Teemu Taipale

KENTTÄVÄYLÄT VALVOMOTEKNIIKASSA

Automaatiotekniikan koulutusohjelma

2016

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

KENTTÄVÄYLÄT VALVOMOTEKNIIKASSA

Taipale, Teemu
Satakunnan ammattikorkeakoulu
Automaation koulutusohjelma
Kesäkuu 2016
Ohjaaja: Laine, Kari
Sivumäärä: 35

Asiasanat: Kenttäväylä, Fidelix, Valvomo, Modbus

Opinnäytetyö käsittelee Fidelixin Modbus-moduulien ja alakeskusten käyttöä kiinteistövalvomotekniikassa. Opinnäytetyön alkupuoli esittelee Modbus väylätekniikkaa. Fidelixin kehittämää omaa modbus-väylätekniikkaa esitellään tarkemmin ja Fidelixin laiterakennetta avataan mahdollisimman yksityiskohtaisesti käyttäjälle.

Opinnäytetyön loppuosio käsittelee yleistä tietoturvaa automaatiossa ja organisaatiossa yleisesti.

Laitteistoa tutkiessani totesin väylätekniikat erittäin toimiviksi kiinteistövalvomotekniikassa.

FIELDBUSSES IN CONTROL ROOM TECHNOLOGY

Taipale, Teemu
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in automation
June 2016
Supervisor: Laine, Kari
Number of pages: 35

Keywords: Modbus, Fidelix, Fieldbus, Control room

My thesis deals with the use of Fidelix Modbus modules and sub-centers in control room technology. The first half of the thesis presents the Modbus technology and Fidelix's own Modbus technique is described in more detail. Fidelix device structure is attempted to describe up to in great detail.

The rest of the thesis deals with the overall security in automation and the organization security in general.

While learning about the system I came to conclusion that fieldbus techniques are good in control room use.

SISÄLLYS

TERMISTÖ JA LYHENTEET

RTU	Remote Terminal Unit
PLC	Programmable Logic Controller
SCADA	Supervisory Control And Data Acquisition
LSB	Least Significant Bit - Vähiten merkitsevä bitti
MSB	Most Significant Bit - Eniten merkitsevä bitti
OSI	Open System Interconnection
ISO	International Organization for Standardization
ASCII	American Standard Code for Information Interchange
FIELDBUS	Kenttäväylä
MODBUS	Modiconin kehittämä kenttäväylätekniikka
BPS	Bits Per Second - Siirtonopeus – Bittiä/sekunnissa
LT	Line Termination, päätevastus
RxD	Receive Data
TxD	Transmit Data

1 JOHDANTO

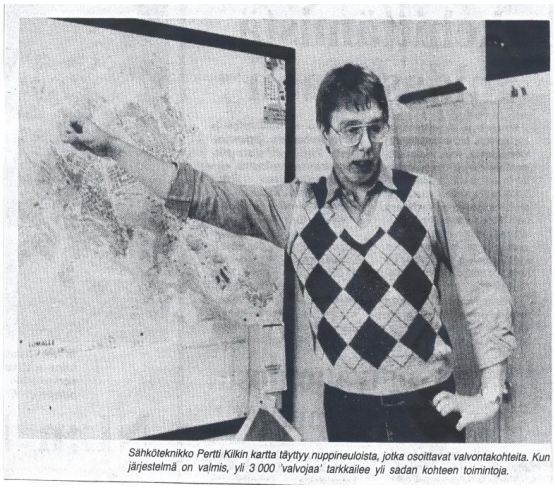
Tämä opinnäytetyö on kirjoitettu osana Tekme Oy:n tilaamaa Ruununmyllyn ala-asteella suoritettavaa automaatiouudistusta. Uudistuksen yhteydessä Ruununmyllyn ala-asteella on otettu käyttöön Fidelixin Modbus-tekniikkaa kiinteistöautomaatiossa.

Selvityksessä käydään lyhyesti läpi Modbusin toiminta, sovellutuksia, rajoituksia ja käyttö yleisesti. Lopussa oleva tietoturvaosio käsitteleekin lähinnä mahdollisten tietoturva-aukkojen muodostumista ja mahdollisia ongelma kohtia kiinteistövalvonnassa ja organisaatiokehityksessä.

Käsittelen Tekme Oy:n omassa käytössä olevaa Fidelixin Modbus-laitteistoa ja sen rakennetta. Tekme Oy on asennuttanut muun muassa Ruununmyllyn ala-asteelle tällaisen laitteiston, mutta Fidelixin muuta valvomotekniikkaa on monessa muussakin kiinteistössä. Mainitut tekniikat ja toteutukset ovat kuitenkin keskiössä juuri tämän kyseisen uudistuksen vuoksi juuri tässä opinnäytetyössä.

1.1 Yritysesittely

Tekme Oy on Hämeenlinnan kaupungin omistuksessa ollut kiinteistövalvomo, joka muuttui omaksi yhtiöksi vuonna 2008. Nykyään Tekmessä työskentelee yli 300 henkeä ja se käsittää yli 300 kiinteistön valvonnan. Kuvassa 1 sähköteknikko Petri Kilkki esittelee vuonna 1983 aikaista järjestelmää, jolloin kiinteistöjä seurattiin vielä myös kartan avulla. Kuvassa 2 puolestaan esitellään laitteistoa ja sen kokoonpanoa, tuolloin kyseinen tekniikka on ollut vielä huippu tasoa koko suomen mittapuulla.



Sähköteknikko Pertti Kilkin kartta täyttyy nuppineuloista, jotka osoittavat valvontakohteita. Kun järjestelmä on valmis, yli 3 000 'valvojaa' tarkkailee yli sadan kohteen toimintoja.

Kuva 2. Sähköteknikko Pertti Kilkki (Hämeen sanomat 1983)

Hämeen kansa 13.9.1983

Suomen suurin valvontajärjestelmä Hämeenlinnaan

Hämeenlinnaan rakennetaan Suomen suurinta kiinteistöjen valvontajärjestelmää. Järjestelmään tullaan liittämään yli 70 Hämeenlinnan kaupungin omistamaa kiinteistöä, kuten kouluja, jäähalli, kirjasto jne. Kaksi ensimmäistä rakennusvaihetta on valmiina ja seuraavat neljä vaihetta valmistuvat 1986 mennessä. Rakentaja on kouvolalainen Computecky.

Täydessä laajuudessaan järjestelmään tullaan liittämään yli 4000 hälytys-, ohjaus-, mittaus- ja säätökohdetta. Modulaarisessa, hajautettuun tietojenkäsittelyyn perustuvassa järjestelmässä tulee olemaan yli 250 mikrotietokonetta. Valvomon ATK-laitteet käsittävät hälytys- ja raporttikirjoittimien lisäksi mm. täysgraafisen värinäyttöpäätteen.

Valvontajärjestelmän avulla uskotaan Hämeenlinnassa säästettävän merkittäviä summia lähinnä energiakulutuksen ja koneseisokkien vähenemisen ansiosta.

Hämeenlinnan kaupunki on ostanut järjestelmän valvomo- sekä kiinteistökohtaiset laitteet ja Hämeen Puhelin Oy puolestaan tiedonsiirtolaitteet, kuten keskittimet ja datamodemit.

Kuva 1. Suomen suurin valvontajärjestelmä Hämeenlinnaan (Hämeen kansa 1983)

Valvontaan sisältyy ovien lukitusten, valojen, rikosilmoittimien ja ilmastoinnin aikaohjauksia. Lisäksi itse kiinteistövalvomon toimintaan kuuluu vahvasti 24/7 vikapäivystys, jossa hyödynnetään valvomoon tulleita mittaustietoja. Näin tiedetään vikailmoitukset, mahdolliset kriittiset ongelmapakat ja ennakkohuoltoa vaativat kiinteistöt. Yritys on ottanut hoitaakseen myös siivouspalvelut, jonka ansiosta se kattaa täysivaltaisesti kiinteistöhuollon kaikkia osaamisaloja.

2 KENTTÄVÄYLÄT

Lyhyin määritelmä kenttäväylälle tulee oppikirjasta jonka mukaan: ”Kenttäväylä (Fieldbus) on automaatiojärjestelmän osa, joka siirtää tietoa järjestelmää mittaavien antureiden, järjestelmää ohjaavien toimilaitteiden ja koko automaatiojärjestelmän välillä” (Keinänen, Kärkkäinen, Lähetkangas, Sumujärvi, 9).

Aikaisemmin kenttäväylän käyttöä on perusteltu rahallisilla säästöillä, jotka muodostuvat johtojen määrän pienenemisestä ja kytkentöjen helpottumisesta. Kenttäväylän jotkin osat saattavat kuitenkin maksaa paljon. Kustannukset voivat nousta paljon etenkin silloin, jos kenttäväylän segmentteihin tarvitaan tavallisesta poikkeavia liitännäisiä tai oikeita osia ei ole suoraan saatavilla. Säästöt ovat kuitenkin edelleen realistisia, jos osia on saatavilla tai käytetään joustavampaa kenttäväylää. Säästöjä voidaan myös saavuttaa kohteissa, joita on tarkoitus laajentaa väylää myöhemmin lisää ja tämä on huomioitu jo järjestelmän suunnitteluvaiheessa. (Nakamura n.d)

Todelliset säästöt saattavat näkyä vasta myöhemmin tai niitä on lähes mahdotonta arvioida etukäteen. Mahdollisia lisäsäästöjä voi myöhemmin tulla esimerkiksi laitteiston päivityksessä, diagnostiikassa ja kunnossapidossa. Selviä tuloksia kuitenkin näkee nopeasti muun muassa:

- Johdotuksen määrässä, jossa voidaan säästää 90 % verraten perinteiseen johdotukseen.
- Valvomon tilan säästönä, koska perinteisiä johdotuksia ei enää tarvita. Näin ollen myös laitteiston käyttöön tarvittavat ohjauslaitteet ovat pienempiä.
- käyttöönotossa ja tarkastuksessa. Lähettimen asentamiseen menee keskimäärin 20 minuuttia, kun perinteiseen malliin saattaisi mennä yli 2 tuntia tarkastuksineen ja johtoineen. (Nakamura n.d)

Kenttäväylälle on ominaista erilaiset verkon topologiat. Liikenne on kaksisuuntaista ja digitaalista. Väylässä on aina master-laite, joka ohjaa alempia slave-laitteita.

