

Sikkerhedstrusler og -politikker i industrielle trådløse netværk

SKATT – Sikrere og Klogere Produkter gennem Anvendelse af Trådløs Teknologi

Jakob Illeborg Pagter

Center for it-sikkerhed, Alexandra Instituttet A/S

December 2008

1 Indholdsfortegnelse

1	Indholdsfortegnelse	2
2	Resume	3
3	Dokumenthistorik	3
4	Læserens forudsætninger	3
5	Formål	3
6	Baggrund	4
7	It-sikkerhed	4
8	Trusler	8
8.1	Værdier	8
8.2	Kontrolenheder	8
8.3	Måle-/styringsenheder	8
8.4	Real-time data	9
8.5	Lagrede data	9
8.6	Data under kommunikation	9
8.7	Software på enhederne og konfigurationsdata	10
8.8	Oversigt og kategorisering	10
9	Politikker	11
9.1	Log	11
9.2	Backup	11
9.3	Adgangskontrol	11
9.4	Sikker kommunikation	12
9.5	Heartbeat/alarm	13
9.6	Brugbarhed	13
9.7	Sikring af software	13
9.8	Overblik	14
10	Designprincipper	15
11	Litteratur	17
12	Bilag: OCTAVE-diagrammer	18
13	Bilag: Skema for trusselsanalyse	19

2 Resume

I samarbejde med firmaerne Skov A/S og Grundfos Management A/S har Ingeniørhøjskolen i Århus og Alexandra Instituttet A/S i 2007-2008 deltaget i udviklingen af løsningsmodeller til pålidelige og sikre løsninger på nye produkter, som skal anvendes i et industrielt miljø. Projektets navn er SKATT, som er en forkortelse for "Sikrere og Klogere produkter gennem Anvendelse af Trådløs Teknologi".

Dette White Paper er et sammendrag af projektets undersøgelser af trusler og politikker omkring sikkerhedsproblematikker forbundet med anvendelsen af trådløse netværk i industrielle miljøer.

Grunden til at man ønsker at anvende trådløs kommunikation i industriel sammenhæng er primært at dette kan reducere omkostninger til montering og vedligehold.

Dette afstedkommer dog en række nye udfordringer ifht. sikkerhed: hvordan sikres tilgængelighed og pålidelighed i ofte støjfyldte miljøer; hvordan sikres fortrolighed af data; hvordan

I dette dokument diskuteres disse trusler på et generelt niveau, og der gives eksempler på sikkerhedspolitikker som kan anvendes for at imødegå de beskrevne trusler.

3 Dokumenthistorik

Dette er et levende dokument, som vil blive opdateret såfremt der kommer kommentarer med vægtige argumenter for ændringer. Kommentarer kan sendes til skatt@alexandra.dk.

Version	Dato	Forfatter	Bemærkninger
1.0	December 2008	Jakob I. Pagter, Alexandra Instituttet A/S	Første offentlige udgave.

4 Læserens forudsætninger

Det forudsættes at læseren har et generelt kendskab til datakommunikation.

5 Formål

Formålet med dette dokument er at tjene som en skabelon/inspirationskilde i arbejdet med it-sikkerhed relateret til anvendelse af trådløse teknologier i industrielle miljøer.

Dokumentet er ikke en *fuldstændig* beskrivelse af alle sikkerhedsproblemer i forbundet med trådløse teknologier i industrielle miljøer – langt fra – men det

kan tjene som et fundament for sikkerhedsarbejdet i en virksomheds interne sikkerhedsarbejde eller som baggrundsstof ved brug af eksterne ressourcer.

6 Baggrund

Historisk har kommunikation i industrielle miljøer i vidt omfang være baseret på kablet kommunikation. Af effektiviseringsgrunde er der dog et udbredt ønske om at erstatte kablede løsninger med trådløse. Dette er dog langt fra uproblematisk idet trådløs kommunikation langt fra kan give den samme sikkerhed for kommunikationen som kablede løsninger. Selv med kommercielle meget udbredte standarder kan der være store problemer.

Et eksempel er pålideligheden (se *tilgængelighed* nedenfor) af kommunikation, hvor protokoller udviklet til kontor- og forbrugermarkedet langt fra sikrer at beskeder når frem i tilstrækkelig grad (se mere i [1])

Et andet eksempel er den initiale sikkerhedsløsning i IEEE802.11, kaldet WEP. WEP står for Wired Equivalent Privacy og intentionen var at anvendelsen af web skulle sikre *fortrolighed* på et niveau tilsvarende de kablede løsninger tilbyder. Desværre er designet af WEP så fejlbehæftet¹, at man i dag kan knække WEP på få minutter med værktøjer der er alment tilgængelige.

Et helt andet – og måske vigtigere aspekt – er at efterhånden som industrielle løsninger bliver baseret på standard trådløse teknologier, vil de udsætte den samfundsmæssige infrastruktur som disse industrielle løsninger leverer, for en række sikkerhedsrisici. Dette skyldes bl.a. at man af økonomiske grunde vil benytte standardiserede løsninger (fx TCP/IP-baseret kommunikation og fx Microsoft-styresystemer), hvorved den industrielle løsning *automatisk* udsættes for alle de risici der er forbundet med disse løsninger generelt. Denne trussel er ganske alvorlig, da de samfundsmæssige konsekvenser af nedbrud kan være alvorlige. Dette understreges af at fx det amerikanske Department of Homeland Security (DHS) udarbejder "Recommended best practice guides" for fx industriel anvendelse af ZigBee [4].

