CODEN:LUTEDX/(TEIE-3052)/1-55/(2015)

Industrial Electrical Engineering and Automation

Mobila enheter i DCS-miljö

Sina Bagheri
Sandra Goncalves

Division of Industrial Electrical Engineering and Automation
Faculty of Engineering, Lund University

Mobila enheter i DCS-miljö

Sina Bagheri och Sandra Goncalves

Institutionen för Biomedicinsk Teknik
Avdelningen för Industriell Elektroteknik och Automation (IEA)
LTH Ingenjörshögskolan vid Campus Helsingborg, Lunds Universitet
221 00 Lund, Sverige

Industrial Electrical Engineering and Automation (IEA)
Faculty of Engineering
Lund University
Box 118, SE-221 00 LUND, Sweden

Industriell Elektroteknik och Automation (IEA)
Lunds Tekniska Högskola
Box 118, 221 00 LUND

Abstract

Operators in DCS environments control and supervise the process with the help of *Human-Machine Interfaces* (HMI). The operators are usually stationary (or at least semi-stationary) because the HMI is stationary.

The purpose of this bachelor's thesis is to explore the prospects of using mobile devices, primarily touchpads, in *Distributed Control System* (DCS) surroundings. This includes (but is not limited to) analyzing the risks that come with wireless transmission, such as data tapping and signal interference.

The end goal of our work has been the implementation of a Panasonic Toughpad FZ-G1 (the mobile device) for Perstorp AB, thus we have also spent some time improving the usability of the FZ-G1.

Keywords: DCS, DeltaV, Emerson, HMI, mobile device, Panasonic Toughpad FZ-G1, Perstorp, SCADA, touchpad, Windows 8, wireless, WirelessHART, 802.11

Sammanfattning

Operatörer i DCS-miljö styr och övervakar processerna med hjälp av *Human-Machine Interfaces* (HMI). Eftersom att HMI-stationerna är stationära blir också operatörerna, för det mesta, stationära.

Syftet med denna tes är att utforska möjligheten att använda mobila enheter, främst surfplattor, i *Distributed Control System* (DCS) miljöer. Det har till stor del inneburit att vi analyserat de risker som trådlös kommunikation medför, så som dataavlyssning och signalstörningar.

Ändamålet med vårt arbete har varit att implementera en lösning som inkorporerar Panasonic Toughpad FZ-G1 för Perstorp AB och därför så har vi också lagt ner en del tid på att förbättra användarbarheten hos FZ-G1:an.

Nyckelord: DCS, DeltaV, Emerson, HMI, mobil enhet, Panasonic Toughpad FZ-G1, Perstorp, SCADA, surfplatta, trådlös, Windows 8, WirelessHART, 802.11

Innehåll

Förord

Detta examensarbete har utförts som del av Elektro- och automationsingenjörsprogrammet på LTH Campus Helsingborg. Examensarbetet omfattar 22,5 högskolepoäng och arbetet har delats upp lika mellan Sina Bagheri och Sandra Goncalves.

Vi vill passa på att rikta ett stort tack till alla som har bidragit till detta examensarbete:

Anders Svensson, för sitt stora engagemang och sina goda råd som hjälpt oss att tänka ett steg längre.

Vi vill naturligtvis också tacka Anders och resten av Perstorp AB för att ha gett oss möjligheten att utföra examensarbetet hos dem.

Dr. Ben Smeets, för att med stor glädje ha delat med sig av sin enorma kunskap inom datakrypteringsområdet.

Dr. Christian Nyberg, för sina råd inom datakommunikationsområdet och för att ha hjälpt till med struktureringen av rapporten.

Dr. Mats Lilja, som tack vare sin stora allmänbildning har kunnat upptäcka detaljer som är lätta att missa och för att ha hjälpt oss med struktureringen av rapporten.

Sina Bagheri och Sandra Goncalves

1. Introduktion

Detta examensarbete har utförts för Perstorp AB under perioden januari – maj 2015.

I samband med en systemändring året innan så hade de fått med en Panasonic Toughpad FZ-G1 (som i denna rapport kommer att benämnas som "surfplattan") men av flera skäl så var den väldigt olämplig att använda, inte bara i fabriken utan överhuvudtaget.

Vi fick i uppdrag att undersöka möjligheten att sätta surfplattan i bruk i den befintliga styrmiljön viket bl.a. har inneburit riskanalyser och mjukvaruändringar. Att införa ny teknik i ett befintligt välfungerande system kan medföra nya risker och det är något som har präglat våra tankar under hela arbetets gång.

1.1. Företag

1.1.1. Perstorp AB

Perstorp AB grundades 1881 och till en början tillverkade man bl.a. tjära, träsprit och ättika. Under tidiga 1900-talet började tillverkningen av formalin, kreosot, plastlaminat med mera och företaget har sedan dess bara växt. Idag inriktar man sig främst mot specialkemi och tillverkningen sker i åtta länder.

Koncernen har idag runt 1500 anställda i 22 länder och omsätter omkring 10 miljarder [33][34].

1.1.2. Emerson Electric Manufacturing

Emerson Electric grundades 1890 i St. Louis, Missouri. Företagets verksamhet byggdes upp kring växelströmsmotorer och de sålde den första elektriska fläkten i Nordamerika 1892. Under början av 1900-talet blev växelströmsmotorn kraftfullare och kunde börja användas i symaskiner, tvättmaskiner m.m. [35].

Emerson Electric är i dag ett globalt företag med ca 115 000 anställda runt om i världen och har numera delats upp i fem sektioner [36]. Det är en av dessa sektioner, ”Emerson Process Management”, med sitt svenska huvudkontor i Karlstad, som man på Perstorp AB främst är i kontakt

med. Emerson Process Management levererar kompletta program av produkter och tjänster inom processautomation och där ingår även projektutförande, utbildning m.m. [43].

1.2. Syfte

Syftet med detta examensarbete var att undersöka eventuella användningsområden för mobila enheter i informations- och styrmiljöer. Det innebar främst att vi undersökt vilken inverkan mobila enheter har på datasäkerheten, hur stor risken för signalstörningar är samt hur användarvänlig enheten är.

1.3. Målformulering

1.3.1. Analysera datasäkerheten

Att granska datasäkerhet i information- och styrsystem är fortfarande relativt nytt men ändå aktuellt, minst sagt. Vi skall undersöka om den mobila enheten Panasonic Toughpad FZ-G1 (med operativsystemet Windows 8) kan medföra nya hot mot datasäkerheten och hur det i så fall går att minimera de riskerna.

1.3.2. Förebygga signalstörningar

I en industrimiljö full med givare och annan elektronik så finns mycket som kan störa ut kommunikationen mellan en mobil enhet och accesspunkt. I industrimiljö är det inte acceptabelt att enhetens signaler fördröjs eller tappas, inte ens i några sekunder. Vi skall se över potentiella orsaker bakom signalstörningar och hur de kan minimeras.

1.3.3. Utöka användbarheten

Problemet med surfplattan, så som den levererats till Perstorp AB, är att den är väldigt svår att använda. Alla grafikbilder blir mycket mindre på en 10.1” skärm och det faktum att standardtangentbordet för Windows 8 upptar halva skärmen gör inte situationen bättre. Ifall man kombinerar det med en väldigt dåligt kalibrerad pekpenna

så förstår man nog att surfplattan, i det tillståndet, inte lämpar sig särskilt väl för industribruk.

Som del av vårt uppdrag så skall vi kalibrera pennan samt göra något åt det dåliga standardtangentbordet och de icke anpassade processbilderna.

1.3.4. Undersöka lämpliga arbetsmoment

Tanken med att införa en mobil enhet är att den ska fungera som ett komplement till den befintliga styr- och övervakningsutrustningen, inte som en ersättning för den. Mobila enheters fördelar är bl.a. att de är flexibla och enkla att ha med sig, vilket innebär att användaren ständigt har tillgång till information om processen och inte behöver ta kontakt med kontrollrummet eller ta sig dit för att få reda på aktuell status i fabriken. Arbetsuppgifter där mobila enheter kan komma till nytta är bl.a. operatörsrondering, utlastning och övrigt underhållningsarbete i fabriken.

Det kan visa sig att surfplattan, av olika skäl, inte passar för alla arbetsmoment och därför måste vi eventuellt föreslå en avgränsning av användningsområdet.

1.4. Problemformulering

- Hur påverkas säkerheten i information- och styrmiljöer efter introduktion av mobila enheter och hur kan eventuella risker förebyggas?
- Vilka är de största hoten mot signalstörningar och hur kan man minimera dem?
- Hur kan användarbarheten förbättras med Windows 8?
- Vilka arbetsmoment är surfplattan lämplig att användas till?

1.5. Avgränsningar

1.5.1. Säkerhet hos informations- och styrmiljöer

Vi fördjupade oss inte i allmän säkerhet hos informations- och styrmiljöer utan koncentrerade oss istället på hur introduktionen av mobila enheter påverkar säkerheten i en informations- och styrmiljö.

1.5.2. Grafikbilderna över processerna

Processernas grafikbilder är skapade för 24” monitorer, men surfplattan har en 10.1” display. Det blir väldigt problematiskt eftersom att allting blir mycket mindre på en 10.1” display. Vi valde trots det att inte rita om några grafikbilder över processerna. Det hade varit en möjlighet, men arbetets omfattning hade varit för stort ifall vi skulle genomföra det på samtliga bilder. Vi fokuserade istället på att hitta allmänna lösningar som skall fungera oavsett processbilden.

2. Teknisk bakgrund

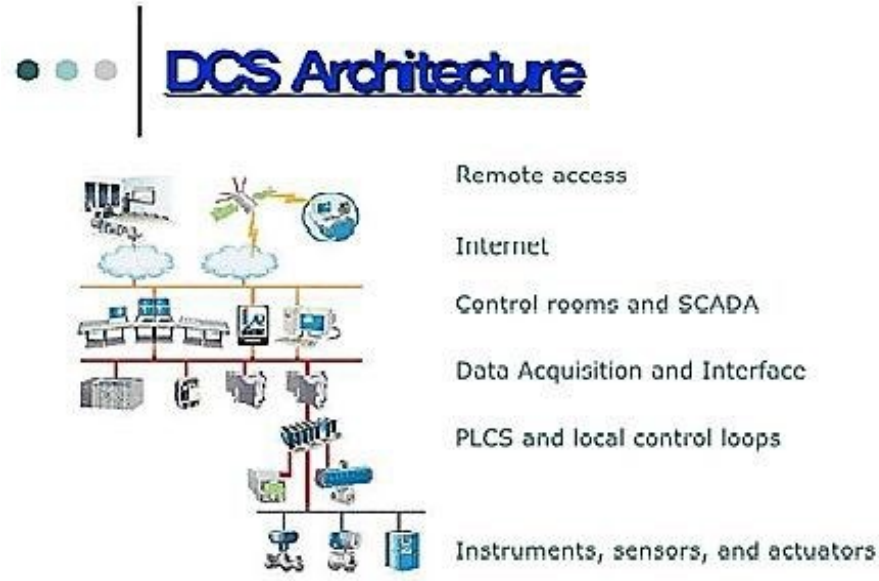
2.1. SCADA-system och DCS

SCADA-system (Supervisory Control And Data Acquisition) och DCS (Distributed Control Systems) är benämningen på industriella informations och styrsystem [1]. Som namnen antyder så används systemen både till att övervaka fysiska processer genom att samla in, lagra och bearbeta information och sedan för att använda informationen till att styra processen. Systemen används bl.a. vid framställning och distribuering av många funktioner i samhället så som värme, el, vatten och mat, samt inom tillverkningsindustrin.

Storleken på systemen kan variera stort och processen som övervakas behöver inte nödvändigtvis finnas på samma plats som övervakningen av systemet sker utan kan vara utsprida i en kommun eller över ett helt land. De lokala obemannade systemen samlar in data som överförs via ett nätverk för att sedan nå fram till det centrala bemannade systemen där processen övervakas och styrs.

