [2] studerade även hur datorrelaterade återkallelser hanterades och fann fem olika typer av återkallelsehantering: (i) enbart notifiering (angående produktens problem), (ii) (undermåliga) instruktioner för reparation, (iii) instruktioner kring mjukvaruuppdatering, (iv) återsändning av produkt till utvecklare för reparation, och (v) återsändning för utbyte eller avveckling. Av dessa är mjukvaruuppdateringar vanligast (58% av alla åtgärder). Näst vanligast är säkerhetsnotifieringar/instruktioner (20% av alla åtgärder). Tredje vanligast är produktutbyten/produktborttagning (13% av alla åtgärder). Reparationer står för 9% av alla åtgärder. Liknande studier har utförts av Bliznakov m.fl. [6], Wallace och Kuhn [42] samt Kramer m.fl. [34]. Dessa författare studerade, likt Alemzadeh m.fl. [2], återkallelser registrerade inom MREDR och i fallet med Kramer m.fl. också negativa avvikelser registrerade inom MAUDE. Dock mellan 1983 och 1997 (Wallace och Kuhn), 1999 och 2005 (Bliznakov m.fl.) samt 2002 och 2011 (Kramer m.fl.). Dessa studier fann, likt Alemzadeh m.fl., att mjukvara är en stor felorsak.

Fu [15][16] summerar den vetenskapliga forskningen kring säkerheten i inbyggda medicinska system. Förutom diskussion kring resultaten presenterade i Alzemadeh m.fl. [2], Bliznakov m.fl. [6], Kramer m.fl. [34] och Wallace och Kuhn [42] beskriver Fu [15][16] att det inte finns några (för USA) systematiska nationella rapporteringssystem för säkerhetsincidenter. Exempelvis innefattar inte MAUDE-databasen någon kategori för problem orsakad av skadlig kod.

Det är därmed inte sagt att skadlig kod inte förekommer. Filkins [14] presenterar statistik kring skadlig kod inom hälso- och sjukvård som registrerats av SANS genom studier av nätverkstrafik. Totalt identifierades cirka 50 000 IT-säkerhetsrelaterade händelser omfattande 723 IP-adresser inom 375 hälso- och sjukvårdsrelaterade organisationer. Diverse olika system identifierades, bland annat bildhanteringsmjukvara (t.ex. PACS/RIS), videokonferenssystem, telefonsystem och perimetersystem (t.ex. brandväggar och routrar). Av särskilt intresse är att system som är tänkta att förmedla IT-säkerhet, nämligen brandväggar och VPN-servar, innefattade överlägset högst andel skadlig kod. Det bör dock poängteras att denna statistik förmodligen är uppblåst av faktumet att brandväggar och VPN behandlar/förmedlar trafik för andra system såsom kontorsdatorer. Majoriteten av dessa datapunkter är därmed sannolikt skadlig kod som skickats från andra system. Att denna trafik inte blockerats tyder dock på bristande säkerhetskontroller, vilket i sig är problematiskt.

Deursen m.fl. [41] studerade informationssäkerhetsrisker inom hälso- och sjukvård genom att skicka ut en enkät till ansvariga för incidentrapportering samt

att låta experter utvärdera sannolikheten för olika riskscenarior (skapade med hjälp av data från enkäten). Den sammanlagda empirin involverade 117 enkätsvar och tolv experter. Ett riskscenario kan exempelvis vara att epost skickas till fel person eller att ett lösenord delas med någon annan. De fem mest sannolika riskscenarierna som identifierades av Deursen m.fl. var: (i) att obevakade tillgångar försvinner (7% av alla incidenter), (ii) att lösenord delas (7%), (iii) att epost skickas till fel personer (6%), (iv) stöld (5.7%) och (iv) att patientinformation felaktigt lämnas ut på grund av at procedurer inte följs.

Lei et al. [26] studerade IT-relaterade incidenter inom hälso- och sjukvård genom att analysera populärvetenskapliga nyheter identifierade via Google och Baidu (den största sökmotorn som används i Kina). Denna studie identifierade 116 IT-relaterade incidenter som inträffat mellan 2001 och 2012. Författarna extraherade bland annat den förmodade nedtiden för varje incident, vilka konsekvenser som gavs (t.ex. antal påverkade patienter och antal dödsfall), samt när och var de inträffade. Författarna identifierade bland annat att de flesta incidenter inträffade på morgonen samt att de flesta registrerings-/betalningsfelen berodde på kapacitetsproblem såsom överbelastade nätverk.

På James Haley Veterans' Hospital i Tampa (USA) hittades datormasken Conficker på 104 system, bland annat en röntgenmaskin, mammografienhet samt en gammakamera för nukleära medicinska studier [43]. En kontorsmaskin som blir infekterad av skadlig kod kan snabbt kontamineras och rensas. Om det inträffar i medicinsk utrustning som påverkar patientsäkerheten kan verksamheten dock ligga nere under lång tid. I New Jersey stängdes ett kritiskt laboratorium [16] ner under januari 2010. Skadlig kod hade infekterat datorsystemen och konsekvensen blev att personalen inte kunde lita på systemen. Detta ledde till att det inte gick att säkerställa att patienterna fick en säker vård. Det finns därmed skäl att tro att mörkertalet som ej tas hänsyn till av [2], [6], [34] och [42] är stort.

Det finns ingen empirisk vetenskaplig forskning motsvarande den gjord av [2], [6], [14], [26], [34], [41] och [42] för datorrelaterade incidenter inom hälso- och sjukvård i Sverige. Däremot har det utförts ett antal andra svenska studier av IT inom hälso- och sjukvård som är relevanta för denna studies forskningsfrågor. Dessa beskrivs i följande stycken.

Andersson och Ewald [3] från MSB presenterar en omfattande studie angående om dagens rutiner och resurser är tillräckliga för att upprätthålla en verksamhet rörande läkemedelshantering i händelse av störningar. Studien analyserar bland annat cirka 52 000 incidenter som inträffat inom hälso- och sjukvård inom Västra Götalandsregionen (varav 207 ansågs som tillräckligt allvarliga för att motivera lex Maria-anmälningar). Studien visar bland annat att verksamhetsprocesser genomgår effektivisering, vilket kan göra verksamheten mindre motståndskraftig mot störningar. Den visar också att läkemedelshantering är en komplex process med möjliga störningar i allt från produktion till användning, och att dess kontinuitets- och krishanteringen är bristfällig.

Angantyr m.fl. [4] utförde under 2011 för Socialstyrelsens räkning en studie av fyra olika IT-haverier som inträffat inom vården:

- *En datormask i Region Skåne under 2009*. Cirka 10 000 datorer och 500 servrar smittades. Konsekvenserna involverade bland annat att det inte gick att läsa patientjournaler, att centralenheten i intensivvårdsövervakningen inte fungerade, att remisser varken kunde skickas eller läsas, att patientadministrativa system ej var åtkomliga, att arbetsstationer kopplade till diagnostik- och laboratorietjänster inte kunde användas, att e-posten inte fungerade, att Internet inte var nåbart och att operativa MTP:er inte fungerade som de var tänkta att göra. Dessa problem varade från den 3 januari till den 26 mars 2009.
- *Ett journalsystembortfall inom Stockholms läns landsting under 2008*. Det elektroniska patientjournalsystemet TakeCare fick på grund av mjukvarufel (i en databas) onormalt långa svarstider vilket ledde till att viss patientdata förlorades och att säkerhetsriskerna vid undersökning och behandling av patienter ökade. Dessa problem varade i cirka 25 timmar.
- *Ett datorhaveri i en serverhall på Länssjukhuset i Kalmar under 2008*. Problem med kylsystemet innebar att 240 servrar var tvungna att stannas. Kontakten med alla vårdinformationssystem och journalsystem förlorades, vilket likt journalsystemsbortfallet i Stockholm medförde säkerhetsrisker vid undersökning och behandling av patienter. Problemen varade i cirka 6 timmar.
- *Förlorade bilder i bildhanteringssystemet i landstinget i Uppsala län under 2009*. Ett nytt PACS/RIS-system beställdes 2004 och driftsattes under 2008 trots att alla granskningstester inte var genomförda. Problem med funktion och säkerhet inträffade under slutet av 2008 och 2009 och ett totalt stopp inträffade den 3 februari 2009 då alla bilder försvann.

Stockholms Läns Landsting (SLL) genomförde under 2014 en översiktlig studie av IT-säkerheten kring MTP:er inom SLL, Danderyds sjukhus, Karolinska universitetssjukhuset och Södertälje sjukhus [24]. Studien granskade styrning och kontroll av IT-säkerheten för nätverksanslutna MTP:er inom de fyra aktörerna och kom fram till att arbetet med IT-säkerhet behöver förbättras. Studien begränsade sig dock till att undersöka förekomsten av övergripande riktlinjer och hantering av dem. Den säger därmed ingenting om den *faktiska statusen* för IT-säkerhet inom hälso- och sjukvård.

IT-utvecklingen inom Sveriges landsting studeras årligen av SLIT (Landstingens IT-strateger/IT-chefer), med den senaste rapporten publicerad 2014 [21]. Den senaste studien fann att IT inom landstingen har ungefär samma resurser som för 10 år sedan, vilket står i skarp kontrast till ambitionen att öka satsningarna inom IT-området. Detta förmodas skapa problem då antalet användare under samma

period har ökat med cirka 90%. Studien visar också att anställda har i snitt en dator var.

Användarnas (t.ex. läkare, läkarsekreterare och sjuksköterskor) upplevelser av IT inom vården studerades 2010 av UserAwards och Vinnova [20]. Denna studie omfattade intervjuer, observationer och en enkät. Resultaten visar att implementationen av IT-systemen de senaste tre åren inte har lett till att användarna har fått mer tid för patienten, och att vården inte heller anpassats bättre för varje enskild patients behov. Enkätstudien visade exempelvis att mycket tid skulle kunna sparas om systemen alltid fungerade som användarna önskat: läkare 56 minuter, sjuksköterskor 35 minuter, undersköterskor 17 minuter och läkarsekreterare 42 minuter (d.v.s., mer än fem miljarder kronor per år). Däremot har det lett till att datormiljön har blivit mer sammanhållen och att patientsäkerheten ökat (då information är mer lättillgänglig).

En liknande studie utfördes under 2013 av Socialdepartementet [36]. Resultaten från denna studie överensstämmer relativt väl med resultaten från [20]. Användarna anser att morgondagens IT-system för hälso- och sjukvård behöver följa arbetsprocesserna avsevärt bättre än vad som görs idag. Systemen ska vara överskådliga, ta kort tid i anspråk för att förstå och navigera i samt ge användaren en känsla av kontroll, i motsats till dagens dubbelkontroller som användarna gör i och mellan system, av både information och dokumentation. Studierna av Vinnova och Socialdepartementet fokuserar dock på MTP:er som IT driftar, såsom patienthanteringsystem. MTP:er med inbyggda tekniska system, såsom infusionspumpar ligger utanför studiernas omfång.

Vissa studier av specifika MTP:er förekommer också. En litteraturstudie om infusionspumpar som utfördes av Davidsson m.fl. [9] under 2008 visade att risker relaterade till användning av infusionspumpar rörde fyra egenskaper: (i) undermålig design som leder till programmeringsmisstag, (ii) produktfel i mjukvara eller hårdvara, (iii) brister i arbetsmiljön (till exempel hög arbetsbelastning), samt (iv) brist på övning och utbildning.