7 It-sikkerhed

It-sikkerhed handler i denne kontekst om de tre primære egenskaber, som forstås i relation til kommunikation mellem to enheder:

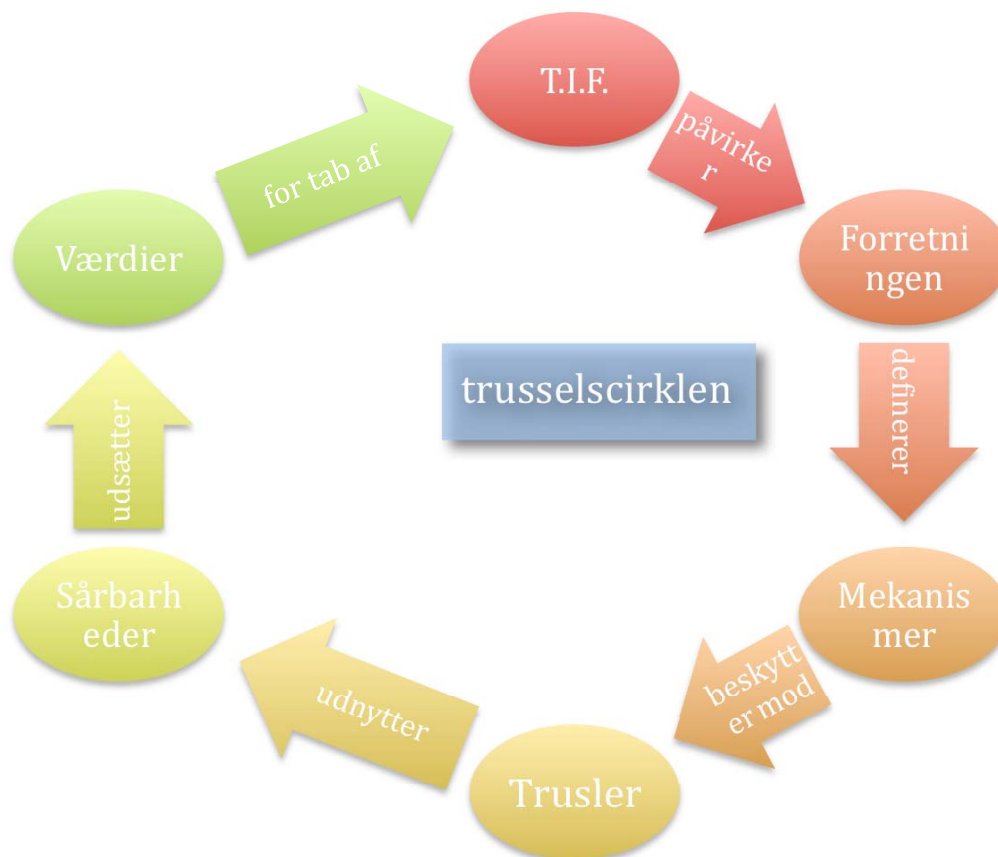
- *Tilgængelighed* – forbindelsen mellem enheder skal være tilgængelig, dvs. at given besked fra den ene enhed til den anden kan nå frem indenfor acceptabel tid. Dette emne diskuteres i dybden i [1].
- *Integritet* – beskeder skal nå uændrede frem og (i visse tilfælde) skal der være vished for hvem afsenderen er (den sidste egenskab kaldes også *autenticitet*).

¹ Se fx http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy.

- *Fortrolighed* – en besked kan kun læses af rette vedkommende, dvs. typisk af modtageren men ofte også af andre (fx i lukkede grupper).

Bag ved disse egenskaber lægger der dog en lang række underordnede sikkerhedsproblemer. Dette inkluderer emner som brugbarhed, nøglehåndtering, anti-virus, netværkstopologi osv., emner som naturligt vil blive diskuteret nedenfor i afsnittet om løsninger.

Disse tre grundegenskaber udsættes for trusler. En risikoanalyse studerer hvor alvorlige de forskellige trusler er ved at kikke på hvor svær en given trussel er at realisere og hvad konsekvensen i givet fald vil være.



Overordnet adresseres it-sikkerhed med udgangspunkt i de trusler som vurderes relevante. Der skabes en trusselsmodel som danner grundlaget for den operationelle it-sikkerhed. I forbindelse med udarbejdelsen af en trusselsmodel vælger man således for hver identificeret trussel om den skal reduceres (dvs. adresseres gennem politik og mekanismer – se nedenfor), delegeres (forsikring) eller accepteres (dvs. ignoreres *bevidst*). Derudover kan der også være ukendte trusler.

Med udgangspunkt i trusselsmodellen samt gældende lovgivning, standarder mm. for problemområdet, defineres en sikkerhedspolitik som opstiller retningslinjer for hvordan forskellige trusler skal reduceres. Eksempelvis kan

politikken ifht. en trussel mod aflytning af trådløs kommunikation være at kommunikation skal holdes fortrolig med stærk kryptering.

Sluttelig realiseres sikkerhedspolitikken operationelt igennem anvendelsen af en række mekanismer. I SKATT, vil den overordnede anvendelse af mekanismer beskrives i en abstrakt sikkerhedsarkitektur, som mere detaljeret beskriver hvad fx stærk kryptering er, som en række andre praktikaliteter. Arkitekturen holdes dog åben for den egentlige realisering, som tænkes gjort vha. de teknologier som besluttes anvendt i det konkrete scenarie. Eksempelvis understøtter wi-fi stærk kryptering i form af 128 bit AES.