Kommunikationen har traditionellt sett skett via trådbundna nätverk men trådlösa mesh-nätverk (bl.a. Zigbee och WirelessHART) blir allt vanligare. Historiskt sett har systemen varit fysiskt isolerade och byggda på specialutvecklad teknik men med tiden har de blivit allt mer integrerade med andra system, något som gjort systemen mer praktiska men även ökat säkerhetsriskerna.

Se figur 1 för en överskådlig bild över DCSs arkitektur.



FIGUR 1: Arkitekturen hos DCS [38]

2.1.1. Termerna SCADA och DCS

För att bättre förstå skillnaden och likheten mellan SCADA och DCS så kan man expandera akronymerna.

SCADA: *Supervisory Control And Data Acquisition*

DCS: *Distributed Control Systems*

Som synes så ingår termen *"Control"* i bägge akronymer men i SCADA ingår även *"Data Acquisition" (datainhämtning)*. Förr i tiden så var det p.g.a. långsamma datanätverk mer praktiskt att ha en tydlig uppdelning där DCS enheterna låg närmre de fysiska processerna och fick sköta processtyrningen. SCADA-systemet samlade sedan information via DCS och kunde dessutom ge nya order till DCS [4].

Se Fig.1 för en illustration över hur SCADA och DCS interagerar. DCS är en benämning på systemet som helhet, där SCADA ingår som en del av systemet.

I takt med att teknologin utvecklas allt fortare så har gränsen mellan DCS och SCADA i många fall mer eller mindre suddats ut. Av bekvämlighetsskäl så kommer vi hädanefter i denna rapport att använda oss utav akronymen DCS då vi syftar till informations- och styrsystemen.

2.1.2. Säkerheten hos DCS

Eftersom att DCS traditionellt sett har varit separerade från andra system så har man generellt sett inte varit orolig för intrång, men i takt med att systemen kopplas upp mot externa publika nätverk (t.ex. Internet) så bör man öka medvetenheten i organisationen om det ökade behovet av informations- och IT-säkerhet [2]. De flesta system utvecklades utan någon åtanke att systemet en dag kommer att kopplas upp mot externa nätverk, vilket leder till många säkerhetshål.

Det finns en hel del bra åtgärder man kan ta för att öka säkerheten hos organisationens DCS, bl.a. att avbryta alla onödiga anslutningar mot systemet, men inte ens fullständig isolering från Internet garanterar att man är säker från intrång. En ögonöppnare för de som arbetar inom DCS-miljö var datamasken Stuxnet som via en USB-sticka gjorde intrång i ett fysiskt isolerat DCS [3][12]. Genom att hacka kärnkraftsanläggningar i Iran så visade man att skadlig kod kan användas som ett vapen eller påtryckningsmedel.

För den som vill fördjupa sig i DCS-säkerhet så finns det numera mycket information att hitta, inte minst hos *Myndigheten för samhällsskydd och beredskap* (MSB) eller *U.S. Department of Energy*, som bl.a. har sammanställt en punktlista [13] med åtgärder för att öka säkerheten hos organisationens DCS.

I denna rapport så tittar vi främst på hur introduktionen av mobila enheter påverkar säkerheten och kommer därför inte att fördjupa oss i allmän DCS-säkerhet.

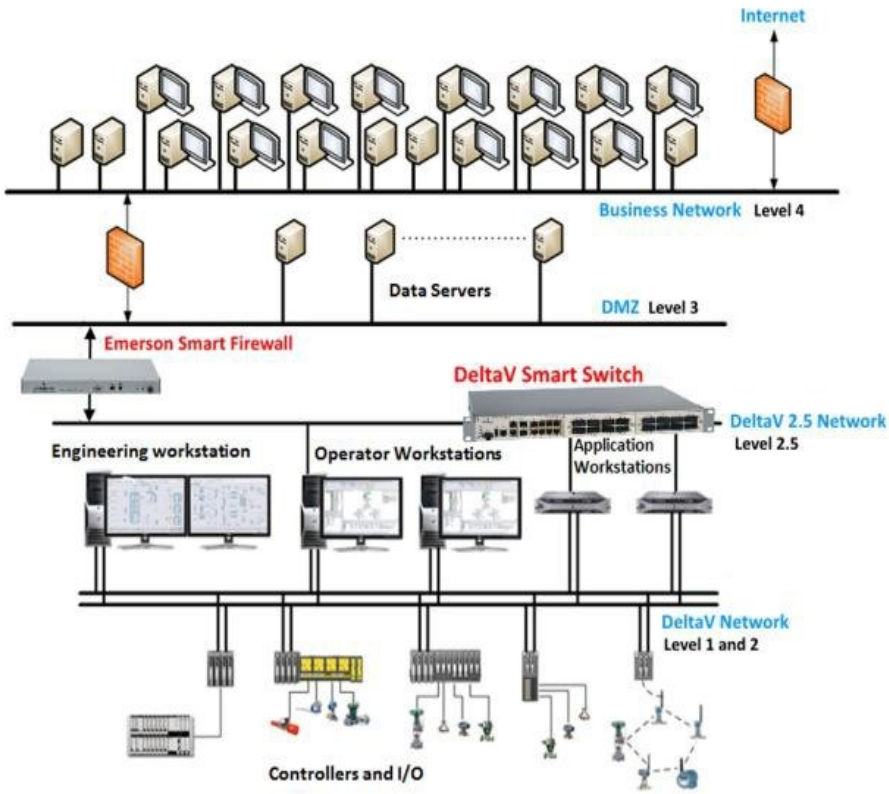
2.1.3. DeltaV

DeltaV är ett DCS utvecklat av Emerson Process Management. DeltaV används i många olika system runt om i världen, oberoende av systemens storlek. Alltifrån 25 till 1 miljon I/O-enheter (Input/Output) fungerar med DeltaV [51]. Den som vill läsa mer om

DeltaV kan titta på översiktsbroschyren som länkas till i referens nummer 51.

Perstorp AB använder sig av DeltaV för att styra processerna i sina fabriker.

2.1.4. Nätverksstruktur hos organisationer



FIGUR 2: DeltaV DCS-miljö [50]

Figur 2 visar hur strukturen av ett nätverk inom ett industriföretag kan se ut. Mellan kontorsnätverket och industrinätverket finns en hårdvarubaserad brandvägg. En brandvägg är till för att filtrera bort otillåten trafik medan behörig trafik släpps igenom. Både ingående och utgående trafik kan filtreras.

Hårdvarubrandväggen är en extern enhet, ofta inbyggd i en router, medan mjukvarubrandväggen är installerad i en dator [44].

I switcharna finns mjukvarubrandväggar som trafiken måste passera igenom för att få åtkomst till servrarna.

Enligt MSB är det viktigt att ha ett djupledsförsvar i sin säkerhetsarkitektur [45]. Med ett djupledsförsvar menas det att ha överlappande säkerhetsmekanismer mellan de olika nivåerna i nätverket. Ifall nätverket är indelat i olika zoner där varje zon består av en grupp komponenter och system med olika kriterier för säkerhet och funktion kan skyddsmekanismerna bevaka zongränserna. MSB ger flera rekommendationer som bygger på standarder, bl.a. ISA-95 och IEC 62443-3-3 (kap 9.4) standarderna:

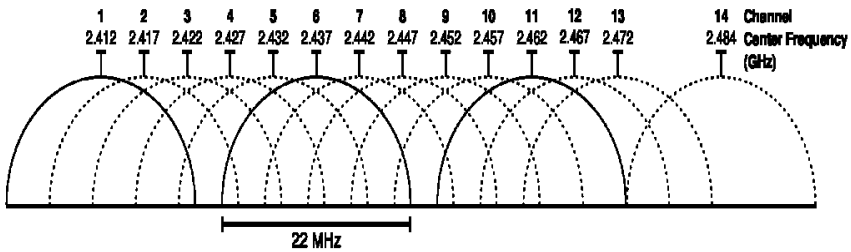
- Dela upp de industriella informations- och styrsystemen i olika zoner med skyddsnivåer som anpassats efter hur kritiska de olika systemen är. Beroende på bland annat system- och informationsklassificering kan även så kallade subzoner behöva skapas [45].
- Datatrafik över zongränserna bör hanteras extra restriktivt och även övervakas och loggas. För vissa typer av IT-miljöer kan det vara bra att använda datadioder och dataslussar [45].
- Undvik att ansluta IT-system och dess stödfunktioner (till exempel datalagring) till flera zoner parallellt (så kallad multihoming), då det kortsluter zonuppdelningen och aktivt motverkar zonmodellen som säkerhetskoncept [45].
- Placera osäkra tjänster och andra externa anslutningar i demilitariserade zoner (DMZ) [45].
- Nätverksarkitekturen bör vara segmenterad med överlappande säkerhetsmekanismer [45].
- Använd gärna olika kommunikationsprotokoll mellan olika delar av nätverket. Om ett protokoll används, för det kommunikationen vidare mellan DMZ:n och organisationens administrativa informationssystem [45].

2.2. Trådlös datakommunikation

Mobila enheter använder av praktiska skäl trådlös kommunikation, inte minst WLAN, där man främst utnyttjar frekvenser kring 2.4- och 5GHz.

2.2.1. 2.4GHz-bandet

Det vanligaste frekvensbandet för WLAN-kommunikation är 2.4GHz-bandet. Det är ett licensfritt band och i de flesta länder så får man använda alla frekvenser mellan 2.40- och 2.48GHz.



FIGUR 3: Grafisk representation över 2.4GHz-bandets kanaler [22]

Som synes i Figur. 3, så är 2.4GHz-bandet uppdelat i 14 kanaler. Eftersom att varje kanal upptar 22MHz så leder det till att många kanaler överlappar varandra. De kanaler som inte överlappar varandra och därmed inte stör varandra är kanal 1, kanal 6, kanal 11 och kanal 14. Kanal 14 är inte laglig att använda i andra länder än Japan [23][24] och därför så återstår det från de ursprungliga 14 kanaler endast 3 lämpliga kanaler att använda. Innan man väljer vilken av kanalerna 1, 6 och 11 man vill ställa in accesspunkten på så kan man göra ett signaltest, där man bl.a. kollar hur belastade de olika kanalerna är.

2.2.2. 5GHz-bandet

Ett alternativ som blir allt vanligare är att kommunicera via 5GHz-bandet istället. 5GHz-bandet har 23 icke-överlappande kanaler mellan frekvenserna 5.17- och 5.83GHz [25][26], vilket ger stora möjligheter

att undvika signalstörningar som kan leda till ett långsamt nät, tappad anslutning m.m.

Det finns också nackdelar med 5GHz-bandet, främst att räckvidden är sämre än hos 2.4GHz-bandet och att penetrationsförmågan är betydligt mycket sämre.

En mycket enkel jämförelse mellan 2.4- och 5GHz-bandet kan göras enligt tabell 1.

TABELL 1**:** 2.4GHz-bandet i jämförelse med 5GHz-bandet.

Frekvensband	**2.4GHz**	**5GHz**
Datahastighet	Sämre	Bättre
Signalstörningar	Fler	Färre
Räckvidd	Bättre	Sämre
Penetrationsförmåga	Bättre	Sämre

För att få det bästa av två världar så kan man använda sig utav Dual Band teknologin.

2.2.3. Dual Band

Dual Band teknologi innebär att accesspunkten kan sända på både 5GHz- och 2.4GHz-bandet. Det kan ske antigen samtidigt (Simultaneous Dual Band) eller med ett band i taget (Selectable Dual Band) [27].

Om man använder Dual Band så är det vanligt att man större delen av tiden är uppkopplad mot 5GHz-bandet och automatiskt kopplas upp mot 2.4GHz-bandet när 5GHz-signalerna blir för svaga, oftast p.g.a. ovan nämnda skäl.

