TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoliikennetekniikka

OPINNÄYTETYÖ

TUNKEUTUMISENESTO JA HAVAINNOINTI KÄYTÖNVALVONTAJÄRJESTELMISSÄ

Työn tekijä: Jani Ekman
Työn ohjaaja: Marko Uusitalo
Työn ohjaaja: Olli Oravainen

Työ hyväksytty: __. __. 2009

Marko Uusitalo
lehtori

Metropolia

ALKULAUSE

Tämä opinnäytetyö tehtiin Helsingin Energian ICT-palveluille. Haluan kiittää kaikkia työssä mukana olleita sekä työnohjausta.

Helsingissä 7.5.2009

Jani Ekman

Metropolia

OPINNÄYTETYÖN TIIVISTELMÄ

Työn tekijä: Jani Ekman	
Työn nimi: Tunkeutumisenesto ja havainnointi käytönvalvontajärjestelmissä	
Päivämäärä: 7.5.2009	**Sivumäärä:** 52 s.
Koulutusohjelma: Tietotekniikka	**Ammatillinen suuntautuminen:** Tietoliikennetekniikka
Työn ohjaaja: lehtori Marko Uusitalo **Työn ohjaaja:** tietoliikennepäällikkö Olli Oravainen	

Tässä insinöörityössä tutkittiin tunkeutumisenesto- ja havainnointijärjestelmien soveltuvuutta nykyaikaisiin käytönvalvontajärjestelmiin. Työ tehtiin Helsingin Energialle, joka on merkittävä energiapalveluita tarjoava yritys Suomessa.

Työssä perehdyttiin ensin teoreettisella tasolla käytönvalvontajärjestelmien arkkitehtuuriin, komponentteihin ja tietoturvavaatimuksiin. Lisäksi tutustuttiin yleisimpiin käytössä oleviin käytönvalvontaprotokolliin ja niiden rakenteisiin. Tämän jälkeen työssä selvitettiin tunkeutumisenesto- ja havainnointitekniikoiden toimintaa sekä suunnittelun perusteita.

Tämä insinöörityö tuotti myös käytönvalvontajärjestelmiin suunnitellun tunkeutumisenesto- ja havainnointijärjestelmän vaatimusmäärittelyn ja toteutussuunnitelman.

Työn tuloksena todettiin tunkeutumisenesto- ja havainnointijärjestelmien protokollakuvauksien tarjonnan olevan niukkaa Pohjoismaissa käytetyille käytönvalvontaprotokollille. Lisäksi kuvausten käyttöönottoon tulee suhtautua varauksella järjestelmien kriittisyyden vuoksi. IDPS-järjestelmien todettiin kuitenkin nostavan käytönvalvontajärjestelmien tietoturvatasoa muilla ominaisuuksillaan. Työssä painotettiin lisäksi tunkeutumisenesto- ja havainnointijärjestelmän integroinnin tärkeyttä ylläpito- ja hallintaprosesseihin, sekä elinkaaresta huolehtimista.

Avainsanat: IPS, tunkeutumisenesto, prosessitietoliikenne, SCADA

Metropolia

ABSTRACT

Name: Jani Ekman

Title: Intrusion Prevention and Detection in SCADA Networks

Date: 7 May 2009 **Number of pages:** 52

Department: Information Technology

Study Programme: Telecommunications

Instructor: Marko Uusitalo, Senior lecturer

Supervisor: Olli Oravainen, Data Communications Manager

The purpose of this study was to research possibilities for implementing intrusion prevention and detection systems into modern SCADA networks. This study was carried out for Helsinki Energy, a significant energy service provider in Finland.

The first part discusses the architecture of SCADA networks, its components and data security requirements on a theoretical level, as well as the most common SCADA protocols and structures. The second part studies the function of intrusion prevention and detection and the basis for its design.

This study also defined the requirements as well as laid out an implementation plan for intrusion prevention and detection in SCADA networks.

The results of this study show that the supply of intrusion prevention and detection protocol filters is insufficient for SCADA networks used in the Nordic countries. Furthermore, the implementation of protocol filters must be viewed critically. Nevertheless, the IDPS systems still seem to raise the data security level of SCADA networks. It was concluded that the integration of intrusion prevention and detection into maintenance and management practice is as important as the lifecycle.

This study was successful in defining the requirements as well as in creating an implementation plan for intrusion prevention and detection in SCADA networks.

Keywords: IPS, Intrusion Prevention, Process Data Communication, SCADA

SISÄLLYS

LYHENTEITÄ JA MÄÄRITELMIÄ

ASCII	*American Standard Code for Information Interchange.* Tietokoneille kehitetty merkistöjärjestelmä.
ASDU	*Application Service Data Unit.* Käytönvalvontaprotokollan sovellustason PDU-kehys.
CD/DVD	*Compact Disc/Digital Versatile Disc.* Ulkoinen massamuisti, jota voidaan lukea siihen soveltuvalla laitteella.
CERT-FI	Viestintäviraston tieturvahaavoittuvuuksien julkaisusta vastaava yksikkö.
CLI	*Command Line Interface.* Merkkipohjainen hallintakonsoliliittymä.
CRC	*Cyclic Redundancy Check.* Virheentarkistusmekanismi verkkoprotokollassa.
DLP	*Data Loss Prevention.* Tietoturvatekniikka, jonka avulla estetään tiedon karkaaminen yrityksestä.
DMZ	*Demilitarized Zone.* Ei kenenkään alue tietoverkoissa. Verkkoalueeseen sijoitetaan verkko- ja www-palveluita. Ei sijaitse yrityksen sisäverkossa, eikä suoraan internetissä.
DNP3	*Distributed Network Protocol 3.* Käytönvalvontajärjestelmissä käytetty protokolla.
DoS	*Denial of Service.* Palvelunestohyökkäys tekniikka, jonka avulla pyritään lamaannuttamaan jokin palvelu.
EIA	*Electronics Industries Alliance.* Yhdysvaltain energiaviraston alaisuudessa toimiva organisaatio.
ELCOM-90	*Electricity Utilities Communication 90.* Norjalaisen Sintef-organisaation kehittämä käytönvalvontajärjestelmien protokolla.
Extranet	Yrityksen tarjoama verkkopalvelu asiakkaille ja kumppaneille.

FEP	*Front End Processor.* Päätepalvelin, jonka kanssa käytönvalvontajärjestelmien kenttälaitteet kommunikoivat.
GOOSE	*Generic Object Oriented Substation Event.* Käytönvalvontajärjestelmissä käytetyn IEC 61850 –protokollan sanomatyyppi.
GPRS	*General Packet Radio Service.* Matkapuhelinverkossa käytettävä tiedonsiirtotekniikka.
HMI	*Human-Machine Interface.* Käytönvalvontajärjestelmien operointikäyttöliittymien yleisnimitys.
HTTP	*Hypertext Transfer Protocol.* Verkkoprotokolla Internet-sivustojen ja asiakasselainten väliseen kommunikointiin.
HTTPS	*Hypertext Transfer Protocol over Secure Socket Layer.* Suojattu verkkoprotokolla Internet-sivustojen ja asiakasselainten väliseen kommunikointiin.
ICCP	*Inter-Control Center Communications Protocol.* Käytönvalvontajärjestelmien väliseen liikennöintiin tarkoitettu protokolla.
ICMP	*Internet Control Message Protocol.* Ongelmanselvitys- ja testausprotokolla tietoverkoissa.
IDPS	*Intrusion Detection and Prevention System.* Tunkeutumisenesto- ja havainnointijärjestelmän yleisnimitys.
IDS	*Intrusion Detection System.* Tunkeutumisenhavainnointijärjestelmä.
IEC101	Sarjaliikenteinen käytönvalvontaprotokolla.
IEC104	Nykyaikaisissa IP-verkoissa käytetty käytönvalvontaprotokolla.
IEC	*International Electrotechnical Commission.* Kansainvälinen standardointiorganisaatio.
IED	*Intelligent Electronic Device.* Älykäs kenttälaite, joita käytetään SCADA-järjestelmissä.
IP	*Internet Protocol.* Internetissä käytetty osoiteformaatti.

IPS	*Intrusion Prevention System*. Reaktiivinen tunkeutumisenesto-järjestelmä.
IPSec	*Internet Protocol Security.* Kokoelma protokollia joiden avulla suojataan verkkoliikennöintiä verkkotasolla.
ITIL	*Information Technology Infrastructure Library.* Viitekehys tietoteknisten palveluiden tuottamiselle.
ITU-T	*International Telecommunications Union.* Tietoliikennesektorin standardeja koordinoima järjestö.
LAN	*Local Area Network.* Paikallinen tietokoneverkko työasemien ja palvelimien väliselle kommunikoinnille.
LRC	*Longitudinal Redundancy Check Character.* Virheentarkistustekniikka verkkokehyksissä.
MMS	*Manufacturing Message Specification.* Kansainvälinen standardi käytönvalvontajärjestelmien reaaliaikaiseen sanomien välitykseen.
MS-Blaster	Microsoftin haavoittuvuutta hyödyntävä verkkomato.
NBA	*Network Behavior Analyses.* Verkon käyttäytymiseen perustuva analysointimekanismi.
NERC	*North American Electric Reliability Council.* Amerikkalainen järjestö, jonka tehtävä on huolehtia sähkönsiirron luotettavuudesta.
OSI	*Open Systems Interconnection.* Seitsemän kerroksinen viitekehys ohjelmistojen ja tietoliikennelaitteiden kommunikointiin.
PDU	*Protocol Data Unit.* OSI-mallin kerrosten välillä siirtyvien kehyksien nimitys.
PKI	*Public Key Infrastructure.* Julkisen avaimen järjestelmä, jossa epäsymmetristä salausta käyttäen tieto suojataan avoimissa verkoissa.

PLC	*Programmable Logic Controller.* Ohjelmoitava logiikkapiiri, joka on erityisesti suunniteltu teollisuuden käyttötarpeisiin.
RTU	*Remote Terminal Unit.* Nimitys käytönvalvontajärjestelmien ala-asemalle.
SCADA	*Supervisory Control and Data Acquisition*. Käytönvalvontajärjestelmä.
SINTEF	*Stiftelsen for Industriell og Teknisk Forskning.* Norjan tieteellinen tutkimuslaitos, vastine Suomen VTT:lle.
SNMPv3	*Simple Network Management Protocol versio 3.* Verkonvalvonta- ja ylläpitoprotokolla.
SSH	*Secure Shell.* Suojattu verkkoprotokolla, jonka avulla voidaan ottaa yhteyksiä kohdejärjestelmään.
SSL	*Secure Sockets Layer.* Kryptograafinen protokolla, joka tarjoaa turvallisen kommunikoinnin tietoliikenneverkoissa.
SSO	*Single Sing On.* Kertakirjautuminen.
TASE2	Käytönvalvontajärjestelmien käyttämä protokolla.
TC57	*Technical Committee 57.* IEC-järjestön tekninen komitea 57.
TCP	*Transmission Control Protocol.* Kuljetuskerroksen siirtoprotokolla.
TCP/IP	*Transmission Control Protocol / Internet Protocol.* Internet-pohjaiseen tiedonsiirtoon kehitetty protokollaperhe.
TLS	*Transport Layer Security.* SSL-protokollan tyyppinen salaus- ja todennusprotokolla.
UART	*Universal Asynchronous Receiver/Transmitter.* Asynkroninen lähetys- ja vastaanottolaite.
UCA	*Utility Communications Architecture.* Käytönvalvontajärjestelmien käyttämä liikennöintiprotokolla.

UDP	*User Datagram Protocol.* Kuljetuskerroksen tiedonsiirtoprotokolla.
USB	*Universal Serial Bus.* Ulkoinen väylästandardi esimerkiksi massamuistien liittämiseen.
VPN	*Virtual Private Network.* Etäyhteystekniikasta käytetty nimitys.
WAN	*Wide Area Network.* Etäverkko.
WiFi	*Wireless Fidelity.* Tuotemerkki langattomalle teknologialle.
WiMAX	*Worldwide Interoperability for Microwave Access.* Pitkän kantaman langaton tekniikka.
WLAN	*Wireless Local Area Network.* Yleisnimitys langattomalle lähiverkolle.
X.25	ITU-T:n standardoima verkkokerroksen protokolla pakettikytkentäisten WAN-verkkojen kommunikointiin.

1 JOHDANTO

Nykypäivänä tietoverkot ovat kasvaneet räjähdysmäisesti. Tavalliset kotikäyttäjät hyödyntävät Internet-palveluita kuten yrityksetkin. Esimerkiksi VPN (Virtual Private Network) -yhteydet ovat lähes jokaisen työntekijän saatavilla, ja yhteydet yrityksen tietoverkkoon on oltava muodostettavissa päätelaitteesta ja sijainnista riippumatta. Verkottuminen näkyy myös teollisuusautomaatioverkkojen kehityksessä. Tekniset ratkaisut pohjautuvat standardeihin malleihin, kun taas aikaisemmin laitevalmistajat rakensivat omia protokollia ja järjestelmiä. Nykyisin infrastruktuuria ylläpitävät tietoverkot toimivat kuten muutkin yritysverkot. Tietoa on kyettävä jakamaan eri käyttäjien ja järjestelmien välillä saumattomasti, eikä niin sanottuja suljettuja verkkoja enää ole.

Markkinoilla on tätä nykyä tarjolla lukuisia uusia teknologioita, jotka tarjoavat suojaa yritysten verkoille. Tunkeutumisen havainnointijärjestelmät ovat jalostuneet estojärjestelmiksi, joiden reaktiivinen toiminta mahdollistaa entistä tehokkaamman suojautumisen tietoturvauhilta. Monet laitevalmistajat ovat laajentaneet segmenttiään. Tunkeutumisenesto- ja havainnointilaitteisiin on lisätty käytönvalvontajärjestelmissä käytettyjen kommunikointiprotokollien protokollakuvauksia. Näillä kuvauksilla pyritään todentamaan protokollan normaalitoimintaa ja estämään protokollien kautta tapahtuvat tietomurrot. Tunkeutumisenesto- ja havainnointijärjestelmät voivat nostaa merkittävästi käytönvalvontajärjestelmien tietoturvatasoa, joten niiden tuomia hyötyjä ja haittoja tulee tutkia.