Ennen nykyistä kenttäväylätekniikka käytettiin muun muassa RS-232 sarjaliitäntää, sillä saatiin yhdistettyä kaksi konetta toisiinsa. Kun kiinteistössä oli satoja antureita ja niistä jokainen toimii hieman eri tavalla, verkkojen topologiat olivat paikoin erittäin monimutkaisia ja muutokset hankalia.

Väylä pystyy käsittelemään digitaalista ja analogista viestiä, mutta väylässä data liikkuu digitaalisena. Ei ole olemassa rajoitetta, että vain joko digitaalinen tai analoginen lähetin voisi olla kytkettynä, vaan nämä voivat olla samaan aikaan kytkettynä väylään kiinni. Väylässä liikkuu niin sanottua raakadataa, jonka voi sitten skaalata varsinaisessa alakeskuksessa vastaamaan haluttua mitattua suuretta. (Control Solutions Minnesota www-sivut 2015)

Kenttäväylätekniikoita on useita. Niistä kuitenkin vain murto-osa on yleistynyt, koska monella yrityksellä on omiin vaatimuksiin perustuvia itse kehitettyjä kenttäväyliä. Jokainen väylä on kuitenkin perustasoltaan, eli standardirakenteeltaan, yleensä lähes poikkeuksetta samanlaisia. (Rantala & Keronen 2007, 15)

"Hintakilpailu on kovaa ja automaationkin hinta osaltaan ratkaisee, jolloin uusi tekniikka korkeampine hintoineen ei aina pärjää kilpailussa. Loppuasiakas ei useinkaan huomioi esimerkiksi diagnostiikan avulla saatavia säästöjä myöhemmässä käytössä eikä heillä ole riittävää koulutusta ja taitoakaan tähän". Kuitenkin, kun asiakas on todennut diagnostiikan edut ja hyödyn sekä päässyt uuden laitteiston kanssa riittävälle käyttötasolle, ei yleensä ole syytä palata perinteisiin tekniikoihin. (Rantala & Keronen 2007, 15)

Asiakkaan on hankala arvioida väylän käytön vaikeutta ja sen hinnan muodostumista. Väylän kokorakenteen muodostuminen voikin olla hankalaa hahmottaa ja antureita tulisi miettiä väylän ulkopuolisena, kun hintaa väylälle mietitään. Toimilaitteet eivät ole loogisella tapaa mukana hinnan muodostumisessa, koska joillekin anturi- ja toimilaitetyypeille voi muodostua käyttökohteen ja laitteen tarkkuustason mukaan hintaa suhteessa enemmän kuin mitä se voisi olla muissa olosuhteissa. Väylä voi kuitenkin mahdollisesti pidentää joidenkin laitteiden ikää,

kun diagnostiikalla pystytään seuraamaan mahdollisia vikatilanteita ja kulumista paljon helpommin. (Rantala & Keronen 2007, 12)

3 MODBUS

Modbus on avoin sarjamuotoinen kenttäväyläprotokolla, jonka kehitti Modicon vuonna 1979. Tarkoituksena oli käyttää sitä Modiconin omissa PLC-laitteissa. Myöhemmin Modbus kuitenkin tehtiin lopulta kaikille avoimeksi. Alun perin Modbus-väylät perustuivat ainoastaan ASCII-muotoiseen viestintään. Huhtikuussa vuonna 2004 Modicon antoi Modbusin oikeudet Schneider Electricille. Tällöin perustettiin myös http://www.modbus.org/-osoitteessa toimiva avoin yhteisö, jonka pääkäyttäjät muodostuvat järjestelmän käyttäjistä ja maahantuojista. Yhteisössä pyritään edistämään ja kehittämään Modbusin käyttöä ja käyttöönottoa. Sivustolta löytyy laajasti tietoa, tukea ja dataa liittyen Modbusiin, sen rakenteeseen ja käyttöön. (Modbus www-sivut 2015)

Modbusista on vakiintunut kolme versiota: RTU, ASCII ja TCP/IP. Modbusin etuja verrattuna perinteiseen kaapelointiin ovat muun muassa:

- Kaapelien ja kytkentöjen määrä vähenee.
- Signaalimuunnosten määrä vähenee mittasuureissa ja häiriösieto on parempi.
- Konfiguroinnin ja parametroinnit pystyytään tekemään suoraan väylän kautta.
- Vikadiagnostiikan pystyytään suorittamaan etänä.
- Ala-asema voi lähettää useita eri mittaussuureita.
- Muunneltavuus on monin verroin parempi kuin kiinteällä langoituksella. Jotkin lisäosat pystytään kaapeloimaan vanhoihin kaapeleihin.
- Myös langaton vaihtoehto on olemassa.
- Suhteelliset siirtovirheet on havaittavissa.

Modbus sisältää useamman siirtokehysmallin. ASCII- ja RTU-mallia ei pysty sekoittamaan keskenään, eivätkä ne toimi ristiin. Näistä RTU:ta ja ASCII:tä käytetään tyypillisten sarjaväylien (kuten RS-485) päällä. TCP/IP-versiota käytetään ethernet-liitännöissä. (Piikkilä 2006, 244)

RS-232-liitäntä toimii kahden pisteen välillä ja vain 15 metrin etäisyydellä. RS-422 ja RS-485 mahdollistavat pidemmän johtovälin ja useamman slave-yksikön. RS-422 ei ole kuitenkaan yleistynyt käytössä, joten siihen törmää harvemmin käytössä. RS-485 on ylivoimaisesti yleisin sarjamuotoinen käytettävä kaapelointi, koska se pystyy käsittelemään 32 haaraumaa päärungosta. Johdotukset toimivat 1200 metriä ilman toistin yksikköä. RS-liitännöistä puhuttaessa tulee olla erityisen tarkkana, koska käytössä on myös virheellisiä nimikkeitä, joita käytetään lähinnä myynnin edistämiseen.

Tiedonsiirtonopeus eli baud rate (Bps) tulisi olla kaikilla väylän laitteistolla sama toiminnan takaamiseksi. Käytössä yleisin on 9600–19200 baudia, mutta se voi vaihdella välillä 300–100000 baudia. Master laite lähettää käskyjä slave-yksiköille. Slave-yksiköt eivät kuitenkaan lähetä viestejä master-yksikölle, jos näiltä ei kysytä mitään. Master-yksikön alaisena voi olla 247 slave-yksikköä. Jokaisella slave-yksiköllä on yksilöllinen slave-tunniste välillä 1–247. (ProSoft Technology 2014)

4 MODBUS RTU

Tekme Oy:n kenttäväylätekniikka on Fidelix Oy:n toteuttama. Ruununmyllyn ala-asteella on käytetty Modbus RTU -tekniikkaa. Fidelixin käyttöliittymä on ollut aiemminkin käytössä muissa kiinteistöissä. Tämän vuoksi avaan kyseistä siirtotekniikkaa enemmän kuin muita vastaavia tekniikoita. RTU eli remote terminal unit tarkoittaa sananmukaisesti etäkäyttö pääteyksikköä. Fidelixin RTU-yksiköt ovat käytännössä pieniä FTP-palvelimia, johon Fidelixin Modbus-yksikkö kerää datan, joissakin tapauksissa data on siirretty myös Fidelixin omalle palvelimelle. Näin tekniset ongelmat ja datan häviäminen on estetty.

Tekmen valvomosta otetaan tarvittaessa yhteys laitteen palvelimeen, kun dataa halutaan tarkastella. Modbus ei ole millään tavalla riippuvainen Tekmen valvomon koneiden toiminnasta, vaan se on täysin itsenäinen prosessikokonaisuus. Niin kauan kuin palvelin on kunnossa ja toimii, tiedot pysyvät tallessa. Palvelimelle pääosin siirtyy mittausdataa ja muita haluttuja pistetietoja. Kiinteistöön on voitu asentaa myös oma päätelaite, jonka ansiosta asetuksia ja tietoja voidaan tarkastella reaaliajassa myös kiinteistössä. Tämä ei kuitenkaan ole välttämätön, jos ei ole syytä tehdä muutoksia paikallisesti.

4.1 Modbus OSI-kerrosarkkitehtuurissa

Kaikki siirtotekniikat on sidottu OSI-rakenteeseen. Se saattaa olla jokaisella hieman erilainen, mutta jokainen on sovitettavissa jollain muotoa OSI-rakenteeseen. International Organization for Standardization (ISO) kehitteli vuonna 1977 ISO-standardin (kuvassa3), jonka mukaan kuuluisi toimiva tietoliikenne rakentaa. Tuloksena oli OSI-kerrosarkkitehtuuri.