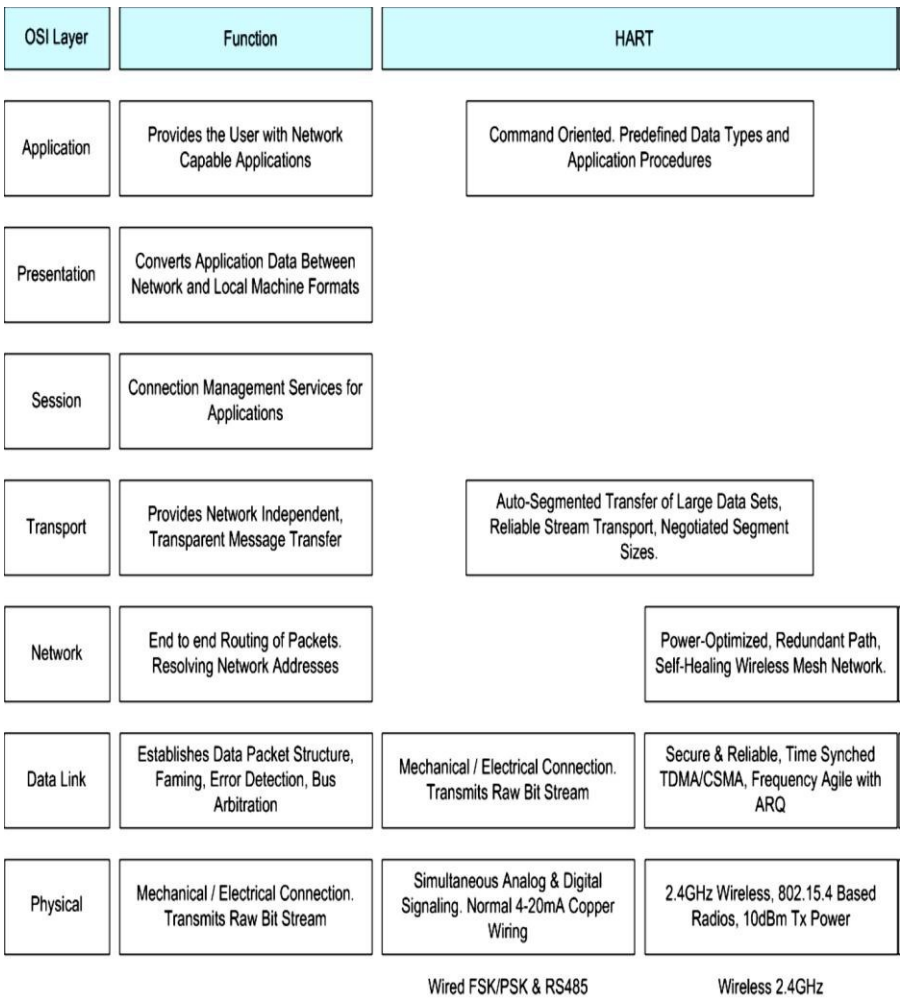
2.2.4. WirelessHART

WirelessHART är ett trådlöst kommunikationsprotokoll som är baserat på HART (Highway Addressable Remote Transducer) protokollet, vilket funnits sedan 1980-talet [10]. Protokollet används

för trådlös kommunikation mellan givare och annan mät- och styrutrustning. Emerson Process Management, som har varit med och utvecklat standarden, inkluderar numera utrustning som använder sig utav WirelessHART i sina processlösningar.

Perstorp AB vill naturligtvis ta del av den bästa teknologin och skall därför börja utnyttja WirelessHART, det innebär att vi måste undersöka hur WirelessHART, som kommunicerar på 2.4GHz-bandet, kan påverka surfplattan.

Figur 4 illustrerar WirelessHARTs arkitektur.



FIGUR 4: WirelessHART ENLIGT OSI-MODELLEN [11]

Kommunikation inom WirelessHART sker via 2.4GHz-bandet och använder sig utav IEEE 802.15.4 standarden (se 2.3 för mer information om IEEE standarder för trådlösa nät). Eftersom kommunikationen sker på 2.4GHz-bandet så kommer signalerna att få trängas med signaler från WiFi-nät, mikrovågsugnar, Bluetooth och flera andra sorters trådlös kommunikation. Detta löser man m.h.a. *Direct-sequence spread spectrum* (DSSS) och *Time Division Multiple Access* (TDMA) [16].

DSSS är en frekvensmoduleringsteknik. En mycket viktig egenskap hos DSSS är att det skyddar mot oavsiktliga och avsiktliga störningar. Avsiktliga signalstörningar hade utan frekvensmoduleringstekniker hade varit ett ännu större hot, inte minst mot verksamheter med DCS-miljö.

TDMA är en accessmetod som låter flera enheter kommunicera på samma frekvensband genom att varje sändare blir tilldelad ett tidsintervall där sändaren har tillgång till kommunikationslinjens hela överföringskapacitet. Sändaren har då möjlighet att skicka information eller låta bli att skicka ifall det inte finns någon information att skicka. När tidsintervallet är slut går turen över till nästa enhet och sändaren kan inte skicka något förrän det bli dess tur igen. Fördelen med TDMA är att inga krockar sker eftersom sändarna enbart tillåts att sicka paket när det är deras tur. Nackdelen är att alla sändare kanske inte alltid har något att skicka vilket betyder att linjens kapacitet blir oanvänd under deras tur [19].

Flera företag erbjuder produkter för WirelessHART och de är alla kompatibla med varandra. Då HART-protokollet är ett master-slave kommunikationsprotokoll så finns det en lista över HART-kommandon som kan delas in i tre kategorier, ”Universal”, ”Common Practice” och ”Device Specific”.

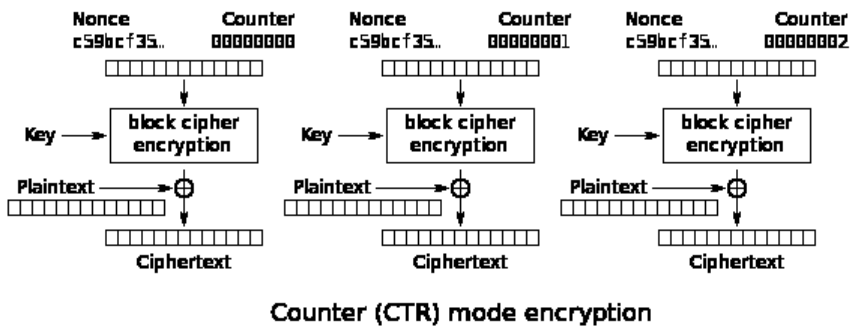
All utrustning som använder sig av HART-Protokollet måste känna till kommandona från Universal för de ger tillgång till användbar information för normal användning. Det är vanligt att utrustningen även stödjer kommandona inom Common Practice men det är inte ett måste. Kommandona inom kategorin Device Specific är mer specifika för utrustningen och information om dem kan fås från tillverkarna [40].

2.2.5. Säkerhet hos WirelessHART

För att skydda data sker all kommunikation inom WirelessHART krypterat med 128 bitars AES kryptering i CCM mode [28]. AES är en förkortning av *Advanced Encryption Standard* och är ett symmetriskt blockkrypto som delar in meddelandet i block om 128 bitar. Längden på nyckeln är i det här fallet 128-bitar men det finns även AES kryptering som använder sig av 192 eller 246 bitars nyckel.

Med en 128-bitars nyckel så sker 10 iterationer. Ett symmetriskt krypto använder sig av samma nyckel både vid kryptering och dekryptering [29].

CCM mode står för *Counter with CBC-MAC* och är enbart definierat att användas tillsammans med ett 128 bitars blockkrypto. CCM kombinerar teknikerna Counter Mode och CBC-MAC [30]. CBC-MAC används för att få fram ett värde för att kunna autentisera informationen genom att skapa en kedja där varje block är beroende av föregående block är rätt krypterat. Ifall ett block ändras kommer hela kedjan att påverkas vilket gör att ändringen upptäcks [31].



FIGUR 5: Counter mode kryptering [37]

För att kryptera datan används Counter Mode som använder sig av en nyckelvektor med unika värden som slås ihop med meddelandets block via XOR. Även värdet som räknas fram med CBC-MAC XOR-beräknas med vektorn. Det krypterade meddelandet skickas sedan tillsammans med verifieringsvärdet. Vid dekryptering återskapas nyckelvektorn och används för att återskapa meddelandet vilket i sin tur används för att räkna fram verifieringsvärdet. De båda

verifieringsvärdena jämförs och i det fall då de är likadana så är meddelandet korrekt [30].

Vid varje session använder sig utrustningen av en individuell krypteringsnyckel. Förutom egna sessionsnycklar delar utrustningen på en allmän krypteringsnyckel för att underlätta för broadcasting. En separat krypteringsnyckel används vid anslutning till nätverket, nyckeln kan antingen vara unik för varje utrustning eller för hela nätverket beroende på säkerhetspolicy. Det är även möjligt att byta anslutningsnyckeln efter att utrustningen har anslutit till nätverket [28].

2.3. IEEE 802.11-familjen

Institute och Electrical and Electronics Engineers (IEEE) är ett icke-vinstdrivande standardiseringsorgan som bl.a. har tagit fram en rad standarder för trådlösa datornätverk, *Wireless Local Area Network,* (WLAN) [8].

Standarden ”802.11” släpptes först 1997 och sedan dess har flera versioner som tillåter olika frekvenser och datahastighet utvecklats.

Radiofrekvenserna är uppdelade i olika frekvensband och för WLAN så används följande licensfria band:

- ***I**ndustrial, **S**cientific and **M**edical* (ISM-bandet). ISM-bandet använder frekvenser kring 0.9-, 2.4- och 5.8GHz [14].
- ***U**nlicensed-**N**ational **I**nformation **I**nfrastructure (U-NII-bandet).* U-NII-bandet använder frekvenser i 5GHz-bandet [15].

Tabell 2 åskådliggör de olika 802.11 versionerna.

TABELL 2: STANDARDER I 802.11-FAMILJEN [9]

Standard	**År**	**Beskrivning**
802.11	1997	Grundstandarden, upp till 2 Mbit/s både via radio i 2,4 GHz ISM-bandet och IR.
802.11a	1999	Utökning av 802.11 med upp till 54 Mbit/s på UNII-bandet (5 GHz).
802.11b	1999	Utökning av 802.11 med upp till 11 Mbit/s på ISM-bandet (2.4GHz).
802.11c	2001	Bryggningsprocedurer, del av IEEE 802.11d.
802.11d	2001	Standard för hur accesspunkter annonserar landskod så att klienter kan anpassa sig till olika länders radioband.

802.11e	2005	Quality of Service (QoS), resurstilldelning av bandbredd beroende på innehåll.
802.11f	2003	IAPP, standard för kommunikation mellan accesspunkter. Tillbakakallad 2006.
802.11g	2003	54 Mbit/s, i 2,4 GHz ISM-bandet, skall vara bakåtkompatibelt med 802.11b.
802.11h	2004	Standard för dynamiskt frekvensval och begränsning av uteffekten för att uppfylla reglerna för 5 GHz-bandet i Europa.
802.11i	2004	Säkerhet för åtkomstkontroll och kryptering av 802.11, implementerar WPA2.
802.11j	2004	En anpassning av frekvensuppdelningen för Japan.
802.11n	2008	600 Mbit/s i 2,4 GHz ISM-bandet, eller användning i 5 GHz-bandet. Skall vara bakåtkompatibelt med 802.11g.
802.11ad	2009	7 Gbit/s i 60 GHz bandet. Ingen konventionell typ av WLAN då den höga frekvensen och låga sändareffekten kräver ett avstånd på max några meter mellan enheterna samt fri sikt.
802.11ac	2012	1 Gbit/s i 5 GHz bandet. Bakåtkompatibel med 802.11b, 802.11g och 802.11n.

