Jan Jacobson

Informationssäkerhet i fjärravlästa elmätare

Jan Jacobson

Informationssäkerhet i fjärravlästa elmätare

SP
Sveriges Provnings- och Forskningsinstitut
Fysik och Elteknik
SP RAPPORT 1994:55

Abstract

Information Security of Remote-Reading Energy Meters

This report presents basic concepts within the field of IT security. The ITSEC criteria and the ITSEM methods given by the European Community are used as a base.

The EC INFOSEC research programme has included the project "PER DOMUM" which focuses on remote reading of energy meters. The project is a co-operation between TACS (U.K.), GPP (Germany), CESI (Italy) and ENEL (Italy). SP has during the spring and summer of 1994 participated in the concluding of the project.

Threats, security objectives, security functions and security mechanisms are given for remote reading of energy meters. All of the listed functions and mechanisms do not origin from the "PER DOMUM" project, but are the experiences of SP.

The security evaluation is explained in two ways. One description of the required by ITSEM is given. Another description is given of which deliverables are required to perform the evaluation.

Key words : information security, IT security, software evaluation, energy meter

SP
SP-RAPPORT 1994:55
ISBN 91-7848-514-2
ISSN 0284-5172
Borås 1994

Swedish National Testing and Research Institute
SP REPORT 1994:55

Postal address:
Box 857, S-501 15 BORÅS,
Sweden
Telephone + 46 33 16 50 00
Telex 36252 Testing S
Telefax + 46 33 13 55 02

Innehållsförteckning

Förord

Begrepp som datasäkerhet, ADB-säkerhet, kommunikationssäkerhet, IT-säkerhet och informationssäkerhet blir allt mer aktuella. De används för att beteckna skydd av information i informationsbehandlande system.

Traditionellt tänker man på säkerhet i stora administrativa datasystem. Register i banker, inom sjukvård och inom försvarsmakten är exempel där lagrad information är viktig och värd att skydda. Numera byggs dock mikrodatorer in i apparater med uppgiften att kunna hantera information. Säkerhetsaspekterna berör alltså även små system och apparater vilka användaren inte primärt uppfattar som "en dator". Exempel på en sådan apparat är en elmätare där mätvärdet fjärravläses av en centralt belägen stordator.

Detta arbete har till stor del finansierats av ELFORSK projekt 3023 "Krav på mätning och avräkning" [ELFORSK]. ELFORSK-projektet har det övergripande målet att ta fram rekommendationer till branschkrav inför den avreglerade elmarknaden.

Ett speciellt tack riktas till Mats Ohlin (Försvarets Materielverk) som tagit sig tid att läsa och bidra med synpunkter på denna SP-rapport.

Sammanfattning

Denna SP-rapport presenterar grundläggande begrepp inom informationssäkerhet samt EGs kriterier (ITSEC) och metoder (ITSEM). Dessutom redovisas hur informationssäkerhet i fjärravlästa elmätare kan behandlas.

Begrepp som sekretess, integritet, tillgänglighet, evalueringsnivå, säkerhetsfunktion och säkerhetsmekanism förklaras. Appendix A ger även definitioner enligt Informationstekniska standardiseringen.

Inom EGs INFOSEC-program finns projektet "PER DOMUM" som arbetar med informationssäkerhet för ett system av fjärravlästa elmätare under utveckling i Italien. Projektet är ett samarbete mellan TACS (England), GPP (Tyskland), CESI (Italien) och ENEL (Italien). SP har under våren och sommaren 1994 deltagit i den avslutande delen av projektarbetet.

Rapporten ger exempel på hot, säkerhetskrav, säkerhetsfunktioner och säkerhetsmekanismer för fjärravlästa elmätare. Dessa exempel gäller allmänt och inte bara för systemet som "PER DOMUM"-projektet analyserat. Vissa funktioner och mekanismer i listorna gäller inte för RCM-systemet.

Utvärderingen av informationssäkerhet beskrivs på två olika sätt. Det ena sättet beskriver i korthet de olika aspekter från vilka resultat förväntas ingå i en provrapport enligt ITSEM. Det andra sättet beskriver vilket underlag som fordras för att göra utvärderingen.

1 Inledning

Information lagras och behandlas i en mängd olika datasystem. Systemens kraftfullhet gör det möjligt att samla in och behandla data mycket snabbare och effektivare än vad som är möjligt manuellt. Samtidigt blir ett system ganska snart så komplext att det inte är självklart att endast behöriga användare har tillgång till informationen. Information ska betraktas som en tillgång värd att skydda. Den utnyttjas på många sätt i företag och i privatlivet. Risken finns alltid för avsiktlig eller oavsiktlig förändring, radering, avslöjande eller missbruk.

Frågor kring informationssystemens säkerhet gäller många olika slags system. Stora administrativa datasystem inom försvar, bank och sjukvård är självklart berörda. Informationssäkerhet är också viktig för system som den enskilde kommer i kontakt med. Betalkort, persondatorer och hushållsmätare för elektrisk energi är exempel på system som dagligen kommer i kontakt med enskilda användare. Krav på tillräcklig informationssäkerhet kommer i framtiden med säkerhet att ställas på ett stort antal produkter med skiftande användningsområden.

Säkerhet i informationsbehandling har behandlats i Sverige av bl.a. [CITI], [SAMS] och [EGIT]. Man har kartlagt omvärlden och lämnat förslag till hur informationssäkerhets-frågor i framtiden ska hanteras.

I denna SP-rapport behandlas informationsteknologi (IT) utifrån säkerhetsaspekterna. Med begreppet "säkerhet" eller "informationssäkerhet" menas här just skyddet av information (engelska "security"). Säkerhet för personer, egendom och miljö (engelska "safety") tas inte upp i denna SP-rapport.

Det finns nu exempel på produkter vilka konstruerats för att ge höjd säkerhet vid hantering och lagring av information. Dataterminaler [DT5-94] och programvara för databaser [DT1-94] är exempel på sådana produkter.

EG-kommissionen har bedömt informationssäkerhet som ett viktigt område. Lagring, behandling och överföring av elektroniskt lagrad information ökar i betydelse för både ekonomiska och sociala aktiviteter. Ministerrådet fattade 1992 ett beslut (92/242/EEG) som betonar behovet av att behandla frågor om informationssystemens säkerhet. En handlingsplan för informationssäkerhet finns inom EGs DGXIII (Telekommunikationer, informationstjänstemarknaden och nyttiggörande av forskning).

Tre serier av studier och utredningar, INFOSEC '92, INFOSEC '93 och INFOSEC '94 har genomförts för att stödja ministerrådets beslut från 1992. Totalt 42 olika projekt belyser både administrativa och tekniska aspekter av informationssäkerhet. Telekommunikationer, kommunikationsprotokoll, "smart cards", operativsystem för datorer, elektroniska signaturer och fjärravlästa elmätare är exempel på områden som behandlats. [INFOSEC93] [INFOSEC94]

Inom INFOSEC '93 finns projekt nummer S2111 "PER DOMUM - Pre-Evaluation of a Remote Reading Domestic Utilities Meter". Projektet tillämpar kriterierna ITSEC (Information Technology Security Evaluation Criteria) och utvärderingsmetoderna ITSEM (Information Technology Security Evaluation Manual) för informationssäkerhet på ett system av fjärravlästa elmätare under utveckling i Italien. Arbetet är en förstudie för utvärdering av mätarsystemet enligt ITSEC/ITSEM. Man ska identifiera grundläggande begrepp för informationssäkerhet och jämföra tolkningar av dessa mellan olika organisationer. Dessutom utreds om ett system som utvecklats utan att känna till kraven från ITSEC/ITSEM ändå kan klara kraven.