Overordnet er der altså tale om:

- Trusselsanalyse
- Beskrivelse af sikkerhedspolitik
- Implementering af sikkerhedsmekanismer

Trusselsanalyse som gennemføres tager udgangspunkt i OCTAVE [6]². Det kardinale punkt er hvilke *værdier* (assets) som trues. Dernæst kikkedes på hvem/hvad der truer, hvad motiverne er, hvordan en trussel kan realiseres og sidst – men ikke mindst – hvad konsekvensen er.

Ifølge OCTAVE, opdeles værdier i: digitale, fysiske og immaterielle værdier. Trusler kan udføres af:

- Mennesker med digital adgang
 - Insider/outsider
 - Bevidst/ubevidst
- Mennesker med fysisk adgang
 - ...
- System problemer
 - Hard-/software-fejl
 - Malware
- Andre problemer
 - Naturkatastrofer
 - Forsyning (el, vand, tele)
 - ...

og konsekvenserne kan være:

- Afsløring eller indblik i følsom information
- Ændring af vigtig eller følsom information
- Ødelæggelse eller tab af vigtig information, hardware eller software

² Alternativt kunne man fx have taget udgangspunkt i Microsofts SDL-metodik [8] som baseres sig på en risikoanalyse kaldet STRIDE [9].

- Afbrydelse af adgang til vigtig information, software, applikation eller services.

Rent metodisk bør der arbejdes med en faseopdelt analyse:

1. Beskrivelse af løsningen og det scenarie den skal anvendes i.
2. Initiel identifikation af værdier og trusler mod disse
 - a. Udgangspunkt i diagrammerne i Bilag: OCTAVE diagrammer.
 - b. Denne fase gennemføres med en projektansvarlig samt repræsentanter for de relevante faglige områder. Dette kan typisk være personer fra udvikling, drift, salg, installation og andre; alle relevante perspektiver på løsninger på være repræsenteret.
 - c. Resultatet fra denne fase dokumenteres i et skema som i Bilag: Skema for trusselsanalyse
3. Eventuel uddybning af særligt relevante og/eller komplekse trusler
4. Kategorisering af trusler for hver værdi
 - a. Dette gøres ud fra skabelonen i Bilag: Skabelon for trusselskategorisering
5. Prioriter og vælg (reducer/deleger/accepter)
 - a. Denne fase gennemføres af de relevante ansvarlige beslutningstagere med relevant teknisk støtte.
 - b. Reducer betyder at sikkerhedspolitikken skal stille krav om håndtering af den beskrevne trussel, og som konsekvens at der skal beskrives mekanismer der adresserer denne trussel.
 - c. Deleger betyder at sikkerhedspolitikken skal nævne denne trussel og beskrive hvorledes den håndteres, fx igennem forsikring eller hvad at den håndteres implicit (eksempelvis at anti-virus-håndtering delegeres til en organisations overordnede sikkerhedspolitik\$ - hvis dette eksempel altså giver mening og er forsvarligt i den konkrete kontekst).
 - d. Accepter betyder at sikkerhedspolitikken skal nævne denne trussel og eksplicit skrive at den ikke håndteres.
6. Definer sikkerhedspolitik
 - a. Sikkerhedspolitikken beskrives kortfattet. Senere i dette dokument gives eksempler på delelementer af en sådan politik.
 - b. Som kontrol sammenholdes sikkerhedspolitikken med trusselsanalysen i en matrix som tydeligt viser hvordan hvilke elementer af sikkerhedspolitikken der adresserer hvilke trusler.
7. Analyser egnethed af forskellige teknologier.
 - a. På baggrund af den beskrevne sikkerhedspolitik kan forskellige trådsløse teknologier nu evalueres for egnethed. Dette kan gøres med udgangspunkt i [1].
 - b. Bemærk at der kan være mange andre perspektiver som stiller krav til løsningen og at den bedste sikkerhedsløsning ud fra et sikkerhedsperspektiv ikke nødvendigvis er anvendelig.

8. Beskriv den endelige sikkerhedsarkitektur ud fra den valgte teknologi.

8 Trusler

8.1 Værdier

De i projektet gennemførte trusselsanalyser identificerede følgende kategorier af værdier (assets):

De fysiske værdier er typisk:

- Kontrolenheder.
- Enheder som styres, med sensorer og aktuatorer.

De digitale værdier er typisk:

- Real-time data., dvs. data som aktuelt behandles men som endnu ikke er lagrede.
- Lagrede data (eksklusiv konfigurationsdata)
- Data under kommunikation.
- Software på enhederne.

I projektet er immaterielle værdier såsom virksomhedens image, intellektuelle rettigheder mv. ikke medtaget, men disse er naturligvis også generelt relevante.

I det følgende gennemgås typiske trusler imod disse værdier ud fra OCTAVE-tilgangen [7].

Det skal kraftigt understreges at dette *ikke* er en udtømmende liste af trusler forbundet med anvendelse af trådløse netværk i industrielle miljøer. Det er de trusler der har været fokus på i projektet.

8.2 Kontrolenheder

En vigtig trussel i denne sammenhæng er *ubevidst* forkert fysisk placering af kontrolenheden (ved montering), således at den fx for langt fra de enheder den skal kommunikere med ifht. radioens rækkevidde eller er udsat for forstyrrende støj.

Ovenstående virker måske ikke som en vigtig trussel, men i relation til kosteffektiv montering af kontrolenheder er det vigtig.