2.4. Mobila enheters påverkan på säkerheten

Med mobil enhet så menar vi smarta telefoner, surfplattor, eller liknande som man har tänkt koppla upp mot organisationens interna resurser. Ifall organisationen äger den mobila enheten, som fallet är på Perstorp AB, så kan organisationen kräva att den anställde följer fastställda regler avseende hanteringen av den mobila enheten samt installera programvara och göra fysiska begränsningar i enheten för att på så sätt öka säkerheten [5].

Information om vilka säkerhetsbrister det innebär att bryta mot regelverket kan vara bra för att ge användarna förståelse för deras nödvändighet.

Att kommunicera trådlöst i DCS-miljö kan ge många fördelar, inte minst vid operatörsrondering, men det innebär också att man måste ta hänsyn till ytterligare säkerhetsrisker. Det är främst tre risker som vi vill ta upp:

- Avlyssning
- Signalstörningar
- Förlust av enhet

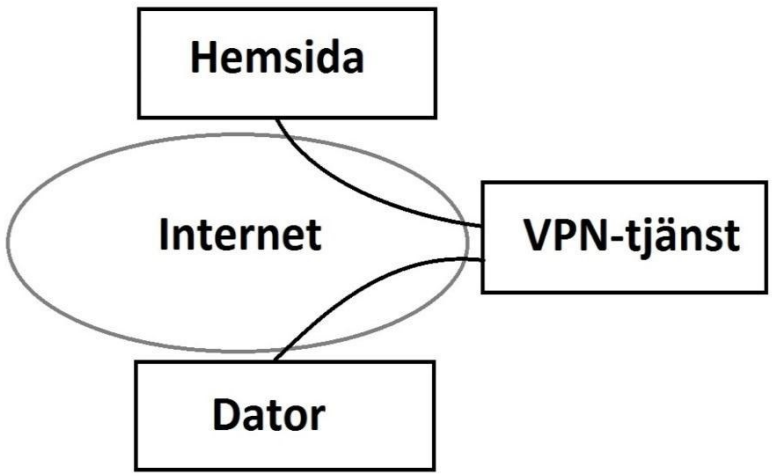
2.4.1. Avlyssning

Information är värdefullt, inte enbart för det egna företaget utan även andra kan vara intresserade av att få tag på den av olika anledningar. Ett sätt att försöka komma åt informationen kan vara genom att avlyssna företagets kommunikation.

Information kan antingen skickas krypterat eller okrypterat där det krypterade alternativet är att föredra eftersom informationen då först måste dekrypteras för att bli läslig. Det finns många olika krypteringsalgoritmer att använda sig av. En trådlös kommunikation är enklare att avlyssna än en trådbunden då den sker genom luften, som är allmänt tillgänglig, till skillnad från kablar.

För att försvåra möjligheterna till avlyssning kan ytterligare ett lager av kryptering läggas till genom att använda sig av VPN, *Virtual Private Network* [17]. Med VPN upprättas en krypterad anslutning

mellan två punkter över ett nätverk vilket kallas för en *VPN-tunnel* [18].



FIGUR 6**:** Enkel skiss över VPN-tunneling.

En VPN-tunnel upprättas mellan datorn och VPN-tjänsten där all information som skickas är krypterad. VPN-tjänsten avkrypterar informationen och sänder den okrypterat vidare till hemsidan som ser det som ett besök från VPN-tjänsten och inte datorn.

VPN-tunnelns kryptering fungerar enbart som skydd så länge som informationen färdas genom VPN-tunneln för informationen dekrypteras vid ankomst till VPN-servern. Från VPN-servern kommer informationen att färdas vidare i sin ursprungliga form. Krypterad data kommer alltså att förbli krypterad, medan okrypterad data kommer att fortsätta skickas okrypterat. Internetleveratören kan enbart avläsa mängden data som skickas och inte själva datainnehållet. VPN-leverantören har däremot tillgång till informationen som skickas och därför är det viktigt att välja en leverantör som är trovärdig.

Det finns flera olika protokoll som kan användas till att skapa ett VPN, två av dem är PPTP (*Point-to-Point Tunneling Protocol*) och IPsec (*Internet Protocol Security*).

Med PPTP kapslas datapaketen in i IP-datagram och bildar därmed en point-to-point anslutning [41]. Dock har PPTP flera kända säkerhetshål som inte är åtgärdade och rekommenderas därför inte att användas mer än i nödfall [18].

IPsec bygger på tre andra protokoll *Encapsulated Security Payload* (ESP), *Authentication header* (AH) och *IP Payload Compression Protocol* (IPComp).

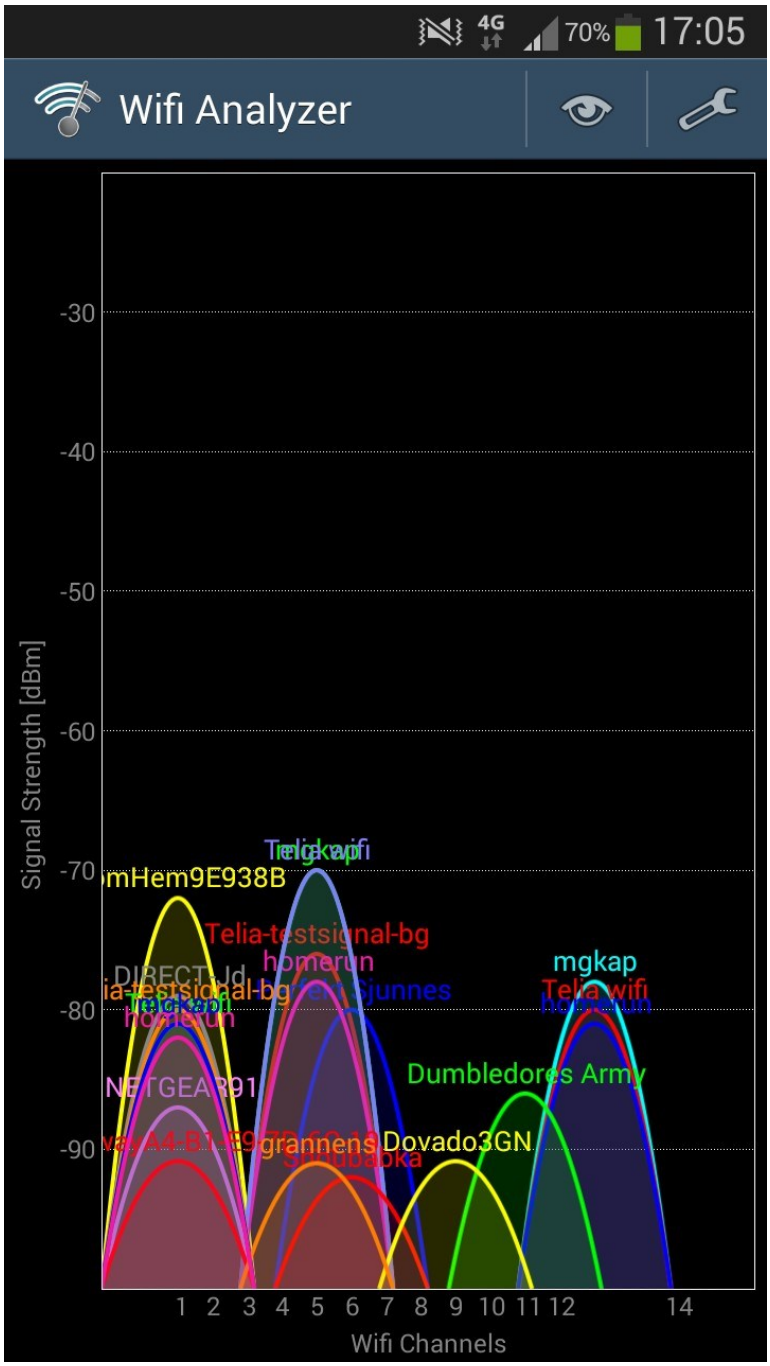
ESP skyddar data i IP-paketet genom kryptering. Med AH skyddas IP-paketets header genom att en checksumma räknas fram och sedan hashas. Hashvärdet skickas sedan med för att det ska gå att kontrollera att ingenting ändrats på vägen. IPComp försöker förbättra kommunikationen genom att komprimera datan i varje paket [42].

2.4.2. Signalstörningar

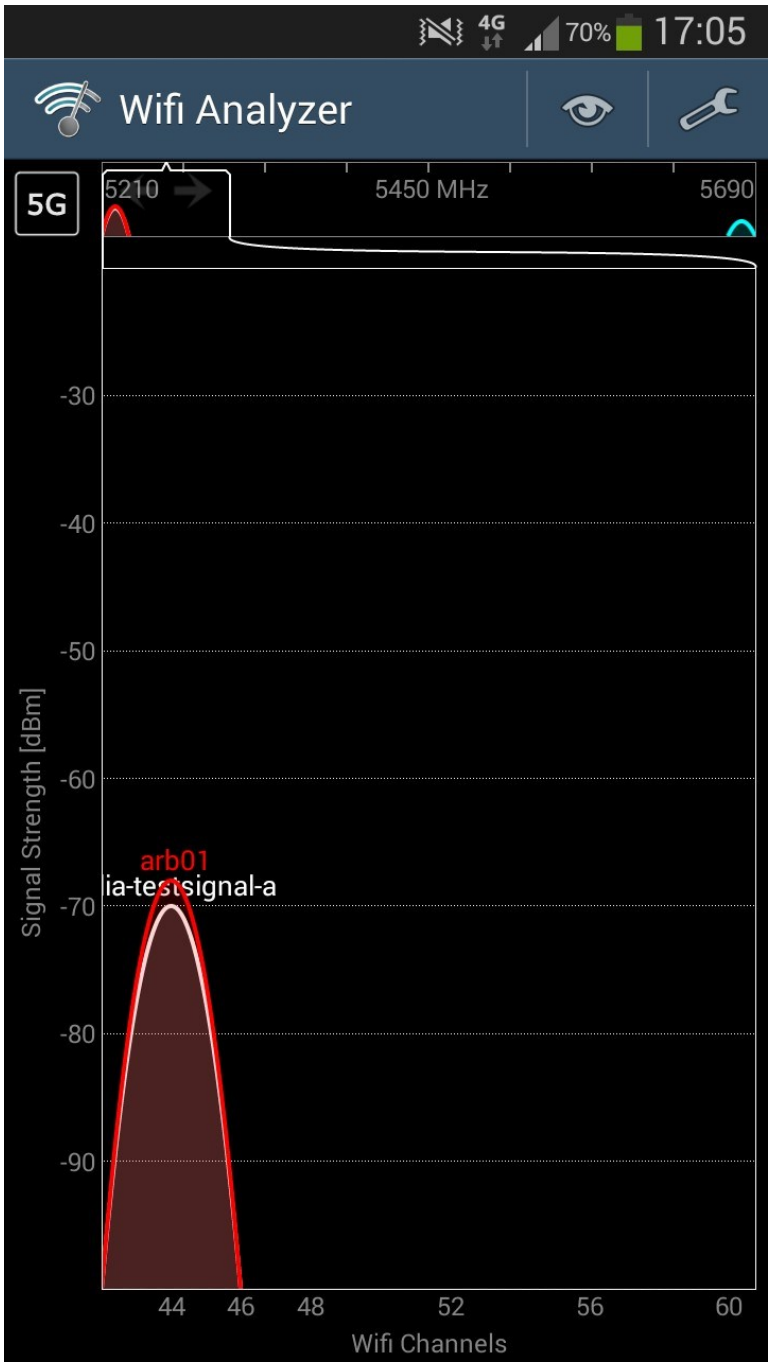
För att bättre kunna utnyttja mobila enheter i DCS-miljö så vill man ofta koppla upp dem mot Internet, oftast via WLAN. Den vanligaste typen av WLAN är ”IEEE 802.11-familjen”, som används av i princip alla routrar. I princip varje gång man kopplar upp sig mot ett trådlöst lokalt nätverk så är det just ”IEEE 802.11” som man utnyttjar, där det vanligaste frekvensbandet är 2.4GHz.