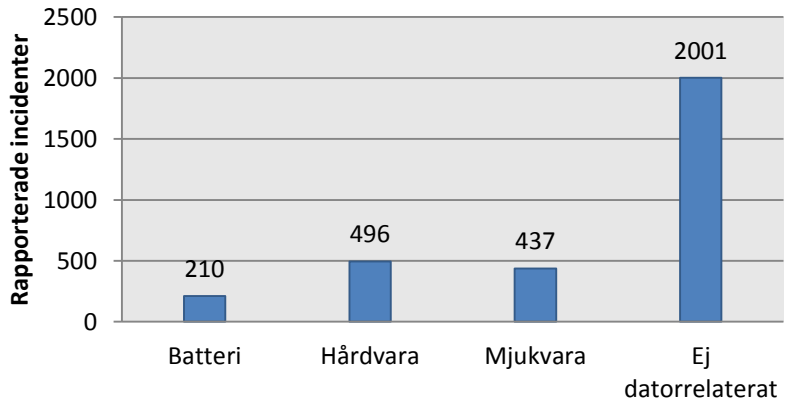
Risker rörande infusionspumpar studerades även av Läkemedelsverket under 2014 [23]. Denna studie involverade en enkät som besvarades av 35 sjukhus. Resultaten från studien visade att cirka 18 000 infusionspumpar nyttjas av de 35 sjukhusen och att både mjukvara, hårdvara och användargränssnitt kan skapa problem. Rapporten visar också att många händelser aldrig rapporteras till Läkemedelsverket, vare sig av tillverkare eller av hälso- och sjukvården.

Studierna kring IT-utvecklingen inom hälso- och sjukvård ([23], [24], [3], [4], [9], [20], [21], och [36]) kan lätt ge en bild av att ”IP-fieringen” enbart har skapat negativa konsekvenser. Detta är dock framförallt en produkt av att studierna utgår ifrån att IT bör finnas i vården, och fokuserar på att analysera dess effekt utan att jämföra med hur det var innan införandet av IT. Utan IT-stöd skulle de allra flesta aktiviteter, såsom patientregistrering, remisser, patientövervakning och

artroskopiska operationer bli långt mer omständiga att utföra [37]. Något som i sin tur skulle ha en negativ effekt på patientsäkerheten.

5.2 Resultat och analys

Det översiktliga resultatet av kategoriseringsarbetet som utfördes med hjälp av NLTK och REIDAR kan ses i Figur 9. 30% av alla incidenter är datorrelaterade och rör kombinationer av batteriproblem (24% av alla datorrelaterade incidenter), datorhårdvaruproblem (57%) eller datormjukvaruproblem (50%)[38]. Dessa siffror överensstämmer relativt väl med de som identifierades av Alemzadeh m.fl. [2] för FDA:s databaser där 23% av alla incidenter var datorrelaterade, 20% rörde batterier, 35% rörde hårdvara och 19% rörde mjukvara[39]. Detta betyder att resultat från Alemzadeh m.fl. [2] troligen är tillämpbara även för hälso- och sjukvården i Sverige. De ej datorrelaterade händelserna i REIDAR behandlas inte vidare i detta kapitel (utöver statistiken i Figur 11).



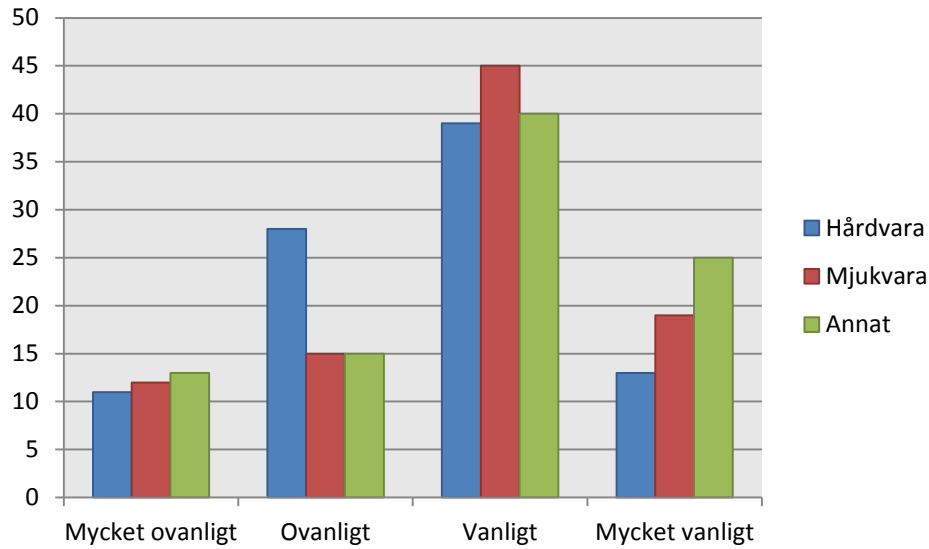
Figur 9. Översikt av incidenter i REIDAR.

En översikt av orsakerna bakom incidenter enligt enkäten ges av Figur 10. Ej datorrelaterade orsaker har högst antal ”mycket vanligt”, vilket stämmer väl överens med resultatet från REIDAR (där 70% av alla incidenter rör ej datorrelaterade händelser). Relationen mellan hårdvaru- och mjukvarurelaterade

[38] Siffran överstiger 100% då en incident kan röra både batteri, hårdvara och mjukvara. Varför Alemzadeh m.fl. [2] inte identifierade incidenter som rör kombinationer av olika typer av datorrelaterade problem är för denna studie oklart.

[39] Förutom dessa kategorier har Alemzadeh m.fl. även kategorierna ”I/O” (2%) och ”annat” (24%). Dessa kategorier involverar en kombination av mjukvara och hårdvara (se fotnot 22).

incidenter skiljer sig dock – enligt enkäten är mjukvaruproblem vanligare än hårdvaruproblem.

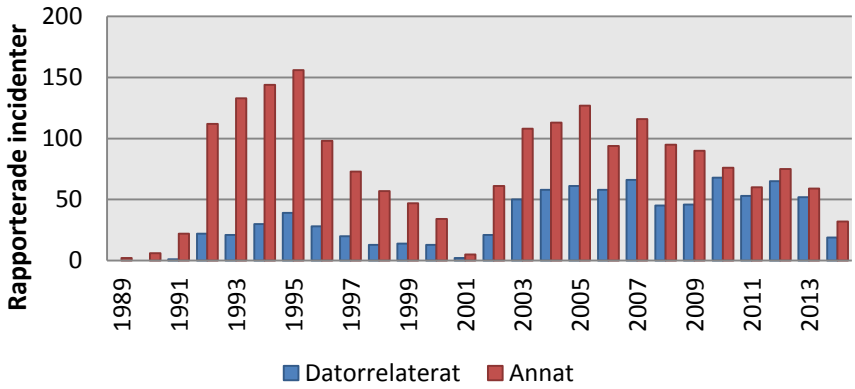


Figur 10. Orsaker bakom incidenter enligt enkät.

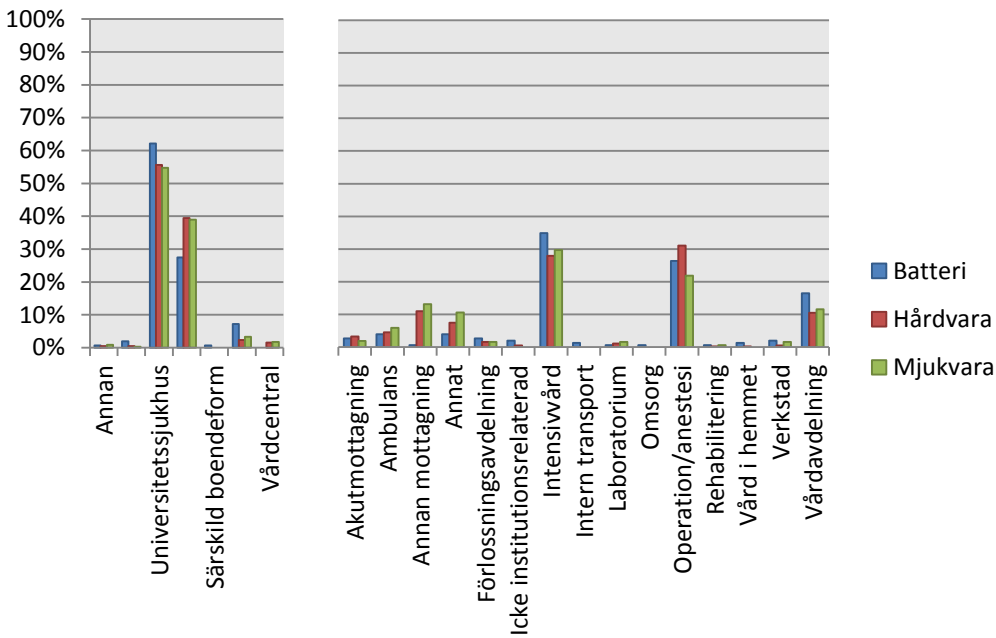
En översikt av när incidenterna i REIDAR rapporterades kan ses i Figur 11 (nummer 2 i Tabell 2). Databasen omfattar totalt 2867 incidenter, inrapporterade mellan 1989 och 2014, med ett snitt på 110 incidenter per år. Som kan ses i figuren ökar antalet datorrelaterade incidenter, medan icke-datorrelaterade incidenter minskar (1991 gick det 22 icke-datorrelaterade incidenter på varje datorrelaterad incident; 2013 var denna siffra 1.1). En tolkning av Figur 11 är även att datakvaliteten för incidenter inträffade mellan 1997 och 2002 är lägre än de övriga (oavsett om det gäller datorrelaterade incidenter eller inte)[40]. Dessutom är (som beskrivs i avsnitt 3.3.2) mörkertalet mycket högt - givet en 1% rapporteringsfrekvens så bör det totala antalet incidenter per år vara cirka 11 000.

Socialstyrelsens statistik över antalet vårdanställda i Sverige[41] visar att det under 2012 (det senast tillgängliga året) fanns 308 086 anställda i Sverige inom hälso- och sjukvårdssektorn. Givet dessa siffror inträffar i snitt 0,035 incidenter per anställd och år, vilket indikerar att en siffra på 11 000 kanske till och med är lågt räknat. Resultatet som presenteras i detta avsnitt bör läsas med detta i åtanke.

[40] Det är oklart varför så är fallet.
[41] http://www.socialstyrelsen.se/statistik/statistikdatabas/halsoochsjukvardspersonal



Figur 11. Rapporteringsfrekvens till REIDAR.