OSI-mallin pääperiaatteena on ollut, että kaksi eri valmistajan laitetta pystyisi keskustelemaan keskenään riippumatta muista kerroksista. Esimerkiksi verkkokerros

voisi keskustella laitteen toisen verkkokerroksen kanssa, ja laitteen ensimmäisen sovelluskerros voisi keskustella laitteen toisen sovelluskerroksen kanssa.

Layer	ISO/OSI Model	
7	Sovelluskerros	MODBUS Application Protocol
6	Esitystapakerros	Tyhjä
5	Istuntokerros	Tyhjä
4	Kuljetuskerros	Tyhjä
3	Verkkokerros	Tyhjä
2	Siirtoyhteyskerros	MOSBUS Serial Line Protocol
1	Fyysinen kerros	EIA/TIA-485 (tai EIA/TIA-232)

Kuva 3. RTU, OSI-kerrosarkkitehtuuriin sovitettuna. (Taipale 2016)

OSI-malli on jaettu seitsemään pienempään kerrokseen, jotta näitä olisi helpompi hallita. Kerrosta voisi verrata navigaattoriin. Navigaattorille on annettu tehtävä ja määränpää. Sille on voitu antaa määritteissä käsky välttää valtateitä ja losseja, mutta muutoin se saa vapaasti ohjeistaa perille. OSI ei kuitenkaan ole mikään muotti mihin kaikki toiminta tulee saada puristettua, vaan se on viitekehys, josta saa apua standardointia ja suunnittelua silmällä pitäen. (Saarelainen 1999, 23)

Modbus RTU hyödyntää OSI-mallin seitsemästä kerroksesta ainoastaan kolmea. Näin ollen vain näihin kolmeen kerrokseen on annettu ohjeistukset, kuinka Modbus-protokollaa tulisi soveltaa laitekokoonpanoissa. Kerrokset ovat kerros 7 - sovelluskerros (Applications), kerros 2 - siirtoyhteyskerros (Data Link) ja kerros 1 - fyysinen kerros (Physical). Muissa kerroksissa laitevalmistajalla on vapaat kädet. Modbus käyttää sarjamuotoista tietoliikennettä data siirtämiseen ja se tapahtuu OSIn siirtoyhteyskerroksessa. (Saarelainen 1999, 23)

4.1.1 Fyysinen kerros

Fyysinen kerros on ensimmäinen taso OSI-mallissa. Fyysinen taso voi hyödyntää erilaisia sarjaporttimuotoja kuten RS485 ja RS232. RS485 (eli TIA/EAI-485) kahden

johdon liitäntä on kaikista yleisin. Lisäksi RS485 neljän johdon liitäntä on mahdollista käyttää joissain tapauksissa. TIA/EIA-232-E (RS232) sarjaliitäntää on mahdollista käyttää, jos tietoliikenteen tarve on pisteestä pisteeseen, ja lyhyen matkan kommunikointiin. Etäisyyden ei näissä tapauksissa suositella olevan yli 20 metriä. Fyysinen kerros on myös ainoa OSI-kerros, missä on ihmiselle ilman laitteita aistittavia asioita. (Modbus 2006, 5)

Fyysisen kerroksen merkitsevin tieto siirrosta on siirtovirhesuhde, siirtonopeus ja siirron viive. Jos data on asynkronoitua, datakehyksen alussa ja lopussa olevat aloitus- ja lopetusbitit ovat suuressa roolissa. Näistä biteistä tiedetään milloin viesti alkaa ja milloin viesti loppuu. Synkronoidussa siirrossa puolestaan käytetään kellopulssia erottamaan yksittäiset bitit. (Kaario 2002, 19)

4.1.2 Siirtokerros

Tieto siirtyy sovitun laisissa kehyksissä fyysistä siirtotietä pitkin. Toinen kerros mahdollistaa virheiden ja korjausten toteuttamisen. Se varmistaa luotettavan tiedonsiirron. Siirtokerros ei kerro kuitenkaan mitään datan oikeellisuudesta. Jos viesti on väärä, esimerkiksi lämpötilamittaus on väärässä +10 °C anturin toiminnan takia, mittaustieto lähetetään myös vääränä ja vastaanotetaan vääränä – eli myös vastaanotettu mittaustieto on väärässä +10 °C.

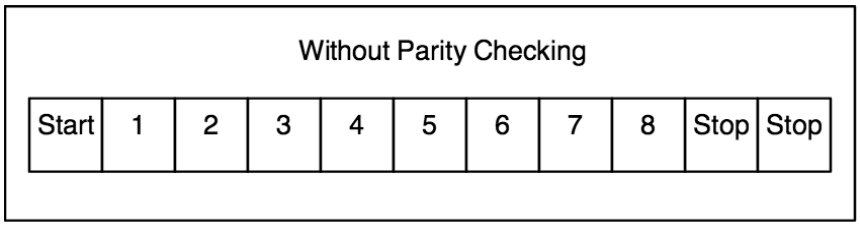
Kerros varmistaa ainoastaan, että lähetetty tieto vastaa vastaanotettua tietoa. Jos vastaavasti lähetetty tieto poikkeaisi +10 °C anturin toiminnan takia ja vastaanotettu tieto näyttäisi silti vain +2 °C, osaisi siirtokerroksen mukainen ohjelmisto ilmoittaa, että siirrossa on tapahtunut virhe. Tuolloin se toimisi tätä varten määrätyn tavan mukaan, joka yleensä on viestin hylkääminen virheen vuoksi. (Kaario 2002, 19)

4.1.3 Sovelluskerros

Sovelluskerros - application layer, määrittelee tietoliikennesovellusten kommunikointirajapinnan rakenteen. Sovelluksia, jotka hyödyntävät tätä kerrosta, voivat olla esimerkiksi sähköposti, hakemistopalvelut, tiedonsiirto ja päätekäyttö. Kerros sisältää sovellukset ja verkkoliikenneyhteyksiä hyödyntävät ohjelmat. Poiketen OSI-mallin muista kerroksista, sovelluskerroksen ei tarvitse palvella muita kerroksia. Se toimii rajapintana sovelluksen ja tiedonsiirron välillä. Se sijaitsee muutoinkin varsinaisen OSI-protokollapinon ulkopuolella. (Modbus 2006, 5)

4.2 Modbus kehysrakenne

Modbus kehysrakenne tarkoittaa lähetetyn viestin muotoa ja yleistä rakennetta. Jokainen 8-bittinen merkkijono lähetetään hexadesimaalimuodossa, tämä vastaa neljää hexadesimaalimerkkiä. Kehysrakenne muodostuu pienemmistä kehyksistä, kuten kuvasta 4 voi todeta. Nämä kehykset ovat lähetetyssä viestissä määrätyssä järjestyksessä. Viesti lähetetään vasemmalta oikealle, eli lukusuunnassa. Vähiten merkitsevästä bitistä (Least Significant Bit - LSB), eniten merkitsevään bittiin (Most Significant Bit - MSB).



Kuva 4. Modbus RTU pariteetiton kehysrakenne (Modbus.org 2006, 12)

Ensimmäinen merkitsevä seikka kehysrakenteessa on pariteetti. Pariteetti tarkoittaa lähetetyn viestin binaariarvon ykkösten yhteenlaskun parillisuutta. Tämä on nopea tapa varmentaa, että viesti ei ole muuttunut matkalla. Asetuksissa on mahdollisuus

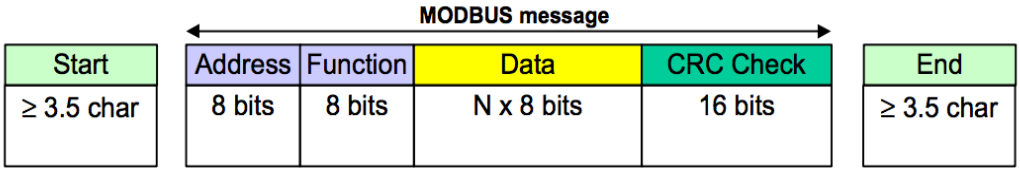
valita viesti pariteetilla tai ilman. Käytännössä kehyksessä on silloin joko pariteetti lopussa taikka kaksi stop kehystä. (Modbus 2006, 8)

Koska Fidelixin laitteilla ei ole pariteettitarkistusta, Fidelixin laitteissa on myös tällöin vain yksi stop kehys. (Fidelix 2003, 6)

Kuvan 5 mukainen Modbusin yleinen kehysrakenne lyhyesti:

- START, pituus 28 bittiä tai 3½ merkkiä pitkä hiljaisuus, joka ilmaisee uuden viestin alkua.
- ADDRESS, osoitetieto, joka viittaa johonkin tiettyyn slave-yksikköön, jolle kuljetettava viesti on osoitettu.
- FUNCTION, toiminto. 8 bittiä pitkä komento, joka kertoo slave-yksiköllе tuleeko sen vastaanottaa vai lähettää tietoa.
- DATA, varsinainen tieto. Pituus riippuu paljon lähetetystä/vastaanotetusta tiedosta ja bittimäärä vaihtelee paljon.
- CRC, Cyclical Redundancy Check. Virheellisen viestin havaitsemiseen tarvittava tarkastusbittijono.
- END, samoin kuin Start, 28 bittiä tai 3½ merkkiä pitkä hiljaisuus, joka erottaa viestin seuraavasta.