Projekt "PER DOMUM" är ett samarbete mellan TACS (TA Consultancy Services Ltd, England), GPP (Gesellscahft für Prozeßrechnerprogrammierung mbH, Tyskland), CESI (Centro Elettrotechnico Sperimentale Italiano, Italien) och ENEL (Ente Nazionale per l'Energia Elettrica, Italien). SP (Sveriges Provnings och Forskningsinstitut, Sverige) har under våren och sommaren 1994 deltagit i den avslutande delen av projektarbetet.

2 Kriterier för informationssäkerhet

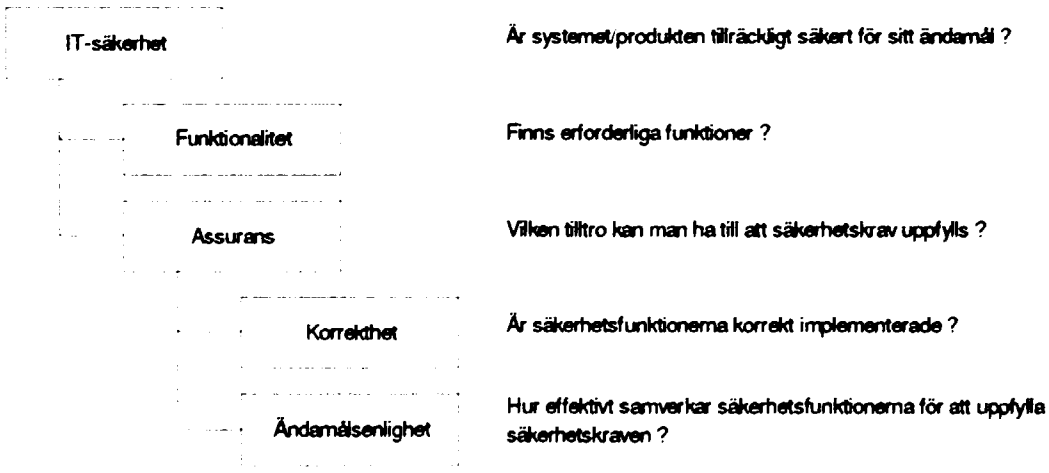
2.1 Grundläggande begrepp

Informationssäkerhet kan delas upp i tre begrepp enligt [ITSEC]:
- sekretess, dvs. skydd mot obehörigt avslöjande av information,
- integritet, dvs. skydd mot obehörig ändring av information,
- tillgänglighet, dvs. skydd mot obehörigt undanhållande av information eller resurser.

Varje apparat (eller system av apparater) har sina krav på hur sekretess, integritet och tillgänglighet ska uppfyllas. För att nå dessa krav finns ett antal tekniska säkerhetsfunktioner i apparaten. Funktionerna kan t.ex. bestå i skydd mot otillbörlig ändring av information.

Man vill sedan kunna förlita sig på dessa funktioner. Begreppet assurans används för att beteckna vilket förtroende som finns för en funktion. Graden av assurans (tilltro) kan inte uttryckas i absoluta mått, utan beskrivs istället som flera olika nivåer där varje högre nivå svarar mot högre krav. Assurans delas upp i förtroende för säkerhetsfunktionens korrekthet samt förtroende för dess effektivitet.

En uppdelning mellan funktionalitet och assurans är grundläggande enligt [ITSEC], [ITSEM]. Man väljer alltså att först definiera vilka säkerhetsfunktioner som finns i apparaten och sedan avgöra vilken assurans man har i dessa funktioner. Figur 1 visar sambandet mellan olika begrepp och deras betydelse.



Figur 1. Samband mellan funktionalitet, assurans, korrekthet och ändamålsenlighet

2.2 Evalueringsnivå

Förtroendet för att en produkt uppfyller de specificerade säkerhetskraven ökar med omfattningen av den evaluering (utvärdering) som görs. För att beskriva evalueringens omfattning definieras sex nivåer; E1 t.o.m. E6 [ITSEC]. Dessutom finns nivå E0 vilken innebär att en produkt underkänts vid evalueringen. På de högsta nivåerna återfinns krav avsedda för särskilt känsliga system eller kvalificerade hot. Både krav på utvecklingsmetodik, underlag från tillverkaren samt kontroller att utföra under evalueringen specificeras.

Nivå E0 innebär att en produkt underkänts vid evalueringen.

Den lägsta nivån för godkännande kallas E1. Nivå E1 kräver att det finns en beskrivning av hot, specificerade säkerhetskrav, säkerhetsfunktioner, säkerhetsmekanismer samt evalueringsnivå. Dessutom ska en informell beskrivning av systemkonstruktionen finnas. På denna nivå kontrolleras att utgångspunkterna är uppfylld genom funktionsprov.

Utvärderingsnivå E2 kräver, utöver kraven för E1, att det finns en informell beskrivning av detaljkonstruktionen. Resultat från funktionsproven ska utvärderas. Dessutom krävs ett system för konfigurationsstyrning (versionshantering) och ett godkänt förfarande för distribution.

För nivå E3 skall, utöver vad som föreskrivs för nivå E2, källkod och/eller hårdvara för säkerhetsmekanismerna utvärderas. Provresultatet ska utvärderas.

Nivå E4 kräver att det ska finnas en formell policy för informationssäkerhet som stöd för utgångspunkterna för evaluering. Säkerhetshöjande funktioner, systemkonstruktion och detaljkonstruktion ska specificeras på ett "halv-formellt" sätt. Dessutom gäller krav för nivå E3.

Nivå E5 kräver, förutom kraven för E4, att det ska finnas en nära överensstämmelse mellan detaljkonstruktion och källkod och/eller hårdvaruritningar.

Den högsta nivån E6 kräver, utöver kraven för E5, en formell specifikation av säkerhetsfunktioner och systemkonstruktion.

Samtliga nivåer i evalueringen ställer alltså krav på utvecklingsmetodiken. Den som konstruerar ett system som senare avses utvärderas enligt [ITSEM] bör redan från början ha erforderlig struktur och formalism i utvecklingsarbetet.

Det är inte alltid enkelt att veta vilken utvärderingsnivå som ska gälla. En tolkning gör gällande att de högsta nivåerna E5 och E6 gäller för produkter och system med mycket höga krav (t.ex. försvarsmakten eller större banksystem). Nivå E3 och E4 skulle sedan gälla för kommersiella system med höga krav (t.ex. operativsystem för stordatormiljö). De lägsta nivåerna E1 och E2 gäller främst mindre applikationer med måttliga krav (t.ex. säkerhetshöjande produkter för persondatorer).

2.3 Utgångspunkt för evaluering

För att göra en evaluering (utvärdering) möjlig behöver man veta vilka hot systemet utsätts för samt vilka tillgångar som ska skyddas. Man behöver också veta vilka säkerhetskrav som ställs och vilken evalueringsnivå som gäller.