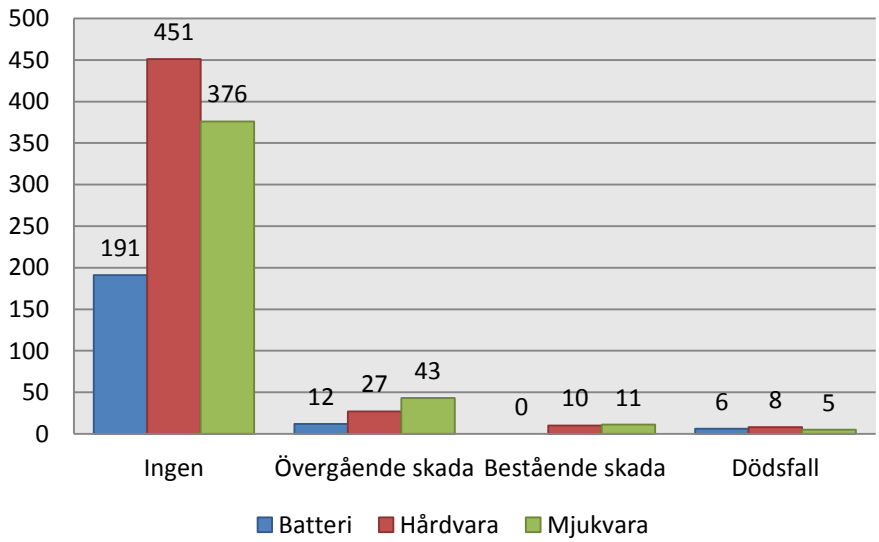
Figur 12. Procentuell fördelning av olika typer av datorrelaterade incidenter över vårdplatser (till vänster) och mottagningar (till höger) i REIDAR.

Den procentuella fördelningen av olika typer av datorrelaterade incidenter i REIDAR över olika vårdplatser och mottagningar ges av Figur 12 (nummer 12 och 13 i Tabell 2). Som kan ses inträffar de allra flesta datorrelaterade incidenter

(oberoende av typ) inom intensivvården, operation och vårdavdelningar inom universitetssjukhus/sjukhus. Med undantaget för *annan mottagning* (där batterifel är extremt ovanliga) finns det inga signifikanta skillnader rörande den procentuella fördelningen av olika typer av datorfel i olika vårdplatser och avdelningstyper.

5.2.1 Orsaker och konsekvenser

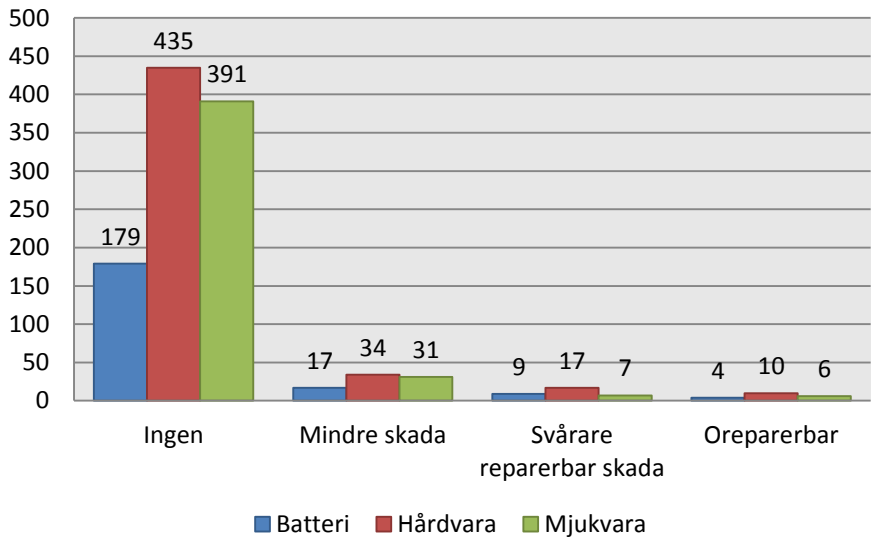
En översikt av olika typer av patientskador som inträffar på grund av olika typer av datorrelaterade incidenter kan ses i Figur 13 (nummer 19 i Tabell 2). Majoriteten av de incidenter som rapporterats in i REIDAR (89%) orsakade ingen patientskada alls. Cirka två av hundra incidenter (1.7%) orsakade dödsfall. Det finns inga tydliga korrelationer mellan datorrelaterad orsak och utfall – med undantaget för att kopplingen mellan batterier och bestående skador ger alla orsaker alla möjliga utfall. Anomalin för batterier är sannolikt resultatet av den begränsade mängden batterirelaterade incidenter i REIDAR. När det gäller skador för vårdpersonal (nummer 20 i Tabell 2) ledde inga incidenter till dödsfall, endast en incident till en bestående skada och 13 incidenter till övergående skador (av 1142 dataposter).



Figur 13. Patientskador som en följd av datorrelaterade incidenter i REIDAR.

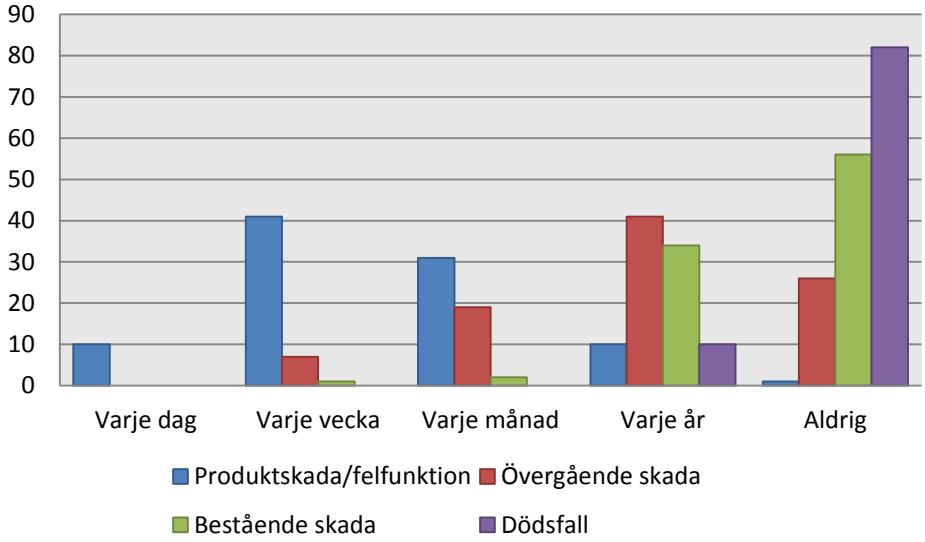
En översikt av produktskador som en följd av olika typer av datorrelaterade incidenter illustreras i Figur 14 (nummer 21 i Tabell 2). De allra flesta incidenter (88%) ger ingen produktskada över huvud taget. Det är intressant att mjukvaruproblem ger produktskador ungefär lika ofta som hårdvaruproblem. Två huvudsakliga orsaker till detta har identifierats utifrån det insamlade materialet:

- Det är svårt att uppdatera mjukvaran i MTP:er på grund av deras isolering och de juridiska egenskaperna som är involverade. På grund av juridiska orsaker är det även svårt för produktleverantörer att snabbt behandla buggar och säkerhetsproblem som upptäcks i produkter.
- Datorrelaterade incidenter rör ofta (26% av alla datorrelaterade incidenter) kombinationer av både mjukvaruproblem och hårdvaruproblem.



Figur 14. Produktskador som en följd av datorrelaterade incidenter i REIDAR.

En översikt av konsekvenserna som ges av incidenter identifierade via enkätstudien kan ses i Figur 15. Produktskador är mer vanligt förekommande än patientskador, övergående patientskador är vanligare än bestående patientskador och bestående patientskador är vanligare än dödsfall. Enkätresultatet gällande patientskador korrelerar väl med REIDAR medan produktskador bedöms vara vanligare enligt enkätsvaren än det REIDAR förmedlar.



Figur 15. Konsekvenser av incidenter enligt enkät.

Totalt finns det 665 produkttyper och 1656 olika modeller som har varit inblandade i incidenter kartlagda i REIDAR. De tio produkttyperna med flest datorrelaterade incidenter beskrivs i Tabell 7. Analys av orsaksområdena (batteri, hårdvara eller mjukvara) visar att batterier är inblandade i varje incident med hjärtstimulatorer och därmed ett stort problem för denna produkttyp. Hårdvara är ett stort problem för alla produkter utom externa hjärtstimulatorer, och i synnerhet för övervakningssystem av olika slag. Mjukvara är ett problem för alla produkter förutom externa hjärtstimulatorer/defibrillatorer. De allra flesta incidenter (oavsett produkt) ger ingen patientskada alls. Dialysapparatur (hemo) och externa hjärtstimulatorer ger flest övergående skador. Lungventilatorer ger flest dödsfall. Dessa resultat är logiska, givet funktionen för dessa produkter. Exempel på incidenter för de fyra vanligaste produkterna är:

- *Infusionspumpar:* för mycket eller för lite infusionsmedel levereras till patienten, displayer fungerar inte och batterier är urladdade.
- *Lungventilatorer*: ger inte bara näst flest datorrelaterade incidenter överlag, utan även flest dödsfall av alla produkttyper (tre stycken). Ett dödsfall skedde på grund av att MTP:en kopplades till ett strömlöst uttag; ett annat fall på grund av att datorhårdvaran i respiratorn var trasig; i det tredje fallet på grund av ett mjukvarufel i respiratorn.

- *Grundenhet för övervakning av patient*: fel information visas på skärmen, batterier laddas inte och trasiga ljudkort. Dödsfallet inträffade på grund av att produktens ljudlarm hade kortslutits.
- *Mobil anestesiapparatur:* mjukvaran ger felaktiga larm (kring mixade nedsövningsgaser), ventilatorskärmar slocknar under användning och fel anestesigas visas på skärmdisplayen under drift.

Tabell 7. De tio produkttyperna med flest datorrelaterade incidenter i REIDAR.

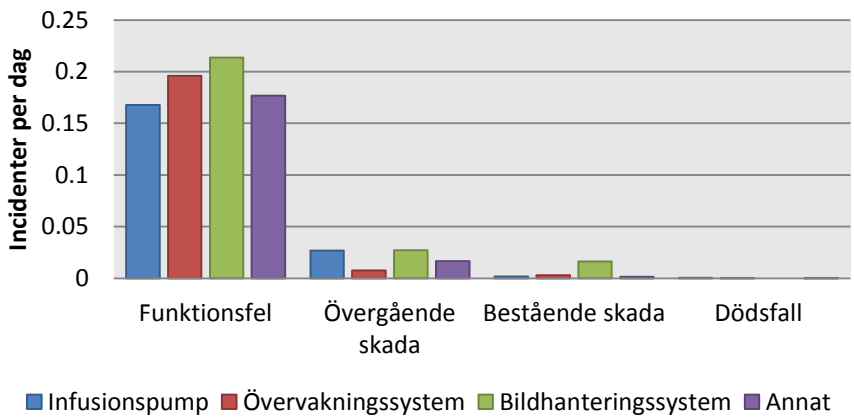
Medicinteknisk produkt	Incidenter	Orsak			Patientskada			
		Batteri	Hårdvara	Mjukvara	Ingen	Övergående skada	Bestående skada	Dödsfall
Infusionspump	99	38%	34%	57%	93%	7%	0%	0%
Ventilator (för lungor)	65	43%	42%	32%	86%	9%	0%	5%
Grundenhet för övervakning av patient	57	14%	89%	39%	98%	0%	0%	2%
Mobil anestesiapparat	43	14%	77%	40%	98%	0%	2%	0%
Dialysapparat hemo	27	4%	37%	74%	78%	19%	0%	4%
Extern hjärtstimulator	21	100%	10%	0%	86%	14%	0%	0%
Defibrillator	18	61%	50%	11%	94%	0%	0%	6%
Övervakningscentral grundenhet	16	0%	88%	63%	94%	0%	0%	6%
Manuell defibrillator	15	47%	67%	13%	93%	7%	0%	0%
Tillsatsenhet för övervakning av patient	12	25%	83%	33%	100%	0%	0%	0%

Resultaten från REIDAR-analyserna överlappar delvis med det som presenteras av Alemzadeh m.fl. [2] rörande återkallade MTP:er i USA mellan 2006 och 2011 (MAUDE och MREDR, se avsnitt 5.1). Produktåterkallelser är inte helt jämförbara med produktincidenter (exempelvis kan en återkallelse involvera åtskilliga incidenter och dess åtgärder innefattar inte utbildning), men säger fortfarande något om hur det ser ut i Sverige jämfört med USA. Infusionspumpar, övervakningssystem och defibrillatorer är vanligt förekommande i båda databaserna. Incidenter rörande bildhanteringssystem (t.ex. PACS/RIS-system) är vanligt förekommande i USA men inte i Sverige (nyckelordssökningen identifierade endast 19 incidenter som involverade PACS/RIS i Sverige). Detsamma gäller pacemakers, som är problematiska i USA men endast är involverade i en enda datorrelaterad incident i Sverige.