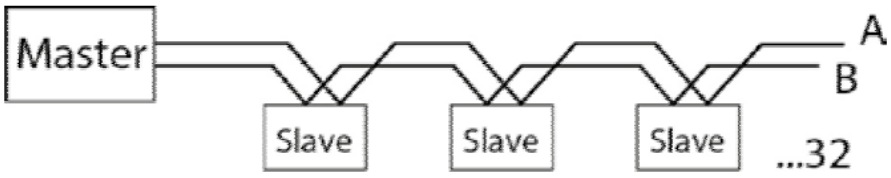
(Modbus 2006, 8)



Kuva 5. Modbus RTU kehysrakenne (Modbus.org 2006, 12)

4.3 Modbus RTU topologia

Master-Slave-tyypin rakenne sisältää aina yhden master-haaran (kuva 6). Master lähettää käskyjä slave-haaroille ja käsittelee näiden haarojen lähettämät vastaukset. Slave-yksiköt eivät lähetä dataa ilman master-haaran pyyntöä, eivätkä kommunikoi muiden slave-yksiköiden kanssa. Malli on samanlainen kuin todella tiukkaa kuria



Kuva 6. Master-Slave kytkentä useammalle laitteelle (Janiza.com 2015)

pitävässä luokkahuoneessa. Opettaja antaa tehtäviä luokan edessä ja esittää kysymyksiä. Oppilaat saavat kuitenkin vastata vasta viitattuaan ja saatuaan luvan puhumiseen. Muuten oppilaat ovat hiljaa, eivätkä puhu keskenään vastauksista.
Toinen malli esimerkki olisi puhelinkeskustelu:

- Henkilö A soittaa henkilölle B.
- Henkilö B vastaa puheluun, kun kuulee hälytysäänen.
- Henkilö B vastaa puheluun: ”Haloo, B kuuntelee” ja samalla varmistaa, että puhelu on tullut oikealle henkilölle.
- Henkilö A vastaa ”Terve B, Täällä puhuu A”, josta B tietää kenen kanssa hän puhuu.

Kun yhteys on luotu, voivat A ja B keskustella, kunnes yhteys katkaistaan. Tämä ei kuitenkaan takaa vielä, että tieto välittyy henkilöltä toiselle. Huono signaali, äänen vääristyminen tai perinteisestä puhelinkäyttäytymisestä poikkeaminen voi aiheuttaa viestinkulussa ongelmia. (Kaario 2002, 19)

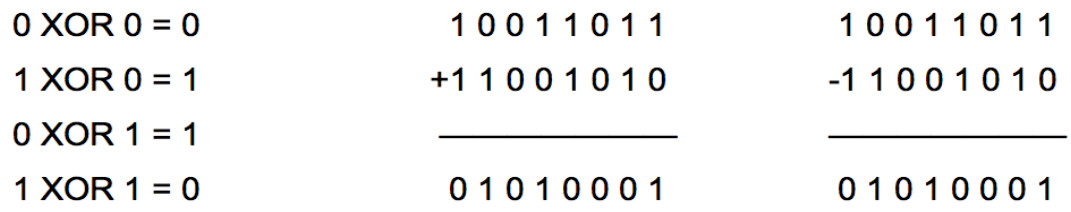
4.4 CRC – Virheenkorjaus

CRC (Cyclical Redundancy Check) on lähtevän viestin loppuun liitettävä lyhyt bittijono, joka tarkastaa saapuneen viestin kehyksen. Bittijono pitää huolen, että viestissä ei ole virheitä. Tämän oikeellisuutta tarkastellaan lisäksi pariteetillä. Jonon viimeinen bitti määräytyy sen mukaan, onko jonon yhteenlaskettu summa parillinen vai pariton. (Humpry 2016)

CRC on yksinkertainen algoritmi, joka suoritetaan sekä tietoa lähettävässä että vastaanottavassa päässä. Lähettävä pää laskee polynomisen kaavan avulla syntyvän

luvun, joka lasketaan koko lähetettävän viestin kanssa yhteen käyttäen XOR-laskumuotoa. XOR on loogisissa lauseissa käytetty funktio, joka antaa tuloksena luvun 1 tai 0 riippuen mitkä kaksi arvoa laskuun on annettu. Allekkain laskettuna ei ole merkitystä suoritetaanko lasku summana vai erotuksena. Algebran laskusääntöjen mukaan tulos on kuitenkin molemmissa tapauksissa sama. (Humpry 2016)

Lähetettävä viesti lasketaan käyttäen XOR:ia (kuvassa 7) niin, että tuloksena viivan alla olisi 0, kunnes päästään viimeiseen bittiin asti, jolloin saadaan CRC-arvo. Tämä CRC-arvo liitetään viestin perään. Vastaanottava pää on ohjelmoitu niin, että se avaa samaa polynomista laskentamallia ja avainta käyttämällä saapuneen viestin. Jos



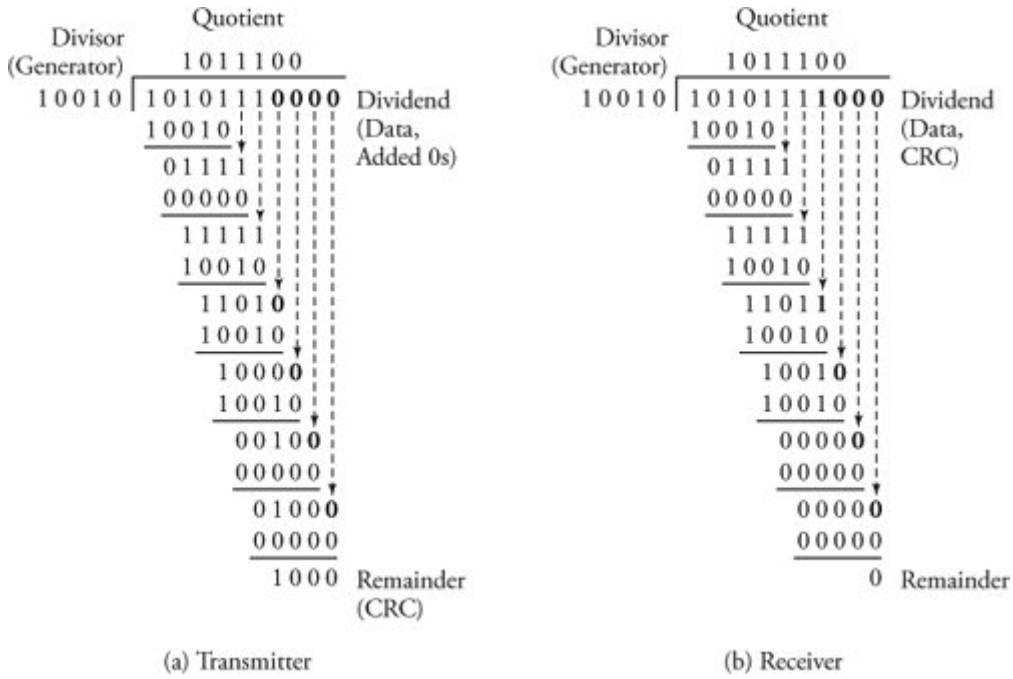
Kuva 7. XOR-laskennan yhteen- ja vähennyslaskut. (Taipale 2016)

viestin viimeiset bitit ovat nyt nollia, ei lähetyksessä ilmennyt virheitä. Näiden lisäksi on olemassa muitakin CRC-muotoja ja pidempiä varmenteita, mutta ne eivät ole suhteessa niin yleisiä. (Modbus www-sivut 2015)

Modbus käyttää 16-bittistä CRC:tä datan varmentamiseen. Tämä esitetään usein polygonimuodossa esim. $X^{16}+X^{15}+X^2+1$. CRC-laskenta kuitenkin tehdään binaarimuodossa. Jos tiedonsiirto ei toimi RTU:ssa yhtäjaksoisesti ja ei ole täysin hyväksytty CRC-tarkastuksessa, lähetetty viesti hylätään. CRC:n kokonais tarkkuus on 99,96%. (Mir 2006).

Laskutoimitus tehdään binaarimuodossa, vaikka tiedonsiirto on hexadesimaalista. Tämä mahdollistaa XOR-operaattorin käyttämisen ja suuremman tarkkuuden. CRC-laskenta on itsessään yksinkertainen prosessi. Koko lähetettävä kehys tarkastetaan läpi binaarimuotoisena. Kuten kuvassa 8 on esitetty vasemmalla puolella lähtevän viestin luonti. Viesti voisi olla muodossa: 10101110000. Neljän viimeisen nollan tilalle muutettaisiin CRC-tarkistusarvo laskun päätteeksi.