En anden umiddelbar type trussel er tyveri af enheder, men det er her generelt antaget at dette håndteres af brugerorganisationens generelle sikkerhedspolitikker ifht. tyveri³.

8.3 Måle-/styringsenheder

Den primære trussel her er at kommunikation ikke kan komme til/fra enheden pga. fx støj.

³ Dette er reelt en forenkling, da kontrolenheder kan repræsentere større værdi end øvrige fysiske komponenter og/eller være lettere at stjæle.

Da placering af enheder af denne type oftest er defineret af anvendelsen (en enhed som måler vandgennemstrømning sidder hvor vandet strømmer), er truslen om forkert placering ikke relevant. Ifht. tyveri gælder de samme kommentarer som ovenfor.

8.4 Real-time data

Den primære bekymring ifht. måledata som endnu ikke er gjort persistente har vist sig at være tab. Dette kan være et udslag af systemfejl, fx personer som bevidst eller ubevidst slår kommunikation af måledata fra eller støj.

Andre typer af trusler såsom afsløring og ændring af data håndteres primært som trusler i relation til kommunikation.

8.5 Lagrede data

Ifht. lagrede data er der potentielle trusler imod

- Afsløring: insidere (eller outsiders) som gennem fysisk (herunder tyveri) eller digital adgang får adgang til lagrede data.
- Ændring: data som ændres af insidere (eller outsiders) med fysisk eller digital adgang.
- Tab og afbrydelse: data som slettes af insidere (eller outsiders) med fysisk eller digital adgang eller data som mistes pga. tyveri.

Generelt vurderes outsiders i projektet at udgøre en større trussel en insidere, men udover "menneskelige fejl", dvs. insidere i god tro, kommer en alvorlig trussel fra insidere fra insidere som i ond tro forsøger at sabotere systemet eller stjæle data. Det kan fx være fyrede medarbejde eller medarbejde som udfører industrispionage.

Systemfejl er nævnt her som årsag til forskellige problemer ifht. lagrede data, men fungerer – naturligvis – også som trusselsagent mod de øvrige assets. I dette projekt har vi generelt afgrænset os fra at håndtere systemfejl, da denne problemstilling er blevet betragtet som en essentiel del af udviklingsprocessen omkring hardware og software, og derfor håndteret af denne proces.

8.6 Data under kommunikation

I projektet er der identificeret følgende generelle trusler imod data under kommunikation:

- Afsløring
 - Insidere som læser data (fx ved aflytning eller ved at erstatte fysiske enheder med andre enheder)
- Integritet ændret/falsk
 - Insidere som ændrer data
- Tilgængelighed
 - Strømafbrydelse eller systemfejl
 - Dette vil typisk være et (stort) problem i tilfælde hvor en alarm "mistes", eller at der ikke kan sendes besked om at stoppe en enhed (fx en pumpe eller ventilator).
 - Insider som bevidst eller ubevidst gennem fysisk adgang
 - Skaber elektriske forstyrrelser

- Flytter enheder for langt væk fra hinanden (typisk ubevidst)
- Outsider som bevidst eller ubevidst gennem fysisk adgang gør som ovenstående. Forskellen er – specielt for ubevidste fejl – at en outsider ikke på samme måde kan gøres opmærksom på problemet, og specielt kan han ikke selv rette det efterfølgende.

8.7 Software på enhederne og konfigurationsdata

Den sidste gruppe af værdier (assets) er software og konfigurationsdata på enhederne. I projektet er der her identificeret to vigtige typer af trusler:

- Afsløring af konfigurationsdata og/eller software, som kan indeholde forretningshemmeligheder.
- Uautoriserede ændringer i software eller konfigurationer som kan føre til at enhederne ikke overfører sig som forventet. Dette kan afstedkomme alvorlige fejl, fx hvis temperaturen i en stald indstilles for højt.

8.8 Oversigt og kategorisering

	Afsløring	Ændring	Tab/ødelæg	Afbrydelse
<i>Fysiske værdier</i>				
Kontrolenheder			Tyveri	Forkert placering
Styrede enheder				Elektrisk støj
<i>Digitale værdier</i>				
Real-time data			Tab	
Lagrede data	insider/outsider digital/fysisk adgang	insider/outsider digital/fysisk adgang	insider/outsider digital/fysisk adgang	insider/outsider digital/fysisk adgang
Kommunikeret data	Aflytning eller "falske" enheder	Insidere	Strømafbrydelse og lign.	Elektrisk støj eller enheder der fejlplaceres
Software	Afsløring af software eller konfigurationssoftware	Uautoriserede ændringer		

9 Politikker

I det følgende vil blive gennemgået forskellige brudstykker af sikkerhedspolitikker, som afhængigt af de konkrete trusler måske kan finde anvendelse. Dette afsnit afsluttes med en tabel som viser sammenhæng mellem disse forskellige politikker og de ovenfor beskrevne trusler.

9.1 Log

En log bruges til at dokumentere hvad der er sket i et system. Det kan fx være nyttigt ifbm. fejlfinding eller hvis det skal dokumenteres at der er begået menneskelige fejl (bevidst eller ubevidst).

Sikkerhedspolitikken har i projektets scenarier haft særligt fokus på at logge konfigurationsændringer. Det kan fx være ændring af parametre, opdatering af software eller initialisering af systemet. Derudover logges ændringer i backup, jf. nedenstående.