Begreppet hot avser i sammanhang med informationssäkerhet en möjlig oönskad händelse som kan sätta säkerheten ur spel. Hot kan till exempel vara störningar vilka ger upphov till driftavbrott, förvanskning av information eller obehörig åtkomst av information. Ett hot kan också vara antingen avsiktligt (angrepp mot systemet) eller oavsiktligt (misstag eller felaktigheter i systemet). Ett exempel på hot är att mätdata läses av obehörig.

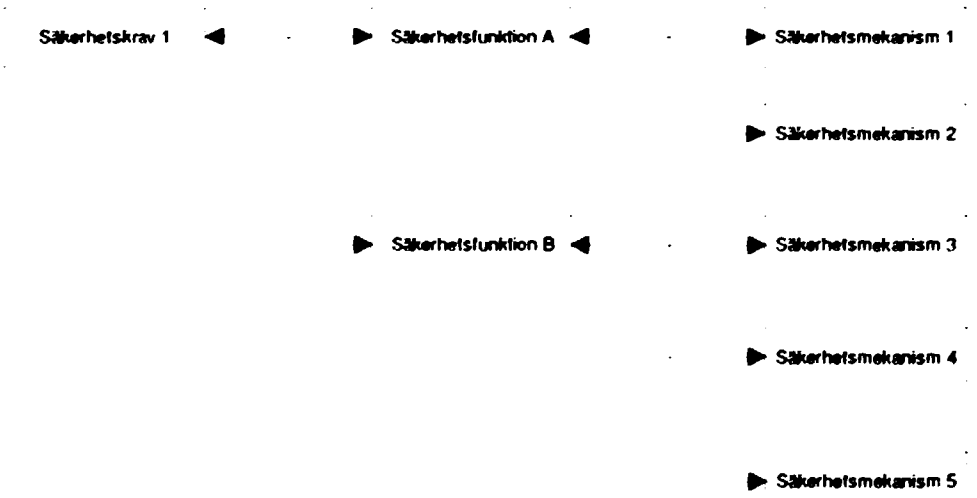
Dessutom brukar man inom informationssäkerhet skilja mellan specificerade säkerhetskrav, säkerhetsfunktioner och säkerhetsmekanismer. På tre olika nivåer beskrivs varför, vad och hur funktionalitet finns i systemet.

De specificerade säkerhetskraven är explicita tekniska krav. De beskriver vilken informationssäkerhet som ska uppnås med systemet och ska vara tydliga tekniska krav. Ett exempel på krav är att korrekt identitet krävs av den som vill läsa mätdata.

Säkerhetsfunktionerna är specifika tekniska egenskaper. Funktionen ska beskrivas som en specifik teknisk egenskap hos ett system vilken gör att säkerheten upprätthålls. Ett exempel på en funktion kan vara att tillgång till mätdata är skyddad genom lösenord.

Mekanismerna är hur en funktion har realiserats. Den teknik som använts vid realisering av en viss funktionalitet ska beskrivas. Ett exempel på en mekanism är den programvaruprocedur som kontrollerar giltigt lösenord innan den skriver ut mätdata.

Ett hot möts alltså med ett eller flera säkerhetskrav. För att sedan kraven ska kunna uppfyllas behöver systemet ha en eller flera egenskaper, s.k. säkerhetsfunktioner. Dessa funktioner realiseras sedan med teknik, s.k. säkerhetsmekanismer. (Se figur 2.)



Figur 2. Exempel på koppling mellan säkerhetskrav, säkerhetsfunktion och säkerhetsmekanism.

För att kunna genomföra evaluering behöver man också veta vilken evalueringsnivå som avses. För system med fjärravlästa elmätare har "PER DOMUM"-projektet bedömt nivå E3 (eller eventuellt E4) vara lämplig. Skäl för detta är systemets komplexitet samt att fel i energileveranserna kan ha inverkan på person- och egendomssäkerhet.

3 Elmätare

3.1 Mätning av elektrisk energi

Elförbrukningen hos hushåll och industrier mäts sedan lång tid med mätare utplacerade hos abonnenten. De ökande kraven på mätning och avräkning ställer nu högre krav på avläsningen av mätarna. Det är inte längre tillräckligt med manuell avläsning av mätaren någon gång per år. Moderna elmätare kan kommunicera med omvärlden för att på elektronisk väg kunna läsas av. Mätvärden lagras sedan centralt i ett överordnat datasystem.

De ursprungliga kraven på tillförlitlighet i informationen förändras inte. Abonnenten vill inte betala för energi han inte har förbrukat, och kraftleverantören vill få betalt för all energi han levererar. Fjärravlästa elmätare måste kunna tillgodose dessa behov lika bra som de etablerade manuellt avlästa mätarna.

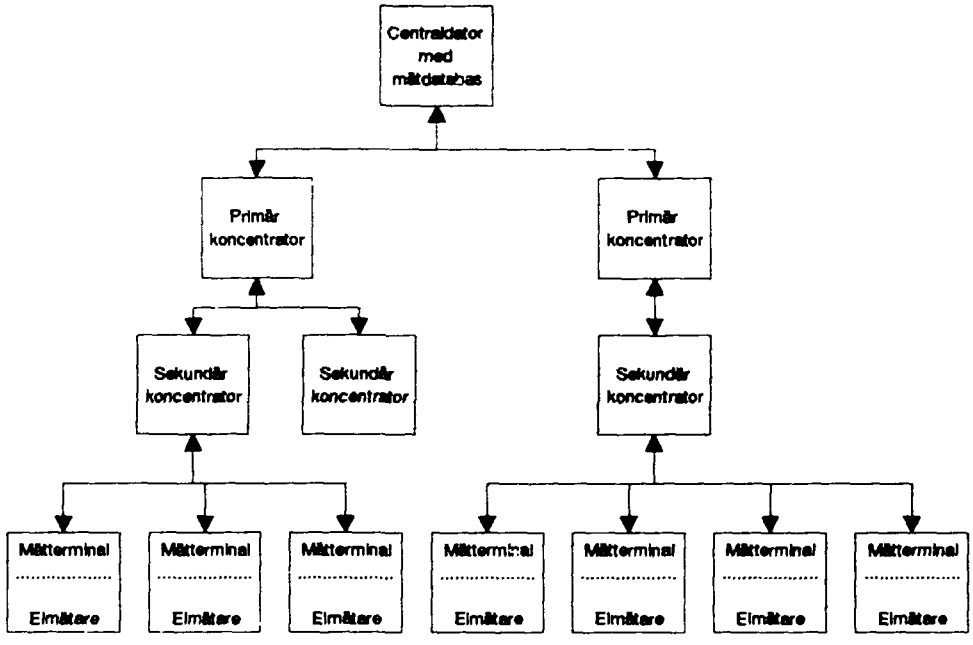
3.2 RCM-systemet

Det system av fjärravlästa elmätare som projekt "PER DOMUM" arbetar med är under utveckling av ett konsortium vilket leds av Ente Nazionale per l'Energia Elettrica (ENEL) i Italien. Man säger att det planeras att under de närmaste 20 åren byta minst 10 miljoner elmätare i Italien till en ny modell. En provanläggning finns idag i drift utanför Rom. Mätaren ska kunna fjärravläsas via elnätet. Genom ett antal sekundära och primära koncentratorer ska systemet kunna erbjuda flexibel och effektiv styrning av energi och avräkning från central nivå. Det kompletta systemet benämns RCM ("Remote Control and Management System").