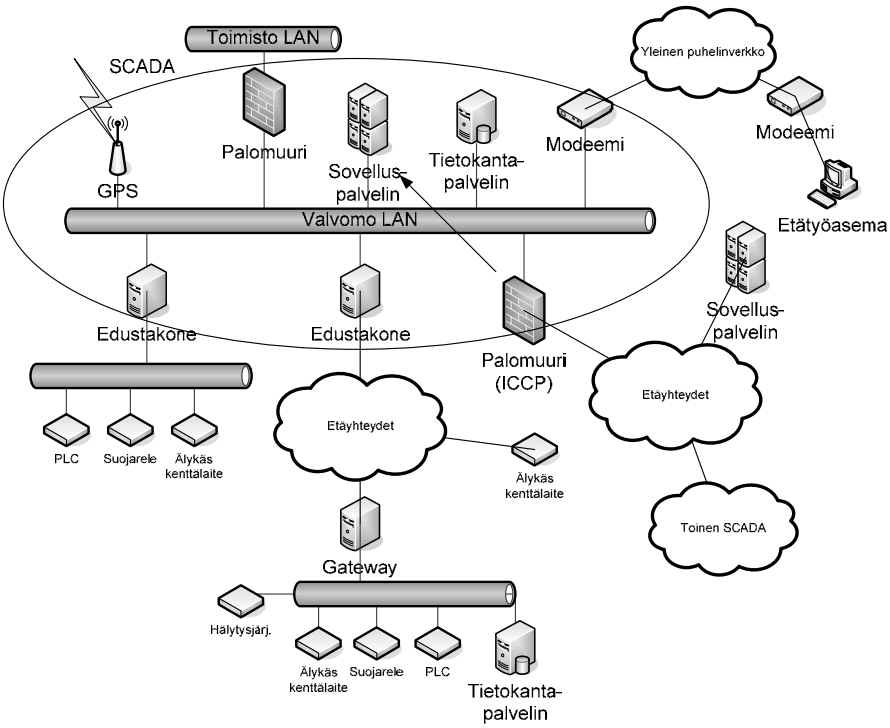
Työn tavoitteena on tutkia teoreettisella tasolla markkinoilla olevien tunkeutumisenesto- ja havainnointijärjestelmien soveltuvuutta nykyaikaisiin käytönvalvontajärjestelmiin. Työssä keskitytään erityisesti siihen, kuinka eri valmistajien tunkeutumisenesto- ja havainnointilaitteet tukevat käytönvalvontajärjestelmissä käytettyjä protokollia. Lisäksi tarkastellaan IDPS (Intrusion Detection and Prevention Systems) -järjestelmäominaisuuksien tuomaa lisäarvoa SCADA (Supervisory Control and Data Acquisation) -verkoille. Työssä määritellään myös yleiset vaatimukset käytönvalvontaympäristön tunkeutumisenesto- ja havainnointilaitteille. Lopputuloksena saadaan vaatimusmäärittely sekä suunnitelma tunkeutumisenesto- ja havainnointijärjestelmän toteutuksesta, ja sen soveltuvuudesta SCADA-verkkojen tietoturvakomponentiksi.

2 KÄYTÖNVALVONTAJÄRJESTELMÄT

Käytönvalvontajärjestelmä on infrastruktuuria ylläpitävä suurempi kokonaisuus, jolla valvotaan, ohjataan ja kerätään tietoa prosessista. Nykypäivänä enemmän käytetty termi on SCADA (Supervisory Control and Data Acquisition). Käytönvalvontajärjestelmiä käytetään energianjakeluverkoissa, kaasu-, vesi- ja jätevesijärjestelmissä sekä muissa teollisuus- ja tuotantoverkoissa. Pienempiä järjestelmiä on paikallisissa kohteissa kuten energianjakeluverkon sähköasemilla ym. paikallisilla ala-asemilla. Näissä kohteissa valvotaan ja ylläpidetään paikallista automaatiota tai prosessia. Ala-asemat, käyttökeskukset ym. laitteet liittyvät tietoverkon kautta varsinaiseen käytönvalvontajärjestelmään, ja näin muodostavat laajemman kokonaisuuden.

Käytönvalvontajärjestelmät koostuvat useista erilaisista komponenteista. Valvomopään ratkaisut koostuvatkin yleensä monista nykyaikaisista palvelimista ja työasemista. Valvomot voidaan hajauttaa palveluineen useisiin eri sijainteihin, jolloin myös vikatapauksissa saatavuus paranee. Valvomo-ohjelmistojen käyttöliittymistä käytetään HMI (Human Machine Interface) -yleisnimikettä. Perusohjelmistot ovat nykyisin täysin graafisia, ja näiden lisäksi on myös erikoissovelluksia ja työkaluja, jotka voivat sisältää ainoastaan tietyn sovellusalueen, esim. sähkö- tai kaukolämpöverkon kuvat. Tietokannat ovat merkittävässä roolissa SCADA-verkoissa. Näissä sijaitsee kaikki oleellinen historia- ja mittaustieto järjestelmästä. Käyttökeskuksessa tietojen saatavuus on varmistettava.

Käytönvalvontajärjestelmän periaatteellinen verkko- ja laitearkkitehtuuri on esitetty kuvassa 1.



Kuva 1. SCADA-järjestelmäarkkitehtuuri [lähdettä 1, s. 55 mukaillen]

Liikennöiviä protokollia vanhoissa järjestelmissä voi olla lukuisia, kun taas nykyisin pyritään käyttämään standardeja liikennöintimalleja. Standardimallien avulla voidaan operoida monilaitevalmistajaympäristöissä. Verkkojen monimutkaisuus lisää myös tietoturvauhkia verkossa. Tietoturvaratkaisut edellyttävät yhä enemmän suunnittelua ja toteutukset muuttuvat haasteellisimmiksi. Infrastruktuuria ylläpitävän järjestelmän toiminta tulee taata myös poikkeustilanteissa.

2.1 Vaatimuksia käytönvalvontajärjestelmän tietoturvalle

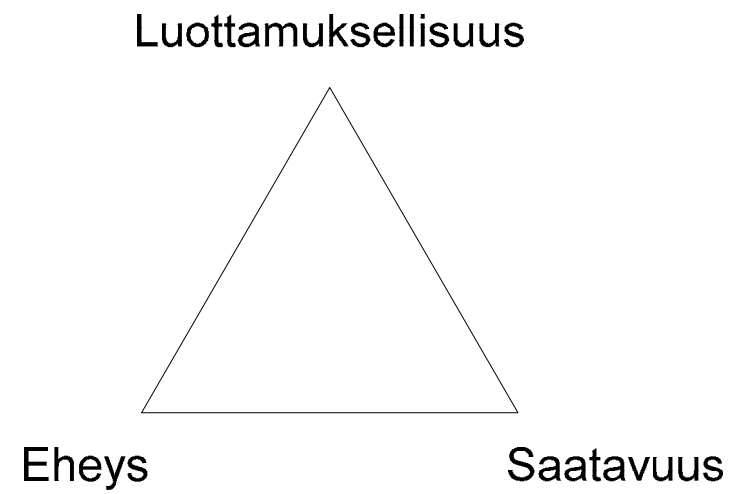
Teollisuusyritysten tuotanto-, valvonta- ym. järjestelmät toteutetaan liiketoimintojen tarpeisiin. Riskienhallinta yleensä kohdistetaankin tulovirtojen varmistamiseen, tulevaisuuden palveluiden ja tuotteiden kehittämiseen sekä omaisuuden suojaamiseen. Tietoriskien näkökulmasta tilanne on hieman toinen. Tietoturva koetaan yleensä rasitteeksi, ellei sitä ymmärretä oikein. Käytönvalvontajärjestelmissä, kuten muissakin teollisuusjärjestelmissä, on pyrittävä löytämään yhteisymmärrys käytettävyyden, tarpeiden ja tietoturvan välillä [1, s. 30].

Järjestelmien on kyettävä tarjoamaan informaatiota myös prosessin ulkopuolelle. Teollisuusverkot eivät ole nykyisin ns. suljettuja, vaan tiedon pitää olla saatavissa eri järjestelmien ja käyttäjien kesken, vuorokauden ympäri. Käytönvalvontajärjestelmien tietoliikenneyhteydet ulottuvat usein myös yrityksen rajojen ulkopuolelle. On tarjottava etäyhteydet laitetoimittajille ja omalle henkilöstölle. Verkkokapasiteettia saatetaan ostaa kolmansilta osapuolilta, ja jotkut yhteyksistä saattavat olla jopa langattomia. Nämä asettavat omat haasteensa tietoverkon toteutukselle, arkkitehtuurille ja tietoturvalle.

NERC (North American Electric Reliability Council) on laatinut ohjeellisia suosituksia sähkölaitosympäristöjen SCADA-verkkojen tietoturvan toteutukselle. Dokumentit ovat kattava kokonaisuus monesta turvallisuuden osa-alueesta. NERC-tiedostot sisältävät mm. seuraavat osa-alueet:

- Kriittisen tietopääoman tunnistaminen
- Turvallisuuden hallintatoimet
- Henkilöstö ja koulutus
- Tieto-pääoman suojaus
- Kriittisen tieto-pääoman fyysinen turvallisuus
- Järjestelmän turvallisuuden hallinta
- Loukkauksien ja tapahtumien raportointi sekä niihin reagointi
- Toipumissuunnitelmat.

Tietoverkkojen tietoturva voidaan kiteyttää kolmeen pääalueeseen, jotka muodostavat ns. tietoturvakolmion. Kuvassa 2 on esitetty tietoturvakolmion tavoitteet, joita tulee soveltaa myös käytönvalvontajärjestelmissä.



Kuva 2. Tietoturvakolmio [lähdettä 1, s. 28 mukaillen]

Tiedon on oltava saatavilla kun sitä tarvitaan, jolloin järjestelmän häiriöajat on minimoitava. Luottamuksellisuudella tarkoitetaan sitä, että tietoon pääsevät käsiksi vain sellaiset henkilöt ja tahot, joilla on siihen oikeus. Salasanapolitiikka ja pääsynhallinta ovat tässä keskeisessä roolissa. Lisäksi on huolehdittava tiedon oikeellisuudesta, eli eheydestä. [1, s. 28; 3, s. 445.]

Käyttökeskusvaatimukset

Valvomotiloissa pääkäyttäjät työskentelevät vuorokauden ympäri, ja käytettävyys- ja viihtyvyystekijöihin on kiinnitettävä erityisesti huomiota. Käyttökeskuksissa on käytössä useita erilaisia järjestelmiä, joihin pääsy saattaa olla usean käyttäjätunnuksen takana. Näihin järjestelmiin tulisi kuitenkin kirjautua ns. SSO (Single Sign-On) -tyyppisesti, jolloin kirjautuminen tehdään vain kerran. Kertakirjautumisen jälkeen kaikkien järjestelmien tiedot olisivat saatavilla, eikä jatkokirjautumisia tarvita. Yhden valvontatyöaseman tai muun laitteen rikkoutuminen ei saa vaikuttaa palvelun saatavuuteen, ja mahdolliset varalaitteet tulee olla nopeasti saatavilla.

Ala-aseman vaatimukset

Tietoliikenneyhteyksien tulee olla ala-asemilla vikasietoiset, riippuen tietysti aseman koosta ja funktiosta. Ala-asemat jakaantuvat maantieteellisesti laajalle alueelle, jolloin voidaan joutua vuokraamaan yhteyksiä kolmansilta osapuolilta. Ala-asemien kaukokäyttöyhteyksissä tulee käyttää suojausta. Tässä tapauksessa suojauksella tarkoitetaan liikenteen salaamista. Salauksella voidaan varmistaa tiedon eheys. Vanhat, puhelinverkon kautta etäkäytettä-

vät ala-asemayhteydet on syytä poistaa, ja siirtyä käyttämään moderneja VPN-etäyhteyksiä.

Ala-asemilla on yleensä paikallisohjauspiste, jolla voidaan ohjata paikallista automaatiota huolto- ym. töissä. Nämä työasema- tai palvelinmalliset koneet ovat hyvin usein Windows-käyttöjärjestelmällä varustettuja, ja laitetoimittajat harvoin suosittelevat virusohjelmien tai käyttöjärjestelmäpäivitysten lataamista. Paikallisohjauspisteiden päivityksistä on kuitenkin huolehdittava, jotta voidaan taata palvelun jatkuvuus. Mikäli päivityksiä ajetaan paikallisohjauspisteille, tulee sen olla jatkuvaa ja suunnitelmallista, mikä taas vaatii taakseen organisaation.

Tietoverkkovaatimukset

Käytönvalvontajärjestelmissä tietoverkon on oltava saatavissa vuorokauden jokaisena hetkenä. Verkon on pystyttävä tarjoamaan palveluita kaikille verkon komponenteille luotettavasti. Järjestelmissä kaistanleveyttä ei niinkään tarvita, vaan oleellista on viiveen minimointi ja yhteyksien luotettavuus. Käytönvalvontajärjestelmissä on syytä segmentoida verkon eri osat ja rajoittaa liikennettä näiden välillä palomuurilla.

Käytönvalvontajärjestelmien laitetoimittajia on monia. Haasteellista on saada sovitettua kaikki järjestelmän osat yhteen turvallisesti ja toimintavarmasti. Varsinaisen käyttökeskuksen ja sen komponentit toimittaa yleensä yksi laitevalmistaja. Ala-asemat voidaan vastaavasti toteuttaa taas toisen laitevalmistajan komponenteilla. Tämä voi aiheuttaa tiettyjä komplikaatioita toteutuksessa. Standardiprotokollien käytön ansiosta on mahdollista liikennöidä eri laitevalmistajien laitteiden välillä, jolloin järjestelmien yhteensovittaminen helpottuu.

Tietoverkon on mahdollistettava turvallinen etäkäyttö mm. ala-asemille. Etäkäyttöön soveltuvaa tekniikkaa on nykypäivänä tarjolla, toteutusmalleja on lukuisia. Skaalautuvaa käyttäjätietokantaa ei yleensä ole, vaan jokaiseen järjestelmään kirjaudutaan paikallisilla tunnuksilla. Keskitetyllä käyttäjätietokannalla saavutetaan etuja järjestelmän ylläpidossa ja hallinnassa. Käyttäjätunnukset hallitaan yhdestä paikasta ja käyttäjäpoliittiset määritykset voidaan tehdä suoraan yhdellä ylläpito-ohjelmalla. Tietokantojen ym. ohjelmistojen varmuuskopiointimahdollisuus tulee varmistaa. Tämän lisäksi tiedot tulee varastoida tietyn ajanjakson ajan.