9.2 Backup

En backuppolitik kan fx være:

- Der laves back-up af log i beskyttet hukommelse (fx på write-once read-many RAM, hvor end det fås). Således vil alle ændringer altid kunne spores.
- Der laves back-up i almindelig overskrivbar hukommelse af alle måledata som ikke er "bekræftet afsendt".
Når data er bekræftet modtaget vurderes det ikke at være kritisk at gemme dem, og derfor kan de slettes/overskrives.
- Back-up-lageret kan være fysisk beskyttet med fx en plomberingsmekanisme, såfremt risikoen for tab af data retfærdiggør dette.

9.3 Adgangskontrol

Der arbejdes med to typer adgangskontrol. Adgang for brugere til systemet og adgang for enheder til at kommunikere på det trådløse netværk.

I begge tilfælde består adgangskontrol af 3 skridt:

1. Identifikation – et id præsenteres for systemet.
2. Autentifikation – brugeren eller enhed beviser at han/enheden faktisk har dette id.

Dette kan for brugere foregå udfra et eller flere af følgende paradigmer:

- Noget man er – typisk i form af biometri
- Noget man ved – typisk et password
- Noget man har – typisk en eller anden form for hardware

For enheder giver kun det midterste paradigme – noget man ved – mening.

3. Autorisation – systemet afgør hvilke rettigheder brugeren/enheden har.

En politik for adgangskontrol er altså baseret på en *adgangskontrolmodel* som specificerer en række ting for hhv. brugere og enheder:

- Hvordan identificeres brugere hhv. enheder
- Hvordan autentificeres brugere hhv. enheder
- Hvordan autoriseres brugere hhv. enheder

Derudover er det for både enheder og brugere vigtigt at holde sig life-cycle management for øje, dvs. oprettelse af brugere, styring af rettigheder og nedlæggelse af brugere. Særligt det sidste er ofte et element der ikke er tilstrækkeligt fokus på.

9.3.1 Adgangskontrol for brugere

Adgangskontrolpolitikkerne for brugere i projektet har haft fokus på en enkel rollebaseret model til autorisation, dvs. med få roller, fx:

- Roller
 - Administrator
 - Ejer/Manager
 - Driftsansvarlig
 - Servicetekniker
 - Auditør
 - ...
- De forskellige ressourcer har to typer af rettigheder: læs og ændr (inkl. skriv).
- Bruger- og rettighedsadministration foretages af en bruger i Administrator-rolle:
 - Oprettelse og nedlæggelse af brugere.
 - Redigering af ACLs for ressourcer. ACLs angiver hvilke roller og eventuelt hvilke brugere der må hvad.
- Sikkerhedspolitikken håndhæves lokalt på hver enkelt enhed.

Ifht. identifikation og autorisation af brugere er det ikke muligt at komme med generelle anbefalinger, da det afhænger meget af brugen. Det kan dog anbefales at udnytte infrastruktur der allerede eksisterer i applikationen eller på platformen til dette formål.

9.3.2 Adgangskontrol for enheder

Her anbefales det generelt at benytte den adgangskontrolmodel som den underlæggende kommunikationsteknologi (fx ZigBee eller WiFi) tilbyder, under det forbehold at der tages højde for de forskellige teknologiers styrker og svagheder i relation hertil. Disse styrker og svagheder er beskrevet i [1].

9.4 Sikker kommunikation

I projektet har politikken for sikker kommunikation typisk set således ud:

- Fortrolighed, autenticitet og integritet sikres på et niveau som svarer til AES 128bit.
- Der benyttes sikret nøgleudveksling, som dog skal foregå på "brugbar" vis.
For at sikre at det er let at koble nye enheder på systemet kan man

eventuelt tilføjet til politikken at det accepteres at nøgler transmitteres i klartekst én gang når en ny enhed kobles på systemet.
Problemstillingerne omkring brugbarhed af nøgleudveksling adresseres også nedenfor under politikpunktet "brugbarhed".

- Tilgængelighed af data der skal kommunikeres sikres, dvs. data når altid frem (dog potentielt med forsinkelse hvis forbindelsen er "nede").

Der anbefales stor varsomhed, og hvis ikke man benytter standard løsninger bør man konsultere eksperter i kryptografi. Dette gælder ikke mindst for nøgleudveksling.

9.5 Heartbeat/alarm

Såfremt det er kritisk at sikre sig at der er "hul igennem" kan man benytte en heartbeatpolitik: Enheder opretholder permanent kontakt for at sikre at der kan kommunikeres når der bliver behov for det.

9.6 Brugbarhed

Ifht. brugbarhed er der tre problemområder som kræver særlig opmærksomhed, da dårligt designede løsninger ofte giver problemer her: 1) bruger-login, 2) udveksling af nøgler (typisk ved montering) og 3) konfiguration af sikkerhedsegenskaber (fx roller og deres rettigheder).

Der anbefales derfor at have sikkerhedspolitik elementer som fx:

- Brugerlogin skal designes således at det er tilpasset andre lignende loginsystemer som brugeren møder i sin dagligdag.
- Initial nøgleudveksling/parring kan overvejes at gøres i klartekst: der trykkes på en knap på begge enheder (evt. vises et id) og nøglen udveksles i klartekst.
Benyttes et lukket system – hvis alt udstyr fx er fra samme producent – kan det overvejes at udstyre alle enheder med en fælles masternøgle, som så bruges til at beskytte og evt. generere den udvekslede nøgle.
- Sikkerhedskonfiguration: alle enheder er som default konfigureret med "security-by-default", dvs. de fleste sikkerhedsfeatures slået til.
Derudover bør alle enheder have et sæt af prædefinerede roller og rettigheder.