Kuvassa 8 Vasemmalla näkyy 10010 -arvo, joka on sekä lähettävälle, että vastaanottavalle laitteelle sama avainarvo, jolla viesti puretaan. Tätä käytetään varsinaisen viestin jakamiseen XOR-operaattoria käyttäen. Aina kun jakojäännökseksi tulee nolla, siirrytään rivillä eteenpäin kunnes vastaan tulee seuraava ykkönen. Numeroita tiputetaan alkuperäisestä viestistä vastaamaan jakajan pituutta. Lopullinen viivan alle jäävä nelinumeroinen luku on itse CRC-arvo, joka lisätään lähetettävään viestiin neljän nollan tilalle. Esimerkin lähtevä viesti olisi 10101111000. (Humpry 2016)

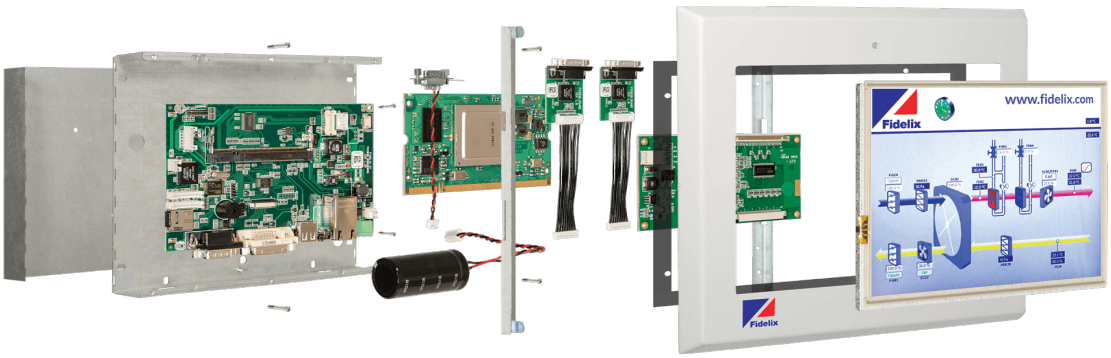


Kuva 8. Esimerkki XOR-operaattorin käytöstä CRC:n laskemisessa. (Mir 2006)

Saapuvan viestin purku tapahtuu lähes samoin. Jakajana toimii edelleen laitteille yhteinen 10010-arvo. Tällä kertaa kuitenkin laskun lopputulokseksi jää aina nolla, jos viesti on mennyt virheittä perille. Yhden bitin virheet löytyvät poikkeuksetta. Useamman bitin virheet eivät myöskään ole ongelma. Varsinainen 0,04 % lähetysvirheen mahdollisuus tuleekin siitä, että viestissä on kaksi virhettä, sekä vastaanottavassa että lähettävässä päässä samassa kohtaa. Teoreettinen laskennallinen virhe on 0,04 % sille, että yhdessä lähetetyssä ja sen vastaanotetussa vastineessa voisi olla virhe samassa kohtaa viestiä. Laskennallisesti miljoonasta viestiparista neljässätuhannessa voisi olla virhe. (Humpry 2016)

5 FIDELIX FX-2030A ALAKESKUS

FX-2030A (kuvassa 9) toimii Windows CE Professional -käyttöjärjestelmässä. CE-järjestelmä on samanlainen kuin perinteinen Windows käyttöliittymä, mutta se on tarkoitettu pienille kämmentietokoneille eikä se tarvitse juurikaan muistia toimiakseen. Alakeskus on varustettu sisäisellä web- ja FTP-palvelimella. Yksikkö on vapaasti ohjelmoitavissa ja se käyttää avointa PLC-tietokoneille tarkoitettua standardia. Laitteiden määrää pystytään lisäämään multiLINK-moduulilla, jolla saadaan lisää Modbus- ja M-bus-väyliä liitettyä järjestelmään.



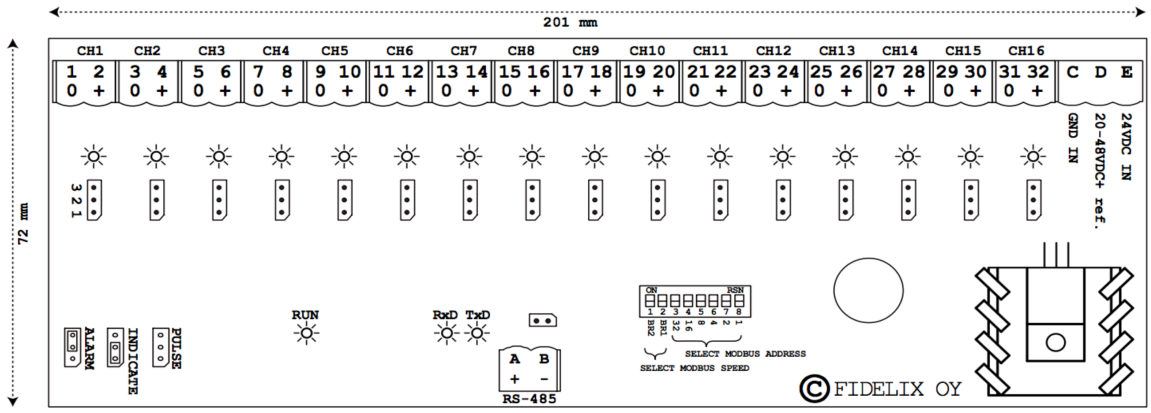
Kuva 9. FX-2030 alakeskus (Fidelix.se 2015)

Alakeskus toimii 12-24V tasajännitteellä. Suositeltu käyttölämpötila on 0°C…+50°C. I/O-liitäntöjen enimmäismäärä on 2000 fyysistä ja virtuaalista pistettä/ala-asema. (Fidelix 2003, 4)

Kaikki RTU-485 -sarjaliikenneväylää käyttävät moduulit kytketään sarjaporttiin COM3. Moduulien maksimimäärä on 63. Niiden osoitteet ovat 1–63. Lisää moduuleja saadaan lisäämällä multiLINK-mediamuunnin. Laitteeseen on mahdollista liittää ulkoinen näyttö, hiiri ja näppäimistö. COM1-porttiin voidaan liittää SMS-modeemi. RJ45-Ethernet-porttia voidaan käyttää kiinteällä IP-osoitteella. Tekmen omistamat Fidelixin laitteet ovat kaikki lähes poikkeuksetta 3G-yhteyden takana. (Fidelix 2003, 4)

5.1 Fidelixin I/O moduulit

Fidelixin moduulien käyttöjännite on 24V tasajännitettä. Liittimien navat on merkitty E = 24VDC ja C = 0VDC, kuvassa 10 yläoikealla. Tietoliikenne toimii sarjaliikenteisellä RS-485 signaloinnilla ja käyttää Modbus RTU-protokollaa. Fidelix-laitteissa on moduuleilla omat sarjaliikenneliittimille tarkoitetut paikat, jotka on merkitty A- ja B-navoiksi. Napaan A kytketään DATA+ ja napaan B kytketään DATA-, kuvassa alhaalla keskellä. Liitännässä tulisi käyttää 120 ohmin nimellisimpedanssi-parikaapelia. Kytkentä tehdään kuitenkin aina B-B ja A-A -pisteiden välillä. Yhteen liittimeen tulee silloinkin vain kaksi johdinta. (Fidelix 2003, 4)



Kuva 10. Fidelix Modbus piirikortin kytkentäkaavio. (Fidelix.fi, 2)

Väylän viimeinen moduuli päätetään liittimen lähellä olevalla jumpperilla, joka on moduulikohtainen. Tästä käytetään myös termiä Line Termination (LT), päätevastus, joka on yleensä 120 tai 150 ohmia. Maadoitus ja muut vastukset ovat yleensä laitekohtaisia. Jokaisella moduulilla ja ala-asemalla tulisi olla sama siirtonopeus. (Fidelix 2003, 5)

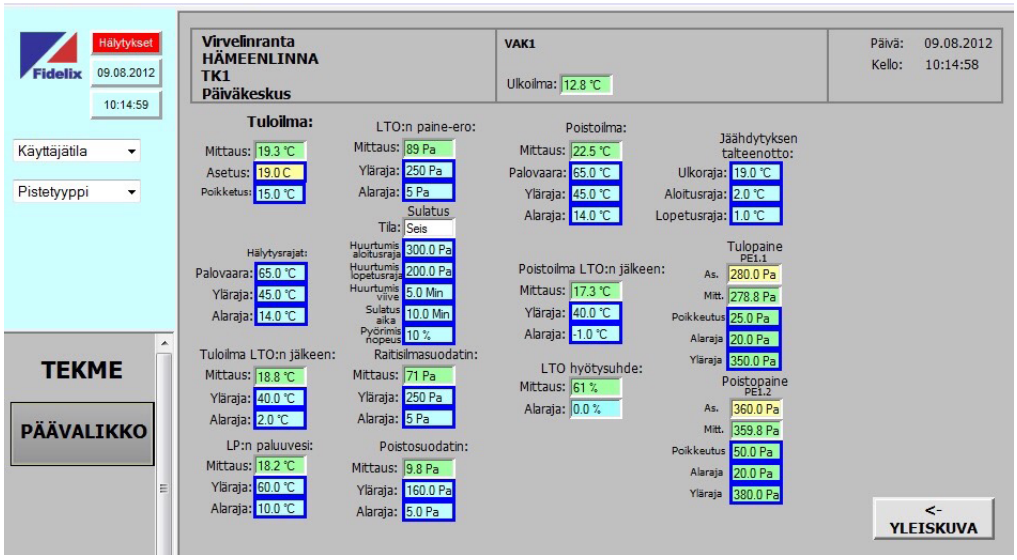
Moduuleja ovat digitaaliset sisääntulot (Digital Input -moduulit) DI-8 ja DI-16, digitaaliset ulostulomoduulit DO-8 ja DO-16, analogiset sisääntulot (Analog Input) AI-8, analoginen lähtömoduli (Analog Output) AO-8. Lisäksi on erikoismoduli COMBI-36. COMBI-36:ssa on yhdistettynä 12 digitaalista tuloa, 8 relelähtöä, 8

analogista tuloa ja 8 analogista lähtöä. Se näkyy käyttäjälle kuitenkin neljänä erillisenä moduulina. SI-8 -moduuli on turvamoduuli, jolla pystyy tekemään analogista mittausta nopealla vasteajalla. (Fidelix 2003, 5)

5.2 Fidelix käyttöliittymä

Fidelixin käyttöliittymät on tehty HTML-editorilla. Varsinainen etäkäyttöliittymä on internetselainpohjainen. Etäyhteys muodostetaankin yleensä laitteeseen itseensä suoraan, samalla tavalla kuin FTP-palvelimeen. Kuten FTP-palvelimessa, myös käyttöliittymän yhteydellä voidaan tietoa viedä ja tuoda. Asetuksien muodossa dataa ensin haetaan, tehdään siihen muutoksia ja päivitetään se sitten Fidelixiin.