De flesta accesspunkter är av praktiska skäl förinställda till att använda 2.4GHz-bandet, även om de klarar att använda 5GHz-bandet, eller t.o.m. 2.4GHz- och 5GHz-bandet samtidigt.

Se figur 7 och figur 8 för en jämförelse mellan 2.4GHz-bandet och 5GHz-bandet.



FIGUR 7: Nätverkstest i stadsmiljö på 2.4GHz-bandet.

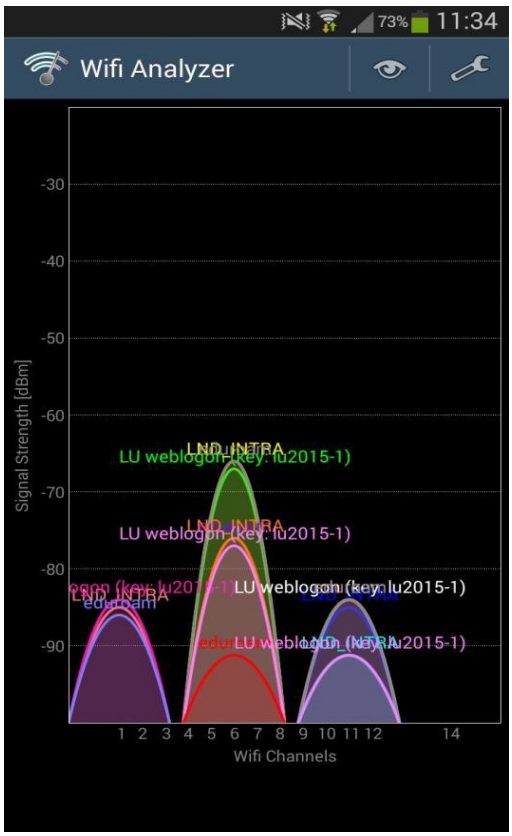


FIGUR 8: Nätverkstest i stadsmiljö på 5GHz-bandet.

Som synes i figur 8 så är 5GHz-bandet betydligt mindre belastat än 2.4GHz-bandet, något vi tror beror främst på okunskap, inte på medvetna val.

I figur 7 syns det på överlappningen hur dåligt konfigurerade de flesta accesspunkter är.

Se figur 9 för ett exempel på hur man som organisation kan konfigurera accesspunkterna för att minska störningsrisken.



FIGUR 9: Nätverkstest på Campus Helsingborg, på 2.4GHz-bandet.

Som synes i figur 8 så är accesspunkterna konfigurerade till att sända ut på antigen kanal 1, 6 eller 11. Det leder till 0 % överlappning mellan kanalerna, men en enskild kanal kan fortfarande belastas tungt.

Ifall många enheter vill kommunicera på samma band och kanal så resulterar det ofta i att nätverket upplevs som långsamt och man kan

t.o.m. tappa anslutning ibland, trots att man använder accessmetoder för att undvika signalkollisioner.

I DCS-miljö så är det naturligtvis inte acceptabelt att man skulle tappa anslutning mot systemet och därför så är det viktigt att undersöka hur man kan optimera sin trådlösa anslutning mot accesspunkten och minimera riskerna för signalstörningar.

2.4.3. Förlust av enhet

Det finns en risk för att den trådlösa enheten blir stulen eller tappas bort vilket kan leda till att viktiga data förloras och/eller hamnar i fel händer. Ifall enheten dessutom är dåligt skyddad eller t.o.m. saknar lösenord så finns det en risk att en eventuell förövare försöker styra processer i fabriken.

För att kringgå dem ovan nämnda riskerna så är det viktigt att man har en tydlig policy kring hanteringen av enheten (t.ex. vad som skall/inte skall lagras på enheten samt hur den skall förvaras). Man bör dessutom helst använda komplicerade lösenord i enheten. Ifall det finns en möjlighet av konfigurera enheten så att den endast kan styra processerna då man befinner sig i fabriken så bör det övervägas. Dessutom så bör man ha en handlingsplan för hantering av stulen eller borttappad enhet.

MSB har skrivit en hel del om rekommendationer på krav som bör ställas på användare samt rekommendationer för utformning av tekniska skydd.

Vi har valt att plocka ut följande punkter från MSB, som vi anser är relevanta för process- och tillverkningsindustrin:

- Användaren skall förpliktigas att ha fysisk kontroll över den mobila enheten och inte lämna den obevakad på t.ex. allmän plats, hotellrum eller synlig i bil [6]
- Hur användaren vid förlust av enhet ska anmäla detta till organisationen och om det bör göras skyndsamt [6]
- Att användaren bara använder den mobila enheten för internetsurfing i enlighet med organisationens regelverk [6]

- Att den mobila enheten i första hand skall anslutas mot kända trådlösa nätverk som har skydd i form av kryptering [6].
- Att användaren ska lösenordskydda enheten så att den är låst när skärmsläckaren är aktiv. Det rekommenderas att undvika de mest uppenbara pinkoderna eller lösenorden t.ex. 1111, 1234 samt aktivering av tidsinställning för inaktivitet innan skärmsläckaren startas [6].

Det finns även en del tekniska skydd man kan anamma och följande punkter är det ännu en gång MSB som har tagit fram, vi har plockat ut det vi anser är mest relevant för process- och tillverkningsindustrin:

- Implementera en säker uppkoppling (VPN) till organisationens interna resurser. Vid behov av extra skydd, överväg att implementera två-faktors autentisering [7]
- Implementera processer för att återställa angripna mobila enheter till ett känt säkert läge, till exempel fabriksinställningar [7]
- Implementera lösningar för detektering och skydd mot skadlig kod i den mobila enheten [7]

2.5. Panasonic Toughpad FZ-G1

Panasonic Toughpad FZ-G1 är en surfplatta som har utvecklats för tuffare industrimiljöer. De senare versionerna av surfplattan är ATEX Zone 2 klassade, vilket innebär att de kan användas i områden där explosiva blandningar bestående av gas, ånga eller dimma inte är vanligt förekommande vid normal hantering, eller där den ovanliga förekomsten bara varar under kort tid [49]. Den version av surfplattan som Perstorp AB för närvarande besitter (FZ-G1AABZEE3) är **inte** ATEX Zone 2 klassad.

FIGUR 10: Toughpad FZ-G1 med operativsystemet Windows 8

Se tabell 3 för surfplattans specifikationer:

TABELL 3: Specifikationer för Panasonic Toughpad FZ-G1

OPERATIVSYSTEM	Windows® 8 Pro 64-bit
PROCESSOR	Intel® Core™ i5-3437U 1.9GHz
RAM	4GB
HÅRDDISK	128GB SSD
DISPLAY	1920x1200 pixlar, 10.1”
WLAN	Wi-Fi 802.11a/g/n/
BATTERI	10.8V, 4400mAh

DIMENSIONER	10.6” x 7.4” x 0.8”
VIKT	1.1kg
TÄTHETSKLASSNING	IP65

För en fullständig specifikationslista, se [32].

3. Resultat

3.1. Applikationer för att förbättra användarbarheten

För att göra surfplattan mer användarvänlig och tackla problemen som beskrivs i 1.3.3 så har en handfull applikationer, varav de flesta finns tillgängliga i Windows 8, utnyttjats.

En stor fördel med att använda applikationer som ingår i Windows 8 är att systemleverantören (Emerson Process Management) stödjer det mesta som ingår i operativsystemet. Det är möjligt att det finns andra applikationer att ladda ner för att uppfylla samma ändamål, men det är säkrast att använda applikationer som systemleverantören stödjer.

En riktlinje som vi har följt är att applikationerna skall vara minimalistiska, de skall alltså vara mycket lättanvända samt inte kräva mycket processorkraft. Samtliga applikationer som har valts att inkluderas kan konfigureras så att de automatiskt körs då surfplattan startar.

3.1.1. f.lux

Surfplattan ska kunna användas dygnet runt och för att anpassa skärmens ljusstyrka efter omgivningens ljus laddades applikationen ”f.lux” ner från [20]. Applikationen är dels utvecklad för att anpassa ljusstyrkan efter rådande omständigheter men ändrar även ljussammansättningen beroende på tiden på dygnet, detta eftersom att ljus med våglängderna 420-490nm (blått ljus) har negativa effekter på sömnen [39].

Den intresserade kan läsa mer om det blå ljusets inverkan på sömnen, bl.a. genom att besöka [21].

3.1.2. Windows 8 On-Screen Keyboard

Problemet med det ursprungliga standardtangentbordet var dess storlek som täckte halva skärmen. Vid användandet av DeltaV, DCS-miljön som Perstorp AB använder, betydde det att en stor del av

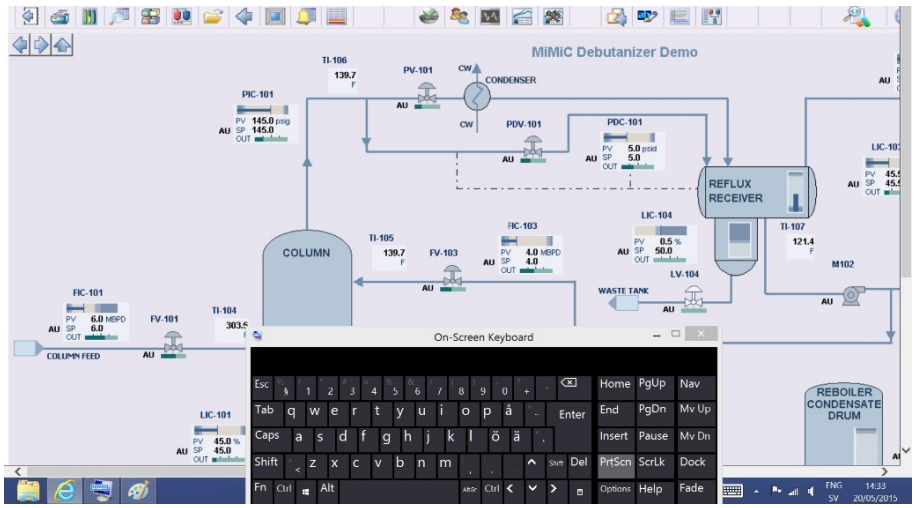
operatörsbilderna täcktes över, i vissa fall även rutan där värdena matas in, vilket försvårar användandet då det som sker inte syns.

Problemet löstes genom införandet av ”Windows 8 On-Screen Keyboard”, som man kan ändra storleken, layouten och positionen på.

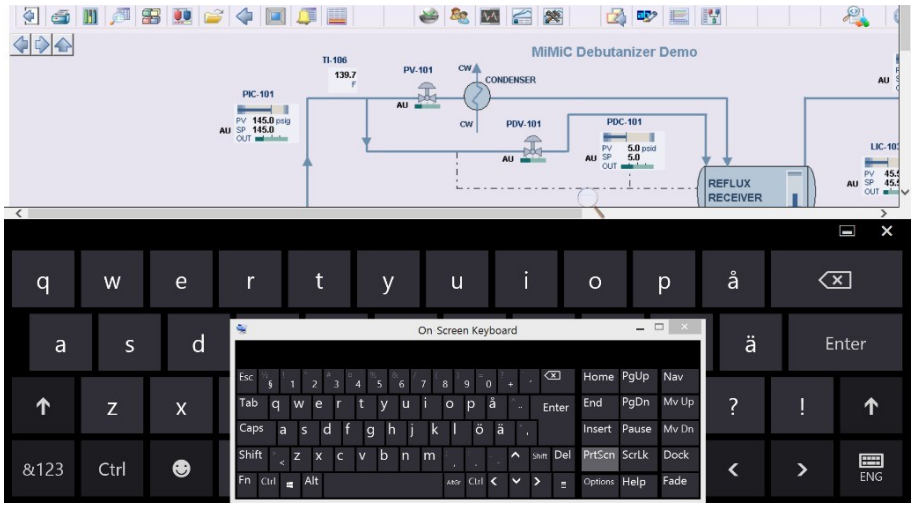
Det snabbaste sättet att komma åt ”On-Screen Keyboard” är att dra ut högerpanelen och sedan klicka på ”Search”. Skriv sedan in ”On-Screen Keyboard” och kör programmet så är det klart.