I RCM-systemet ingår koncentratorer på två olika nivåer. Utrustningen hos kund består av själva elmätaren med mätterminal för kommunikation integrerad. Dubbelriktad kommunikation mellan mätaren och den sekundära koncentratorn sker sedan över kraftnätet. Information från och till flera sekundära koncentratorer samordnas av en primär koncentrator. De primära koncentratorerna kopplas sedan samman till den centraldator där databasen med mätvärden finns. (Se figur 3.) Kommunikationen mellan koncentratorer samt mellan koncentratorer och centraldator sker över kommunikationslinjer med högre kapacitet än kraftnätet.

Industrikunderna förutsätts vara högspänningskunder, medan hushållskunderna är lågspänningskunder. För de flesta industrikunderna finns mätutrustningen i kraftleverantörens (ENELs) lokaler. Däremot har hushållsabonnenterna sin mätutrustning i hemmet. Varje mätutrustning innehåller en processor som lagrar mätdata och på begäran sänder dessa till en sekundär nod. Processorn kan också ta emot order om förändrade parametrar till mätutrustningen. Systemet innehåller redundans vilken ska ge möjlighet till snabb omkonfigurering så att användaren inte ska förlora kontakten med övriga systemet vid fel eller service.

RCM-systemet utvecklades först som ett projekt för att pröva tekniska möjligheter till mätning, avräkning och styrning. Det har sedan successivt vuxit i betydelse till dagens målsättning att sprida systemet över hela Italien. Utvecklingsarbetet har genomförts för att få god säkerhet i systemet, dock inte primärt för att uppfylla EG-kriterierna ITSEC.



Figur 3. Princip för RCM-systemets logiska uppbyggnad.

Kraftleverantören (ENEL) bedömer att det nya sättet att överföra mätvärden och annan information är det som gör systemet mest sårbart. Det finns en risk att hushålls-abonnenten genom manipulation försöker påverka systemet så att för låg förbrukad energi registeras. Den del av systemet där informationssäkerheten behöver utvärderas är alla delar som hushållsabonnenten kan nå, dvs. mätaren, den sekundära koncentratorn, ledningsnätet (som förbinder mätare och koncentrator) samt den användarterminal som kommer att kunna anslutas till mätaren.

RCM-systemet är avsett att fylla flera olika behov. Både mätdatainsamling och styrning av tillgången på elektrisk energi hos abonnenten ska skötas. De viktigaste funktionerna är

- att periodiskt avläsa alla mätdata, utan att fysiskt komma i kontakt med mätaren.
- att styra tillgången på elkraft hos användaren, utan att fysiskt behöva komma i kontakt med anläggningen.
- att ändra tillåten maximal effektförbrukning, utan att manuellt behöva ställa om anläggningen.
- att tillämpa olika taxor vid olika tider på dygnet och/eller året.
- att tillåta olika maximal effektförbrukning vid olika tider på dygnet och/eller året.
- att tillfälligt kunna reducera tillåten maximal effektförbrukning hos en kund (i händelse av nödfall).
- att övervaka balansen mellan levererad och förbrukad energi.
- att övervaka kvaliteten i elkraftleveranserna.
- att sända tekniska eller kommersiella budskap till abonnenterna (via mätarens display).

Dessutom förbereds systemet för en användarterminal som ska kunna anslutas till systemet och tillåta användaren att övervaka sin egen förbrukning av energi.

4 Informationssäkerhet i fjärravlästa mätare

För system med fjärravlästa mätare och till/frånkoppling av energi kan man definiera hot, säkerhetskrav, säkerhetshöjande funktioner och säkerhetsmekanismer. Under projekt "PER DOMUM" samt under SPs arbete med utvärdering av elmätare har flera synpunkter kommit fram. Punkt 4.1 t.o.m. 4.4 ger exempel på viktiga synpunkter. Dessa synpunkter gäller allmänt och inte bara för RCM-systemet som projekt "PER DOMUM" analyserat. Vissa funktioner och mekanismer i listorna gäller inte för RCM-systemet.

4.1 Exempel på hot

De olika hoten kan grupperas som hot mot sekretess, tillgänglighet och integritet.

Bland hot mot sekretess finns
- Mätdata från en förbrukare avläses av obehörig.
- Styrdata till mätare avläses av obehörig.

Bland hoten mot tillgänglighet märks
- Mätaren slutar att registera förbrukad energi.
- Kommunikationen mellan mätare och sekundär nod slutar fungera.
- Periodisk avfrågning av mätvärden slutar fungera.

Bland hoten mot integritet finns
- Felaktigt värde (för högt eller för lågt) registeras på kontot.
- Mätvärden förvanskas.
- Mätdata kopplas till felaktigt konto (dvs. en annan kund än förbrukaren).
- Felaktig tariff tillämpas.
- Mätarens funktion ändras av obehörig.
- Maximalt tillåtet energiuttag ändras av obehörig.
- Kraftleveransen till en abonnent avbryts av obehörig.
- Kraftleveransen till en abonnent kopplas in av obehörig.

4.2 Exempel på specificerade säkerhetskrav

De olika säkerhetskraven kan grupperas för sekretess, tillgänglighet och integritet;

Bland säkerhetskrav relaterade till sekretess finns
- Korrekt identitet krävs av den enhet som begär läsning av mätvärde.
- Korrekt identitet krävs av den enhet som ändrar mätarens funktion.
- Mätvärden får inte avläsas av obehörig.
- Styrdata får inte avläsas av obehörig.
- Data får inte skickas i klartext.

Bland säkerhetskrav relaterade till tillgänglighet finns
- Systemet ska kunna starta om kommunikationen vid "låsningar".
- Mätaren får inte kunna kopplas bort av obehörig.
- Mätaren ska vara försedd med strömkälla för drift vid nätspänningsbortfall.

Bland säkerhetskrav relaterade till integritet finns
- Mätarens funktion får inte obehörigen kunna ändras.
- Mätvärden ska lagras på ett icke-flyktigt sätt.

- Den sekundära koncentratorn får inte innehålla programkod som kan förvanska den överförda informationen.
- Mätaren får inte innehålla programkod som kan förvanska den överförda informationen.
- Systemet ska garantera att avläst värde kopplas till avsett konto.
- De parametrar som definierar mätarens funktion måste vara korrekta.
- Mätarens klocka måste vara korrekt.
- Koppla mätvärden till rätt kund.
- Mätvärdet sänt från mätaren måste vara korrekt.
- Meddelanden och data får inte förvanskas vid överföring.
- Meddelanden och data får inte förvanskas vid transienta förlopp såsom spänningsavbrott eller omkonfigurering av kommunikationsnätet.
- Maximalt tillåtet effektuttag får inte otillbörligt kunna ändras.
- Ett summaregister i mätaren ska innehålla ett mätvärde för all förbrukad energi.
- Mätarens summaregister får inte kunna nollställas.
- Minnet för lagring av programkod får inte kunna förändras.