Käyttöliittymä on varsin räätälöitävissä ja joustovaraa antaa lisää HTML-koodit. Käyttöliittymän ulkomuoto on pitkälti kiinni henkilöstä, joka sen laatii, kuten kuvassa 12 on mitattavat arvot itse päätettävissä. Yleensä tässä kysytäänkin käyttäjältä, minkälaisia tietoja hän haluaa mitata ja seurata. Käyttöliittymän pääsivu muotoillaan pitkälti tämän perusteella.



Kuva 11. Fidelixin ohjausnäkymä Virvelinrannan kiinteistöstä. (Taipale 2016)

Yleisesti pidetään hyvänä käytäntönä, että ainakin LVI-koneista olisi kuva, joka näyttää missä kohtaa prosessia mittauspisteet ja asetukset sijaitsevat fyysisesti. Ovi-

ja valo-ohjauksille yleensä riittää tilatieto ja kuvaus mitä ohjataan. Loogista olisi myös, että jos rakennus on yhtenäinen eikä jaettu moneen osaan, olisi kaikki ovi-ohjaukset joko samalla sivulla tai lähekkäin toisiaan. Moneen osaan jaetun rakennuksen ovi- ja valo-ohjaukset olisivat joko asetettuna kaikki samalle sivulle tai rakennusten mukaan kaikki rakennukseen liittyvät ohjaukset samalle sivulle.

6 TIEDONSIIRTO JA TIETOTURVALLISUUS

Kaikessa dataliikenteessä ja tietojenkäsittelyssä tärkeimpiä asioita on tietoturva. Myös suljetut järjestelmät ovat uhattuna, vaikkakin vain välillisesti. Verkossa olevat palvelut ja tieto ovat kuitenkin suoraan uhattuna, vaikka uhka ei olisi ilmeinen tai välitön hyökkäys.

Tietojenkäsittelyyn liittyy aina tietoturvallisuus. Kun kyseessä on asiakkaan omaisuudesta tai kiinteistöstä kerättävä data, on voitava varmistaa, että ulkopuolinen ei pysty dataa hyödyntämään omaksi edukseen. Tietoturvallisuus on käytännössä hieman suhteellista kerättävän datan suhteen. Jos data ei ole kriittistä tai ”vaaranna” asiakasta, ei tietoturva ole välttämättä suoraan uhattu, vaan kyseessä on kohtalainen riski. Välillisesti tällainen tiedon kerääminen voi kuitenkin osoittautua kohtalokkaaksi. Jos dataa ei pysty kohdentamaan mihinkään tiettyyn prosessiin tai sen osaan, ei data ole suhteessa vaarallista. Parhaimmillaankin suuri määrä dataa ilman selkeää alkuperää on vain dataa ja näin ollen kutsuisin sitä vain lievästi potentiaaliseksi riskiksi.

Koneella voi kuitenkin olla käynnissä apuohjelmia, joista käyttäjä ei edes tiedä. Nämä ohjelmat voivat mahdollistaa järjestelmään tunkeutumisen ja ovat huomattavasti vaarallisempia kuin järjestelmän kuuntelu. Ongelma muodostuu yleensä ohjelman turva-aukosta, josta julkaisija ei vielä joko tiedä tai siihen ei ole korjaavaa päivitystä. ”Zero-day vulnerability”, joka tunnetaan nollapäivähaavoittuvuutena. Se tarkoittaa vikaa, josta julkaisija on tiennyt nolla päivää. Muussa tapauksessa julkaisija voi hyvinkin paikata aukon, jos saa sellaisen tietoonsa. Tämäkään ei ole itsestään selvää. Niin sanottu ”Security through obsecurity”- ajattelumalli on erittäin yleinen suurilla ohjelmointiyrityksillä. Vapaasti tuon ajatuksen voisi suomentaa ”Se ei voi satuttaa, mitä ei tiedä”. Tämä malli perustuu pitkälti siihen, että jos vika ei päädy julkiseksi, hyökkääjät eivät osaa sitä todennäköisesti etsiä ja hyödyntää. (Hakkerin käsikirja, 8.)

Hyökkäykselle alttiita ja todennäköisiä riskiohjelmia voi olla esim.:

- verkkotulostuohjelmat

- järjestelmän etäkonfigurointiohjelmat
- tiedostonjako-ohjelmat
- laitteistojen oletussalasanat
- näyte-CGI-ohjelmat ja –skriptit

Edellä mainittujen lisäksi turva-aukon voi aiheuttaa ohjelma, joka ei ole päällä. Virustorjunta, jota ei päivitetä tai käytetä ollenkaan, ei juuri hyödytä käyttäjää tai järjestelmää ja näin ollen jättää järjestelmään täysin turhan aukon. (Hakkerin käsikirja, 8.)

6.1 Suomen automaatioverkkojen haavoittuvuus

Aalto-yliopiston sähkötekniikan korkeakoulu julkaisi 21.3.2013 laajan raportin ”Suomen automaatioverkkojen haavoittuvuus”, jonka ovat kirjoittaneet Seppo Tiilikainen ja Jukka Manner.

Raportti esitteli internetissä julkisesti olevia automaatiolaitteita. Listalta löytyi vankila, sairaala, useampia tehtaita, pankki, sähköntuotannon ja vedenjakelun yrityksiä sekä runsaasti kiinteistönohjaukseen käytettävää taloautomatiikkaa. (Tiilikainen & Manner, 2013, 8.)

Tutkimuksessa käytettiin kaikille avointa Shodan-palvelua Suomen verkon skannaamiseen. Tällä tavoin löytyi 185000 HTTP-vastausta antavaa laitetta. Arvion mukaan vain alle 20 % koko Suomen IP-verkostosta on vasta skannattu Shodaniin. Lisäksi löydetyistä laitteista noin 60 % sisälsi tunnetun julkisen tietoturvariskin, joka löytyy internetistä suoraan ”googlaamalla”. (Tiilikainen, Manner, 2013, 2.)

Shodan on Venäjältä toimiva sivusto, joka on perustettu vuonna 2009. Shodan kerää tietoa pääsääntöisesti internet-palvelimilta ja skannaa niistä asiakkaiden rajapinnat etsien HTTP-portteja ja yhteyksiä (portti 80) sekä FTP- (portti 21), SSH- (portti 22), Telnet- (portti 23), SNMP- (portti 161) ja SIP-portteja (portti 5060).

Tietokoneohjelmoija John Matherly sai idean hakuohjelmasta, jolla voi etsiä internetiin yhdistettyjä laitteita jo vuonna 2003. (Shodan www-sivut 2015)

Varsinainen tutkimus rajattiin Suomen sisäisiin IP-osoitteisiin rajaamalla hakusanoja, maa-asetuksia ja IP-osoitteita. Hakusanoja hyödynnettiin rajaamaan tuloksia vain automaatiolaitteisiin. Hakusanoina oli muun muassa valmistajia, tuotenimiä, protokollia ja palveluita, kuten esimerkiksi Modbus. (Tiilikainen, Manner, 2013, 3.)

"Sähkönjakeluyksiköitä ja UPS-hallintalaitteita löytyi yhteensä 73 kappaletta. Sähkönhallinta liittyy rakennusautomaatioon, mutta pidetään usein erillisenä järjestelmänä.” Näistä suurin osa oli tietokonesaleja, hotelleja ja verkkosivupalvelimia. UPS-laitteisiin hyökkäämällä saadaan aikaan kyllä vahinkoa, mutta hyökkääjä ei voi tarkalleen tietää esimerkiksi mitä muita laitteita UPS-laitteessa on kiinni. Näin ollen uhka näille laitteille on suhteellinen. Vaara on olemassa, mutta laitteet eivät välttämättä valikoidu kohteeksi, jos ne eivät osoita mahdollisuutta jatkohyökkäystä silmällä pitäen. UPS-laitteiden perässä on kuitenkin usein tietokoneita. Jos hyökkääjä tietää missä kiinteistössä UPS-laite sijaitsee, voi hän yrittää siihen hyökkäämällä saavuttaa itselleen lisähyötyä isomman hyökkäyksen yhteyteen. (Tiilikainen, Manner, 2013, 7)

Suomessa olevien HTTP-vastauksia antavien laitteiden määrä on lähes mahdotonta arvioida. Shodan ei ole skannannut Suomen verkosta kuin murto-osan. Luku voi kuitenkin olla yli miljoona laitetta. "Tähän on laskettu mukaan laitteet, jotka ovat mahdollisia hyökkäysrajapintoja yrityksen laitteisiin tai verkkoihin, kuten etäkäyttöliittymät, palomuurit ja reitittimet, VPN:t, automaatiolaitteet tai haavoittuvat protokollat, kuten telnet, RDP ja netBIOS. Löytöjen vakavuutta on vaikea arvioida ilman järjestelmiin tunkeutumista tai sen yrittämistä". (Tiilikainen, Manner, 2013, 9)

Tästä voidaan päätellä, että löydettyjen puutteiden ja aukkojen vakavuutta tai laajuutta ei voida arvioida, ennen kuin kaikki kohteet on haravoitu läpi ja niihin on yritetty tunkeutua, vaihtoehtoisesti joko hyökkääjien tai turvallisuusuhkien kartoittajien puolesta. Kuten tutkimuksessa on todettu, avoimen portin vakavuutta ei voi arvioida, ennen kuin siihen on yritetty tunkeutua. Tämä olisi jo turvallisuutta

silmällä pitäen hankala toteuttaa laajemmassa mittakaavassa, mutta yksittäisiä tunnistettavia kohteita kartoittaessa varsin tehokasta. Niin sanottu PEN-test, Penetration-test voisi paljastaa yksittäisen järjestelmän heikkoudet.