Ifall man använder en svensk version av Windows 8 så står det istället ”Sök” och ”Skärmtangentbord”.

Se figur 11 och figur 12 för att bättre förstå skillnaden mellan On-Screen tangentbordet och standardtangentbordet.



FIGUR 11: On-Screen tangentbordet, med en DeltaV processbild i bakgrunden.



FIGUR 12: Standardtangentbordet i jämförelse med On-Screen tangentbordet samt en DeltaV processbild i bakgrunden.

3.1.3. Magnifier

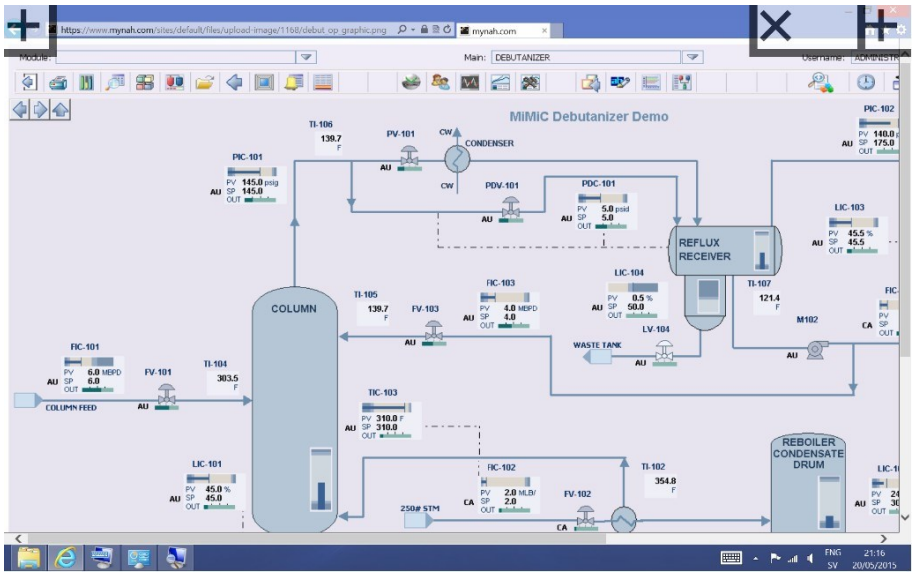
Processbilderna som används för att styra och övervaka fabriken var ursprungligen anpassade efter att ses på 24” datorskärmar vilket medförde att bilderna blev mycket förminskade när de visades upp på surfplattans 10,1” skärm. De förminskade bilderna ledde i sin tur till att olika texter och processvärden knappt var läsbara, något som sannolikt skulle försvåra för operatörerna.

Lösningen blev att använda en inbyggd zoom-funktion hos Windows 8 som heter Magnifier. Vid aktivering av funktionen dyker det upp plustecken för inzoomning i de övre hörnen och minustecken för utzoomning i de undre hörnen samt ett kryss för att stänga av funktionen.

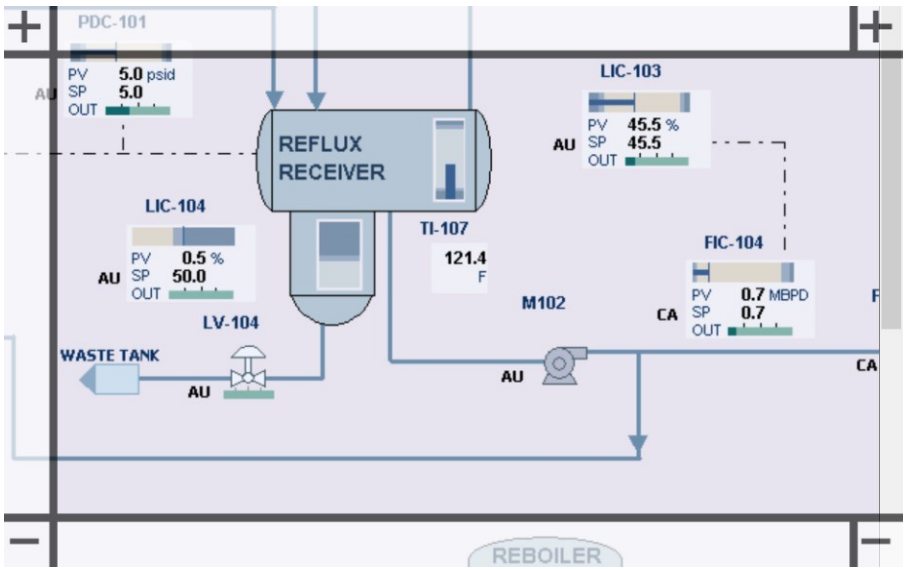
Magnifier hittas enklast genom att dra ut högerpanelen och sedan klicka på ”Search”. Skriv sedan in ”Magnifier” och kör programmet så är det klart.

Ifall man använder en svensk version av Windows 8 så står det istället ”Sök” och ”Förstoringsglaset”.

Figur 13 visar zoom-knapparna i neutralläge (i de övre hörnen) och figur 14 visar zoom-knapparna i inzoomat läge.



FIGUR 13: Zoom-knapparna i neutralläge med en DeltaV processbild i bakgrunden.



FIGUR 14: Zoom-knapparna i inzoomat läge med en DeltaV processbild i bakgrunden.

Skulle man vilja stänga av zoom-funktionen så kan man enkelt starta den igen genom att klicka på surfplattans  och  knappar samtidigt.

3.2. Kalibrering av surfplattan

Att styra surfplattan med hjälp av fingrarna har fungerat bra men när man kräver högre precision så är den medföljda pekpennan att föredra. Problemet som vi hade med pekpennan var att den var mycket dåligt kalibrerad. I närheten av kanterna så gick den inte att använda alls eftersom att muspekaren hoppade runt tvärs över hela skärmen så fort man närmade sig kanterna.

Vår ursprungstanke efter att ha testat Windows inbyggda kalibreringsmetod, som inte hjälpte alls, var att det är något fel på pennan. Vi provade ett par olika universalpennor men hittade ingen med bra precision eftersom att ändarna var för stora. Vi bestämde oss därför för att ge kalibreringen ytterligare en chans och efter att ha sökt runt en del så visade det sig att det finns en välfungerande metod [46], som vi sedan testade.

Den välfungerande metoden innebär en 273-punkts kalibrering, till skillnad från Windows 16-punkts kalibrering.

För att utföra den bättre kalibreringsmetoden så måste man först återställa all kalibreringsdata. Det gör man genom följande steg:

1. Dra ut högerpanelen
2. Klicka på ”Settings”
3. Klicka på ”Control Panel”
4. Klicka på ”Tablet PC Settings”
5. Under Display fliken, klicka på ”Reset”

När man har återställt all kalibreringsdata så skall man skriva in en stor rad i kommandotolken, denna rad gör det möjlig att kalibrera med hjälp att 273 punkter istället för 16 punkter.

Raden för kalibrering med 273 punkter är följande (för 1920x1080 upplösning):

Tabcal devicekind=pen lincal novalidate XGridPts= 10, 60, 110, 160, 260, 360, 460, 560, 660, 810, 960, 1110, 1260, 1360, 1460, 1560, 1660, 1760, 1810, 1860, 1910 YGridPts=10, 60, 110, 160, 250, 400, 540, 680, 830, 920, 970, 1020, 1070

Efter att man har kört raden i kommandotolken så uppstår ett rutnät med 273 punkter som man skall träffa med pennan.

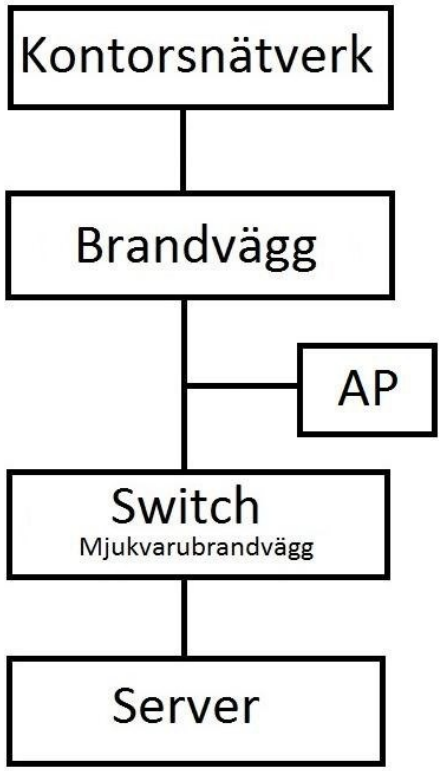
Man bör hålla surfplattan och pekpannan på ett bekvämt och naturligt sätt, helst så som den sedan kommer användas. Man skall strunta i vart muspekaren befinner sig och istället fokusera på att spetsen av pekpennan landar mitt i markeringarna.

Efter att ha provat denna metod så fungerade pennan mycket bättre, över hela skärmen.

3.3. Uppkoppling av surfplattan

För att kunna använda surfplattan effektivt i fabriken behöver den ha tillgång till en trådlös nätverksanslutning. I fall det inte finns något trådlöst nätverk sedan tidigare så behöver ett nätverk installeras.

I vårt fall så kopplas de nya accesspunkterna upp mellan de fysiska brandväggarna och switcharna (se figur 15). Det innebär att vi förbigår en säkerhetsbarriär, förutsatt att den fysiska brandväggen och mjukvarubrandväggen i switcharna kompletterar varandra. Därför är det extra viktigt att regelbundet uppdatera brandväggarna så att de lär sig identifiera de nya hot som regelbundet uppstår [52].