Resultatet överlappar även till stor del med resultatet från enkätstudien (se Tabell 8). Infusionspumpar ses som det största problemområdet, följt av övervakningssystem och bildhanteringssystem (t.ex. PACS/RIS). En orsak till att bildhanteringssystem är problematiska enligt Alemzadeh m.fl. [2] och enkäten, men inte i REIDAR kan vara att avvikelser med bildhanteringssystem rapporteras via andra system än de som slussar data till REIDAR. Exempelvis nyttjade det fallstuderade universitetssjukhuset två olika system för rapportering av incidenter – Medusa (av MT-enheten) och Synergi (av IT-enheten). Av dessa rapporterades endast information från Medusa in till REIDAR, medan Synergi ofta innehöll incidenter kring bildhanteringssystem såsom PACS/RIS.

Tabell 8. Översikt av problematiska produkter enligt enkätstudien.

Medicinteknisk produkt	Mest problematisk	Näst mest problematisk	Tredje mest problematisk	Summa
Infusionspump	11	8	2	21
Övervakningssystem	4	4	6	14
Bildhanteringssystem	0	5	4	9
Annat	21	13	15	49



Figur 16. Incidentfrekvenser för produkter enligt enkät.

Den relativa incidentfrekvensen per dag kan beräknas givet det konservativa antagandet att varje dag/vecka/månad/år innebär en incident per dag/vecka/månad/år. Resultatet för de olika problematiska produkterna (normerat mot antal produkter) kan ses i Figur 16. Fördelningen är relativt lik för produkterna och liknar även resultatet från REIDAR. Det är dock intressant enkäten visar att problem med infusionspumpar påstås vara involverade i dödsfall – detta är något som inte rapporterats en enda gång i REIDAR.

Infusionspumpar har tidigare detaljstuderats av Davidsson m.fl. [9] och Läkemedelsverket [23]. Resultaten från dessa studier överensstämmer relativt väl med de som ges av enkätstudien och REIDAR: Fördelningen i REIDAR stämmer delvis överens med fördelningen i Läkemedelsverkets studie [23] (mjukvara är klart mest problematisk enligt båda, men med batterier på andra plats i REIDAR och hårdvara på andra plats i enkäten). Enkätresultatet att infusionspumpar kan orsaka dödsfall stöds av Läkemedelsverkets studie, där infusionspumpar anses kunna orsaka både bestående skador och dödsfall [23].

Totalt 52 kommentarer gavs på enkätens tre öppna frågor rörande problem med produkter, med en stor spridning kring innehåll. Det vanligast kommenterade problemet var att systemen och deras kopplingar har blivit för komplexa (elva kommentarer), exempelvis:

> ”*Flera problem är relaterade till kombinationen av olika mjukvaror och överföring av patientdata mellan systemen*.” och
>
> ”*Ofta komplexa miljöer vilket innebär att det är svårt att veta vad en förändring i miljön kan skapa för konflikter*.”.

Det näst mest diskuterade problemet rörde infusionspumpar av olika slag, som anses vara för komplexa och kvalitetsundermåliga (nio kommentarer). Exempelvis:

> ”*Tillverkare har mer eller mindre säkra lösningar t.ex. för mätning av occlusionstryck. Ofta är sprutpumpar avsedda för flera fabrikat av sprutor och det verkar vara mycket svårt för tillverkaren att säkerställa kvalitén för detta engångsmaterial - detta påverkar säkerheten till stor del och det blir inte bättre av att vi har en mycket svag standard för sprutor som egentligen inte tar hänsyn till den kvalitetsnivå som behövs för användning i sprutpumpar*.”,
>
> ”*Dessa produkter har blivit programmerbara vilket ställer stora krav på organisation och förvaltning så att användarna kan förutse utrustningens beteende*.” och
>
> ”*Problemen uppstår pga att det finns en kunskapsbrist i kombination med en övertro på vad infusionspumpar kan larma för*.”.

De resterande kommentarerna är spridda, från att produkter går sönder när de tappas till att användargränssnitt är för komplicerade.

Slutligen presenteras de tio leverantörerna med flest datorrelaterade incidenter i REIDAR i Tabell 9. Vid tolkningen av denna tabell bör läsaren ha i åtanke att det inte är känt hur många produkter som är operationella ute i vården, utan endast hur många produktvarianter (modeller) som olika leverantörer har. Det är därför inte möjligt att säga någonting om kvaliteten på produkter från olika leverantörer. Det är även så att relativt få modeller i leverantörernas sortiment är drabbade av

incidenter. Exempelvis är endast 33 av Phillips 626 modeller (cirka 5%) involverade i incidenter. En analys med grund i leverantörer bidrar ändock med värde då det är möjligt att jämföra normerade datamängder, i synnerhet angående incidentorsaker och påföljande patientskador. De bakomliggande orsakerna till incidenter varierar mellan olika leverantörer. Exempelvis har Medtronic nästan uteslutande batteriproblem, medan Gambro nästan uteslutande har mjukvarurelaterade problem. Gällande patientskador så har incidenter för vissa leverantörer medfört en större andel patientskador än för andra leverantörer. Exempelvis har incidenter involverande Datex inte medfört några patientskador alls medan 25% av alla incidenter som inträffat för Fresenius gav någon typ av patientskada.

Tabell 9. De tio leverantörerna med flest datorrelaterade incidenter i REIDAR[42].

Leverantör	Modeller	Incidenter	Orsak			Patientskada			
			Batteri	Hårdvara	Mjukvara	Ingen	Övergående skada	Bestående skada	Dödsfall
Dräger	18	55	15%	75%	44%	96%	4%	0%	0%
Philips	33	50	10%	86%	64%	86%	10%	2%	2%
Alaris	8	33	30%	36%	58%	88%	12%	0%	0%
Marquette	19	32	13%	84%	34%	91%	0%	3%	3%
Siemens	17	29	24%	55%	38%	93%	3%	3%	0%
Datex	8	27	19%	85%	11%	100%	0%	0%	0%
Medtronic	5	24	88%	17%	8%	83%	17%	0%	0%
Ortivus	11	20	15%	80%	80%	90%	5%	0%	5%
Gambro	12	19	5%	11%	95%	84%	16%	0%	0%
Fresenius	7	16	6%	31%	69%	75%	19%	0%	6%

5.2.1.1 Riktlinjer och kompetensutveckling

Totalt 24 respondenter svarade på enkätfrågan om det finns specifika riktlinjer kring MTP:er som försvårar det dagliga arbetet. Fyra av dessa svarade nej. Av de övriga 20 nämnde fem de luddiga gränserna mellan IT och MT (med påföljande riktlinjer), exempelvis:

> ”*Diffust gränsland mellan IT och MTA medicinteknisk verksamhet. IT och MTA står inte under samma organisation och kan därmed inte dra*

[42] Se även text ovan för förklaring av tabellen.

> *gemensamma riktlinjer samarbete (olika chefer sitter på olika ställen). Inköp, upphandling och MTA/IT är inte under samma organisation. Flera IT-system köps in utan att IT har fått med krav för att klara att handha hjälp till att supporta systemen*.” och
>
> ”*Landstingsledningens uppdrag till IT-direktören att styra samtidigt som IT-direktören inte är kompetent eller förstår sjukvårdens krav*.”

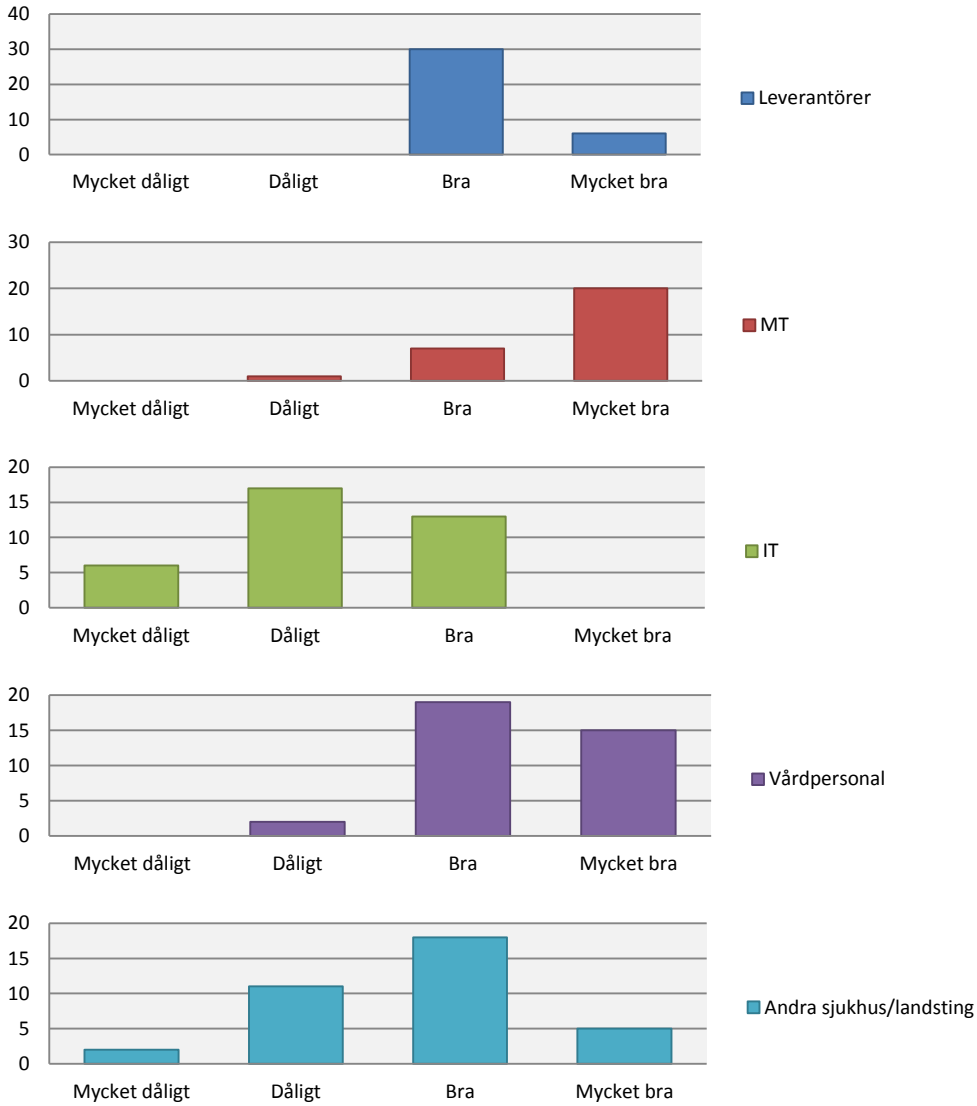
Tre respondenter nämnde lagen om offentlig upphandling, vilken anses skapa problem då den bidrar till en heterogen systemmiljö där samma typ av produkt kan kräva fundamentalt skilda handhavanden (vilket blir en säkerhetsrisk). Tre respondenter nämnde patientdatalagen, exempelvis:

> ”*Patientdatalagen, PDL, kolliderar fullständigt med regelverket för MTP. Det pågår en översyn av PDL. Det hade varit bra om förslaget om en ny Hälso- och sjukvårdsdatalag harmoniserade med Lagen om MTP och att Läkemedelsverket fick i uppdrag att ta fram författningen om behörighetssystem till MTP*.”