2.1.1 Käytönvalvontajärjestelmiin kohdistuvat tietoturvauhat

Tietoturvassa kokonaistietoturva voidaan ajatella koostuvan ketjusta, jossa jokainen lenkki kuvaa yhtä tietoturva-aluetta. Hyökkääjän tarvitsee kohdistaa hyökkäyksensä ainoastaan yhteen lenkkiin ja murtaa se, jolloin tietomurto on jo saavutettu. Pienenkin tietomurron vuotaminen julkisuuteen voi haitata merkittävästi yrityksen imagoa, etenkin infrastruktuuria ylläpitävissä yrityksissä. Tietomurron tai -hyökkäyksen takana on aina, suoraan tai epäsuorasti, ihminen tai joukko ihmisiä. Koska tietomurtojen tai hyökkäyksien takana on aina ihminen, voi uhka muodostua myös yrityksen sisältä, joko tahallisesti tai tahattomasti. Viallisen asennustiedoston lataaminen ala-aseman IED (Intelligent Electronic Device) -laitteelle voi aiheuttaa palvelun keskeytymisen. Samoin irtisanomistilanteissa tulee noudattaa tarkkaavaisuutta, ja huolehtia henkilön pois lähtemisestä ilman järjestelmän väärinkäyttömahdollisuutta.

Yleensä tunkeutuminen käytännössä tapahtuu siten, että hyökkääjä tutkii yrityksen verkkoa ja palveluita ulkopuolelta, verkkotiedustelun avulla. Tiedustelu voidaan kohdentaa myös erilaisiin modeemiyhteyksiin, joita esimerkiksi pohjoismaissa on vielä tänäkin päivänä monia. Näin yritetään löytää haavoittuvuuksia palvelimista, jotka sijaitsevat yrityksen ekstranet ja DMZ (Demilitarized Zone) -vyöhykkeillä, tai muilla haavoittuvilla alueilla. Heikkouden löydyttyä suoritetaan tunkeutuminen palvelimelle käyttäen hyväksi löydettyä ohjelmisto- tai käyttöjärjestelmähaavoittuvuutta. Tämän jälkeen hyökkääjä lataa tarvittavat työkalut palvelimelle ja kohdistaa hyökkäyksen eteenpäin [1 s. 59].

Järjestelmään tunkeutuminen

Järjestelmään tunkeutuminen voi tapahtua fyysisesti esim. laitetilasta tai tietoverkon kautta etäkäyttöisesti, kuten aikaisemmin on todettu. Yleensä heikot salasanapolitiikat ja ulkoiset tietoliikenneyhteydet aiheuttavat eniten uhkia. Ikääntyneet modeemiyhteydet tulisi poistaa ja korvata ne VPN (Virtual Private Network) -tekniikalla [1, s. 18 - 19].

Käytönvalvontajärjestelmän tietoverkon heikkouksia ja haavoittuvuuksia ovat mm. :

- Kaukovalvonta- ja mittausten etälukuverkot
- Järjestelmien etäkäyttö ml. järjestelmätoimittajien etäyhteydet
- Erilaiset modeemiyhteydet, erityisesti ne jotka ovat liitettynä yleiseen puhelinverkkoon
- Internet- ja intranet -yhteydet
- Järjestelmän huolimaton käyttö
- Palvelunestohyökkäykset.

Nykyaikaisissa ala-asemaratkaisuissa saatetaan käyttää kustannustehokkaita, langattomia tekniikoita kuten WLAN, GPRS ja WiMAX. Palveluntarjoajien ratkaisuihin tulisi tutustua ja löytää turvallinen kokonaiskonsepti yrityksen etujen mukaisesti.

Haittaohjelmat

Haittaohjelmilla suoritetut hyökkäykset voidaan jakaa karkeasti kolmeen eri ryhmään: virukset, troijan-hevoset ja roskaposti. Näihin ryhmiin kuuluu myös alijoukkoja, joita ovat tietokonemadot, takaportit sekä loogiset pommit. Haitallisilla ohjelmatyökaluilla suoritetut hyökkäykset ovat yleensä palvelunestohyökkäyksiä. Myös muunlaiset hyökkäykset ovat mahdollisia, sekä hyvinkin yleisiä. Haittaohjelma leviää kriittiseen verkkoon usein Internet-selaimen avulla. Ohjelmistoja ei päivitetä aktiivisesti ja Internet-selainyhteyksiä on mahdollisuus käyttää pääkäyttäjän oikeuksin. Tällöin työasema on erittäin haavoittuva. Näistä koituvat haittavaikutukset voivat olla merkittäviä, mm. erilaisten viruksien aiheuttamat tuhot tuotantolaitoksissa ovat olleet hyvinkin mittavia [1, s. 19 - 21].

Merkittävänä uhkana ovat erilaiset siirrettävät mediat, kuten USB-muistitikut ja CD/DVD-levyt. Paikallisohjauspisteille uudet konfiguraatiot ja päivitykset ladataankin lähes poikkeuksitta näiden medioiden avulla. Kannettavan median mukana virus pääsee leviämään järjestelmään hyvin helposti.

Yhdysvalloissa vuonna 2003 ydinvoimalaan tunkeutunut MS-Blaster -mato esti ohjaajien tukijärjestelmän toiminnan noin neljäksi tunniksi, ja prosessitietokoneen toiminnan noin seitsemäksi tunniksi. Mato levisi järjestelmään yhteistyökumppanin tietoverkosta [1, s. 146].

Puskuriylivuodot

Puskurivuoto on ohjelmassa oleva virhe, jonka avulla hyökkääjä pääsee syöttämään haluttua ohjelmakoodia järjestelmään, tai mahdollisesti kaappaamaan koko järjestelmän käyttöönsä. Näin voidaan ohittaa kaikki perinteiset suojausmekanismit kohdekoneessa. Puskuriylivuodolla voidaan aiheuttaa myös palvelunestohyökkäyksiä erilaisiin sovelluksiin.

Viestintäministeriön CERT-FI -ryhmän julkaisemia haavoittuvuuksia vuonna 2008 oli syyskuuhun mennessä 114 kappaletta. Näistä lähes kaikki koskivat erilaisia sovelluksia tai käyttöjärjestelmiä [2].

2.1.2 Suojautuminen tietomurroilta ja hyökkäyksiltä

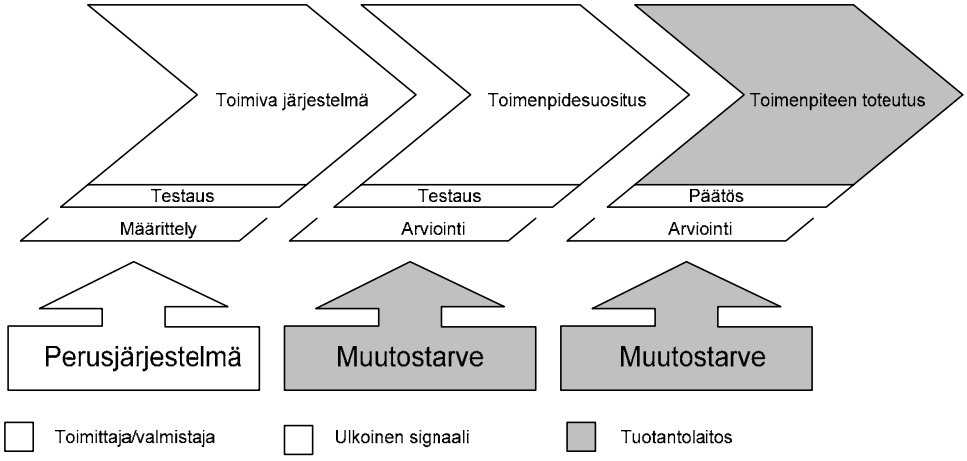
Tietoturvauhkia on monia erilaisia. Niiltä suojautuminen vaatii suunnittelua, aikaa ja tekniikkaa. Tietoturvakolmion tavoitteet mielessä pitäen voidaan parantaa huomattavasti järjestelmien tietoturvatasoa. Hyvin suunniteltu tietoturvapolitiikka, yhdessä teknisten tietoturvaratkaisujen kanssa, auttaa yritystä selviämään nykypäivän haasteista. Kuitenkin perusajatus on, että jokainen työntekijä huolehtii tietoturvasta ja sen toteuttamisesta omalla henkilökohtaisella panoksellaan. Siksi työntekijät tulee kouluttaa jo töihin tullessa toimimaan yrityksen säännösten mukaisesti. Useissa yrityksissä järjestetäänkin jo tämän tyyppisiä koulutuksia, ja mm. sisäasiainministeriön henkilöstön on mahdollista suorittaa sisäinen tietoturvadiplomi. Vastaavaa perehdyttämistä tulisi suosia muissakin organisaatioissa.

Tietoturvauhat voivat kohdistua järjestelmään monesta suunnasta, myös sisältä ns. omasta verkosta. Tämän takia yritysten tulee suorittaa riskianalyysi mahdollisten tietomurtojen varalta, selvittää infrastruktuurin heikkoudet ja pisteyttää ne kriittisyyden mukaan, jolloin saadaan selville ne kehityskohteet joihin tulee panostaa ensimmäisenä. Yhdessä analyysien ja säännöllisten tietoturva-auditointien kanssa käytönvalvontajärjestelmät pysyvät ajanmukaisina. Järjestelmäkomponenttien päivitys on jatkuva prosessi johon tulee vastuuttaa tietyt henkilöt tai organisaatio.

Saatavuusriskejä voidaan pienentää huomattavasti huolellisella suunnittelulla, keinoja ovat muun muassa

- ratkaisujen vakiointi
- muutosten arviointi ja testaus
- muutosten hallittu toteutus.

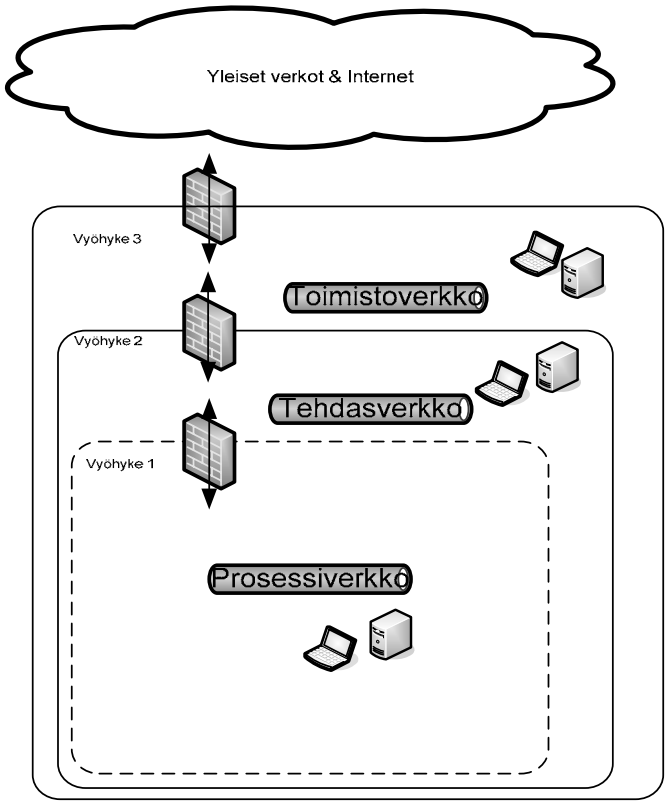
Muutostenhallinta on merkittävä osa järjestelmän ylläpitoa. Varsinainen muutostarve voi tulla yrityksen sisältä tai ulkoa. Muutos pitää arvioida järjestelmävastuullisen henkilön kanssa ja testata ennen tuotantoon ottoa. Kattava muutostenhallinta on mekanismi dokumentoida ja arvioida muutosten vaikutukset järjestelmässä. Näin estetään suunnittelemattomat muutokset, ja niistä aiheutuvat tuotannolliset katkokset. Kuvassa 3 voidaan nähdä muutosprosessin kulku.



Kuva 3. Muutostenhallinnan toimenpiteet [lähdettä 1, s. 71 mukaillen]

Yksittäinen tietoturvalaite ei aina estä kaikkia uhkia. Tehokas suojautuminen vaatii monikerros-suojautumista engl. *Defence-In-Depth*. Ajattelumalli perustuu siihen, että mikäli yksi turvavyöhyke murretaan, on jäljellä vielä muut turvaavat tasot. Tätä kutsutaan yleisemmin syvyyssuuntaiseksi suojautumiseksi. Kerroksien välillä tulee suodattaa verkkoliikennettä palomuurein, ja mielellään vielä keskenään eri valmistajien tuotteilla.

Syvyyssuuntainen suojautuminen on helpompi havainnollistaa kuvalla. Kuvassa 4, keskellä on suojattava järjestelmä tai tietoverkko, jonka ympärille rakentuvat turvakerrokset. [1, s. 69]



Kuva 4. Syvyyssuuntainen suojautuminen. [lähdettä 1, s.69 mukaillen]

2.2 Yleisimmät käytössä olevat protokollat

Käytönvalvontajärjestelmissä käytettävät protokollat jakaantuvat maantieteellisiin alueisiin. Amerikassa on ollut tapana käyttää tiettyjä protokollia, kun taas Euroopassa käytetään toisia. Protokollia on maailmanlaajuisesti erittäin monia, mikäli lasketaan mukaan myös järjestelmätoimittajien omat järjestelmäkohtaiset protokollat. Protokollia pääsääntöisesti käytetään ala-asema-, järjestelmä- ja markkinaosapuolten väliseen kommunikointiin.