Ifht. særligt nøgleudveksling anbefales stor varsomhed, og hvis ikke man benytter standard løsninger bør man konsultere eksperter i kryptografi.

9.7 Sikring af software

Ønskes et højt niveau af sikkerhed for oprindelsen af software, kan sikkerhedspolitikken specificere at software der installeres skal være digital signeret og at denne signatur kan verificeres ud fra en certifikatkæde der starter med certifikater som er installeret på enheden.

Benyttes dette element i sikkerhedspolitikken skal der også være en politik for hvordan der installeres nye certifikater (for certifikater bør udløbe). Det kan fx blot være ved at de kan verificeres med de allerede installerede certifikater ved installationstidspunktet.

9.8 Overblik

		Log	Backup	Adgangs kontrol	Sikker kommunikation	Heartbeat/alarmer	Brugbarhed	Sikring af software
Kontrolenheder	Afsløring	X						
	Ændring	X						
	Tab/ødelæggelse	X	X					
	Afbrydelse		X			X	X	X
Styrede enheder	Afsløring	X						
	Ændring	X						
	Tab/ødelæggelse	X	X					
	Afbrydelse		X			X	X	X
Real-time data	Afsløring	X		X	X		X	
	Ændring	X		X	X		X	
	Tab/ødelæggelse		X	X				X
	Afbrydelse	X	X			X		
Lagrede data	Afsløring	X		X	X		X	
	Ændring	X		X	X		X	
	Tab/ødelæggelse		X	X				X
	Afbrydelse	X	X					
Kommunikation	Afsløring	X		X	X		X	
	Ændring	X		X	X		X	
	Tab/ødelæggelse		X	X				X
	Afbrydelse	X	X					
Software	Afsløring	X		X	X			
	Ændring	X		X	X		X	X
	Tab/ødelæggelse		X	X				X
	Afbrydelse	X	X					X

10 Designprincipper

Ken Masica har udarbejdet to dokumenter [4,5] som kommer med anbefalinger for brug af IEEE 802.11 og ZigBee (de to trådløse protokoller SKATT-projektet har haft fokus på) i proceskontrollsystemer, hvilket er tæt relateret til dette projekt. Begge disse dokumenter er værd at læse, også selvom man arbejder med andre trådløse teknologier end de to nævnte.

Særligt beskrives en række designprincipper som er generelle for brug af trådløse netværk i industrielle miljøer:

1. *Defense-in-depth.*
 - Dette princip handler om at man ikke skal forlade sig på en enkelt sikkerhedsmekanisme, men kombinere mange for på den måde at få mange lag sikkerhed.
 - En sikkerhedsløsning som realiserer et passende antal af de her beskrevne sikkerhedspolitikker vil følge dette princip.
2. *Analyser og hærd alle komponenter.*
 - Dette princip siger at man skal kikke på alle enheder og komponenter i et system når man laver sikkerhed. Det er ikke tilstrækkeligt fx at kikke på den del som specifikt handler om den trådløse kommunikation, men også de udenom liggende dele må nødvendigvis tages i betragtning.
 - Som beskrevet i dette dokument skal sikkerhedsarbejdet tage afsæt i en trusselsanalyse af de relevante værdier. Herigennem bør alle relevante komponenter blive analyseret og hærdet i relevant omfang.

I en række scenarier kan man nemt forestille sig at sikkerhedsanalysen bliver endnu mere omfattende en her beskrevet, fx hvis man har særlige servere til log eller backup eller hvis det betragtede system er en del af og kan kommunikere med et større netværk (fx via traditionel trådet kommunikation).
3. *Separer og opdel trådløs og trådet kommunikation.*
 - Dette er et generelt princip som har det formål at sikre at data kun flyder hvor det er nødvendigt. Med andre ord, hvis ikke der er behov for kommunikation mellem enheder på det trådede og det trådløse netværk, så bør det undgås.

Som et eksempel på et specifikt problem dette princip adresserer, gives det forhold at et trådet netværk fx kan give adgang til internettet, hvorfor de trådløse enheder derfor vil kunne ses fra internettet hvis ikke netværket er adskilt.
 - I dette projekt har der kun været fokus på den trådløse kommunikation, så dette princip har ikke været aktiveret, men det er særdeles relevant.
4. *Begræns trafikken til det trådløse netværk.*
 - Såfremt det er nødvendigt med trafik imellem det trådede og det trådløse netværk, bør denne trafik minimeres. Fx kan man arbejde med en firewall med en default "deny-all" politik, som så kan udvides efter behov med åbninger for kommunikation mellem specifikke netværksadresser og -porte.

- I dette projekt har der kun været fokus på den trådløse kommunikation, så dette princip har ikke været aktiveret, men det er særdeles relevant.
5. *Brug de indbyggede sikkerhedsfeatures.*
- Givet at de indbyggede sikkerhedsfeatures i netværksprotokollerne ikke er fejlbehæftede (som fx WEP), vil det være en fordel at benytte disse fordi 1) det er lettere og 2) man benytter en offentligt kendt løsning (hvilket klart er at foretrække ifht. selv at implementere sikkerhed). Derudover kan der være tekniske fordele i relation til fx hand-over mv.
 - Fokus i dette projekt har bl.a. været på at finde ud af hvor og hvornår de indbyggede features er tilstrækkelige ifht. det identificerede behov. De her givne anbefalinger (og anbefalingerne i [1]) er i overensstemmelse med dette princip, tilgangen her er som udgangspunkt at muligheden for at realisere dette princip bør inddrages i beslutningen om hvilket form for trådløs kommunikation der benyttes. Videre skal den indbyggede sikkerhed – såfremt den ikke er tilstrækkelig og andre forhold gør at den bruges alligevel – suppleres med kommunikationssikkerhed mv. på applikationslaget.