Två respondenter nämnde att riktlinjer från leverantörer ibland är felaktiga. De resterande sju respondenterna gav varierande svar, från att all dokumentation bör kunna ges ut på engelska istället för svenska (vilket skulle öka produktkonkurrensen) till att viss förenklad egentillverkning bör vara möjlig.

Totalt 29 respondenter svarade på frågan gällande om någon typ av kompetensutveckling behövs. Sju av kommentarerna rörde att verksamheten (t.ex. läkare och sjuksystrar) behöver lära sig mer om hur MTP:er och IT-system fungerar. Sex rörde att IT-ansvariga behöver lära sig mer om MT och verksamheten. Fyra rörde att MT-tekniker behöver lära sig mer om IT. Fyra rörde upphandlingsprocessen av MTP:er, där verksamheten ansågs ha mycket att lära sig. Resterande kommentarer varierade, t.ex. rörande kurser i avvikelserapportering för vårdgivare och kurser inom medicin för MT-tekniker utan medicinsk bakgrund.

Intervjuerna med IT-enheten under fallstudien visade på en riktlinje som ansågs vara problematisk: idag får verksamhetschefer köpa in system utan att gå via den formella inköpsprocessen om kostnaden understiger 500 000 SEK. Ibland görs därmed inköp av system utan att IT har koll på det. Leverantörer kommer helt enkelt in och sätter upp system utan att rådfråga med IT. Då ett system kan kräva implementation i flera olika VLAN och därmed förändringar av olika tekniska regelverk (såsom brandväggsregelverk) kan detta skapa stora problem. Det finns riktlinjer för riskanalys kring inköp även av system under 500 000 SEK, men dessa tillämpas inte alltid på ett bra sätt. Kravspecifikation görs ofta när ett system redan är färdigt och IT kommer ofta in för sent i processen för att få med sina synpunkter även i vanliga upphandlingar.



Figur 17 Kommunikationen mellan olika aktörer. Utöver dessa kategorier tillkommer kategorin ”ej applicerbart”, vilken beskrevs för MT av åtta respondenter.

Fallstudien identifierade också att vårdpersonalen i regel inte har någon teknisk bakgrund, vilket skapar problem vid användning av MTP:er då dessas gränssnitt ofta inte är särskilt användarvänliga. För att minska risken för användarfel ges kortare utbildningar för hur man använder olika MTP:er. Dessa utbildningar är dock oftast på en ganska ytlig nivå och ger därför inte tillfredsställande kunskap

för att förstå om någonting utöver det vanliga (t.ex. ett mjukvarufel) inträffar, eller vad som bör göras om sådana händelser inträffar.

5.2.1.2 Kommunikation mellan aktörer

En översikt av hur respondenterna upplever kommunikationen med andra aktörer visas i Figur 17. Vid tolkning av Figur 17 är det viktigt att betänka att de allra flesta respondenter kommer från MT (därav de åtta svaren för ”ej applicerbart”). Kommunikation inom MT anses fungera bäst (ett medelvärde på 3.7 givet en skala på 1: mycket dåligt – 4: mycket bra), följt av vårdpersonal (3.4), leverantörer (3.2) och andra sjukhus/landsting (2.7). Kommunikation med IT kommer en bit efter med ett medelvärde på 2.2. Troligen är detta resultat direkt korrelerat med att de arbetar på samma fysiska plats.

Det gavs totalt 20 förslag på hur kommunikationen mellan olika aktörer bör vara utformad gällande daglig drift. De flesta förslagen rörde IT, såsom att IT bör finnas på plats i sjukhusen, eller att IT och MT bör slås ihop. Exempelvis:

> ”*Särskilt avdelade IT-ingenjörer med ansvar för MT-system bör finnas verksamhetsnära*.”,
>
> ”*De bör arbeta med verksamhetsnära förvaltning av system som är medicintekniska produkter*” och
>
> ”*Samarbete, ökad förståelse. Vi har slagits ihop (MT och IT) och det är en bra början. Men det kommer att ta 2-3 år innan vi ser frukterna av det. Kommunikation och ökad förståelse är A och O*.”.

Totalt 23 respondenter gav förbättringsförslag gällande kommunikation vid inträffande av incidenter. Flertalet av dessa förslag rörde samplanering och koordination av incidenter på en mer nationell nivå, något som inte tycks fungera väl idag. Exempelvis:

> ”*Rapportering, samkörd statistik samt forum nationellt, som nu fast mer. Gemensamma avvikelsesystem eller åtminstone kompatibla för att få fram lika data*.”,
>
> ”*Mer inriktad på gemensam problemlösning*.”,
>
> ”*En bättre samordning när det sker större incidenter som drabbar flera kliniker eller sjukhus*.” och
>
> ”*I varje landsting, region eller sjukhus (beroende på storlek) bör det finnas en person i den medicintekniska organisationen som har i uppdrag att fånga upp medicintekniska avvikelser. Den/de personerna gör riskanalyser, utreder avvikelser tillsammans med verksamheten och övriga aktörer (t.ex. IT, fastighet), rapporterar till leverantören, LV och Reidar (Reidar.se) och bör samla en grupp som driver ett proaktivt arbete inom området. LfMT (lfmt.se)*

har nyligen startat upp ett nätverk för sådana personer som förhoppningsvis kan driva på arbetet ute i landet.".

Detta stödjer resultatet från fallstudien, där REIDAR ansågs ha en mycket stor potential.

5.2.2 Åtgärdsförslag

En översikt av åtgärder som föreslås för datorrelaterade incidenter i REIDAR visas i Tabell 10.

Tabell 10. Översikt av åtgärder i REIDAR.

Åtgärd	Antal	Andel
Förändrade rutiner	117	12%
Övrig åtgärd	110	12%
Modifiering av programvara	109	12%
MTP repareras	101	11%
Förbättring av konstruktion/ergonomi	94	10%
Utbildning av vårdpersonal	82	9%
Förbättrad tillverkning	48	5%
Förbättrad dokumentation	47	5%
MTP tas ur drift	42	4%
Förbättrat/infört förebyggande underhåll	36	4%
Förbättrad installation	33	3%
Utbildning av patienter	26	3%
Ingen åtgärd	23	2%
Förbättrad systemtillsyn	21	2%
Förbättrad planerad återanskaffning	17	2%
Utbildning av tekniker	15	2%
Översyn org./ansvarsfördelning	13	1%
Förbättrad ankomstkontroll	8	1%
Förbättring av standarder	2	0%
Förbättrad bemanning	1	0%

Den vanligaste typen av åtgärd som förslås är *förändrade rutiner*, exempelvis att produktleverantörer vid personalutbildningar ska informera om handhavande av produkters mjukvara eller att all nätverksutrustning som servrar och medicintekniska produkter ska ges en tydlig märkning. Den näst vanligast

åtgärden är modifiering av programvara, t.ex. en uppgradering av mjukvaran Spirare3 (en typ av diagnostisk mjukvara) till version 3.37.10.2778. *MTP repareras* och *förbättring av konstruktion/ergonomi* rör primärt hårdvara, så som byte av batterier eller reparation av kretskort. *Utbildning av vårdpersonal* är generellt sett viktigare än *utbildning av patienter och tekniker*. *Förbättrad tillverkning* kan röra både utveckling av mjukvara och hårdvara. *Förbättrad dokumentation* rör primärt tillägg/förändringar av produktmanualer (från leverantörens sida).

Som framgår av statistiken så finns det likheter mellan åtgärdsförslagen i USA (se Alemzadeh m.fl. [2] i avsnitt 5.1) och Sverige (det som görs i USA görs också i Sverige), men med ett större fokus på mjukvaruförbättringar i USA och hårdvaruförbättringar i Sverige.

5.2.3 Incidenter på grund av skadlig kod

Våra sökningar mot MAUDE och MREDR identifierade en incident relaterade till skadlig kod, vilken inträffade 2006 och omfattande en datormask i en MTP som användes för nukleärmedicin[43]. Totalt tre maskiner fick problem som en följd av tillgänglighetsbristen hos den infekterade datorn, men ingen personskada skedde. Detta stämmer överens med slutsatserna från Fu [15][16], som meddelar att rapporteringen av skadlig kod till dessa databaser är undermålig.

Sökningarna mot REIDAR identifierade två incidenter som rör IT-angrepp (nummer 00272 och 00581). Den ena rör en förmodad datormask som infekterade alla MTP:er från General Electrics på ett nätverk som hanterade patientövervakning av 53 patienter. Konsekvensen blev omfattande driftstörningar. Den andra rörde datorviruset MSBLAST som infekterade en dator som hanterar ultraljudsutrustning och skickade stora mängder datapaket till Internet (oklart vad). För att undvika överbelastning blockerades datatrafiken från maskinen av en switch, vilket innebar att patientregistrering och nätverksdataöverföring till PACS-system inte var möjligt.

Det finns även en stor mängd incidenter i REIDAR där den bakomliggande incidentorsaken är oklar, men skulle kunna röra IT-angrepp, exempelvis incident nummer 01102: ”*Audiometer: Under mätningen började plötsligt pilen röra sig på datorskärmen*”. Orsaken till dessa fall är sannolikt bristen på kompetens kring detektering av IT-angrepp och/eller brist på verktyg för säkerställande av IT-angrepp. Mörkertalets storlek är oklart.

Fallstudien gav inte mycket information avseende incidenter relaterade till IT-angrepp. Den enda IT-säkerhetsincidenten som respondenterna kunde minnas var när en datormask infekterade ett stort antal datorer på landstinget under början av

[43] http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/Detail.CFM?MDRFOI__ID=772836

2000-talet. Det var i samband med det utbrottet som det huvudsakliga arbetet med IT-säkerhet började på universitetssjukhuset.