Modernisoidut käytönvalvontajärjestelmät keskustelevat infrastruktuurin eri yksiköiden kanssa IP (Internet Protocol) -verkon avulla. Vanhat järjestelmät kommunikoivat sarjaliikenteisesti, ja protokollat ovat hyvin usein järjestelmätoimittajien kehittämiä. Protokollatyyppejä on useita ja standardoimisjärjes-

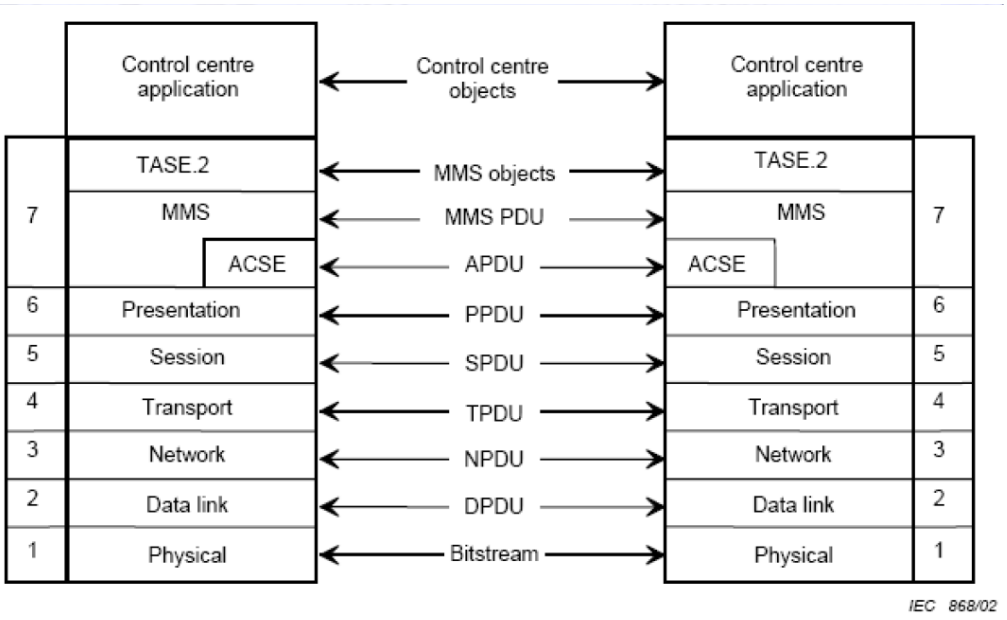
töt, kuten IEC (International Electrotechnical Commission), on luonut ja kehittää edelleen yhteisiä liikennöintimalleja.

2.2.1 Valvomoiden väliset protokollat

TASE.2 / ICCP

Energiantuotannossa SCADA-verkot ovat yleensä yhteydessä RTO (Regional Transmission Organizations) kantaverkkoyhtiöihin tai muuhun vastaavaan valtakunnalliseen sähköverkko-operaattoriin. Myös suuremmissa, hajautetuissa SCADA-ympäristöissä on kahdennettujen valvontakeskusten kyettävä kommunikoimaan keskenään. ICCP (Inter-control Center Communications Protocol) -protokolla tarjoaa tähän mahdollisuuden, ja sitä käytetäänkin näiden osapuolten tai komponenttien väliseen liikennöintiin LAN- ja WAN -verkkojen ylitse [3, s. 344 - 350].

Kuvassa 5 on esitetty ICCP-protokollamoduulien suhde OSI (Open System Interconnect) -malliin, sekä PDU (Protocol Data Unit) -yhteiskäytäntötyypit eri OSI-mallin kerroksilla.



Kuva 5. ICCP/TASE.2 protokollapino ja yhteiskäytännön tyypit [5, s.10]

ICCP-protokolla, joka Euroopassa tunnetaan paremmin TASE.2-nimellä, on IEC:n standardoima. Toiminnallisuus näiden kahden protokollan välillä on lähes sama. Protokollan jatkuvan kehittymisen myötä on nykyään tarjolla tietoturvallinen ratkaisu yleisen asiakas-palvelinarkkitehtuurin kommunikointiin SSL (Secure Socket Layer) -tekniikalla. SSL:n avulla voidaan todentaa liikennöivät päät PKI (Public Key Infrastructure) -tekniikalla, ja samalla yhteys saadaan salattua päiden välillä aina sovelluskerrokselle asti.

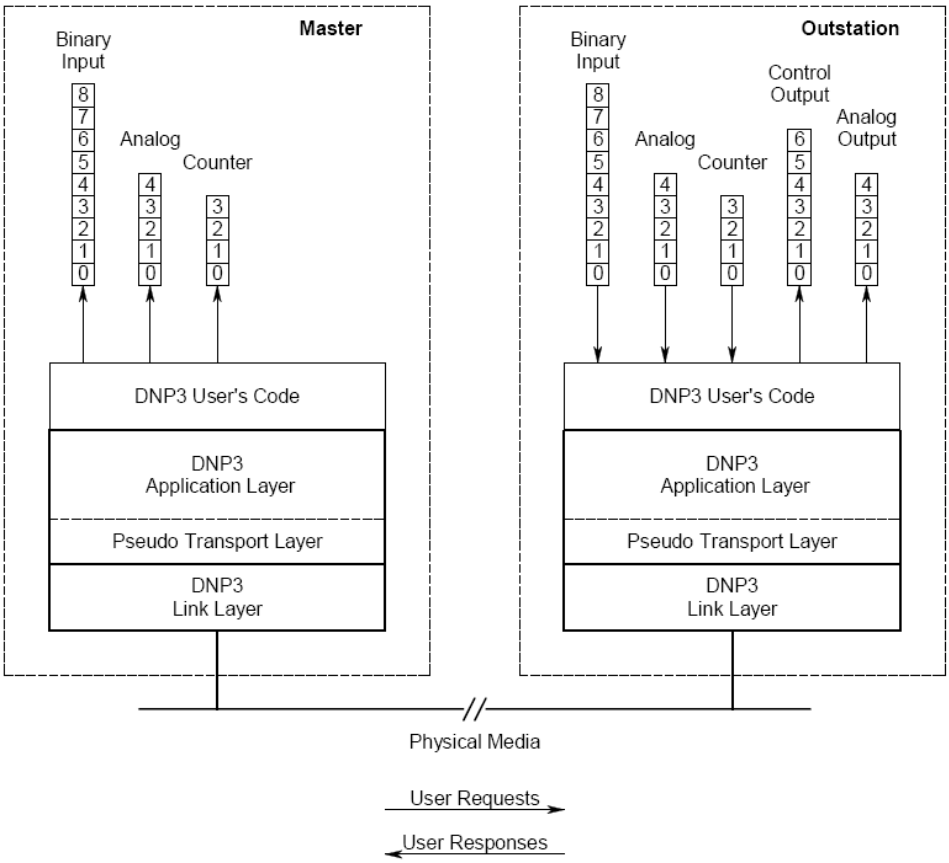
DNP 3.0

IEC 60870-5 -protokollaperheen ollessa vielä kehityksen alla oli tarvetta kehittää standardi, joka sallii liikennöinnin eri SCADA-valmistajien komponenttien välillä. Ratkaisuna on universaali DNP3 (Distributed Network Protocol) -protokolla, joka on General Electric -yhtiön kehittämä. Se on IEC 60870-5 -protokollakomponenttien pohjalta kehitetty vastaamaan erityisesti Pohjois-Amerikan tarpeita ja vaatimuksia. Protokollan alkuvaiheilla liikennöinti oli sarjamuotoista ja hidasta [7].

Viime vuosien verkottumisen myötä on DNP3-protokolla kehittynyt, ja se on muunnettu toimimaan pakettikytkentäisten TCP/IP-verkkojen päällä. Näin DNP3 onkin yksi maailman käytetyimmistä IED-laitteiden ja RTU-yksiköiden välisen liikenteen protokollista. Protokolla soveltuu myös ala-aseman ja valvontakeskuksen väliseen liikennöintiin. Siirtokerroksen kehykset ovat sisällytetty TCP/IP-paketteihin. Tämä lähestymistapa on mahdollistanut DNP3:sen hyödyntämisen IP-tekniikassa. Lisäksi se mahdollistaa tehokkaan tiedonkeräilyn ja hallinnan laajalle levitettyjen laitteiden välillä [3, s. 352; 7, s. 4].

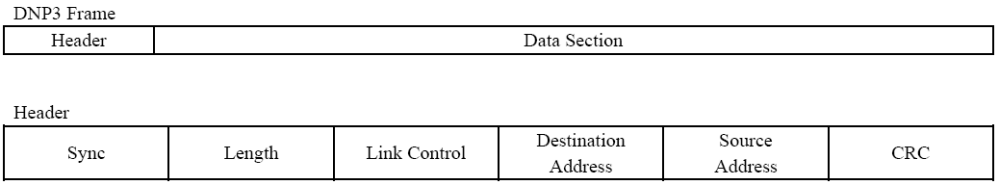
DNP3-järjestelmäarkkitehtuureja on monenlaisia, mutta liikennöinti kuitenkin perustuu ns. isäntä - asiakas -periaatteeseen. Ohjelmisto on rakennettu OSI-mallin mukaisesti kerroksittain tarjoamaan luotettavan tiedonsiirron sekä tehokkaan organisoidun lähestymistavan datan ja komentojen siirtämiseen.

Kerrosajattelutavan mukainen DNP3 protokollapino on esitetty kuvassa 6. Kuvassa ylin kerros on ohjelmakoodi, josta seuraavat tasot alaspäin ovat sovellus-, kuljetus- ja linkkikerrokset.



Kuva 6. DNP3-pinon kerrokset [7, s. 4]

Linkkikerroksen tehtävänä on huolehtia fyysisen linkin luotettavuudesta. Luotettavuudesta huolehditaan virheiden ja kaksoiskehysten havaitsemistekniikalla. DNP3 terminologiassa linkkikerros vastaanottaa ja välittää paketteja, joita kutsutaan kehyksiksi. DNP3-kehys sisältää otsakkeen ja hyötykuorman. Otsakkeessa määritellään kehyksen koko, linkkikerroksen hallinnointitieto sekä DNP3 lähde- ja kohdeosoitteet. Kuva 7 havainnollistaa kehyksen komponentit.



Kuva 7. DNP3-kehysrakenne [7, s. 5]

Jokainen kehys alkaa tahdistusbitillä, jonka avulla vastaanottaja voi havaita kehyksen alkavan. Pituus määrittää oktettien lukumäärän kehyksessä ilman CRC (Cyclic Redundancy Check) -oktettia. Linkinhallintaoktettia käytetään linkkikerroksien lähetys- ja vastaanottopäissä koordinoimaan niiden toimintoja. Lähde- ja kohdeosoitteiden perusteella tietoa välitetään DNP3-kehyksissä, mikä mahdollistaa päästä-päähänyhteydet. DNP3-protokollassa on määriteltävissä 65 520 eri osoitetta. Kolme kohdeosoitetta on varattu ns. all-call -viesteiksi ja loput 12 osoitetta on varattu tulevaisuuden tarpeisiin. Hyötykuormassa on CRC-oktettipari joka kuudessatoista data-oktetissa, jonka ansiosta protokolla havaitsee virheet tarkasti. Oktettien maksimimäärä hyötykuormassa on 250, pois lukien CRC-oktetit.

Hyödyllinen ominaisuus DNP3-protokollassa on linkkikerroksen kuittaus. Lähettäjän on mahdollista pyytää kuittaus vastaanottajalta vastaanotetusta kehyksistä. Ominaisuus on valinnainen, eikä kovin usein käytössä, sillä kehysten kuittaamiseen on olemassa muitakin menetelmiä. Kuittauspyynnöt lisäävät sovelluksen viivettä.

Kuljetuskerroksen vastuulla on katkoa pitkät sovelluskerroksen sanomat pienempiin paketteihin alaspäin linkkikerrokselle. Kooltaan suurin kehys on määritelty vastaanottopään puskurissa. Normaali koko on 2048 – 4096 tavua. [7, s. 5 - 6.]

IEC 60870-5-101

IEC 60870-5 -perheen TC57 (Technical Committee) -komitean kehittämä protokollastandardi SCADA-verkkojen valvontajärjestelmien ja ala-asemien väliselle tiedonsiirrolle. DNP3-protokollan tavoin IEC101 koostuu komponenteista, jotka mahdollistavat myös liikennöinnin ala-aseman RTU-yksiköiden ja IED-laitteiden välillä. 90-luvun alkuvaiheilla kehitetty protokolla tuki ensivaiheessa tiedonsiirtoa ainoastaan sarjaliikenteisillä siirtoteillä, myöhemmin kehitettiin liikennöintimallit myös TCP/IP-verkolle. IEC101-protokollan suhde OSI-malliin on kuvattu kuvassa 8.