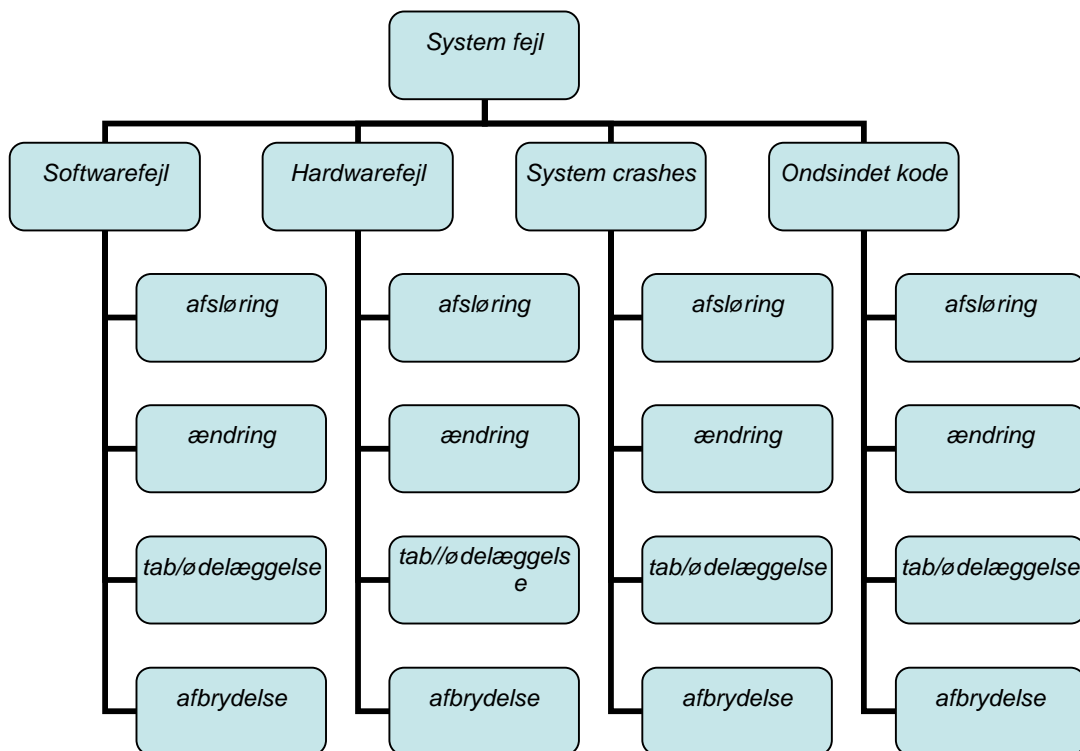
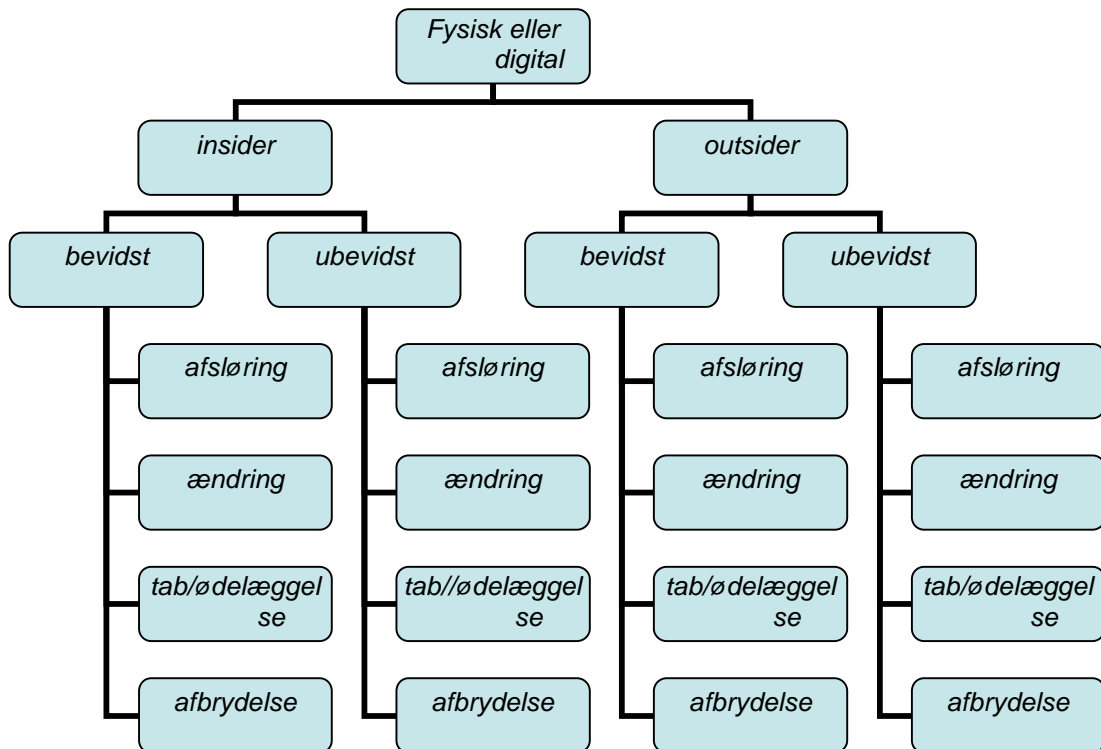
Masicas to dokumenter har også en række recommended practices som er ikke er generelt relevante, men som det kan anbefales at kikke på såfremt man har planer om at benytte IEEE 802.11 eller ZigBee.