6 Diskussion

De viktigaste identifierade resultaten ges i punktlistan nedan.

- Tanken med ”*IP-fieringen*” är att minska den administrativa och operativa arbetsbördan vid daglig drift, och öka precisionen för medicinska manövrar. Den bidrar dock även med mer komplexa system vilket ökar risken för att diverse IT-typiska problem, såsom haveri av nätverkshårddiskar och spridning av datormaskar, kan påverka patientsäkerheten. Den försvårar även incidenthanteringen vid sådana händelser. Statistiken i databasen REIDAR talar även för att antalet datorrelaterade incidenter kommer öka i framtiden.
- En *nationell samverkan* behövs för att motarbeta och mer effektivt hantera incidenter. REIDAR är en bra start på detta men behöver en högre rapporteringsfrekvens och bättre synkronisering mot lokala incidentdabaser.
- Det behövs en bättre *intern samverkan* mellan IT, och MT/vården. Detta kan exempelvis genomföras i form av fysisk samverkan, utbildning eller möjligen sammanslagning av MT och IT (vilket har gjorts inom vissa landsting).
- *Antagonistiska hot* (t.ex. datormaskar) ses än så länge som relativt oproblematiska då få har upptäckts och orsakat någon större skada. Dock finns det stora sårbarheter vilka potentiellt kan skapa problem i framtiden.

Dessa punkter diskuteras i mer detalj i avsnitt 6.1 till 6.5.

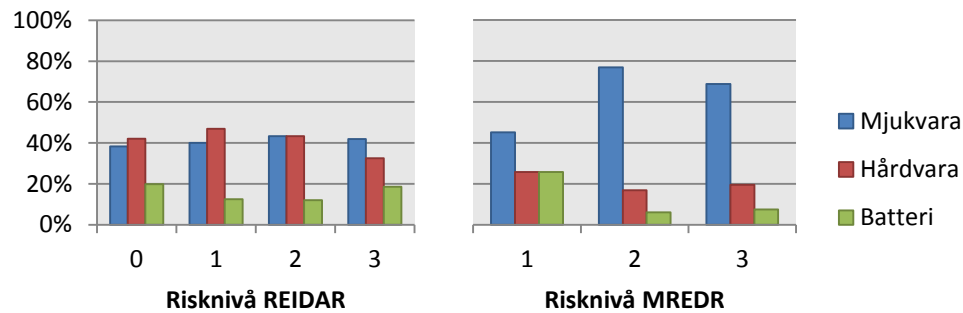
6.1 Möjliga framtida incidenter

För cirka 20 år sedan var de medicinska systemen väl separerade från datornätverk. Trenden kring IT inom hälso- och sjukvård är dock samma som trenden kring IT i världen i stort: det är attraktivt att system är ihopkopplade eftersom det bedöms underlätta den administrativa och operativa bördan. Idag är det vanligt att MTP:er är uppkopplade till nätverksareor, nätverkshårddiskar eller även i vissa fall till kontorsnätet. Det är troligt att denna ökade komplexitet kommer leda bättre funktionalitet, men även till fler datorrelaterade incidenter (något som stöds av datamaterialet i REIDAR, se Figur 11).

Givet de långa livscyklerna för MTP:er så kommer utrustningen de närmaste åren att se ut ungefär på samma sätt som det ser ut idag: infusionspumpar, bildhanteringssystem och övervakningsenheter lär finnas kvar och bidra med problem - att ta fram fundamentalt nya teknologier (t.ex. hårdvara eller mjukvara) är på grund av certifieringskravet en mycket trögrörlig process.

Riskbedömningarna i REIDAR kan ge en inriktning avseende framtida möjliga incidenter med MTP:er. En översikt av riskklasserna för olika typer av datorrelaterade incidenter i REIDAR och MREDR (från [2]) ges av Figur 18. I REIDAR nyttjas en matris beskrivande allvarlighetsgrad (mindre/måttlig/betydande/katastrofal) samt sannolikhet för upprepande (mycket liten/liten/stor/mycket stor) för att härleda ett riskvärde för incidenten mellan 0-4.

MREDR använder tre risknivåer (se avsnitt 5.1). Löst tolkat kan en MREDR risk på 1 kartläggas mot en REIDAR risk på 0-1, en MREDR risk på 2 mot REIDAR risk på 2, samt en MREDR risk på 3 mot en REIDAR risk på 3. Det finns en relativt hög andel incidenter som bedöms vara av hög risk, oavsett vilken orsaksbakgrund som rörs. Mjukvara anses ha högst risk enligt både REIDAR och MREDR (men med större betoning i MREDR än REIDAR). Det finns med andra ord skäl att tro att många av de incidenter som inträffat de senaste åren även kommer inträffa i framtiden.



Figur 18. Risknivåer för datorrelaterade incidenter i REIDAR (till vänster) och MREDR (från [2], till höger).

Gällande IT-säkerhetsincidenter så är det relativt få omfattande sådana som hittills har upptäckts inom hälso- och sjukvård. Och när sådana har inträffat så har signifikanta åtgärder vidtagits. Exempelvis ledde det stora utbrottet med datormasken på det fallstuderade universitetssjukhuset till omfattande IT-säkerhetsåtgärder, såsom genomgripande VLAN-separation. Stora problem kvarstår dock – problem som IT har svårt att ensamt hantera (se avsnitt 6.4). Dessa problem medför att det i framtiden sannolikt kommer inträffa förhållandevis fler IT-säkerhetsrelaterade incidenter inom hälso- och sjukvård.

6.2 En nationell samverkan kring incidenterhantering

Fallstudien och enkäten visade att det finns ett stort behov av en nationell samverkan kring incidenthantering – vad som händer på en plats kommer förr eller senare att ske även på en annan plats, och goda strategier för att motverka och behandla incidenter bör kommuniceras. REIDAR nämndes frekvent som en god idé med stor potential som ännu inte realiserats – detta trots att applikationen funnits i över tio år. Rapportering till REIDAR sker över lag sällan, i synnerhet för mer IT-relaterade problem som nätverkshaveri då systemen som hanterar dessa incidenter (t.ex. Synergi som det studerade landstinget nyttjade) hanteras av IT (som till skillnad från MT har en mycket begränsad kunskap om REIDAR). Respondenterna bedömde att de främsta orsakerna till den undermåliga rapporteringen var att det var krävande att tvätta incidenter innan de rapporteras REIDAR, samt att det saknas kunskap/förståelse för varför incidentrapportering är viktig.

En annan orsak bedömdes vara att webbformuläret för sökningar i REIDAR är mycket begränsat (vilken är orsaken till att ett skript togs fram under denna studie för att automatiskt ladda ned databasen, se avsnitt 3.3). En modernisering av REIDAR med god sök- och analysfunktionalitet skulle sannolikt bidra till att öka incidentrapporteringen till det. Detta är för övrigt samma slutsatser som identifierades av en studie utförd 2003 för incidentrapporteringsapplikationen MedControl, vilket REIDAR baseras på [27]. Som ett alternativ till sökning i den nuvarande webbimplementationen av REIDAR tillhandahåller vi för övrigt gärna skriptet, eller den nedtankade databasen, till intresserade läsare.

6.3 Förbättrad intern samverkan

Fallstudien identifierade att det finns arbete att göra kring samverkan, varför enkäten utformades med frågor behandlande detta. Resultatet visade att det finns mycket att förbättra rörande kommunikationen mellan olika aktörer, och då kanske främst med IT-enheten. Bakgrunden till detta tros vara det intensiva arbetet med att digitalisera vården, såsom att koppla upp administrativa system (t.ex. journalsystemet Cosmic eller remiss-och-svar systemet ROS) mot operativa system (t.ex. röntgenkameror). Då dessa system både innefattar komponenter som IT-enheten är ansvarig för (t.ex. journalsystemet och nätverkskopplingar) och komponenter som MT-enheten (eller vårdpersonal) är ansvarig för (t.ex. röntgenkameror och infusionspumpar) krävs det att de inblandade aktörerna har förståelse för varandras områden.

Ett sätt att behandla detta problem är att låta alla aktörer genomföra mer omfattande utbildningar inom dessa områden för att öka kunskapen och de krav som ställs på varandras arbetsområden. Ett annat (men inte motverkande)

alternativ vore att låta aktörerna sitta på samma plats rent fysiskt, såsom MT och vårdpersonal idag gör (MT nyttjar för övrigt samma typ av vita klädsel som är vanlig bland vårdpersonal). Eller att slå ihop MT och IT som redan gjorts på ett par platser i landet. Tiden lär utvisa hur väl det senare alternativet fungerar.

6.4 Förbättrad hantering av antagonistiska hot

Våra fallstudier visar att IT-sidan av vården har kunskap om IT-säkerhet och goda processer för IT-säkerhetsrelevanta egenskaper såsom administration av användarrättigheter, nätverkssegmentering, trafikkontroll och intrångsdetektion (se avsnitt 4.2). Vår fallstudie visar dock också på problem som IT har begränsade möjligheter att hantera:

- IP-fieringen bidrar med mycket ny funktionalitet och minskad arbetsbörda, och är ingen temporär trend utan något som kommer fortsätta inom den försebara framtiden. Förutom ökad funktionalitet och minskad arbetsbörda vid daglig drift bidrar den även med att skapa mer komplexa system där alla aktörer får mindre koll på hur allt faktiskt fungerar. Detta påverkar naturligtvis även IT-säkerhetsegenskaper. Ett bra exempel är PACS/RIS-system. Dessa är komplicerade datormiljöer som är utspridda över ett flertal olika nätverkszoner med skilda säkerhetsegenskaper, från servermiljöer (som driftas av IT) till operativa MTP-miljöer (som driftas av MT). Ett intrång i en av dessa maskiner kan medföra stora problem.
- Känsliga system finns ofta i öppna miljöer där det är enkelt att få fysisk access. Exempelvis kan en antagonist nyttja detta för att injicera skadlig kod via USB, eller för att koppla in sin egen dator i ett nätverkssegment. Detta problem har ingen enkel lösning då patienter i många fall naturligtvis behöver vara fysiskt nära systemen.
- Slutanvändare (t.ex. läkare och sköterskor) har ofta en begränsad kompetens kring IT i allmänhet och IT-säkerhet i synnerhet. Detta i kombination med IP-fieringen medför en risk både för såväl generella IT-haverier som antagonistdrivna IT-haverier.
- Drift av operativa MTP:er sker främst av leverantörer och mjukvarufixar måste genomgå rigorösa driftsäkerhetstester innan de får implementeras. Detta innebär att de flesta operativa MTP:er använder gamla (och därmed sannolikt sårbara) operativsystem och mjukvaror. Driftsäkerhetstester är dessutom inte samma sak som IT-säkerhetstester (som involverar antagonistiska hot), vilket innebär att nyligen uppdaterade system kan vara sårbara även för enklare IT-attacker.
- MTP:er från samma tillverkare placeras generellt i samma nätverkssegment. Givet den förra punkten medför detta att vanliga icke-riktade antagonistiska hot, så som datormaskar, bedöms kunna orsaka stora driftstörningar inom

segmenten (och beroende på nätverkskopplingar, även mellan segment). Leverantörerna har (för att kunna uppdatera systemen) även möjlighet att fjärransluta direkt till dessa nätverkssegment, vilket är en potentiell intrångsvektor för skadlig kod.