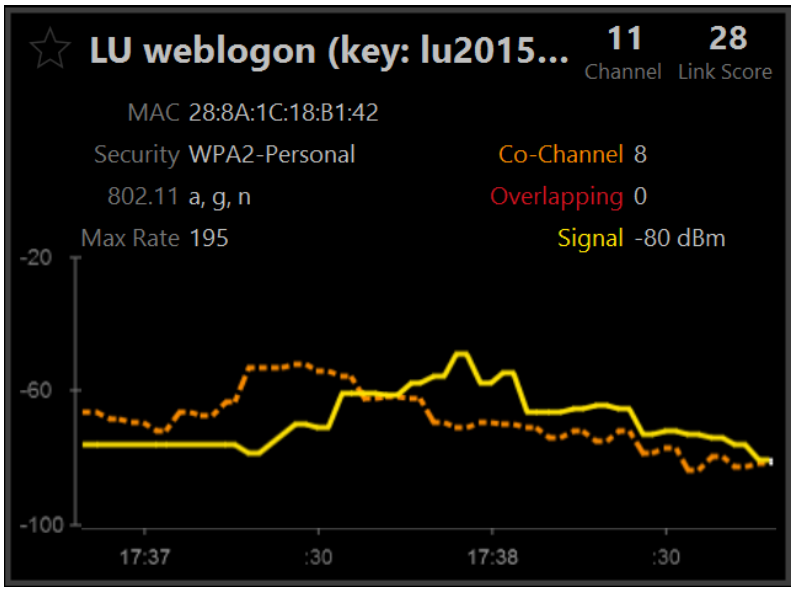


FIGUR 15: Inkopplingen av en trådlös accesspunkt i nätverket

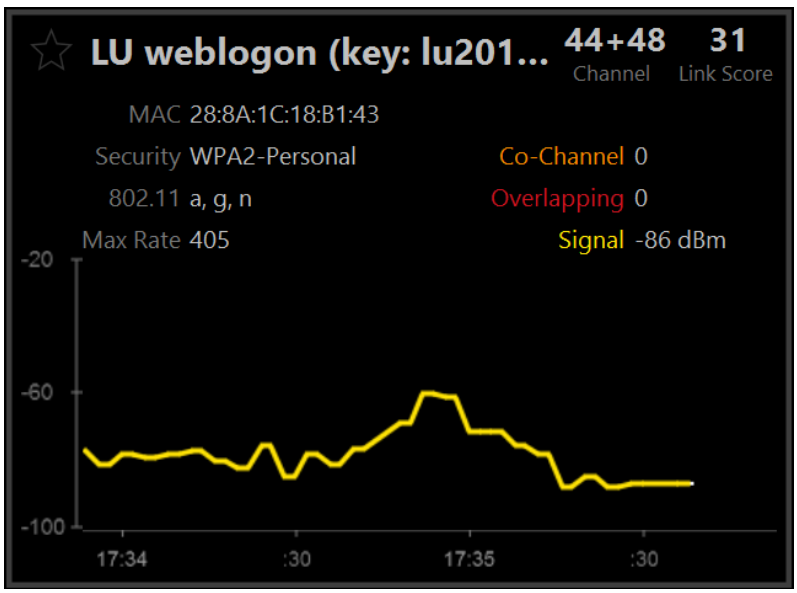
På grund av omständigheter som vi inte kunnat råda över så har vi inte haft möjlighet att ansluta surfplattan mot nätet i den miljö som det är tänkt att den skall användas hos Perstorp AB. För att ändå kunna få någon uppfattning om surfplattans egenskaper genomfördes en simulering på skolan där vi försökte återskapa realistiska störningar så som mikrovågsugnar och stängda rum. Nätverk på både 2.4 och 5 GHz-bandet testades. Visserligen är det inte den riktiga miljön med de störningar den kommer utsättas för där men det kan ändå ge en fingervisning.

Testet utfördes med hjälp av InSSIDER, ett program som visar information om de trådlösa nätverken i omgivningen [54]. Programmet visade en lista över de tillgängliga nätverken och deras signalstyrka, kanaluppdelningen hos nätverket på antingen 2.4- eller

5GHz-bandet samt en graf över hur signalstyrkan varierats över tiden hos det nätverk som valts.

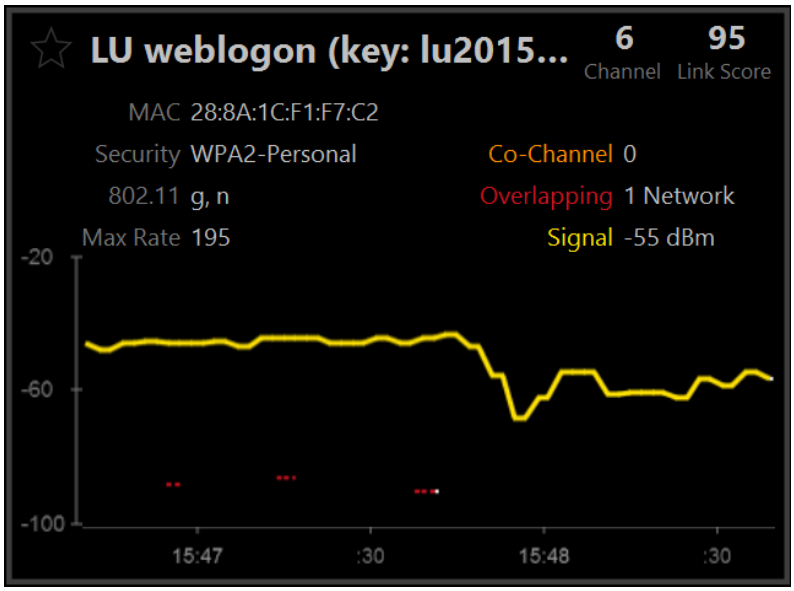


FIGUR 16: Signalstyrkan från ett Campus-nät (2.4 GHz)

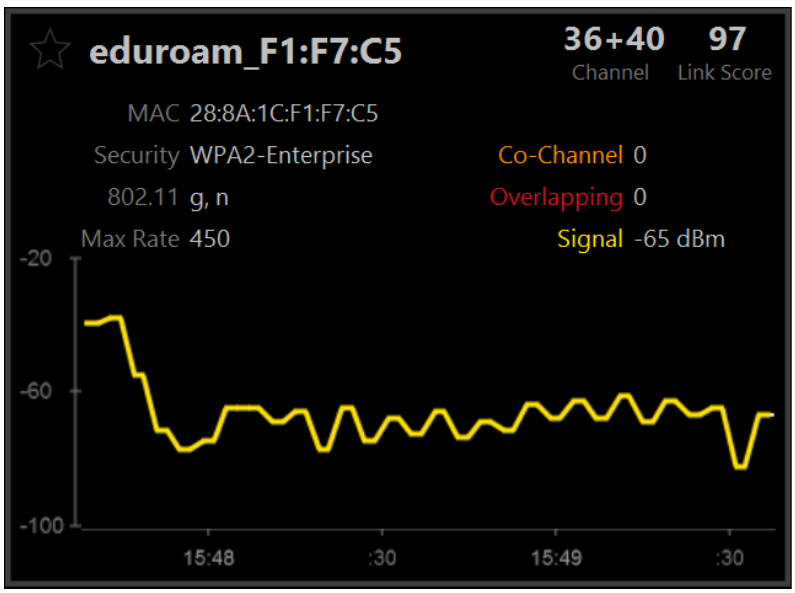


FIGUR 17: Signalstyrkan från ett Campus-nät (5 GHz)

Som synes i figur 17 så avtar signalstyrkan hos 5GHz-bandet relativt fort (jämför med figur 16) då avståndet till accesspunkten ökar.

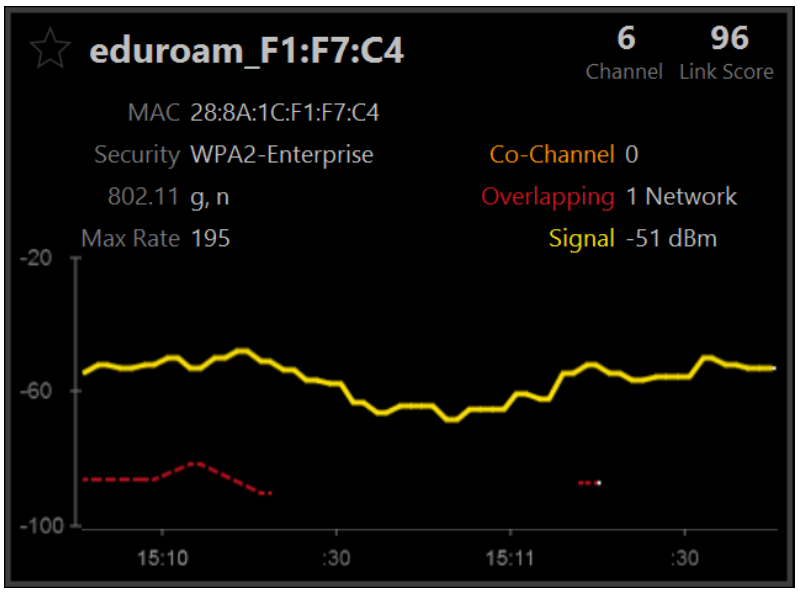


FIGUR 18: Signalstyrkan från ett Campus-nät (2.4 GHz), mätt mellan väggar



FIGUR 19: Signalstyrkan från ett Campus-nät (5 GHz), mätt mellan väggar

Som man kan se i figur 19 så avtar signalstyrkan för 5GHz-bandet väldigt fort då har väggar mellan sig. Jämför med figur 18 (2.4GHz-bandet) där signaltappet är lägre.



FIGUR 20: Signalstyrkan över tid hos ett Campus-nät (2.4 GHz), delvis mätt bredvid mikrovågsugn

Som synes i figur 20 så minskar signalstyrkan något när mäter i närheten av mikrovågsugnar. När man sedan går ifrån mikrovågsugnarna så förbättras signalstyrkan igen.

Mikrovågsugnar opererar på frekvenser kring 2.45 GHz, därför utfördes samma test inte för 5GHz-bandet.

Eftersom surfplattan aldrig togs i drift fanns det ingen möjlighet att utvärdera vilka användningsområden som den varit lämplig att användas till. Tanken hade varit att låta operatörerna använda sig av surfplattan i sitt vardagliga arbete under en viss tidsperiod för att sedan låta dem utvärdera den. Deras åsikter skulle sedan ha legat till grund för rekommendationer av vilka användningsområden surfplattan bäst lämpar sig för.

Det innebär att vi delvis har kunnat avsluta målformulering 1.3.2 (Förebygga signalstörningar) och inte alls kunnat avsluta målformulering 1.3.4 (Undersöka lämpliga arbetsmoment).

4. Slutsats

Vi har utfört en analys om hur en DCS-miljö skulle påverkas av införandet av en surfplatta. Tre risker analyserades främst, *avlyssning* (2.4.1), *signalstörningar* (2.4.2) och *förlust av enhet* (2.4.3). Vi har dessutom förbättrat användbarheten hos surfplattan (3.1 och 3.2). Läs respektive delkapitel för mer ingående analyser.

4.1. Det trådlösa

För att göra avlyssning svårare bör informationen skickas krypterat och en VPN-tunnel kan användas för att öka säkerheten ytterligare.

Ett väl konfigurerat trådlöst nätverk där de olika kanalerna inte överlappar varandra kan förbättra förutsättningarna för att undvika signalstörningar.

4.2. Försvunnen enhet

För att förhindra förlust av enheten bör företaget ha en policy om hur enheten skall hanteras. Man bör även ha en handlingsplan för vad som skall göras ifall den ändå skulle tappas bort eller bli stulen.

4.3. Förbättring av användarbarheten

Applikationen ”f.lux” installerades för att anpassa skärmens ljussammansättning samt ljusstyrka utefter tid och omgivning.

Windows 8 standardtangentbord ersattes med det mer flexibla ”On-Screen” tangentbordet som man kan ändra bl.a. storlek och position på.

Processbilderna som var anpassade till 24” skärmar blev något plottriga på surfplattans 10,1” skärm men genom att zooma med ”Magnifier” blev bilderna och värdena tydligare.

Den mycket dåligt kalibrerade pekpennan som inte gick att använda alls i nederkanten av skärmen kalibrerades om ordentligt med hjälp av 273-punkters kalibrering.

Surfplattan blev till sist mycket mer lättanvänd och bättre lämpad för sitt ändamål men tyvärr hann den inte sättas i drift innan deadlinen för examensarbetet vilket resulterade i att vi inte kunde testa den i verkligheten.

Då surfplattan i skrivande stund inte blivit satt i bruk så har operatörerna inte kunnat utvärdera den. Operatörernas åsikter skulle ha legat till grund för utvärderingen av surfplattans lämplighet för de olika arbetsmomenten.

4.4. Sammanfattat

Vårt examensarbete hade fyra primära mål: analysera datasäkerheten (1.3.1), förebygga signalstörningar (1.3.2), utöka användarbarheten
(1.3.3) och undersöka lämpliga arbetsmoment (1.3.4).

Det första målet (1.3.1) och det tredje målet (1.3.3) har kunnat avslutas.