7	Application Layer	IEC 60870-5-101 Companion Standard IEC 60870-5-5, IEC 60870-5-4, IEC 60870-5-3	
6	Presentation Layer	n/a	
5	Session Layer	n/a	
4	Transport Layer	n/a	
3	Network Layer	n/a	
2	Link Layer	balanced IEC 60870-5-2 IEC 60870-5-1 (FT 1.2)	unbalanced IEC 60870-5-2 IEC 60870-5-1 (FT 1.2)
1	Physical Layer	RS232 (V.24)	X.24/X.27

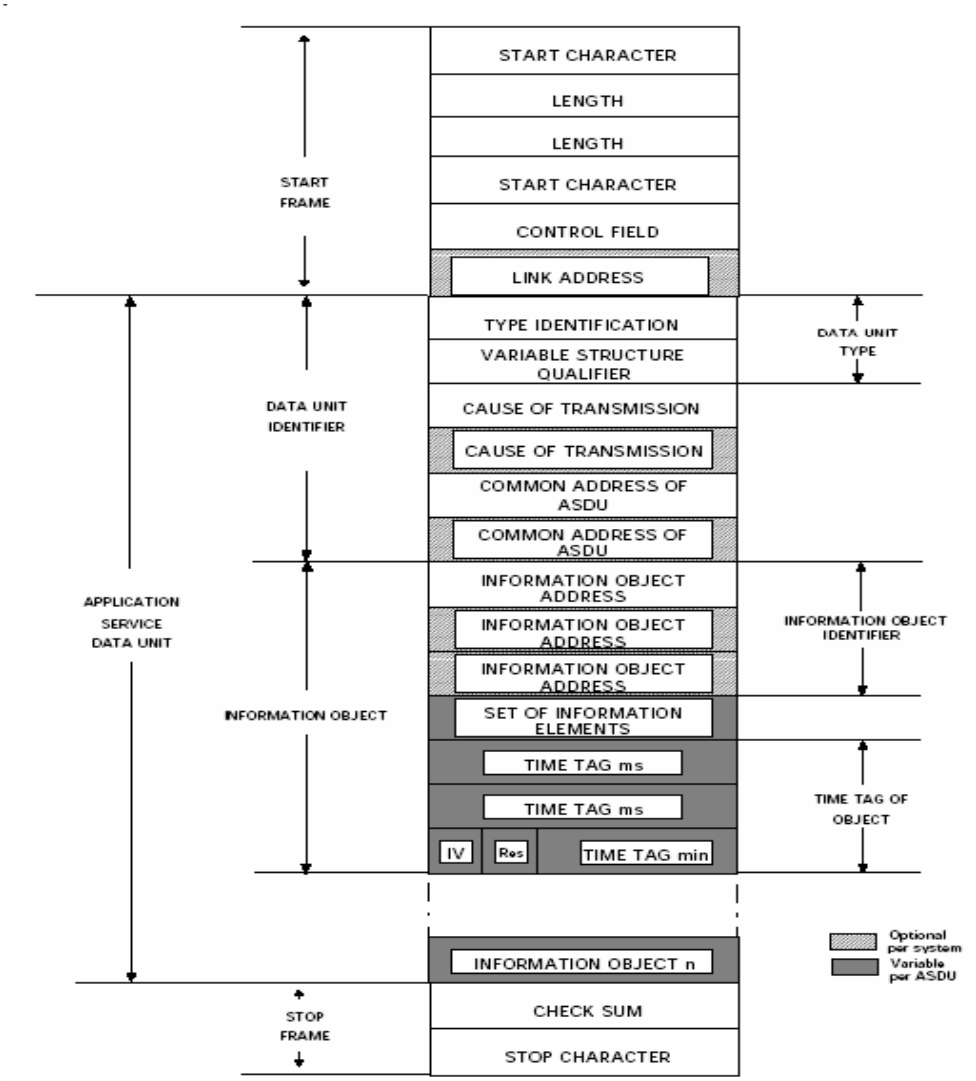
Kuva 8. IEC 101 -OSI malli

Fyysisellä kerroksella IEC101 tarjoaa ITU-T-standardin käyttömahdollisuuden, joka on yhteensopiva EIA (Electronic Industries Association) -standardien RS-232 ja RS-485 sekä valokuituyhteyksien kanssa. Kehysformaattina käytetään FT 1.2:ta, jossa tarjotaan datan eheys ja tehokas siirtolinjan hyödyntäminen. Kehysformaatti perustuu asynkroniseen siirtotekniikkaan, jota voidaan käyttää UART (Universal Asynchronous Receiver/Transmitter) -laitteilla.

IEC101-protokollaa voidaan käyttää linkkikerroksella kahdessa eri siirtotilassa, balansoimattomassa tai balansoidussa. Linkin siirtokäytännöt on määritelty IEC 870-5-2 (1992) -dokumentin mukaisesti. Standardissa on määritelty SEND/NO REPLY, SEND/CONFIRM ja REQUEST/RESPOND -sanomat, jotka ovat tuettuja päätelaitteen toiminnallisuuden mukaan. Lisäksi IEC101 määrittelee tarvittavat liikennöintisäännöt laitteille, jotka operoivat balansoimattomassa ns. multidrop- ja balansoidussa päästä-päähän siirtotilassa.

Sovelluskerros määrittelee ASDU (Application Service Data Unit) -komponentin, jonka rakenne on tarkemmin kuvattu IEC 870-5-3 (1992) -dokumentissa. Ennalta määritellyt tietoelementit ja tyypit on määritelty kiinteästi, eikä järjestelmänvalmistajien ole mahdollista muuttaa niitä. IEC 101 -profiilissa on valmiit tietotyypit suojauslaitteille, jännitesäätimille ja mittausarvoille IED sekä RTU-komponenttien liityntärajapinnassa.

Kuva 9 havainnollistaa ASDU-kehyksen tiedot, näyttäen myös kiinteät ja dynaamiset kentät. Osoiteavaruus määräytyy siten, että yleisiä osoitteita on 1-65 535 kpl, informatiivisia objektiosoitteita 1 - 16 777 215 kpl sekä linkkiosoitteita on määritettävissä 1 - 65 535 kpl. [8, s. 7 - 9.]



Kuva 9. ASDU-kehys [8, s. 9]

IEC 60870-5-104

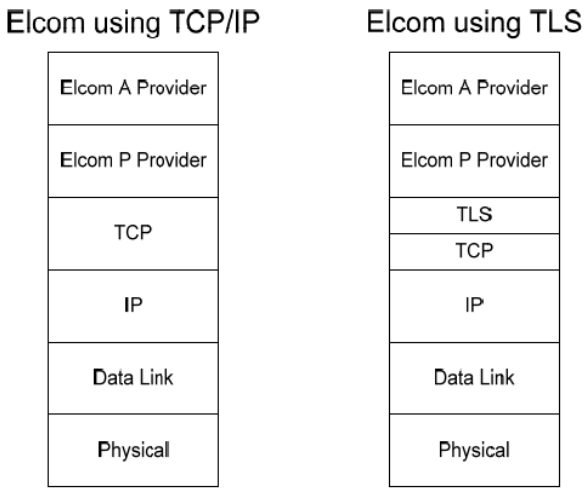
2000-luvun alussa paineet siirtyä liikuttamaan IEC 101 -protokollaa TCP/IP-verkon päällä, ajoi IEC:n kehittämään jatko-osan vanhalle IEC 101 -protokollalle. Toiminnallisuus sovelluskerroksella on lähes sama, joitain ominaisuuksia on kuitenkin jouduttu rajoittamaan IEC 101 -protokollan informaatiotyyppien ja ohjelmointiparametrien vuoksi. IEC 104:ssa ei ole lainkaan tukea lyhyille 3-bitin aikaleimoille. Lisäksi erilaisille osoite-elementeille on määritelty maksimiarvot IEC 104 -protokollassa. Käytännössä kuitenkin useat

valmistajat sekoittavat IEC 101 -protokollan sovelluskerroksen IEC 104 -protokollan kuljetusprofiileiden kanssa, kiinnittämättä huomiota näihin osoiterajoituksiin. Tämä taas voi johtaa ongelmiin jos laite on tiukasti standardissa kiinni.

ELCOM-90

ELCOM-kommunikointiprotokolla on syntynyt EFI:n (Norwegian Electric Power Research Institute), nykyisin SINTEF Energy Research:n, käynnistämästä yhteishankkeesta. Protokollan uusin versio tunnetaan nimellä ELCOM-90, se kulkee saumattomasti TCP/IP tai X.25-verkkojen päällä. Pääasiallinen käyttötarkoitus protokollalle on siirtää informaatiota eri järjestelmäntoimittajien valvontakeskusten, mm. kantaverkkoyhtiöiden ja muiden energiamarkkinaosapuolten välillä. Viimeisimpiä lisäyksiä protokollaan ovat tietoturvaominaisuudet, kuten TLS. Elcom-protokolla kapseloidaan TLS-tekniikan avulla, jolloin saavutetaan todennus, salaus ja sisällön eheys [9, s. 5].

TLS-kapselointi tapahtuu TCP siirtokerroksella, kuten kuvasta 10 havaitaan. Protokollan suojaamaton ja suojattu versio käyttää TCP/IP-protokollapinoa.



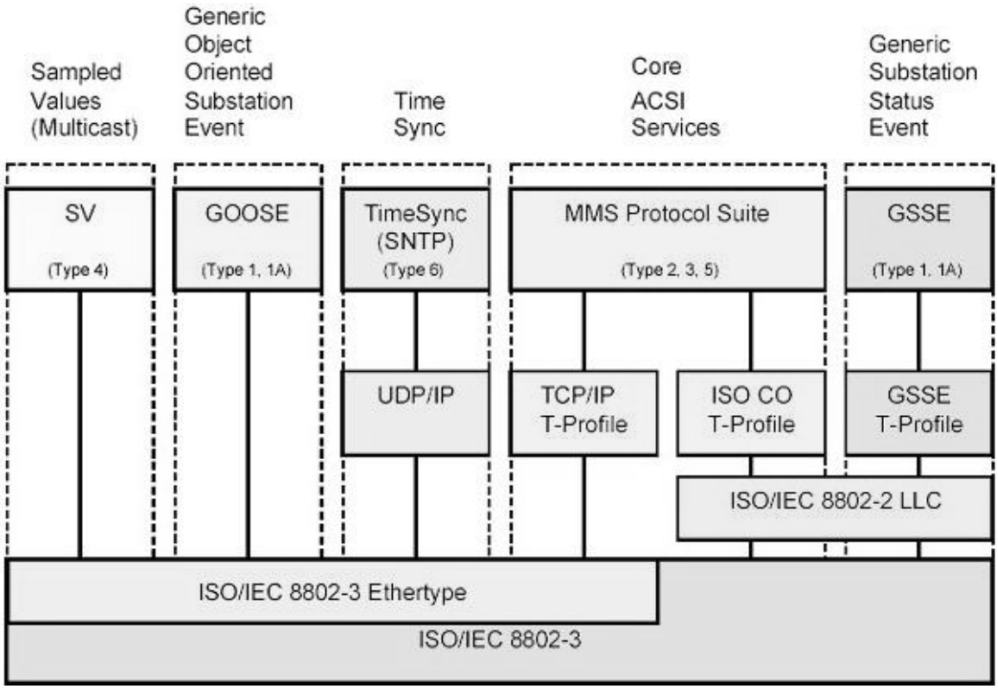
Kuva 10. Elcom-protokollapino [9, s. 10]

2.2.2 Ala-asemien sisäiset protokollat

IEC 61 850

IEC 61 850 -standardin tavoitteena on kehittää yksi älykäs kansainvälinen protokollaperhe Amerikan, Euroopan ja Aasian tarpeisiin. ICCP-protokollan tavoin 61 850 pohjautuu oliosuuntautuneeseen MMS-protokollaperheeseen, jonka lisäksi se toimii TCP/IP-verkon päällä. Protokolla on suunniteltu käyttämään nopeaa 10/100Mb Ethernet-kytkinverkkoa. Ethernet-verkossa sanomat välittyvät nopeasti ja vikatilanteissa toipuminen tapahtuu nopeasti. Protokollaperhe sisältää monia sanomatyyppejä, niistä tärkein on GOOSE (Generic Object Oriented Substation Event) -sanoma. Se on suunniteltu erityisesti nopeaan tiedonsiirtoon I/O-laitteiden välillä [3, s. 351 - 352].

Kuvasta 11 nähdään kuinka 61 850 -protokollan sanomatyypit ja kirjastot ovat sidoksissa toisiinsa.

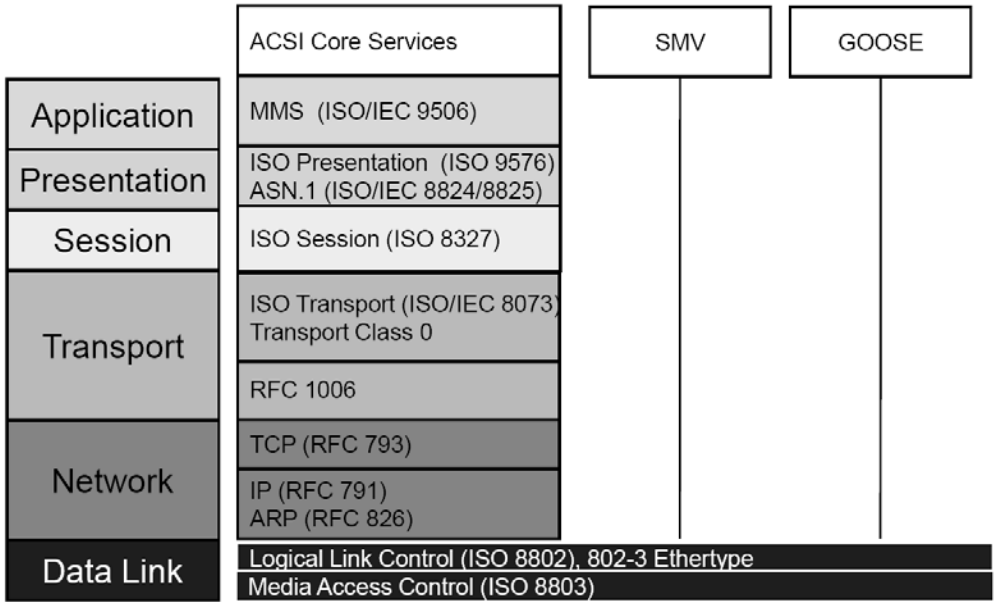


Kuva 11. IEC 61850 protokollasidokset [4, s. 45]

Protokolla tukee ala-asemaympäristöissä kahta erilaista IP-protokollan välitystapaa. Monilähetys-ethernet-verkon avulla, julkaisija voi lähettää yhden sanoman useammalle tilaajalle samanaikaisesti. Lisäksi voidaan käyttää päästä-päähän yksilähetystä. Protokollan päälle on helppo rakentaa lisätie-

toturvaa, esim. ottamalla käyttöön IPSec-tunnelointi järjestelmien reitittimien välille. Muunkin tietoturvan implementointi on helppoa IP-protokollan skaalautuvuuden vuoksi. IP-maailmassa sovelluskerros ei ota kantaa siihen mitä tapahtuu alemmilla OSI-mallin tasoilla [4, s. 48].

Kuvassa 12 on nähtävissä IEC 61850 -protokollapino suhteessa OSI-malliin. Kuvasta nähdään kuinka protokollan eri moduulit linkittyvät OSI-viitemalliin.