4.3 Exempel på säkerhetsfunktioner

- Mätaren skyddas mot bortkoppling.
- Mätaren skyddas mot fysiskt intrång.
- Batteristatus övervakas.

- Mikroprocessorns arbete övervakas och mätaren kan återstarta om sig själv om den slutar fungera ("hänger sig").

- Ordningsföljd mellan meddelanden övervakas.
- Dubblering och förlust av meddelanden övervakas.
- Varje meddelande är övervakat mot förändring.
- Korrekt identitetskod krävs av det meddelande som begär läsning av data.

- Tillgång till lagringsminnet för exekverbar kod eller data i en mätare eller en sekundär koncentrator förhindras.

4.4 Exempel på säkerhetsmekanismer

- Mätaren registrerar alla strömavbrott och förändringar i fasläge. Värden sparas i skyddade register (vilka endast kan läsas av nätägaren). Därigenom ges ett sätt att detektera avsiktlig bortkoppling av mätaren eller fel i kraftöverföring.
- Plombering av mätare.

- De skyddade registren skyddas mot otillbörlig läsning genom att det helt enkelt inte finns några kommandon för läsning.
- Parametrar skyddas mot otillbörlig läsning med lösenord.

- Skydd mot förändring av data genom duplicering. (Alla skyddade register finns lagrade på två olika platser i mätarens minne. Dessa två platser kontrolleras för överensstämmelse vid varje läsning eller skrivning. Då de inte stämmer överens indikeras fel.)

- Skydd mot förändring av data genom skrivskydd. (Det finns inget meddelande i kommunikationsprotokollet som tillåter en extern enhet att ändra värdet i ett skyddat register. Skyddade register kan endast skrivas av mätaren själv.)
- Skydd mot förändring av data genom kontrollsummering av dataareor med mätdata. (En kontrollsumma beräknas över en minnesarea med mätdata. Då kontrollsumman inte stämmer med vad som förut beräknas indikeras fel.)
- Skydd mot förändring av data genom kontrollsummering av dataareor med parametrar som styr mätarens funktion. (En kontrollsumma beräknas över en minnesarea med mätdata. Då kontrollsumman inte stämmer med vad som beräknas indikeras fel.)

-Mätaren skyddas mot att oavsiktligt sluta fungera ("hänga sig") genom en krets som övervakar mikroprocessorns arbete och kan återställa processorn om den slutar fungera. (En oberoende krets, "watchdog", triggas periodisk av processorn vid normal funktion. Om triggningarna upphör ger övervakningen larm och återställer mikroprocessorn.)
- Mjukvarumässig övervakning av att sekvensen i programvaran löper korrekt. (De olika delarna av programvaran ska sinsemellan kontrollera att de arbetar i korrekt följd. Då fel i sekvensen detekteras återstartas mikroprocessorn.)

- Varje överfört meddelande ges ett nummer.
- Varje mätare har en (och endast en) unik identitetskod.
- Kontrollsummering av varje överfört meddelande.
- Identifikation av avsändare i varje meddelande.
- Kvittens av varje mottaget meddelande.

5 Utvärdering av informationssäkerhet

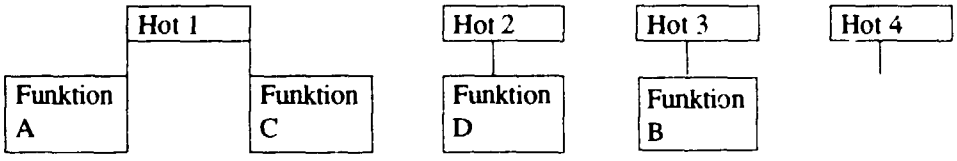
Det finns olika sätt att beskriva hur informationssäkerhet i en produkt eller ett system kan utvärderas. Ett sätt är att i korthet beskriva de olika aspekter från vilka resultat förväntas ingå i en provrapport enligt ITSEM. Avsnitt 5.1 t.o.m. 5.7 beskriver några av de aspekter som ska utvärderas. Ett annat sätt att beskriva utvärderingen är vilket underlag som fordras. Avsnitt 5.8 t.o.m. 5.10 sammanfattar ITSECs krav på dokumentation att använda vid evaluering av korrekthet. [CITI] [ITSEC]

5.1 Ändamålsenlighet hos konstruktionen

5.1.1 Funktionernas lämplighet

Avsikten med att analysera funktionernas lämplighet (engelska "suitability of functionality") är att visa att produkten klarar av att möta de hot den är konstruerad att möta. Hoten mot produkten ska specificeras i säkerhetsmålsättningen. Analysen ska sedan koppla säkerhetsfunktioner och mekanismer till dessa hot. Varje hot ska mötas av en eller flera funktioner. Om så inte är fallet har man funnit en svaghet i produkten.

Figur 4 visar ett exempel där ett av hoten (hot 4) inte möts av minst en funktion. Detta system möter alltså inte samtliga de hot som är förutsedda. Resultatet av analysen blir en anmärkning.



Figur 4. Funktionernas lämplighet

5.1.2 Samverkan mellan funktioner

Samverkan mellan funktioner (engelska "binding of functionality") analyseras för att visa att olika säkerhetsfunktioner och mekanismer knyts till varandra och samverkar på ett tillfredsställande sätt. Funktioner och mekanismer ska stödja varandra för att skapa en integrerad och effektiv helhet. De får inte komma i konflikt med varandra på ett sådant sätt att säkerheten riskeras. Det får alltså inte vara möjligt att två funktioner motverkar eller motsäger varandra.

5.1.3 Mekanismstyrka

Även om en säkerhetsmekanism inte kan kringgås, deaktiveras, förvanskas eller överlistas kan det ändå vara möjligt att komma förbi mekanismen. Beroende på de algoritmer m.m. som mekanismen är baserad på kan man med tillräckliga resurser sätta den ur spel. Denna aspekt av ändamålsenlighet skiljer sig från övriga aspekter genom att den tar hänsyn till vilka resurser en angripare har till sitt förfogande.

Ett exempel på en mekanism som skulle kunna betecknas som svag är en åtkomstkontroll vilken är för lätt att komma förbi. Användning av korta lösenord ihop med möjlighet till ett stort antal åtkomstförsök gör att en angripare med tid kan prova sig fram med olika lösenord. Angriparen kanske kan automatisera förfarandet genom att låta sin egen dator försöka gissa det korrekta lösenordet.

5.1.4 Utvärdering av konstruktionens sårbarheter

Sårbarheter i konstruktionen införs under utvecklingsarbetet. De kan senare komma att utnyttjas av en angripare för att nå information.

En tänkbar sårbarhet är att det minne som tillfälligt används inte "städas" efteråt. En temporär fil på hårddisken kanske inte raderas efter användning. Då kan en angripare läsa den information som finns "kvarglömd" där.

5.2 Ändamålsenlighet vid användning

5.2.1 Lätthet att använda

Risken finns att produkten kan konfigureras eller användas på ett sätt vilket inte ger tillfredsställande säkerhet utan att användaren inser detta. Användaren fortsätter att använda produkten i tron att tillräcklig säkerhet fortfarande finns. Produkten ska vara lätt att använda på så sätt att användaren inte av misstag kan orsaka säkerhetsrisker vid användningen.