6.2 Oletusarvot turvallisuusaukkoina

Rakennusautomaatiolla voidaan helpottaa valvontaa ja kiinteistöjen ohjausta, Mutta kuten raportissa on todettu, on automaatiotekniikassa toistaiseksi eniten aukkoja. Rakennusautomaatioon sisältyy oviohjauksia, valaistuksia, hälytyksiä, ilmastointia ja lämmitystä. Shodan-ohjelmalla näitä löyty 2229 kappaletta. Valtaosa näistä oli kerrostaloja, toimistorakennuksia ja kauppakiinteistöjä. Suomessa on näitä aukkoja vielä muita pohjoismaita enemmän. (Tiilikainen & Manner, 2013, 11)

Todella heikkoja kohtia ovat järjestelmiin jääneet oletuskäyttäjätunnukset ja oletussalasanat, jotka on laitteiden omat oletusarvot. Nämä luovat erittäin ilmeisiä turvallisuusaukkoja. Näiden hyödyntäminen ei vaadi järjestelmään tunkeutuvalta paljoakaan koulutusta tai aikaa. Oletuskäyttäjätunnukset ja -salasanat pystyy etsimään internetistä nopeasti esimerkiksi laitevalmistajan ohjekirjoista heidän omilta internet-sivuiltaan. Etähallintakäyttöliittymät jäävät helposti avoimiksi, kun oletusarvoja ei osata muuttaa tai niitä ei muisteta vaihtaa.

Myös avoimeksi jääneet tietoliikenneportit tuottavat oman tietoturva-aukon. Kyse ei todellakaan ole mistään pienestä turva-aukosta tai mitättömästä riskistä. Pahimmassa tapauksessa laite, johon murtaudutaan, voi olla palomuuri tai jokin muu verkon rakenteelle kriittinen osa. Murtautuja voi saada oikeuksia verkkoon enemmän kuin voisi kuvitella pienellä ohjekirjan selailulla saavuttavan, ja siksi tämä on vaarallinen hyökkäys-muoto. Hyökkääjä saa suuren hyödyn käyttämäänsä aikaan nähden, minkä takia se on myös todella suosittua. Tällaisen hyökkäyksen automatisointi on myös todella helppo toteuttaa, mikä tekee siitä suhteessa vielä vaarallisemman. (Hakkerin käsikirja, 2002, 47)

Muita tutkimuksessa löydettyjä riskikohteita olivat voimalaitoksen ADSL-reititin, tuulimylly, lämpövoimala ja vedenkäsittelylaitos. Lisäksi vedenhuoltoyrityksestä löytynyt riski oli palomuurissa. Salasana oli tallennettuna web-käyttöliittymään. Näiden lisäksi listalla oli myös vankilan rakennusautomaation hallintajärjestelmä. Liikenteenohjausjärjestelmästä löytyi myös avoin Telnet-portti. Selvää on, että nämä ovat suhteessa paljon vakavampia riskejä kuin pelkkä internetsivuja ylläpitävälle palvelimelle murtautuminen.

Kaikilla yllä olevilla riskikohteilla on kuitenkin jotain yhteistä. Kaikissa näissä oli avoimia Telnet-portteja. Telnet on vanhentunut palvelu, missä tieto kulkee selvätekstinä. Salausta Telnet-tekniikassa ei ole. Salaamattomien salasanojen kaappaaminen on todella helppoa. Telnet-tekniikka tulisikin korvata suuren riskin kohteissa mahdollisimman nopeasti (Tiilikainen & Manner, 2013, 8).

6.3 Räätälöity täsmähyökkäys

Kun hyökkäyksessä tiedetään valmiiksi kohteen konekanta esimerkiksi Shodanin tyyppistä hakukonetta hyväksi käyttäen, voidaan hyökkäystä varten kehittää ”ohjelmisto” tai virus. Esimerkiksi ”Stuxnet-mato” ohjelmoitiin hyökkäämään nimenomaan Siemens Simatic S7 -järjestelmän kimppuun. Kyseinen järjestelmä on myös Suomessa paljon käytetty. Varsinaista vahinkoa mato ei onneksi onnistunut tekemään siinä mittakaavassa kuin olisi ollut mahdollista.

Stuxnet on kohtalaisen kuuluisa muutamastakin syystä. Hyökkäävää osapuolta ei tähänkään päivään mennessä tunneta varmasti. Toisena seikkana on kohteen korkea profiili. Kohteena oli iranilainen ydinvoimala. Stuxnet oli ohjelmoitu aiheuttamaan tuhoa ydinvoimalan sentrifugeissa (William, Markoff & Sanger, 2011).

Stuxnet oli myös siinä mielessä poikkeuksellinen hyökkäys, että se eteni muistitikulla. Järjestelmät olivat irrotettuja verkosta, joten suoran internetin hyökkäyksiltä järjestelmä oli kyllä turvassa. Virus pystyi elämään saastuneessa

koneessa ja raportoimaan takaisin palvelimelle, kun se saastutti koneen, joka oli yhteydessä internetiin (Chien 2010).

Mato oli räätälöity hyökkäämään sentrifugeja ohjanneen Siemensin logiikan kimppuun. Tarkoitus oli halvauttaa järjestelmä ohjaamalla sentrifugit toimimaan turva- ja toimintarajojen yli. Saastuneet tietokoneet ohjasivat suomalaisen Vaconin valmistamia taajuusmuuttajia pyörimään väärällä nopeudella. Stuxnet antoi pienen ajan sisään taajuusmuuttajille asetusarvoiksi 1410 Hz, siitä muutti nopeasti arvoon 2 Hz ja lopulta arvoon 1064 Hz. Ensin vika vaikutti rakenteelliselta, ennen kuin varsinainen ongelma edes selvisi. Pyörimisnopeuden nopeat muutokset aiheuttavat suuria vaihteluita niin laitteiston toimintaan kuin myös sähköverkkoon (Chien 2010).

6.4 Yrityksen muutokset turvallisuusaukkoina

Toinen huomattava tietoturvariski on vielä inhimillisempi, nimittäin muuttuva henkilöstö. Koko ajan muuttuva ihmisten ja tietokoneiden verkosto luo pitkällä ajalla väistämättä turva-aukkoja. Ilman selvää tietoturvaprotokollaa ei voida välttää ei-toivottuja tapahtumia. Ilman selkeää toimintaohjeistusta voi jo pelkkä järjestelmään luvatta kytketty USB-tikku olla suuri uhka (Kähkönen 2014, 29).

Isommat yritykset kärsivät myös organisaatiomuutoksista tietoturva-aukkoina. Esimerkiksi Espoo havahtui joulukuussa 2015, että heillä on yli 9000 leasing-sopimuksella olevaa pöytätietokonetta hukassa. Voisi kuvitella, että tällainen on periaatteessa mahdotonta. Tällaisen sotkun aikaansaamiseksi kuitenkin riittää jatkuvat organisaatiomuutokset ilman inventaariota tai selvitystyötä. Vahingot ovat usean miljoonan arvoiset. Espoolle tulee maksettavaksi lisäksi leasing-vuokria palauttamatta jätetyistä koneista. Koneiden mukana kadonnut informaatio on ollut mahdotonta kartoittaa, ja sen käyttö tai hyödyntäminen on näin ollen mahdotonta todentaa. (Laitinen 2015)

Vahingon suuruutta on mahdoton arvioida, koska koneista ei ole voitu pitää kirjaa. Vahinko kuitenkin osoittautui odotettua pienemmäksi, koska koneiden kirjanpito ja käytöstä poisto on ollut jatkuvasti laiminlyötynä. Poliisin esitutkinta uskoo todellisen laitemäärän olevan 2300–2900 laitetta. (Jokinen 2015)

Esimerkiksi yksi kannettava tietokone löytyi valtuuston puheenjohtajan omasta komerosta. Tehdyssä arviossa laitteiden suuren määrän aiheuttivat epäselvät turvamerkinnät, huono laitekirjanpito ja kahden kirjanpidon päällekkäisyys. Laitteiden valvonta oli ulkoistettu kahdelle osapuolelle. Alkuperäisen laitevahinkojen määrän oli arvioitu nousevan miljooniin euroihin. Todelliset vahingot kuitenkin osoittautuivat pienemmiksi. (Torvinen 2015)

Suuren organisaation yrityksillä on toinenkin yleinen ongelma. Kun työntekijöiden määrä on huomattava, on ulkopuolisten liikkumista hankalampi seurata. Kulunvalvonta ei ole mikään varma järjestelmä itsessään ulkopuolisia vastaan. Kulunvalvonta enemminkin tarkkailee järjestelmään kuuluvia henkilöitä kuin niitä, jotka eivät siihen kuulu. Se ainoastaan hankaloittaa ulkopuolisten etenemistä, etenkin jos he eivät tunne järjestelmää. Pitäisi myös olla selvää mitä tehdään tapauksessa, joka esitellään Tivin artikkelissa ”Tämä on tietomurto”. Ulkopuolinen urkkija levittää tässä esimerkissä tahallaan muistitikkuja, jotka on kyllästetty vakoiluohjelmilla.