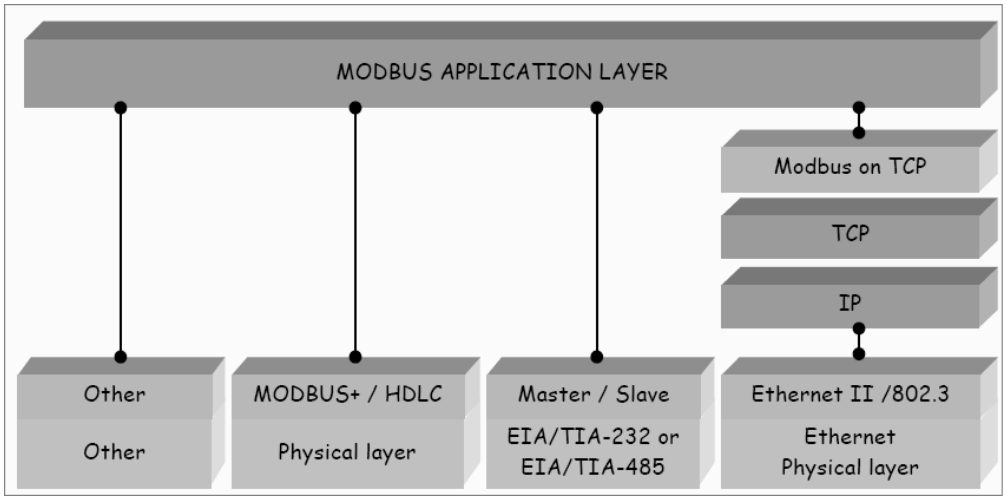
Kuva 12. IEC 61850 protokollapino [4, s.46]

Suomessa nykyiset toteutukset IEC61850 -protokollalla ovat energia-alan ala-asemilla IED (Intelligent Electronic Device) -laitteiden välillä, eikä protokolla yleensä liikennöi ala-aseman ulkopuolelle. Nykyaikaisen suunnittelun ansiosta protokolla soveltuu muuhunkin SCADA-verkon liikennöintiin, jopa ala-asemaverkon ulkopuolelle.

Modbus

Modbus on alun perin Modicon vuonna 1979 kehittämä sarjaliikenneprotokolla yrityksen omien PLC-laitteiden väliseen asiakas/palvelinkommunikointiin, joka sijoittuu OSI-mallin kerrokselle 7. Sarjaliikenteisestä Modbus-protokollasta on kaksi liikennöintitilaa, RTU ja ASCII. Myöhemmin protokolla on kehittynyt toimimaan myös TCP/IP:n päällä.

Seuraavasta kuvasta 13 on havaittavissa Modbus-protokollan kommunikointipino, sekä skaalautuvuus linkkikerroksella.



Kuva 13. Modbus-protokollan kommunikointipino [11, s. 2]

RTU-tilassa Modbus-protokolla siirtää sanomat 8-bitin binaariformaatissa, joka sisältää myös kaksi 4-bitin heksadesimaalimerkkiä. Tämän siirtotilan etuutena on suurempi merkkien tiheys, jolloin saavutetaan parempi datan läpimeno samalla siirtonopeudella verrattuna ASCII-siirtotilaan.

Kuvassa 14 on RTU-kehys. Kehyksen alku ja loppu on tahdistettu ns. hiljaisella aikavälillä. Kehyksen alussa on 3,5 merkkiä, jotka aloittavat kehyksen, sekä lopussa vastaavat 3,5 merkkiä, jotka lopettavat sen. Kehys lähetetään aina jatkuvana virtana, joten jos hiljainen aikaväli on pidempi kuin 1,5 merkkiä, tulkitaan se uudeksi kehykseksi. Kehysformaatissa käytetään CRC-virheentarkistusta [12, s. 16].

START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1–T2–T3–T4	8 BITS	8 BITS	*n* x 8 BITS	16 BITS	T1–T2–T3–T4

Kuva 14. Modbus RTU-kehys [12, s. 18]

ASCII-siirtotilassa jokainen 8-bitin tavu on lähetetty kahdella ASCII-merkillä. Suurin etu tällä siirtomoodilla on se, että siinä sallitaan pidemmät viiveet merkkien välillä vastaanottopäässä. Kehys alkaa kaksoispisteellä ja päättyy rivinvaihtoon. Virheentarkistus eroaa RTU-kehyksestä ja se onkin toteutettu ASCII:ssa LRC (Longitudinal Redundancy Check) -tekniikalla. Tyypillinen ASCII-kehys kuvassa 15.

START	ADDRESS	FUNCTION	DATA	LRC CHECK	END
1 CHAR :	2 CHARS	2 CHARS	*n* CHARS	2 CHARS	2 CHARS CRLF

Kuva 15. Modbus ASCII-kehys [12, s. 17]

Modbus-protokollassa on mahdollisuus määritellä virheentarkistustekniikka kehysten mukaan. Valittavina vaihtoehtoina ovat pariteetin tarkistus, CRC ja LRC virheentarkistustekniikat.

3 TUNKEUTUMISEN HAVAINNOINTI- JA ESTOJÄRJESTELMÄT

IPS (Intrusion Prevention System) -komponentit ovat yleensä yksittäisiä laitteita tai kohdekoneelle asennettavia ohjelmistoja. Usein kuitenkin implementoidaan kokonaisia järjestelmiä, joissa on useita IPS-laitteita. Työasemien varusohjelmistoihin on nykyään sisällytetty palomuurin ja virusohjelmien lisäksi myös tunkeutumisen havainnointi- ja torjuntaohjelmia. IDPS (Intrusion Detection and Prevention Systems) -toiminnallisuutta voidaankin hyödyntää monella eri tasolla, mm. verkko-, työasema- ja palvelintasoilla. Järjestelmillä on myös heikkoutensa. Salattuja yhteyksiä ei voida tutkia kryptauksen takia, ja suuret laitemäärät tuovat mukanaan ylläpidollisia haasteita [13, s. 5].

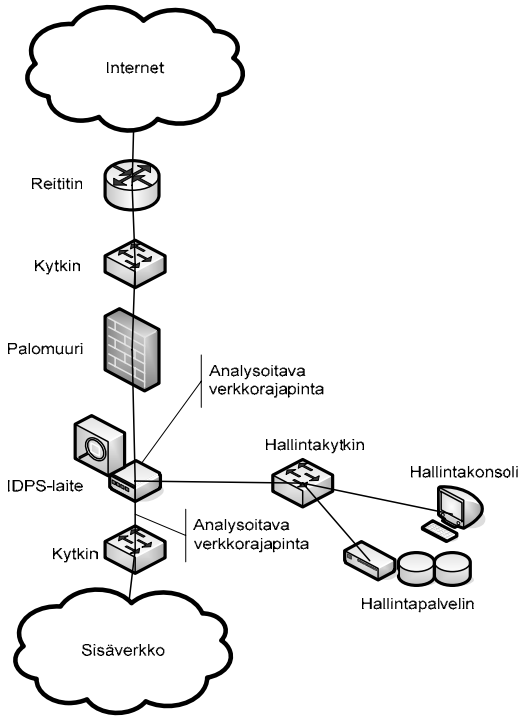
3.1 Komponentit ja arkkitehtuuri

IDPS-järjestelmä on yleensä suurempi järjestelmäkokonaisuus, johon kuuluu useita laitteita ja komponentteja. Näitä ovat agentit työasemilla tai palvelimilla, IDPS-sensorit ja erilaiset hallintaohjelmistot. Lähes kaikkien valmistajien järjestelmissä on löydettävissä toiminnallisuuksiltaan yhteneviä komponentteja. Merkittävimmät erot löytyvät raportoinnista ja ylläpidollisista tekijöistä, kuten haavoittuvuuksien julkaisu- ja laitteen päivitettävyysominaisuuksista. Toteutetut ratkaisut ovat usein hybriditekniikoita, jotka mahdollistavat tehokkaamman analysoinnin, hyödyntäen useita tekniikoita sekaisin [14, s. 23].

Suunniteltaessa järjestelmäarkkitehtuuria on suoritettava riskiarviointi yrityksen tietoverkosta, etenkin niistä pisteistä, joista on fyysinen pääsy yrityksen tietoverkon palveluihin. Tarkoituksena on tuottaa dokumentti kriittisimmistä verkkopisteistä, joihin IDPS-järjestelmän sensorit on kannattavaa sijoitella. Suunnittelussa on myös huomioitava laitteen ominaisuudet, kuten luotettavuus-, suorituskyky-, haavoittuvuuspäivitys-, palvelunestohyökkäys- ja läpikytkentäominaisuudet. Käytettävä tunnistusmetodi asettaa arkkitehtuurillisia rajoitteita laitteelle. IDPS-järjestelmä on reaktiivinen ja kytkentöjä voi olla muihinkin aktiivilaitteisiin, kuten palomuureihin, reitittimiin ja kytkimiin. Integrointi muihin aktiivilaitteisiin tekee järjestelmästä monimutkaisemman. Käytössä on syytä noudattaa tarkkaavaisuutta [14, s. 26 - 27].

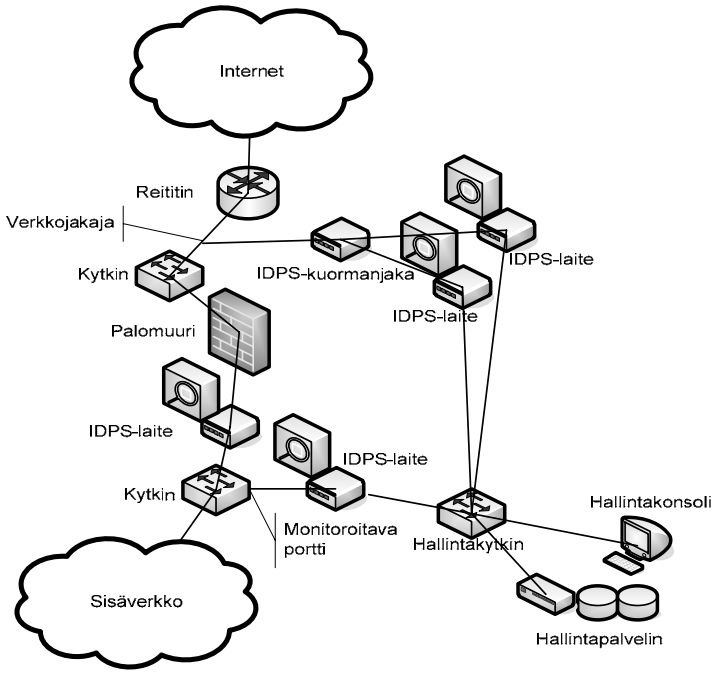
Sensoreiden kytkentä verkkoon tapahtuu pääsääntöisesti kahdella tavalla, linjaan tai passiivisesti. Linjaan kytkettäessä aktiivilaite on suoraan tutkittavan verkkosegmentin välissä. Näin voidaan estää hyökkäykset katkaisemalla haitallinen verkkoliikenne suoraan segmentistä. Linjaan kytketyt laitteet on tyypillisesti asennettu arkkitehtuurimielessä hyvin samantyyppisiin sijainteihin palomuurien ja muiden tietoturvalaitteiden kanssa. Useammat sensorit tarjoavat alkeellisimpia palomuuriominaisuuksia siirto- ja verkkokerroksilla. Laitteen suorituskyky on huomioitava linjaan kytkettäessä, muutoin sensori voi hidastaa merkittävästi verkkoliikennettä ja aiheuttaa pullonkauloja [14, s. 38 - 40].

Linjaan kytketyn laitteen sijoittelu on esitetty kuvassa 16. Laitteet sijoitellaan suoraan datapolulle, ja mielellään vielä useampaan kohtaan, riippuen verkkoarkkitehtuurista.



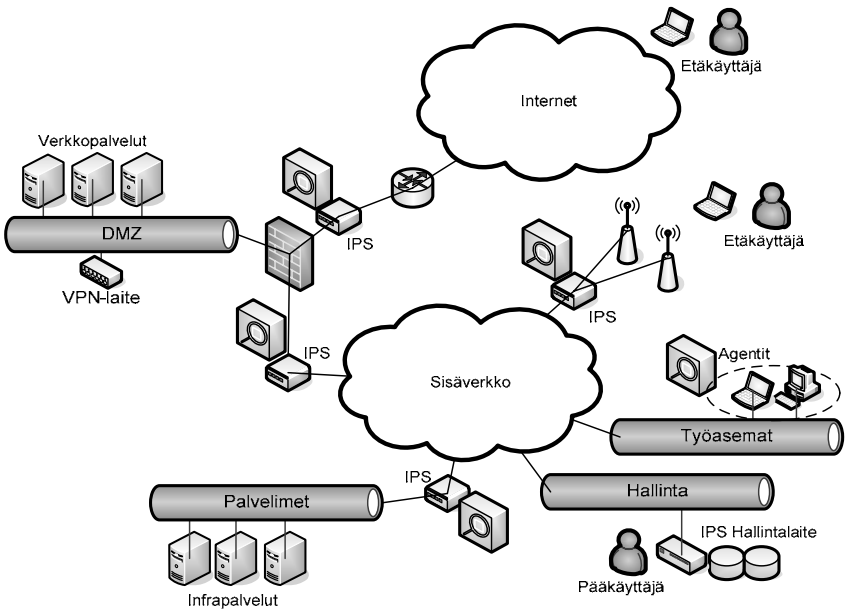
Kuva 16. Linjaan kytketty sensori [14, s.39]

Passiivinen sensori analysoi verkkosegmentin kopioitua verkkoliikennettä. Kopioimiseen tarvittava tekniikkaa ja äly on sisällytetty ainoastaan älykkäimpiin verkkolaitteisiin. Fyysinen verkkojakaja tai IDPS-kuormanjakaja on vaihtoehtoinen ratkaisu, joka ei kuormita itse verkon aktiivilaitetta. Kuormanjakoratkaisuissa liikenne kopioidaan segmentistä jakajalla, ja älykäs laite jakaa kopioidun verkkoliikenteen yhdelle tai useammalle sensorille. Kuvassa 17 havainnollistetaan passiivisesti kytkettyä laitteistoa.



Kuva 17. Passiivisesti kytketty IDPS-laiteympäristö [14, s. 41]

IDPS-järjestelmä sisältää useita aktiivilaitteita ja laitesijoittelu jakaantuukin maantieteellisesti hyvin laajalle alueelle. Paras mahdollinen suoja saadaan käyttämällä kaikkia hyväksi havaittuja tekniikoita sopivassa suhteessa. Peruskomponentit, mm. hallintapalvelin, sensorit ja ohjelmalliset agentit työasemilla on esitetty arkkitehtuurikuvassa 18.



Kuva 18. IDPS-arkkitehtuuri

Sensorit on sijoiteltu kuvan mukaisesti kaikkien kriittisten verkkosegmenttien eteen. Ensisijaisesti on suojattava verkon palvelimia Internetistä kohdistuvilta hyökkäyksiltä. Nykypäivänä yhä useammin virukset leviävät yritykseen verkkoon myös sisältä, jolloin työasemalle lisätty massamuisti aiheuttaa koneen saastumisen. Sensorien sijoittelu yrityksen sisäverkkoon voi estää viruksen leviämisen segmentistä toiseen.