- Vårdanställda har generellt sett endast ytliga kunskaper kring IT i allmänhet och IT-säkerhet i synnerhet. Användarmisstag som bäddar för framgångsrika IT-attacker (t.ex. nätfiske [19] eller skadlig kod via USB [33]) är därmed ett potentiellt hot. Att verksamheten har möjlighet att köpa system för under en halv miljon kronor utan att involvera IT är ett problem relaterat till detta (men ett sådant mandat har naturligtvis även sina fördelar).
- Med den nuvarande incidentrapporteringsfunktionen i REIDAR finns det ingen möjlighet att beskriva om en incident involverade skadlig kod – detsamma gäller databaserna som tillhandahålls av FDA. Att denna studie enbart identifierade ett fåtal IT-säkerhetsrelaterade incidenter har sannolikt att göra med en kombination av bristande kunskap om vad som kännetecknar en IT-säkerhetsincident och bristande förståelse att detta är en viktig egenskap som bör rapporteras.

En sökning efter attackskript för de tio vanligast medicintekniska produkterna i REIDAR i Exploit Database[44] inga träffar. Vid en första anblick kan detta tyckas vara bra – det finns ingen lättillgänglig attackkod för vanliga medicintekniska produkter. Vid närmare eftertanke är dock även det problematiskt – det betyder nämligen att få ännu har varit tillräckligt intresserade av att leta efter sårbarheter i medicintekniska produkter. Med IP-fieringen av vården kan detta komma att förändras. Som en jämförelse fanns det inte en enda publikt känd sårbarhet för Siemens WinCC och Siemens SIMATIC S7 PLC innan datormasken Stuxnet[45] blev allmänt känd (se US National Vulnerability Database[46] [NVD]). Efter Stuxnet blev säkerhetsforskare intresserade av att leta efter brister i dessa produkter och som ett resultat finns det idag 52 identifierade sårbarheter i WinCC och 64 i SIMATIC S7.

6.5 Framtida arbete

NCS3 rekommenderas fortsätta med omvärldsbevakning och studier av hälso- och sjukvård enligt nedan nämnda framtida arbeten i prioriterad ordning.

1. *Studier av hur aktörer bäst bör kommunicera*. Denna studie skrapade bara på ytan kring kommunikationen mellan aktörer inom hälso- och sjukvård, och involverade inte IT-avdelningens bild på ett tillfredsställande sätt.

[44] http://www.exploit-db.com/
[45] En datormask som angrep Siemens WinCC och Siemens SIMATIC S7.
[46] http://web.nvd.nist.gov/

Studiens enkät och fallstudier identifierade dock tydliga problemområden som bör fortsätta studeras med stöd av vedertagna teorier och empiri så som [30], [1] och [29].

2. *Djupstudier av hur olika teknologier skapar driftstörningar*. IT-säkerhet ges typiskt på bekostnad av funktionalitet och användbarhet. Det vore intressant att studera hur många funktionsproblem, såsom driftstörningar, som orsakas av konflikter med olika implementerade IT-säkerhetsfrämjande teknologier. Exempelvis identifierade fallstudien (se avsnitt 3.2.2) att signaturbaserade intrångspreventionssystem nyttjades för att blockera förmodad skadlig kod i nätverken på ett antal platser, t.ex. för operativa MTP:er. Dessa typer av system har ibland fel, vilket i praktiken innebär att viktig funktionalitet kan blockeras. Hur ofta det var fallet för det studerade universitetssjukhuset var oklart (mer än att det ibland hände). Inom akademisk forskning har systemet som landstingets intrångsdetektionssystem baserats på dock testats med upp emot 96% falska larm [39]. Ett annat mer konkret exempel beskrivs i REIDAR för avvikelse nummer 00461[47]: ”*MTP som ej får innehålla antivirusprogram har uppdateras med antivirusprogram via rutinmässig uppdatering. Detta orsakar hängning av bildhanteringen*”.

3. *Säkerhetstesta MTP:er*. Som framgår av studier av NVD och Exploit Database så har få MTP:er säkerhetstestats. För att bedöma IT-säkerhetsrisken av de nuvarande använda MTP:erna inom vården vore det värdefullt att genomföra säkerhetstester för att identifiera okända kodbuggar (t.ex. hårdkodade lösenord eller bufferöverskridningsbuggar [31]) och konfigurationsbuggar (t.ex. veka lösenord).

4. *Se över utvecklingsprocessen för MTP:er*. MTP:er genomgår rigorösa tester rörande driftsäkerhet (även om det trots allt ibland blir fel), men få tester rörande IT-säkerhet. Att arbeta med IT-säkerhet i utvecklingsprocessen (och studera dess effektivitet) skulle minska sannolikheten för driftstörningar på grund av IT-attacker såsom datormaskar, vilket kanske inte ses som problematiskt idag men som kan bli det i framtiden.

5. *Systematiska sökningar efter sårbarheter i MTP:er och korrelera dessa mot kända IT-attacker*. Denna studie gick ej in på djupet kring vilka kända sårbarheter som nuvarande MTP:er har. En framtida studie skulle kunna kartlägga sårbarheter och sedan korrelera dessa mot de IT-attacker som förekommer i praktiken (t.ex. Symantec’s databas av skadlig kod[48]). En

[47] http://www.reidar.se/RC?Inputopen-14_04793_Time=140924154958
[48] http://www.symantec.com/security_response/landing/threats.jsp

sådan studie skulle kunna bedöma hur mycket skada (t.ex. driftstörningar) som vanlig skadlig kod kan åsamka inom hälso- och sjukvård.

6. *Djupstudera incidenter i REIDAR som skulle kunna röra skadlig kod*. Det finns ett stort antal incidenter i REIDAR som har oklart ursprung och därmed skulle kunna kan vara ett resultat av skadlig kod (se avsnitt 5.2.3). Framtida studier skulle kunna djupstudera relevanta sådana incidenter för att erhålla en mer valid bild av hur ofta IT-angrepp har inträffat inom hälso- och sjukvård och hur dessa kan undvikas.

Utöver dessa områden rekommenderas aktörer inom hälso- och sjukvård att *modernisera REIDAR*. En modern version av REIDAR med enklare möjligheter att genomföra omfattande sökningar och analyser (exempelvis sådant som detta projekt har innefattat) är en förutsättning för att öka rapporteringsfrekvensen till REIDAR och därmed skapa en valid, delad nationell bild av incidenter inom hälso- och sjukvård.

Referenser

[1] Lisa C Abrams, Rob Cross, Eric Lesser, and Daniel Z Levin. Nurturing interpersonal trust in knowledge-sharing networks. *The Academy of Management Executive*, 17(4):64–77, 2003.

[2] Homa Alemzadeh, Ravishankar K Iyer, Zbigniew Kalbarczyk, and Jai Raman. Analysis of safety-critical computer failures in medical devices. *Security & Privacy, IEEE*, 11(4):14–26, 2013.

[3] Tom Andersson and Fia Ewald. Kontinuitetshantering i praktiken - fallstudier av läkemedelshantering och informationshantering i händelse av verksamhetsstörningar, 2014.

[4] Lars-Göran Angantyr, Johan Carlstedt, Björn-Erik Erlandsson, Susannah Sigurdsson, Åsa Molde, Helena Andersson, and Svante Nygren. It-haverier i vården - erfarenheter och förslag till åtgärder från aktuella fall - kamedo-rapport 96, 2011.

[5] BBC. Us hospital hack 'exploited heartbleed flaw'. http://www.bbc.com/-news/technology-28867113, 2014. Accessed: 2014-11-07.

[6] Zhivko Bliznakov, G Mitalas, and N Pallikarakis. Analysis and classification of medical device recalls. In *World congress on medical physics and biomedical engineering 2006*, pages 3782–3785. Springer, 2007.

[7] Kjell Brännström. Slutrapport för undersökning av sjukhus/landsting/regioners rutiner och inställning till avvikelsehantering, 2013. Accessed: 2014-11-21.

[8] Lee J Cronbach. Coefficient alpha and the internal structure of tests. *psychometrika*, 16(3):297–334, 1951.

[9] Carolina Davidsson, Malin Johansson, and Birgitta Trevik. Det ska vara lätt att göra rätt - sjuksköterskans handhavande av infusionspump, 2008.

[10] Martin Eriksson. Vägledning till ökad säkerhet i industriella informations och styrsystem, 2014.

[11] Scott Erven. The urgent need for independent validation and verification of security controls in medical devices. *SecMedic*, 2014.

[12] Elizabeth Fanning. Formatting a paper-based survey questionnaire: Best practices. *Practical Assessment Research & Evaluation*, 10(12):2, 2005.

[13] Federal Communications Commission (FCC). Good can become better - the 2009 swedish health care report. http://www.fcc.gov/guides/wireless-devices-and-health-concerns, 2014. Accessed: 2014-11-21.

[14] Barbara Filkins. Health care cyberthreat report - widespread compromises detected, compliance nightmare on horizon, 2014.

[15] Kevin Fu. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510 (k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*, page 102. National Academies Press Washington, DC, 2011.

[16] Kevin Fu and James Blum. Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, 56(10):35–37, 2013.

[17] Guy G Gable. Integrating case study and survey research methods: an example in information systems. *European journal of information systems*, 3(2):112–126, 1994.

[18] Jonas Hallberg, Mikael Wedlin, David Lindahl, Jonas Almroth, Mats Persson, and Teodor Sommestad. Ncs3: årsrapport 2012, 2012.

[19] Hannes Holm, Waldo Rocha Flores, and Goran Ericsson. Cyber security for a smart grid-what about phishing? In *Innovative Smart Grid Technologies Europe (ISGT EUROPE), 2013 4th IEEE/PES*, pages 1–5. IEEE, 2013.

[20] Lars Jerlvall and Thomas Pehrsson. Vård-it-rapporten. https://-www.vardforbundet.se/Min-profession/sakervard/IT-for-varden-e-halsa/-Anvandbara-IT-system/, 2010. Accessed: 2014-11-07.

[21] Lars Jerlvall and Thomas Pehrsson. ehälsa i landstingen. http://www.sll.se/-Global/Om%20landstinget/S%C3%A5%20granskas%20landstinget/-Projektrapporter/Rapporter%202014/Rapport-2-2014-IT-sakerhet-i-natverksansluten-MTU.pdf, 2014. Accessed: 2014-11-07.

[22] Rolf Johansson. Case study methodology. In *the International Conference on Methodologies in Housing Research, Stockholm*, 2003.

[23] Läkemedelsverket. Infusionspumpar - identifiering av risker. http://-www.lakemedelsverket.se/Alla-nyheter/NYHETER-2014/Identifiering-av-patientrisker-med-infusionspumpar/, 2014. Accessed: 2014-11-07.

[24] Landstingsrevisorerna. It-säkerhet i nätverksansluten medicinteknisk utrustning. http://www.sll.se/Global/Om%20landstinget/-S%C3%A5%20granskas%20landstinget/Projektrapporter/Rapporter%202014/-Rapport-2-2014-IT-sakerhet-i-natverksansluten-MTU.pdf, 2014. Accessed: 2014-11-07.