Yrityksellä olisi hyvä olla selkeä tietoturvakäytäntö, jota on helppo soveltaa, vaikka kaikki tapaukset eivät välttämättä olisi täysin esimerkkien mukaisia. Ohjeissa olisi hyvä käydä ilmi ainakin mitä tehdään, kun vika ilmenee ja keneen otetaan hätätapauksissa yhteyttä. Toimintasuunnitelman olisi myös hyvä kattaa löydetyt USB-muistitikut tai käsitellä niille joku toimintaprotokolla. Normaalisti tällaiset löydökset pyydettäisiin palauttamaan tekniseen tukeen, jossa niiden kohtalosta päätetään. Myös tietoturvapaperit ja dokumenttien käsittely olisi hyvä käsitellä ohjeistuksissa. Hakkereille yleistynyt toimintamalli on niin sanottu ”dumpster diving”, roskien tonkiminen väärin hävitetyn aran materiaalin toivossa. Tätä tietoa on sitten helppo hyödyntää omiin tarkoituksiin. (Kähkönen 2014 26–31).

7 YHTEENVETO JA JOHTOPÄÄTÖKSET

Modbus-tekniikka on avoimen lähdekoodin esimerkillinen kannattaja. Tällä pystytään takaamaan, että kuka tahansa voi antaa kehitykseen oman työpanoksensa. Avoimen lähdekoodin lisensseihin yleensä kuuluu, että koodiin saa tehdä muutoksia ja parannuksia tahtonsa mukaan. Hyvää käytäntöä on tietenkin julkaista näitä tuloksia, mutta suuremmassa mittakaavassa ja yrityskentällä tätä ei välttämättä tehdä. Laitteiston kaikinpuolinen avoimuus kuitenkin avaisi uusia mielenkiintoisia rakenne- ja sovellusmahdollisuuksia.

Saatavilla olevan materiaalin alue on erittäin laaja ja yksityiskohtainen juuri avoimen pohjansa ansiosta. Modbus.org-sivustolla on käsitelty paljon viestien rakennetta, lähettämistä, laitteiston asentamista, rakennetta, ja materiaalia tulee lisää päivittäin yhteisön toimesta. Itse uskon, että Modbus-tekniikka kehittyy jatkossa paljon ja se tulee kestämään kauan juuri avoimuutensa ja kannattajakuntansa ansiosta. Tämä antaa myös Tekmen käyttämälle laitteistolle mahdollisuuden pitkään ikään.

Suomessa on muutamia pieniä räätälöityjä kenttäväyliä, joita ei käytetä kuin muutamalla tehtaalla. Näille laitteistoille ei saa koulutusta, tukea tai kehitysapua juuri mistään. Itse kannatan Modbus-pohjaisten kenttäväylien lisäämistä kiinteistöautomaatiossa, juurikin sen joustavuuden, toiminnallisuuden ja avoimuuden ansiosta.

Tutkielmaa voisi jatkokehittää erilaisten laitekokoonpanojen ja kenttälaitteiden kokeisiin, käyttöönottoihin ja keskenäiseen toimivuuteen. Väylään sopii Tekmen laitteiden kanssa keskustelevat yksiköt, näihin voisi aloittaa tehdä liitäntäkokeiluja ja käyttöönotto ratkaisuja.

Yksi alkuperäisistä tavoitteista oli pilvipalvelun käytön kartoitus. Tämä kuitenkin karsiutui aika alkuvaiheessa pois erittäin laajan sisällön takia. Pilvi on tulossa ja siltä ei voi välttyä millään tekniikan alalla. On kuitenkin ensin selvitettävä mitä pilvipalvelulta halutaan ja mihin sitä halutaan hyödyntää. Pilvi itsessään tarkoittaa

yleensä isoa laitekokoonpanoa, jonka rakenne on käytännössä niin monimutkainen piirtää, että se on helpompi summata pilven näköisen kuvan alle. Jossakin oli osuvasti verrattu sitä vanhoihin merikarttoihin, mihin on kirjoitettu ”here be dragons”, kun ei oltu varmoja mitä kyseisellä alueella on.

Pilvi voi nykyään käsittää vuokratun palvelimen, taikka ison määrän vuokrattuja koneita, jotka ovat verkostoituneita toisiinsa. Palvelu muoto, mistä alussa puhuimme muistuttaa jonkin verran palvelua, jonka Fidelix tarjoaa laitteistollaan tälläkin hetkellä.

Alkuperäiseen suunnitelmaan ei tietoturva osio kuulunut, mutta selvitystä tehdessäni annoin sille koko ajan lisää rivitilaa ja lopulta sovinkin, että mahdutan sen lopulliseen tekstiin hieman isommalla osiolla. Tekmellä on tulossa siirtyminen vanhasta puhelinkaapelitekniikasta langattomiin palveluihin ja muuttuneisiin yhteysmuotoihin. Samalla myös tietoturva nousee lisää esille.

Liikenneyhteyden muuttuessa myös pilvi tulee enemmän esille ja tälle varmasti kysyntä ja palvelut lisääntyvät. Modbus on myöskin erittäin kykenevä uudelle tiedonsiirto-mallille ja jopa todennäköisesti tulee helpottamaan sitä. Oma näkemykseni on, että kyseinen tekniikka voi nostaa Tekmen tasoa ja teknistä osaamista helposti muiden kilpailijoiden tasolle, ellei jopa siitä selvästi ohi valvomo tekniikkaansa.

LÄHTEET:

Chien, E. 2010 Stuxnet: A Breaktrought. Viitattu 12.7.2015
http://www.symantec.com/connect/blogs/stuxnet-breakthrough

Control solutions Minnesota www-sivut 2015. Viitattu 20.8.2015
http://www.csimn.com/

Fidelix I/O-moduulien käyttöohje 15.12.2003
http://www.fidelix.fi/documents/FI/modules_1_suomi.pdf

Fidelix.fi. 16-kanavainen digitaalinen sisääntulomoduuli. 2010.
http://www.fidelix.fi/documents/tuki/DI16_FI.pdf, 2

Fidelix.se. Product FX2030A. 2015.
http://media.fidelix.se/2015/10/products-FX2030A_big.png

Hakkerin käsikirja, 2002. IT Press. Viitattu 10.10.2015
https://samk.finna.fi/Record/tyrni.44754

Hämeen kansa. 1983.

Hämeen sanomat. 1983.

Humpry, M. Polynomial codes for error detection. Viitattu 18.2.2016
http://www.computing.dcu.ie/~humphrys/Notes/Networks/data.polynomial.html)

Janiza , know how - Comminication via the RS485 interface. Viitattu 20.2.2016
http://www.janitza.com/communication-via-the-rs485-interface.html

Jokinen, J. 2015. Poliisitutkinta päättyi – Espoon tuhansien kadonneiden tietokoneiden mysteeri johtui huolimattomuudesta. Viitattu 23.12.2015
http://www.hs.fi/kaupunki/a1450844721102

Kaario, K. 2002 TCP/IP. Jyväskylä: Docendo Finland Oy.
http://www.ellibs.com.lillukka.samk.fi/fi/book/951-846-107-4

Kähkönen, H. 2014. Tämä on tieto-murto. TIVI 6, 26–31.

Laitinen, J. 2015. Espoon kaupungilta katosi lähes 10 000 tietokonetta – poliisi epäilee törkeää kavallusta. Viitattu 12.9.2015
http://www.hs.fi/kaupunki/a1433209862567

Mir, N. 2006. Computer and Communication Networks. Prentice Hall. Viitattu 19.7.2015. http://flylib.com/books/en/2.959.1.33/1/

Modbus www-sivut 2015. Viitattu 21.8.2015 http://www.modbus.org/

Nakamura, T. n.d. Introduction to Fieldbus. Viitattu 20.7.2015
http://www.automation.com/pdf_articles/fieldbus.pdf

Piikkilä, V. 2006 Kiinteistöjen tiedonsiirtoväylät, ST-käsikirja 21, Sähkötieto ry.

ProSoft Technology. 2014. Understanding Modbus Serial and TCP/IP. Viitattu 24.7.2015 https://www.youtube.com/watch?v=k993tAFRLSE

Rantala, T. & Keronen, T. 2007. Kenttäväylien käytöstä sinkkitehdasprojektissa, Automaatioväylä 4, 12–15

Saarelainen, K. 1999. Lähiverkkojen tekniikka, Suomen ATK-kustannus Oy

Shodan www-sivu. Viitattu 21.3.2015. http://www.shodanhq.com

Specification and Implementation Guide V1.02. [2006]. Modbus. Viitattu 23.8.2015 http://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf

Taipale, T. 2016. henkilökohtainen kuvakokoelma.

Tiilikainen, S., Manner, J. 21.3.2013. Suomen automaatioverkkojen haavoittuvuus – Raportti Internetissä julkisesti esillä olevista automaatiolaitteista. Aalto-yliopisto. Viitattu 21.3.2015. https://research.comnet.aalto.fi/public/Aalto-Shodan-Raportti-julkinen.pdf

Torvinen, P. 2015. Espoon kadonneiden tietokoneiden mysteeri jatkuu: yksi kone löytyi valtuuston puheenjohtajan komerosta. Viitattu 20.9.2015 http://www.hs.fi/kaupunki/a1305961829986

William, B. Markoff, J. Sanger, D. 2011. Israeli Test on Worm Called Crucial in Iran Nuclear Delay. Viitattu 16.9.2015 http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html