3.2 Tunkeutumisen havainnoinnin ja eston periaatteet

Tunkeutumisen havainnointi on prosessi, jossa tutkitaan tapahtumia verkosta, palvelimilta ja työasemilta. Kerätty tieto analysoidaan ja luokitellaan mahdollisiksi tapahtumiksi. Tunkeutumisenesto käy läpi tapahtumien luokittelun havainnointiprosessin tavoin, mutta havaittuaan loukkauksen laite pyrkii estämään löydetyn haavoittuvuuden käytön. Voidaan sanoa, että laite on jossain määrin reaktiivinen. Laitteet voivat haavoittuvuuden huomattuaan muuttaa esimerkiksi palomuurisäännöstöä. Markkinoilla olevat IDPS-laitteet ovat hyvin monipuolisia ja tuovat tunkeutumisenesto-ominaisuuksien lisäksi myös muita hyödyllisiä ominaisuuksia, mm. tietoturvapoikkeuksien kirjaukset ja virtuaalipäivitykset.

Luonnollisesti on otettava huomioon myös se, että laitteiden haavoittuvuuksien tarkkuus vaihtelee, ja on mahdotonta päästä 100 % tunnistustarkkuuteen. Mikäli IDPS-laite tunnistaa virheellisesti luvallisen liikenteen haitalliseksi, kutsutaan tapahtumaa virhepositiiviseksi. Jos laite ei tunnista haitallista liikennettä lainkaan, kutsutaan sitä virhenegatiiviseksi tapahtumaksi. Useimmat organisaatiot valitsevat mieluummin virhenegatiivisten tarkkuuden nostamisen virhepositiivisten kustannuksella. Tämä taas johtaa siihen, että useampi haitallinen tapahtuma on tunnistettu, mutta vaatii vastaavasti enemmän ylläpito- ja analysointityötä, jotta virhepositiiviset saadaan eroteltua todellisesta haitallisesta liikenteestä. Yleisesti tarkkuuden muokkausta kutsutaan IDPS-laitteiden säätämiseksi, engl. *Tuning*. [13 s. 16 - 17.]

3.2.1 Tunnisteisiin perustuva tunnistus

Tunniste on kuvio ennalta tiedetystä haavoittuvuudesta, joka voidaan analysoida verkkoliikenteestä. Tunnisteisiin perustuva tekniikka, engl. *Signature-Based Detection*, on erittäin tehokas tekniikka pyrittäessä löytämään jo tiedettyjä haavoittuvuuksia. Tekniikka pohjautuu verkkoliikenteen tarkkailuun, jossa analysoitujen pakettien sisältöjä verrataan haavoittuvuustunnisteisiin

käyttäen merkkijonovertailua. Heikkoutena tekniikassa on sen yksinkertaisuus; mikäli hyökkääjä muuttaa tunnetun haavoittuvuuden merkkijonoa ei IDPS-laite enää havaitse haavoittuvuutta merkkijonovertailun avulla, ennalta tuntematonta haavoittuvuutta ei voida tunnistaa ilman tunnistetietoa. Tämä aiheuttaa haasteita IDPS-laitteiden tunnistekuvauksien päivitysvälille, erityisesti ns. nollapäivän aukkoja vastaan suojauduttaessa [13, s. 18].

3.2.2 Poikkeavuuteen perustuva tunnistus

Poikkeavuuksiin perustuvassa tekniikassa, engl. *Anomaly-Based Detection*, vertaillaan normaaliksi määriteltyä verkkoliikennettä havaittuihin tapahtumiin, etsien merkittäviä poikkeamia. IDPS-laite hyödyntää valmiiksi määriteltyjä profiileja, jossa on määriteltynä ns. normaalin liikenteen kuvio. Valmiita profiileja voi olla verkkoliikenteestä tai käyttäjien toiminnasta, tunnettujen protokollien osalta. Käytännössä profiili muodostetaan tarkkailemalla ominaispiirteitä verkon toiminnasta tietyn ajanjakson ajan. Näin saadaan muodostettua referenssitaso. Päätös haitallisesta tapahtumasta suoritetaan kynnysarvojen avulla, esim. sovelluksen normaalikäyttö aiheuttaa keskimäärin 14 % kuorman verkkoon. Mikäli tämä raja ylittyy merkittävästi, voi laite tehdä päätöksen epänormaalista käytöksestä ja toimia sen mukaisesti, tosin tämä voi olla hyvinkin epätarkka tapa tunnistaa poikkeus. Tekniikan suurimpana etuutena on sen kyky tunnistaa ennalta tuntemattomia haavoittuvuuksia, joihin ei ole vielä julkaistu kuvausta. Uusi virus voi aiheuttaa huomattavasti suuremman verkkokuorman, joka havaitaan IDPS-laitteessa ja raportoidaan eteenpäin [13, s. 18 - 19].

3.2.3 Protokollaan perustuva tunnistus

Toisin kuin poikkeavuuksiin perustuvassa tunnistuksessa, profiilit luodaan verkon käyttäytymisen perusteella. Protokollan tunnistuksessa, engl. *Stateful Protocol Analysis*, hyödynnetään jo tunnettujen protokollien ns. syvätutkimista. Profiilit luodaan valmistajien, tai standardointijärjestöjen kehittämillä kuvauksilla, joissa määritellään protokollan normaali toiminnallisuus. Syvätutkinnalla tarkoitetaan sitä, että IDPS-laite on kyvykäs tunnistamaan määritellyn protokollan komennot ja tulkitsemaan ne oikeellisiksi. Näin voidaan rajoittaa esimerkiksi HTTP (Hyper Text Transfer Protocol) -protokollan käyttö ainoastaan tiettyihin HTTP-komentoihin.

Valmistajakohtaisista protokollista ei yleensä ole valmiita kuvauksia ja tieto protokollan toiminnasta jää yleensä valmistajille, jolloin IDPS-laitetta ei voida hyödyntää tehokkaasti. Merkittävin haitta tässä tekniikassa on sen resursse- ja vaativa protokollien tutkimismenetelmä. Paketteja tutkitaan istuntokohtaisesti, joka vaikuttaa oleellisesti laitteen suorituskykyyn. Toinen merkittävä ongelma on palvelunestohyökkäykset. Mikäli protokollaa käytetään oikein, ei poikkeusta havaita. Oikean näköisellä käytöllä on kuitenkin mahdollisuus kuormittaa sovelluksia palvelunestohyökkäyksillä. [13, s. 19 - 30.]

3.3 Tunkeutumisenesto- ja havainnointitekniikat

Tunkeutumisenestojärjestelmissä on erilaisten tunnistusmenetelmien lisäksi perus IDPS-teknologiat. Tekniikat on jaettu kolmeen ryhmään, jossa niitä pääsääntöisesti hyödynnetään. Jotkin tekniikat ovat huomattavasti toisia kypsempiä. Verkko- ja isäntäperusteinen tunnistus on ollut kaupallisesti saatavilla jo lähes kymmenen vuotta, kun taas esimerkiksi langattomuuteen ja verkon käyttäytymiseen perustuvat tekniikat ovat saaneet jalansijaa vasta viime vuosina [14, s. 35].

3.3.1 Verkkoperusteinen tekniikka

Verkkoperusteinen tekniikka tarkkailee verkkoliikennettä määritellyistä segmenteistä analysoiden liikennettä verkko-, kuljetus- ja sovelluskerroksilla. Tekniikan komponentit ovat samanlaisia verrattuina muihin IDPS-teknologioihin, pois lukien sensorit. Sensorit analysoivat ja keräävät tietoa verkkoliikenteestä, yhdestä tai useammasta segmentistä samanaikaisesti. Markkinoilla olevia sensoreita on kahdenlaisia; fyysisiä IDPS-optimoituja laitteita, sekä ohjelmistopohjaisia sovelluksia.

Verkkoperusteisessa tunnistustekniikassa laitteiden sijoittelu nojaa linja- tai passiiviratkaisuihin. Käytettäessä estotoiminnallisuuksia on laite sijoiteltava linjaan, suoraan tutkittavan segmentin väliin. Näin haitalliset yhteysyritykset voidaan katkaista sessiokohtaisesti lähes viiveittä.

Verkkoperusteinen tunnistustekniikka tarjoaa laajan skaalan turvaominaisuuksia. Laitteet voivat kerätä verkosta monipuolista informaatiota mm. liikennöivän isännän käyttöjärjestelmän tai vaikkapa sovelluksen version. Jotkut tuotteet tarjoavat jopa datan kaappauksen laitteen paikalliselle kiintolevylle. Useimmat tuotteet käyttävät tunnisteisiin, poikkeavuuteen ja protokollaan perustuvaa tunnistusta saavuttaakseen kattavan ja tarkan liikenneanalyysin.

Tekniikassa on myös merkittäviä rajoituksia, joita on huomioitava. Segmentistä ei voida analysoida hyökkäyksiä, mikäli verkkoliikenne on salattua. Tämä voidaan mahdollisesti estää laitteen oikealla sijoittelulla ja isäntäperusteisella IDPS-tekniikalla. Laitteet eivät myöskään voi suorittaa analysointia kunnollisesti, mikäli ne ovat ylikuormittuneita.

Verkkoperusteinen tunnistustekniikka tarjoaa monipuolisesti esto-ominaisuuksia. Useimmat passiiviset sensorit voivat yrittää katkaista TCP (Transmission Control Protocol) -istunnon lopettamalla sen, mutta passiivisessa tekniikassa se ei ole täysin reaaliaikaista, eikä se myöskään sovellu muille protokollille, kuten UDP (User Datagram Protocol) ja ICMP (Internet Control Message Protocol) -protokollille. Linjaan kytketyillä laitteilla voidaan saavuttaa hieman erilaisia toiminnallisuuksia, kuten palomuuri, kaistanrajoitus ja haitallisen sisällön muuttaminen. [14, s. 48 - 49.]

3.3.2 Isäntäperusteinen tekniikka

Isäntäperusteinen, engl. *Host-based* tekniikka, monitoroi yhden isännän käyttäytymistä työasemalla tai palvelimella, ja raportoi isännällä tapahtuvista poikkeavista aktiviteeteista. Tekniikassa isäntätyöasemaan tai palvelimeen asennetaan erillinen ohjelma, jota kutsutaan agentiksi. Agenteissa voi olla tunnistusmetodien lisäksi myös estotekniikkaa, ja haavoittuvuuden havaittuaan voi se estää liikenteen pääsyn verkkoon jo asiakaspäässä. Agentit keskustelevat hallintajärjestelmän kanssa olemassa olevan tietoverkon avulla.

Verkkoarkkitehtuuri isäntäperusteisessa tekniikassa on yleensä hyvin yksinkertainen. Agentteja on yleensä saatavilla useille palvelin- ja työasemakäyttöjärjestelmille, tai jopa tunnetuimmille palvelinsovelluksille. Tämä tekee tek-

niikan käyttöönoton helpohkoksi. Organisaatioiden tulee ottaa kuitenkin huomioon useita eri vaatimuksia valittaessa agentteja. Näitä ovat mm.

- Agenttien hinta ja kohdekoneiden lukumäärä
- Ylläpito- ja monitorointiominaisuudet
- Agenttien sovellus-, käyttöjärjestelmä- ja tietoverkkotuki.

IDPS-tekniikka tarjoaa monipuolisia tietoturvaominaisuuksia. Tunnistustekniikkaan yleensä sisältyy koodin- ja verkkoliikenteen analysointi, verkkoliikenteen suodatus, tiedostojärjestelmän monitorointi ja lokien seuranta. Verkkoperusteinen järjestelmä, joka hyödyntää kaikkia em. mekanismeja on tarkka tunnistamaan haitallista toimintaa kohdekoneella. Suositeltavaa on säätää ja asentaa agentit juuri omien tarpeiden mukaisiksi. Näin pyritään välttämään turha ylläpitotyö.

Organisaatiot voivat määritellä ohjelmistot tarkastelemaan isäntäkoneen toimintaa, kehittäen automaattisesti referenssejä tai profiileja sovellusten käytöksestä. Toiset organisaatiot taas määrittelevät tiukkoja sääntöjä kuinka jokainen sovellus isäntäkoneella voi käyttäytyä. Molemmissa on puolensa. Ympäristön muuttuessa myös agenttien tulee muuttua. Suuret ympäristöt saattavatkin teettää huomattavasti ylläpitotyötä muutostilanteissa.

Estotekniikoita on isäntäperustaisessa tunnistuksessa lukuisia. Koodin analysointiominaisuuksilla voidaan estää haitallisen ohjelmakoodin suoritus isäntäkoneella. Verkkoliikenteen tutkiminen voi taas estää tulevan ja lähtevän liikenteen hyökkäykset verkko-, kuljetus- ja sovelluskerroksilla. Tehokasta on myös käyttää tiedostojärjestelmän monitorointia, jolla voidaan havaita käyttäjän tai viruksen toimia työasemalla. Agenttien ominaisuuksiin kuuluu usein myös ulkoisten massamuistien liittämisen estäminen ja automaattisesti suoritettava käyttöjärjestelmän koventaminen karsimalla siitä tarpeettomia palveluita ja protokollia.

Tekniikalla on myös heikkouksia. Jotkin tunnistusmekanismit suoritetaan ainoastaan tietyin aikavälein. Tapahtumien poiminta järjestelmästä viivästyy ja tämä voi aiheuttaa merkittäviä menetyksiä. Agentit lähettävät usein hälytystietonsa vain muutaman kerran tunnissa hallintapalvelimelle. Tästä seuraa viive tapahtumien käsittelyssä. Agenttien asennuksessa voi ilmetä ongelmia muiden tietoturvaohjelmistojen välillä. Näitä ovat mm. työasemakohtaiset palomuurit, varusohjelmat ja VPN-asiakasohjelmistot, joten huolellinen toimintaympäristön kartoittaminen edeltää isäntätekniikkaan pohjautuvaa IDPS-projektin käynnistystä. [14 s. 82 - 83.]

3.3.3 Verkon käyttäytymisperusteinen tekniikka

Verkon käyttäytymisperusteisessa, engl. *Network Behavior Analysis* teknologiassa, tutkitaan verkkoliikennettä ja pyritään löytämään liikennevuosta poikkeuksellista liikennöintiä. Vertailut suoritetaan luotuja liikenneprofiileja vasten. Sensorit ovat samantyyppisiä verkkoperusteisen tekniikan kanssa. Verkkoliikennettä analysoidaan yhdestä tai useammasta pisteestä. Jossakin tapauksissa sensori ei ole verkon solmupisteessä, vaan liikenne välitetään analysoitavaksi reitittimien tai muiden verkkolaitteiden toimesta. Tämän takia useat NBA -tekniikat liitetäänkin verkkoon passiivisesti.