Eventuella möjligheter att användaren alltför enkelt "råkar" radera information i en dataarea är ett exempel på sårbarheter vid användning.

5.2.2 Utvärdering av sårbarheter vid drift

Sårbarheter vid drift drar fördel av brister i icke-tekniska motåtgärder. Dessa motåtgärder kan bygga direkt på informationsteknologi, men även på andra tekniker. En motåtgärd som bygger fysiska hinder (lås, dörrar etc.) kan bestämma vilka som har rätt att närvara vid drift.

Exempel på en sårbarhet under drift kan vara att produkten (systemet) kan nås av den som uppsnappar eller tilltvingar sig ett lösenord.

5.3 Utvecklingsprocessen

Även den process enligt vilken utvecklingen skett analyseras för att ge en mer täckande bild av säkerheten. [ITSEC punkt 4.18 t.o.m. 4.22.] Korrektheten i produkten är mycket beroende på hur den utvecklats.

ITSEC och ITSEM talar om 4 olika faser; krav, systemkonstruktion, detaljkonstruktion och implementering. Under kravfasen ska en säkerhetsmålsättning arbetas fram. Därefter inleds konstruktionen på systemnivå genom att bl.a. specificera de hård- och mjukvaruenheter som ska ingå. Det är viktigt att redan från början kunna peka ut vilka

enheter som har betydelse för säkerheten. En låg grad av koppling till enheter vilka inte påverkar säkerheten är viktig. Detta kommer att underlätta en framtida utvärdering.

Den tredje fasen i utvecklingsprocessen är att överföra systemkonstruktionen till en så detaljerad nivå att den kan ligga till grund för programmering och hårdvarukonstruktion. Implementeringen är sedan den fas där mjukvaran och programvaran görs färdig.

5.4 Utvecklingsmiljön

Utöver produktens ändamålsenlighet och utvecklingsprocessen enligt vilken den tagits fram analyseras även utvecklingsmiljön. Konfigurationsstyrning, programmeringsspråk och det tillverkande företagets säkerhet är viktiga. [ITSEC punkt 4.23 t.o.m. 4.26.]

Med konfigurationsstyrning menas hur tillverkaren håller reda på exakt vilken programvara och vilken hårdvara som används i olika versioner av produkten. Allteftersom utvecklingen fortskrider kommer nya versioner av produkten. För varje version måste man veta exakt vilka programvarumoduler och block av elektronikhårdvara som används. Det måste gå att senare kunna exakt återskapa ett visst utförande av produkten.

Valet av programmeringsspråk och kompilatorer påverkar också utvecklingsmiljön. För att ha produkten entydigt bestämd måste man veta exakt vilken version av en viss kompilator som använts under utvecklingen.

Det tillverkande företagets interna säkerhet är viktig. Det får inte finnas risk för att specifikationer, ritningar, programkod m.m. kan läsas av obehöriga. All information om produktens (eller systemets) säkerhetsfunktioner och säkerhetsmekanismer måste vara lagrad på ett skyddat sätt. Detta gäller naturligtvis under hela den tid som produkten kan förväntas vara i användning hos kunden.

5.5 Dokumentation för användning

Tillverkaren behöver försäkra sig om att produkterna och systemen används så att säkerheten inte äventyras. Dokumentationen till användarna är ett viktigt medel. [ITSEC punkt 4.27 t.o.m. 4.29.]

5.5.1 Användardokumentation

Slutanvändaren ska med hjälp av användardokumentationen kunna förstå produktens säkerhetsaspekter. Det är också mycket viktigt att dokumentationen hjälper användaren att förstå vad som kan krävas av honom för att upprätthålla säkerheten. En beskrivning av den "normala funktionen" är inte nog för att man ska förstå hur säkerheten vidmakthålles.

5.5.2 Dokumentation för systemadministratören

Det finns ofta flera olika användare av ett system eller en produkt. Däremot ligger ansvaret för drift och underhåll oftast inte utspritt. De som sköter driften av produkten (systemet) ska ha tillräcklig dokumentation för att kunna konfigurera och hålla systemet i drift på ett sätt som är säkert.

5.6 Driftmiljö

Driftmiljön beskriver leverans, installation och drift av en produkt eller ett system. [ITSEC punkt 4.30 t.o.m. 4.32.]

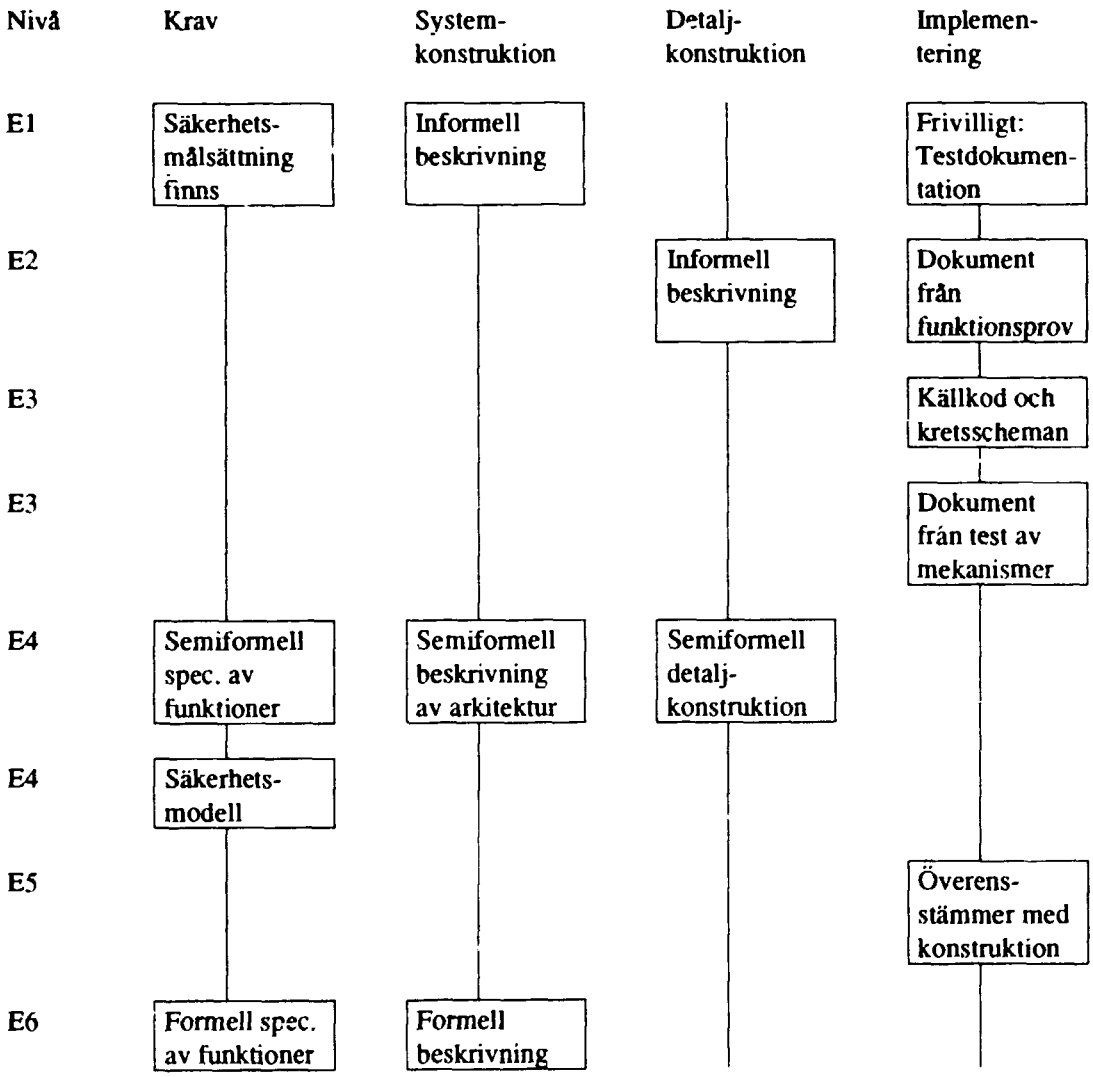
Redan från början i en ny applikation måste man ta hänsyn till informationssäkerheten. Leverans och installation ska ske på ett sådant sätt att säkerheten inte eftersätts. Rutiner för den dagliga driften ska sedan beskriva t.ex. hur systemet startas och stängs. Dessutom ska rutiner vid undantagsfall (t.ex. hårdvarufel) beskrivas.