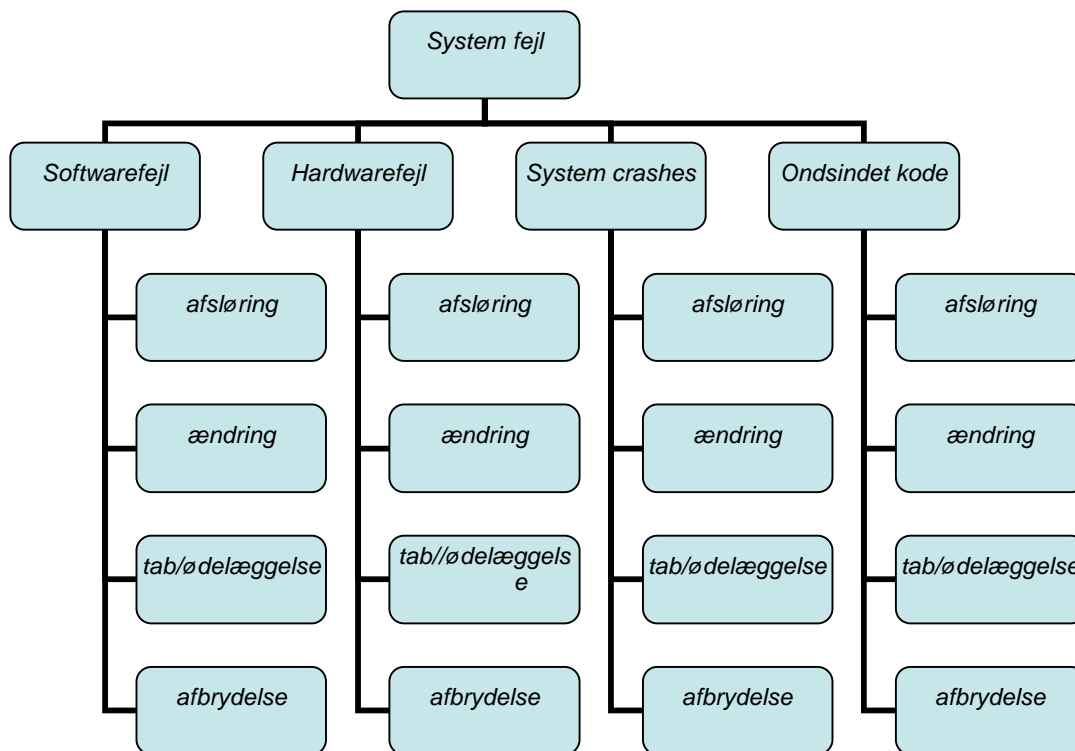
11 Litteratur

1. Torben Gregersen og Jakob I. Pagter: "White Paper: Trådløse netværk i industrielle miljøer". Alexandra Instituttet A/S, 2008.
2. Torben Gregersen, Dan Vinge Madsen, Lars Glavind, Jens Rasmussen, Martin Vestergaard, Sune Wolff og Jakob I. Pagter: "Et pålideligt og sikkerhed IEEE802.11 a/b/g netværk til anvendelse i landbrug", Ingeniørhøjskolen i Århus, 2008
3. Steen Krøyer: "Protokol og algoritmer til optimalt kanalvalg i 802.15.4-baseret peer netværk", Ingeniørhøjskolen i Århus, 2008.
4. Ken Masica: "Securing ZigBee Wireless Networks in Process Control System Environments (Draft)", Lawrence Livermore National Laboratory, 2007.
<http://csrp.inl.gov/Documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%20Control%20System%20Environments.pdf>
5. Ken Masica: "Securing WLANs using 802.11i (Draft)", Lawrence Livermore National Laboratory, 2007.
<http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf>
6. Octave. <http://www.cert.org/octave/>.
7. Christopher Alberts and Audrey Dorofee: "Octave Threat Profiles". Software Engineering Institute, Carnegie Mellon University.
<http://www.cert.org/archive/pdf/OCTAVETHREATProfiles.pdf>
8. The Microsoft SDL Threat Modelling Tool, Microsoft.
<http://msdn.microsoft.com/en-us/security/dd206731.aspx>
9. The STRIDE Threat Model, Microsoft.
<http://msdn.microsoft.com/en-us/library/ms954176.aspx>

12 Bilag: OCTAVE-diagrammer

Disse er oversat til dansk efter [7].





13 Bilag: Skema for trusselsanalyse

Dette skema kan bruges under trusselsanalysen ud fra OCTAVE-diagrammerne. Felterne kan – fx – udfyldes således

- Nummer: forløbende nummering, evt. Subnumre for hver værdi, således at trusler under værdi nummer 5 nummeres 5.1, 5.2 osv.
- Værdi: den værdi som trues.
- Aktør: hvem udfører truslen (første punkt i diagrammet)
- Metode: Andet niveau i diagrammet, gerne med konkrete eksempler.
- Konsekvens: afsløring, ændring, tab/ødelæggelse eller afbrydelse, evt. med konkrete eksempler.
- Prioritet: hvor vigtig er denne trussel.

Nummer	Værdi	Aktør	Metode	Konsekvens	Prioritet