[25] Linus Larsson. Gammal mask angrep sjukhuset. http://-computersweden.idg.se/2.2683/1.251215, 2009. Accessed: 2014-11-07.

[26] Jianbo Lei, Pengcheng Guan, Kaihua Gao, Xueqin Lu, Yunan Chen, Yuefeng Li, Qun Meng, Jiajie Zhang, Dean F Sittig, and Kai Zheng. Characteristics of health it outage and suggested risk management strategies: An analysis of historical incident reports in china. *International journal of medical informatics*, 83(2):122–130, 2014.

[27] Lars Löfstedt and Christine Girod. Uppföljning av "granskning av avvikelsehantering inom medicinsk teknik i region skåne" som gjordes 2003. https://www.skane.se/upload/Webbplatser/Revisionen/Dokument/-Granskningsrapporter/Slutrapport69.pdf, 2006. Accessed: 2014-11-21.

[28] Elaine McColl, A Jacoby, L Thomas, J Soutter, C Bamford, N Steen, R Thomas, E Harvey, A Garratt, and J Bond. *Design and use of questionnaires: a review of best practice applicable to surveys of health service staff and patients*. Core Research, 2001.

[29] Jakki J Mohr, Robert J Fisher, and John R Nevin. Collaborative communication in interfirm relationships: moderating effects of integration and control. *The Journal of Marketing*, pages 103–115, 1996.

[30] United States General Accounting Office. Information sharing - practices that can benefit critical infrastructure protection. http://www.gao.gov/products/-GAO-02-24, 2001. Accessed: 2014-11-10.

[31] Aleph One. Smashing the stack for fun and profit. *Phrack magazine*, 7(49):14–16, 1996.

[32] Eric D Perakslis. Cybersecurity in health care. *The New England journal of medicine*, 371(5):395–397, 2014.

[33] Dung Vu Pham, Ali Syed, and Malka N Halgamuge. Universal serial bus based software attacks and protection solutions. *digital investigation*, 7(3):172–184, 2011.

[34] Benjamin Ransford, Andres Molina-Markham, Quinn Stewart, Kevin Fu, Daniel Bruce Kramer, Matthew Charles Baker, and Matthew R Reynolds. Security and privacy qualities of medical devices: An analysis of fda postmarket surveillance. 2012.

[35] Per Runeson and Martin Höst. Guidelines for conducting and reporting case study research in software engineering. *Empirical software engineering*, 14(2):131–164, 2009.

[36] Isabella Scandurra. Störande eller stödjande? http://www.swenurse.se/Vi-arbetar-med/e-halsa/E-halsosystemens-anvandbarhet/, 2013. Accessed: 2014-11-07.

[37] Socialstyrelsen. Good can become better - the 2009 swedish health care report, 2009. Accessed: 2014-11-21.

[38] Socialstyrelsen. Sosfs 2008:1. socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården. http://-www.socialstyrelsen.se/sosfs/2008-1, 2013.

[39] Gina C Tjhai, Maria Papadaki, SM Furnell, and Nathan L Clarke. Investigating the problem of ids false alarms: An experimental study using snort.

In *Proceedings of the IFIP TC 11 23rd International Information Security Conference*, pages 253–267. Springer, 2008.

[40] Lisa Vaas. Doctors disabled wireless in dick cheney's pacemaker to thwart hacking. http://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/, 2013. Accessed: 2014-11-07.

[41] Nicole Van Deursen, William J Buchanan, and Alistair Duff. Monitoring information security risks within health care. *computers & security*, 37:31–45, 2013.

[42] Dolores R Wallace and D Richard Kuhn. Failure modes in medical device software: an analysis of 15 years of recall data. *International Journal of Reliability, Quality and Safety Engineering*, 8(04):351–371, 2001.

[43] Christopher Weaver. Patients put at risk by computer viruses. http://-online.wsj.com/article/-SB10001424127887324188604578543162744943762.html. Accessed: 2014-11-07.

[44] Gi Woong Yun and Craig W Trumbo. Comparative response to a survey executed by post, e-mail, & web form. *Journal of Computer-Mediated Communication*, 6(1):0–0, 2000.

Bilaga A. Enkätfrågor

Enkät rörande medicintekniska produkter

Hej!

Totalförsvarets forskningsinstitut (FOI) utför på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) en studie kring hur tekniska system används inom hälso- och sjukvård i Sverige. Studien analyserar vilka problem som finns kring medicintekniska produkter. Enkätresultatet analyseras i samspel med resultatet från fallstudier och databaser. Slutsatserna presenteras i en publikt tillgänglig rapport.

Genom att svara på enkäten hjälper du till att skapa en nationell förståelse för vilka problem och utmaningar rörande medicintekniska produkter som hälso- och sjukvård idag står inför. Du erhåller även en bild av vilka specifika problem som andra brukare av medicintekniska produkter har.

* Enkäten bör inte ta mer än 10-15 minuter att svara på.
* Enkäten kommer att finnas tillgänglig till och med fredagen den 24e oktober 2014.
* Enkäten är helt anonym och resultatet kommer endast att presenteras i aggregerad form.
* Du svarar på enkäten utifrån din organisationsroll och dina egna erfarenheter.
* Sprid gärna enkäten till kollegor som du bedömer som relevanta (exempelvis från MT, IT eller vårdpersonal).

Hör av dig till hannes.holm@foi.se med eventuella frågor eller kommentarer.

Stort tack på förhand för din medverkan, den är värdefull!

* Required

Vilken är din huvudsakliga organisationsroll? *

Exempelvis "medicinteknisk chef"

Hur många år har du arbetat med medicintekniska produkter (MTP)? *

Continue »

14% completed

Enkät rörande medicintekniska produkter

* Required

Översikt av medicintekniska produkter (1/3)

Svara på frågorna utifrån din organisationsroll och dina egna erfarenheter

Vilken medicinteknisk produkt i er verksamhet är mest problematisk? *

Hur ofta uppstår problem med denna produkt som leder till händelserna nedan? *

	Varje dag	Varje vecka	Varje månad	Varje år	Aldrig
Felfunktion/produktskada	○	○	○	○	○
Övergående skada	○	○	○	○	○
Bestående skada	○	○	○	○	○
Dödsfall	○	○	○	○	○

Vad är orsakerna bakom dessa händelser för denna produkt? *

Datorhårdvara/elektronik kan exempelvis röra ett batteri eller ett moderkort. Datormjukvara/programvara kan exempelvis handla om ett användarfel på grund av ett undermåligt gränssnitt eller att felaktig information presenteras.

	Mycket vanligt	Vanligt	Ovanligt	Mycket ovanligt
Datorhårdvara/elektronik	○	○	○	○
Datormjukvara/programvara	○	○	○	○
Ej datorrelaterad orsak	○	○	○	○

Är det något annat rörande denna produkt som du vill förmedla?

« Back Continue »

28% completed

Enkät rörande medicintekniska produkter

Översikt av medicintekniska produkter (2/3)

Svara på frågorna utifrån din organisationsroll och dina egna erfarenheter

Vilken medicinteknisk produkt i er verksamhet är näst mest problematisk?

Hur ofta uppstår problem med denna produkt som leder till händelserna nedan?

	Varje dag	Varje vecka	Varje månad	Varje år	Aldrig
Felfunktion/produktskada	○	○	○	○	○
Övergående skada	○	○	○	○	○
Bestående skada	○	○	○	○	○
Dödsfall	○	○	○	○	○

Vad är orsakerna bakom dessa händelser för denna produkt?

Datorhårdvara/elektronik kan exempelvis röra ett batteri eller ett moderkort. Datormjukvara/programvara kan exempelvis handla om ett användarfel på grund av ett undermåligt gränssnitt eller att felaktig information presenteras.

	Mycket vanligt	Vanligt	Ovanligt	Mycket ovanligt
Datorhårdvara/elektronik	○	○	○	○
Datormjukvara/programvara	○	○	○	○
Ej datorrelaterad orsak	○	○	○	○

Är det något annat rörande denna produkt som du vill förmedla?

« Back Continue »

42% completed

Enkät rörande medicintekniska produkter

Översikt av medicintekniska produkter (3/3)

Svara på frågorna utifrån din organisationsroll och dina egna erfarenheter

Vilken medicinteknisk produkt i er verksamhet är tredje mest problematisk?

Hur ofta uppstår problem med denna produkt som leder till händelserna nedan?

	Varje dag	Varje vecka	Varje månad	Varje år	Aldrig
Felfunktion/produktskada	○	○	○	○	○
Övergående skada	○	○	○	○	○
Bestående skada	○	○	○	○	○
Dödsfall	○	○	○	○	○

Vad är orsakerna bakom dessa händelser för denna produkt?

Datorhårdvara/elektronik kan exempelvis röra ett batteri eller ett moderkort. Datormjukvara/programvara kan exempelvis handla om ett användarfel på grund av ett undermåligt gränssnitt eller att felaktig information presenteras.

	Mycket vanligt	Vanligt	Ovanligt	Mycket ovanligt
Datorhårdvara/elektronik	○	○	○	○
Datormjukvara/programvara	○	○	○	○
Ej datorrelaterad orsak	○	○	○	○

Är det något annat rörande denna produkt som du vill förmedla?

« Back Continue »

57% completed

Enkät rörande medicintekniska produkter

Riktlinjer och kompetens

Svara på frågorna utifrån din organisationsroll och dina egna erfarenheter

Finns det några specifika riktlinjer rörande medicintekniska produkter som du anser försvårar (skapar problem) för ert dagliga arbete? Om ja, vilka?

Exempelvis riktlinjer från leverantörer eller landsting. Bortse från lagar och förordningar.

Finns det någon kompetensutveckling som du anser behövs rörande medicintekniska produkter? Om ja, vilka grupper saknar vilka kompetenser?

« Back Continue »

71% completed

Enkät rörande medicintekniska produkter

* Required

Kommunikation

Svara på frågorna utifrån din organisationsroll och dina egna erfarenheter

Hur bra fungerar kommunikationen generellt med följande aktörer? *

	Mycket bra	Bra	Dåligt	Mycket dåligt	Ej applicerbart
Leverantörer av medicintekniska produkter	○	○	○	○	○
MT	○	○	○	○	○
IT	○	○	○	○	○
Vårdpersonal	○	○	○	○	○
Andra sjukhus/landsting	○	○	○	○	○

Med vilka aktörer kan kommunikationen vid incidenthantering förbättras?

Exempelvis med leverantörer, IT, MT eller vårdpersonal.

Hur anser du att kommunikationen vid incidenthantering med dessa aktörer bör se ut?

Med vilka aktörer kan kommunikationen vid daglig drift förbättras?

Exempelvis med leverantörer, IT, MT eller vårdpersonal.

Hur anser du att kommunikationen vid daglig drift med dessa aktörer bör se ut?

« Back Continue »

85% completed

Enkät rörande medicintekniska produkter

Avslut

Svara på frågorna utifrån din organisationsroll och dina egna erfarenheter

Anser du att det finns något av stor vikt som enkäten inte addresserat? Om ja, vad?

Beskriv relevansen utifrån din egen erfarenhet.

Anser du att det finns några problem med utformningen på enkäten? Om ja, vilka problem?

« Back Submit

100%: You made it.

Never submit passwords through Google Forms.

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se