5.7 Penetrationstest

Ett penetrationstest, eller intrångstest (engelska "penetration testing") går ut på att försöka påvisa brister i förhållande till specifikationen. [ITSEM punkt 3.3.35 t.o.m. 3.3.36 och 4.7.49 t.o.m. 4.7.54.] Man försöker utnyttja de sårbarheter som upptäckts i evalueringsobjektet. Evalueringsobjektet ska användas under normala betingelser, men av testpersonal som har tillgång till samtlig dokumentation om objektet.

5.8 Krav på utvecklingsprocessen

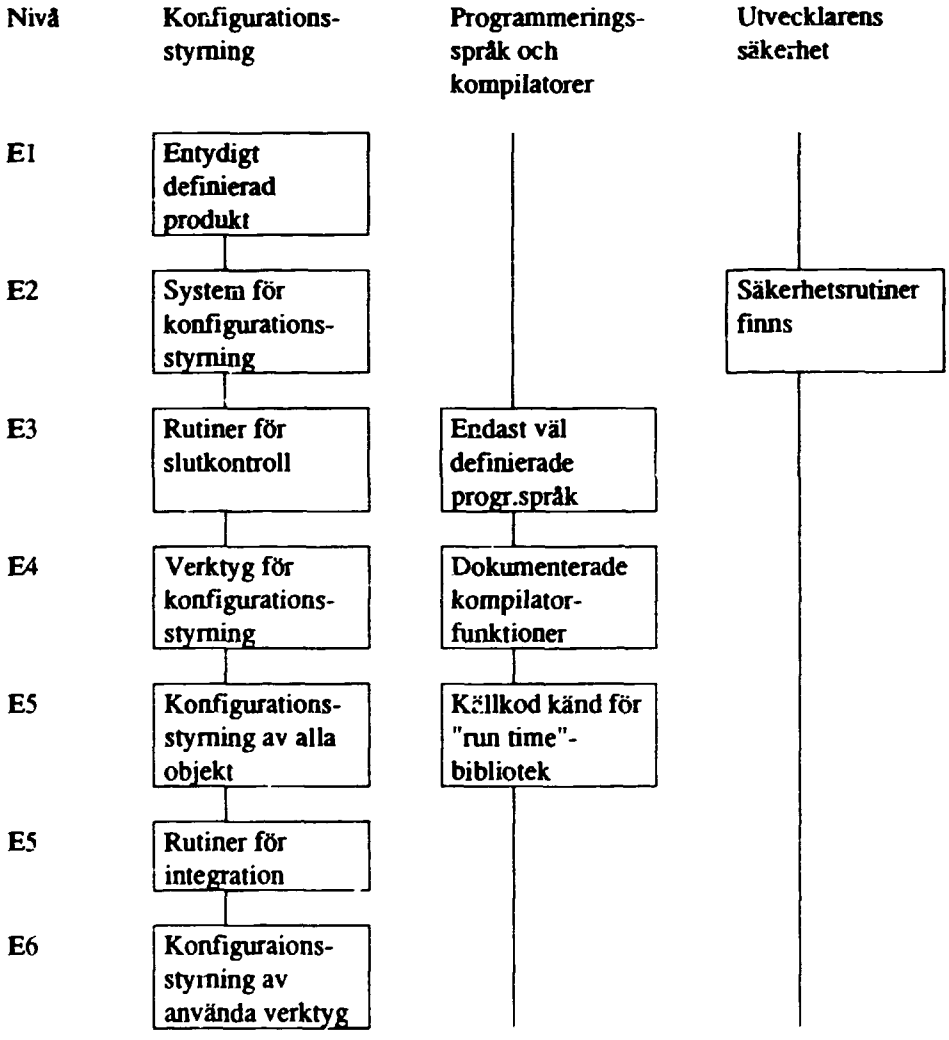
Med ökande evalueringsnivå ökar kraven på utvecklingsprocessen. Tillverkaren behöver presentera fler och mer formella dokument ju högre nivå som avses. Figur 5 visar hur ITSEC beskriver de ökande kraven. Vid varje högre nivå tillkommer ett eller flera dokument som ska utvärderas.