Det andra målet (1.3.2) har utförts om än inte riktigt på det sätt som först varit planerat. Tanken hade varit att i driftsätta surfplattan i fabriken för att kunna testa den teoretiska analysen i verkligheten men förutsättningarna i fabriken var ännu inte de rätta. Istället för att testa surfplattan i fabriksmiljö gjordes en simulering på skolan med ett par vanliga störningsmoment. Detta är inte helt optimalt eftersom det inte gick att simulera exakt samma förhållande på en skola som i en fabrik men det är bättre än inget test alls.

Som en konsekvens av att surfplattan inte har blivit satt i drift ännu så kunde vi inte avsluta fjärde målet (1.3.4). Vi har kunnat prata med operatörer, som har haft en del idéer, men utan att testköra surfplattan i rätt miljö så kan man omöjligt ta rätt beslut angående vilka arbetsmoment den bör användas för.

5. Framtida arbeten

Det finns en hel del möjligheter till att vidareutveckla arbetet. Vi vill lyfta fram två förslag, som främst påverkar användarbarheten hos surfplattan. Det ena förslaget är att undersöka möjligheterna att använda sig av NFC vid inloggningsprocessen för att uppnå en tvåfaktorsautentisering. Det andra förslaget är att undersöka möjligheterna och lämpligheten hos makro för att automatisera vissa repetitiva steg (vi tänker främst på inloggningsprocessen). För att öka säkerheten så hade man dessutom kunnat kombinera NFC med ett makro.

5.1. NFC

NFC är en förkortning av *Near Field Communication* och som namnet antyder är det en teknik som används för att kommunicera över små avstånd. Tekniken bygger på *Radio-frequency identification* (RFID) som är en trådlös kommunikationsmetod vanligtvis mellan en passiv och en aktiv tagg.

Till skillnad från RFID kan kommunikationen med NFC fungera åt båda hållen, men avståndet är betydligt mer begränsat. NFC-taggarna har begränsningen att enbart en tagg åt gången kan läsas av [47].

Under arbetets gång diskuterades det hur inloggningsprocessen skulle kunna göras säkrare och även hur användningen skulle kunna begränsas till ett visst område. En idé vi fick var att NFC på något sätt skulle kunna vara en lösning. En NFC-tagg skulle kunna fungera som en del i en tvåfaktorsautentisering där två skilda metoder används för att verifiera identiteten hos användaren och samtidigt se till att personen måste befinna sig på industriområdet för att ha åtkomst till taggen som är nödvändig för inloggningsprocessen.

Det hade varit fullt möjligt att implementera en smidig lösning med NFC ifall Panasonic Toughpad FZ-G1 hade haft stöd för NFC men det hade inte. Det finns däremot andra modeller som har det, t.ex. Panasonic Toughpad FZ-M1 [48].

5.2. Makro

Ett makro används för att automatisera arbetsmoment som är repetitiva. För att skapa ett makro så kan man hämta hem program med inspelningsfunktion där användaren utför sekvensen av åtgärdas som skall sparas. Det är också möjligt att skapa makrot genom programkod som stöds av programmet i fråga.

Vi tänkte använda makro för att underlätta inloggningsprocessen för operatörerna men säkerhetsfrågan kring makro var mer komplicerad än vad vi ursprungligen tänkte. Främsta säkerhetsrisken är att lagra lösenord i ett makro eftersom att det hade tillåtit en eventuell förövare att lätt logga in mot servarna utan att kunna lösenorden.

Man kan lösa det på olika sätt, bl.a. genom att inte spela in några kritiska lösenord i makrot eller möjligtvis genom att kräva ett lösenord för att kunna starta makrot, men det går till viss del emot syftet med makro (att underlätta användarbarheten). En lösning vi tänkte på var att trigga makrot med hjälp av en NFC-tagg men tyvärr så hade inte surfplattan stöd för NFC.

Referenser

[1] Myndigheten för samhällsskydd och beredskap (MSB), *”Vägledning till ökad säkerhet i industriella informations- och styrsystem”*, s.7, ISBN: 978-91-7383-462-9, juli 2014

[2] Myndigheten för samhällsskydd och beredskap (MSB), *”Vägledning till ökad säkerhet i industriella informations- och styrsystem”*, s.23, ISBN: 978-91-7383-462-9, juli 2014

[3] Myndigheten för samhällsskydd och beredskap (MSB), *”Stuxnet: IT som vapen eller påtryckningsmedel”,* s.5, Publ.nr MSB331, november 2011

[4] http://www.dpstele.com/scada/dcs-vs.php (Hämtad 2015-04-28)

[5] Myndigheten för samhällsskydd och beredskap (MSB), *”Vägledning för säkrare hantering av mobila enheter”*, s.6, ISBN: 978-91-7383-234-2

[6] Myndigheten för samhällsskydd och beredskap (MSB), *”Vägledning för säkrare hantering av mobila enheter”*, s.12, ISBN: 978-91-7383-234-2

[7] Myndigheten för samhällsskydd och beredskap (MSB), *”Vägledning för säkrare hantering av mobila enheter”*, s.13, ISBN: 978-91-7383-234-2

[8] http://standards.ieee.org/findstds/standard/802.11-2012.html (Hämtad 2015-04-28)

[9] http://sv.wikipedia.org/wiki/IEEE_802.11 (Hämtad 2015-05-06)

[10] https://www.controlglobal.com/assets/12WPpdf/120904-emerson-wirelesshart-isa.pdf s.4 (Hämtad 2015-05-11)

[11] https://www.controlglobal.com/assets/12WPpdf/120904-emerson-wirelesshart-isa.pdf (Hämtad 2015-05-11)

[12] http://www.isssource.com/stuxnet-loaded-by-iran-double-agents/ (Hämtad 2015-05-11)

[13] http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf (Hämtad 2015-05-12)

[14] http://www.pcmag.com/encyclopedia/term/45467/ism-band (Hämtad 2015-05-06)

[15] http://www.pcmag.com/encyclopedia/term/65261/u-nii (Hämtad 2015-05-06)

[16] http://www2.emersonprocess.com/siteadmincenter/PM%20Central%20Web%20Documents/Emerson%20Wireless%20Security.pdf s.2 (Hämtad 2015-05-04)

[17] https://www.iis.se/docs/sakrare-mobiltelefon.pdf s.6 (Hämtad 2015-05-11)

[18] http://www.kjell.com/fraga-kjell/hur-funkar-det/natverk/hemnatverk/vpn-tunnlar#vpn-principen (Hämtad 2015-05-11)

[19] http://117.218.52.222:8080/quality/TelecomBasics%5Ctdma.pdf s.3-5 (Hämtad 2015-05-11)

[20] https://justgetflux.com/ (Hämtad 2015-05-14)

[21] https://justgetflux.com/research.html (Hämtad 2015-05-14)

[22] http://upload.wikimedia.org/wikipedia/commons/thumb/8/8c/2.4_GHz_WiFi_channels_%28802.11b%2Cg_WLAN%29.svg/1700px2.4_GHz_WiFi_channels_%28802.11b%2Cg_WLAN%29.svg.png (Hämtad 2015-05-15)

[23] http://kernelmag.dailydot.com/features/report/8051/the-mystery-of-wifi-channel-14/ (Hämtad 2015-05-06)

[24] http://www.pcpro.co.uk/realworld/356446/banish-your-wi-fi-woes (Hämtad 2015-05-12)

[25] http://www.speedguide.net/faq/is-5ghz-wireless-better-than-24ghz-340 (Hämtad 2015-05-12)

[26] http://www.extremetech.com/computing/184685-what-is-802-11ax-wifi-and-do-you-really-need-a-10gbps-connection-to-your-laptop (Hämtad 2015-05-13)

[27] http://www.netgear.com/landing/dual-band.aspx (Hämtad 2015-05-14)

[28] http://en.hartcomm.org/hcp/tech/wihart/wihart_security.html (Hämtad 2015-05-15)

[29] http://techworld.idg.se/2.2524/1.398247/sa-fungerar-kryptering (Hämtad 2015-05-11)

[30] http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf s.2-4 (Hämtad 2015-05-19)

[31] http://en.wikipedia.org/wiki/CBC-MAC (Hämtad 2015-05-19)

[32] ftp://ftp.panasonic.com/computer/fzg1/fz-g1_specsheet.pdf s.2 (Hämtad 2015-05-19)

[33] https://www.perstorp.com/en/about/history/perstorp_history/ (Hämtad 2015-04-27)

[34] https://www.perstorp.com/en/about/perstorp_in_brief/ (Hämtad 2015-04-27)

[35] http://www.emerson.com/en-us/AboutUs/Pages/history.aspx (Hämtad 2015-04-27)

[36] http://www.emerson.com/en-us/AboutUs/Pages/snapshot.aspx (Hämtad 2015-04-27)

[37] http://upload.wikimedia.org/wikipedia/commons/thumb/4/4d/CTR_encryption_2.svg/601px-CTR_encryption_2.svg.png (Hämtad 2015-05-11)

[38] http://www.slideshare.net/3abooodi/distributed-control-system-3119577 (Hämtad 2015-05-18)

[39] http://www.health.harvard.edu/staying-healthy/blue-light-has-a-dark-side (Hämtad 2015-05-14)

[40] http://en.hartcomm.org/hcp/tech/aboutprotocol/aboutprotocol_commands.html (Hämtad 2015-05-12)

[41] http://www.symantec.com/region/se/resources/vpn.html (Hämtad 2015-05-12)

[42] https://www.freebsd.org/doc/en/books/handbook/ipsec.html (Hämtad 2015-05-14)

[43] http://www2.emersonprocess.com/sv-SE/Pages/AboutUs.aspx (Hämtad 2015-04-27)

[44] http://www.kjell.com/fraga-kjell/hur-funkar-det/natverk/hemnatverk/sakerhet-i-natverk (Hämtad 2015-05-19)

[45] Myndigheten för samhällsskydd och beredskap (MSB), *”Vägledning till ökad säkerhet i industriella informations- och styrsystem”*, s.46-47, ISBN: 978-91-7383-462-9, juli 2014

[46] http://forum.xda-developers.com/showthread.php?t=2171198 (Hämtad 2015-05-19)

[47] https://rapidnfc.com/blog/72/the_difference_between_nfc_and_rfid_explained (Hämtad 2015-05-19)

[48] http://www.business.panasonic.com/7-inch-tablet-fz-m1.html (Hämtad 2015-05-15)

[49] http://www.sini.se/Dokument/Dokument/153001.pdf s.1 (Hämtad 2015-05-19)

[50] http://www2.emersonprocess.com/siteadmincenter/PM%20DeltaV%20Documents/ProductDataSheets/DV_PDS_SmartSwitches.pdf s.4 (Hämtad 2015-05-19)

[51] http://www2.emersonprocess.com/siteadmincenter/PM%20DeltaV%20Documents/Brochures/DeltaV-System-Overview-v11-Brochure.pdf s.2, s.14 (Hämtad 2015-05-19)

[52] http://www.omwlan.se/artiklar/brandvagg.aspx (Hämtad 2015-05-21)

[53] http://sv.wikipedia.org/wiki/Makro_(datateknik) (Hämtad 2015-05-21)

[54] www.metageek.com (Hämtad 15/6 2015)

Akronymlista

AES	Advances Encryption Standard
AH	Authentication Header
AP	Access Point
ATEX	Atmosphères Explosives
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCM	Counter with CBC-MAC
CDMA	Code Division Multiple Access
DCS	Distributed Control Systems
DMZ	Demilitarized Zone
ESP	Encapsulated Security Payload
GSM	Global System for Mobile Communications
HMI	Human-Machine Interface
I/O	Input/Output
IP	Internet Protocol
IPComp	IP Payload Compression Protocol
IPsec	Internet Protocol Security
MSB	Myndigheten för Samhällsskydd och Beredskap
NFC	Near Field Communication
PPTP	Point-to-Point Tunneling Protocol
RFID	Radio Frequency Identification
SCADA	Supervisory Control And Data Acquisition
TDMA	Time Division Multiple Access
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access