Figur 5. Krav på utvecklingsprocessen

5.9 Krav på utvecklingsmiljön

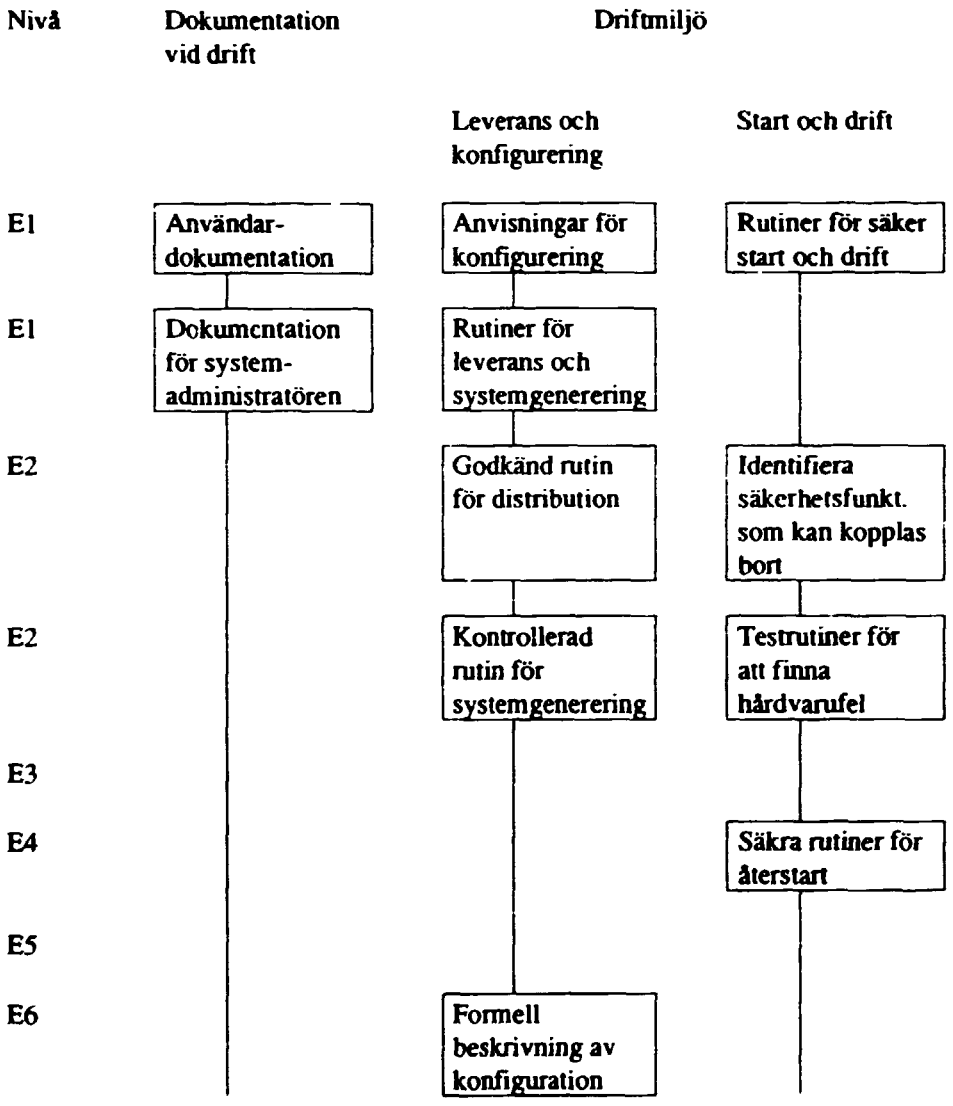
Med ökande evalueringsnivå ökar kraven på utvecklingsmiljön. Tillverkaren behöver en bättre definierad miljö ju högre nivå som avses. Figur 6 visar hur ITSEC beskriver de ökande kraven. Vid varje högre nivå tillkommer ett eller flera krav på utvecklingsmiljön. Det blir alltså viktigt att redan från början bestämma sig för vilken evalueringsnivå som produkten ska klara.



Figur 6. Krav på utvecklingsmiljön

5.10 Krav på stöd för drift

Med ökande evalueringsnivå ökar kraven på det stöd vilket måste ges vid drift av produkten. Tillverkarer behöver en bättre definierad miljö ju högre nivå som avses. Figur 7 visar hur ITSEC beskriver de ökande kraven. Vid varje högre nivå tillkommer ett eller flera krav på utvecklingsmiljön. Det blir alltså viktigt att redan från början bestämma sig för vilken evalueringsnivå som produkten ska klara.



Figur 7. Krav på stöd för drift

Appendix A. Ordlista

Eftersom informationssäkerhetsområdet utvecklas snabbt har ännu inte alla begrepp fått en allmänt accepterad användning och betydelse. I rapporten har strävats efter att följa Informationstekniska standardiseringens terminologi [ITS6]. Förklaringarna i denna ordlista är till största del tagna därifrån. Inom parentes anges den engelska motsvarigheten till termens svenska namn.

assurans (assurance)	tilltro till att ett systems eller en produkts säkerhetsfunktioner, med hänsyn till korrekthet och ändamålsenlighet uppfyller fastställda specificerade säkerhetskrav
informationssäkerhet (information security)	säkerhet vid hantering av information avseende önskad tillgänglighet, kvalitet, sekretess och spårbarhet
IT-säkerhet (IT security)	alla aspekter på säkerhet vid utveckling, drift, användning och underhåll av informations- och kommunikationstekniska system
integrity (integritet)	oberörbarhet, helhet med förmåga att upprätthålla ett värde genom skydd mot oönskad förändring, påverkan eller insyn
hot (threat)	möjlig, oönskad händelse som ger negativa konsekvenser för verksamheten
intrångstest	se penetrationstest
korrekthet (correctness)	vid realisering av en säkerhetsfunktion, egenskapen att en komponents egenskaper, och dess beskrivning i olika abstraktionsnivåer, överensstämmer med specificerade säkerhetskrav
katastrofsäkerhet (safety)	skydd mot katastrofala konsekvenser med skador på person, egendom eller miljö
penetrationstest (penetration testing)	test av säkerheten i ett IT-system i avsikt att påvisa brister i detta i relation till formulerade säkerhetskrav
sekretess (confidentiality)	avsikten att innehållet i ett informationsobjekt (eller ibland även dess existanes) inte får göras tillgängligt eller avslöjas för obehöriga
specificerade säkerhetskrav (security objectives)	explicita tekniska säkerhetskrav
säkerhetsfunktion (security enforcing function)	specifik teknisk egenskap hos ett system genom vilken det, tillsammans med övriga säkerhetsfunktioner, upprätthåller säkerheten

säkerhetsmekanism (security mechanism)	teknik som användes vid realisering av en säkerhets-funktion, eller del av denna
säkerhetsmålsättning (security target)	beskrivning över specificerade säkerhetskrav med hot och tillgångar att skydda. Detta utgör utgångspunkten för evaluering.
tillgänglighet (availability)	möjligheten att utnyttja resurser efter behov i förväntad utsträckning och inom önskad tid
åtkomstkontroll (access control)	funktioner i ett system vilka syftar till att reglera och kontrollera en användares åtkomst till olika resurser
ändamålsenlighet (effectiveness)	mått på i vilken utsträckning ett systems (eller en produkts) säkerhetsfunktioner samverkar för att möta specificerade säkerhetskrav

Referenser

[ITSEC]
Information Technology Security Evaluation Criteria
Version 1.2, 28 June 1991
EG-komissionen DGXIII-F

[ITSEM]
Information Technology Security Evaluation Manual
Version 1.0, 10th September 1993
EG-komissionen DGXIII-B

[INFOSEC93]
INFOSEC '93 Security Investigations
Rev: 5th July, 1993
EG-komissionen DGXIII-B

[INFOSEC94]
INFOSEC '94 Security Investigations
Version 4.1, May 6 1994
EG-komissionen DGXIII-B

[ITS6]
Terminologi för informationssäkerhet
Informationstekniska standardiseringen
ITS-rapport nr 6, mars 1994

[EGIT]
EG & IT, EG och statsförvaltningens informationsbehandling
Statskontorets rapport 1993:23

[SAMS]
Informationssystemens säkerhet i samhället på 90-talet
Finansdepartementet SAMS rapport 1993-06-30
Slutrapport från
Samrådsgruppen för samhällets säkerhet inom dataområdet (C1986:G) (SAMS)

[CITI]
Förslag till svenska insatser rörande informationssäkerhet
Slutrapport från CITI-projektet
IT4-projekt nr 4112, 92-06-24

[DT1-94]
Genombrott för säkerhetsklassade databaser
Datateknik nr 1 1994, sid 42-43

[DT5-94]
Allterminalen svensk uppfinning som gör statens datasystem säkra
Datateknik nr 5 1994, sid. 24-35

[ELFORSK]
Elforsk Rapport 94:9, Krav på mätning och avräkning
September 1994