NBA-tekniikka voi tyypillisesti tunnistaa haitallisesta verkkoliikenteestä mm. DoS (Denial of Service) -palvelunestohyökkäykset, verkkoskannaukset, madot ja erilaiset odottamattomat sovelluspalvelut. Sovelluspalveluita voivat olla esim. asiakkaan jakamat verkkopalvelut muille käyttäjille. Pääsääntöisesti NBA-tekniikka tunnistaa haavoittuvuudet poikkeuksien perusteella normaaliliikenteestä. Teknologia on erityisen tarkka tunnistamaan hyökkäykset, jotka generoivat suuren määrän verkkoliikennettä lyhyessä ajassa ja ne joiden liikennekuvio on poikkeuksellinen.

Tekniikalla on merkittäviä rajoituksia. Teknisesti laitteet ovat hieman hitaita tunnistamaan haitallista liikennettä, mikäli toteutus on tehty siten, että analysoitava verkkoliikenne on lähetetty suoraan reitittimeltä tai muulta verkkolaitteelta. Hyökkäykset leviävät nopeasti ja rikkovat yleensä kohdejärjestelmän ennen kuin ne ehditään havaita. Viivettä voidaan pienentää asentamalla sensori linjaan. Tämä taas vaatii sensorilta huomattavasti enemmän laiteresursseja. Laitevalmistajat valmistavatkin monia erilaisia laitemalleja, joiden tehokkuudet ja porttilukumäärät vaihtelevat tuotteiden mukaan. [14 s. 71 - 72.]

3.4 Ylläpito ja hallinta

3.4.1 Hallinnollinen ylläpito

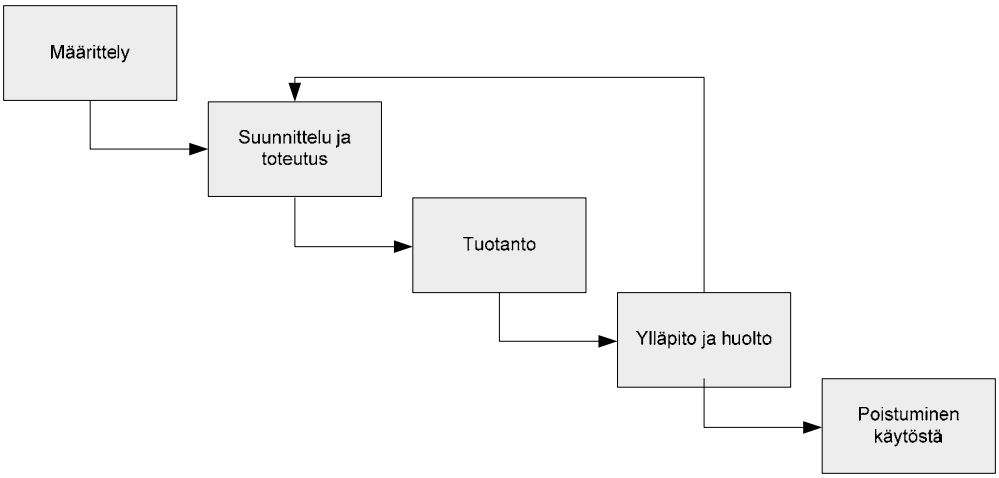
IDPS-laitteiden ylläpito on jatkuvaa ja se tulisikin suorittaa prosessiluontoisesti. Jatkuvaan palvelun kehittämiseen ja ylläpitoon on hyvä soveltaa IT-alan parhaita käytäntöjä esim. ITIL (Information Tehnology Infrastructure Library) -dokumenttikirjastoa. ITIL antaa hyvän suunnittelupohjan IDPS-laitteiden ylläpidolle. ITILv3:n palvelukeskeisen tuotantomallin komponentit ylätasolla koostuvat kuvan 19 mukaisesti. Palveluiden tuotanto alkaa strategisesta suunnittelusta ja päättyy palveluiden jatkuvaan kehittämiseen.

Kuva 19. ITILv3 palveluntuotannon komponentit [17]

ITIL-viitekehystä peilaten ylläpito ja hallinta keskittyy nimenomaan palvelutuotannon aktiviteetteihin. Merkittävimmät palvelun tuottamisen prosessit ovat tapahtumien-, ongelmatilanteiden- ja herätteiden hallinta. Muutostenhallinta kuuluu myös oleellisesti ylläpidollisiin prosesseihin, jonka tehtävänä on käsitellä kaikki järjestelmään kohdistuvat muutokset. Muutoksia varten on suositeltavaa perustaa erillinen muutoksia käsittelevä ryhmä, joka tarkastaa, dokumentoi ja päättää muutoksista. [17.]

Elinkaaren hallinta

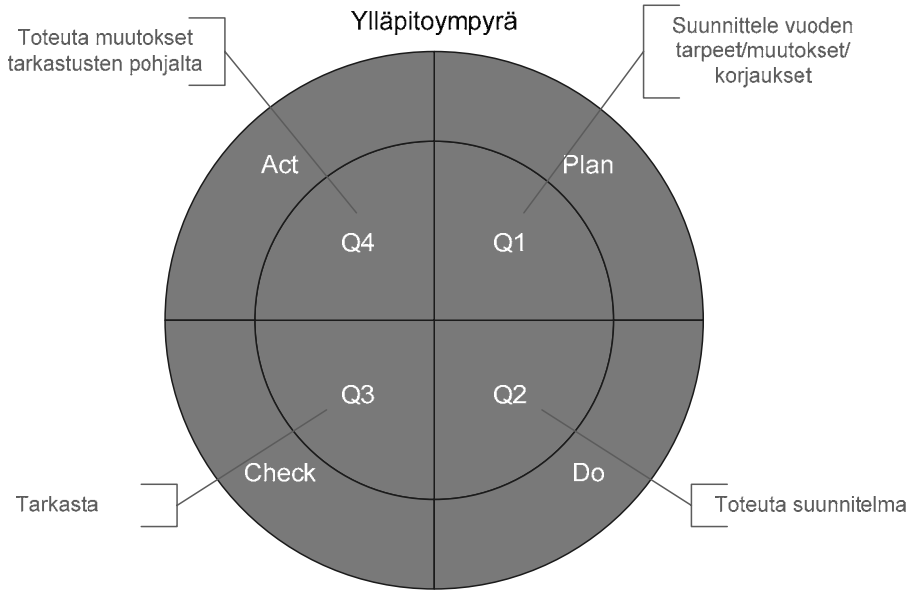
IDPS-laitteiston elinkaari ja elinkaarikustannukset jakautuvat yleensä muiden tietoteknisten laitteiden kanssa hyvin lyhyille ajanjaksoille. Keskiverto poistoaika on noin 3-5 vuotta. Käytönvalvontajärjestelmien käyttöikä voi olla jopa 15 vuotta, joka asettaa haasteet järjestelmän tietoteknisille laitteille. Suunnitellessa tuotteen elinkaarta on hyvä tukeutua perinteisiin toimintamalleihin. Yksi vanhimmista on ns. porrasmalli, jossa laskeudutaan ylemmästä vaiheesta alempaan suorittaen eri aktiviteetti kussakin elinkaaren vaiheessa. Kuvassa 20 on vesiputousmallin mukaisesti kuvattu tuotteen elinkaarta, käyden läpi eri vaiheita.



Kuva 20. Tuotteen elinkaari vesiputousmallissa [16]

Erityisesti ylläpito ja huoltovaiheessa on hyvä käyttää vuosikello-ajattelumallia, joka helpottaa huomattavasti järjestelmän ylläpidollisia suunnittelutöitä. Vuosikelloa on yleensä käytetty johdon suunnittelun tukena, mutta se on sovellettavissa muihinkin käyttökohteisiin. Deming-ympyrä on työkalu suunnitteluun, joka yhdistettäessä organisaation vuosikelloon takaa palvelun jatkuvan kehittymisen sen elinkaaren aikana.

Ympyrä voidaan jakaa kvartaaleittain, kuten kuvasta 21. Tässä tapauksessa toiminnot on jaettu vuodelle, jossa kunkin kvartaalin funktio on eri. Vuoden ensimmäinen kvartaali aloittaa suunnitteluvaiheen, tarkoituksenaan käydä läpi vuoden tarpeet ja palveluun kohdistuvat muutostarpeet. Toinen kvartaali toteuttaa suunnitellut muutokset. Kolmas vaihe tarkastelee tuotannossa olevaa järjestelmää, tarkoituksena etsiä heikkouksia ja parannuskohteita. Viimeisen aktiviteetin funktio on parannella järjestelmää tarkastelujen perusteella.



Kuva 21. Deming-ympyrä [17]

Palvelulle tulee määrittää vastuuhenkilö sen koko elinkaaren ajaksi. Vastuuhenkilön tehtävä on vastata palvelusta tai osasta sitä. Vastuut voidaan jakaa kahtia, hallinnolliseen ja ylläpidolliseen. Vastuuhenkilön tulee laatia palvelusta ylläpitosuunnitelma, josta ilmenee palveluun liittyvät oleelliset asiat, kuten järjestelmäkomponentit, vastuuhenkilöt, arkkitehtuuri, dokumentointi- ja muutoskäytännöt. Huolellisesti suunniteltu ja ylläpidetty elinkaari takaa tuotteen ajanmukaisuuden sekä tarkemman elinkaarikustannusten seuraamisen sen koko elinkaaren aikana. [16; 17.]

3.4.2 Tekninen ylläpito

Lähes kaikkia IDPS-tuotteita hallitaan jonkinlaisen graafisen käyttöliittymän avulla. Graafisen konsoli-liittymän kautta ylläpitäjä voi konfiguroida, päivittää ja monitoroida hallinnassa olevia laitteita. Konsolissa on liittymä myös järjestelmän raportointikomponentteihin. Useimmissa laitteissa on lisäksi merkkipohjainen CLI (Command-line Interface) -hallintaliittymä. Laitteiden valvonta tapahtuu siihen tarkoitetulta hallintapalvelimelta tai yrityksen laajemman valvontajärjestelmän kautta.

Keskitetty hallinta on nykypäivänä lähes kaikkien laitevalmistajien toteutuksissa. Keskitetty hallinta vähentää huomattavasti ylläpidollisia kustannuksia ja koko laiteomaisuus voidaan hallita yhdestä paikasta. Raporttien luonti ja haavoittuvuuksien seuranta tehostuu entisestään keskitetyn hallintaratkaisun avulla. Hallinta voidaan hajauttaa usealle eri palvelimelle, jolloin saadaan erittäin vikasietoinen ja skaalautuva valvontaratkaisu.

Ulkopuoliset yritykset tarjoavat haavoittuvuuksien käsittelyä ja laitteiden ylläpitoa palveluna. Tällaisissa tapauksissa haavoittuvuuksia ja tapahtumia valvoo kolmas osapuoli, jonka verkonvalvontakeskukset valvovat IDPS-komponentteja, raportoiden asiakkaalle säännöllisin väliajoin tapahtumista. Palvelua voidaan tarjota virka-aikana tai sen ulkopuolella, jolloin palvelunvalvonta saadaan jatkumaan katkeamattomana vuorokauden ympäri. Mikäli yrityksellä ei ole omaa ICT-organisaatiota, tai riittävää osaamista tunkeutumisenesto- ja havainnointitekniikoista, on ulkoistaminen järkevä ratkaisu. Näin voidaan vähentää ylläpidollisia kustannuksia ja keskittää osaaminen liiketoiminnan kannalta tuottavampaan työhön.

IDPS-laitteiden ylläpidosta vastaavan organisaation tulee ottaa vastuu palvelun elinkaaresta ja laitteiden teknisestä ylläpidosta. Organisaation tulee huolehtia riittävästä osaamisesta ja sen kehittämisestä. Ylläpito-organisaation tulee huolehtia ainakin seuraavista tehtävistä:

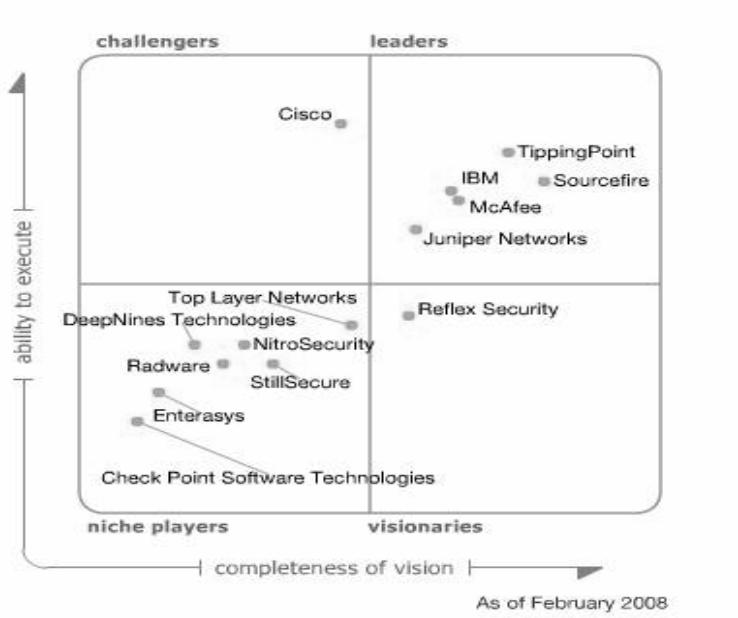
- IDPS-laitteiden monitorointi saatavuus- ja tietoturvanäkökulmasta
- IDPS-laitteiden toiminnallisuuden tarkastaminen mm. tapahtumien käsittely, hälytysten asianmukaisuus ja epäilyttävä toiminnallisuus
- Haavoittuvuuksien säännöllinen tarkastaminen
- IDPS-laitteisiin kohdistuvien tietoturvahaavoittuvuuksien seuraaminen ja reagoiminen niihin.
- Päivityksistä huolehtiminen, sisältää testauksen ja jakelun.

Yksi merkittävimmistä ominaisuuksista laitteissa on niiden haavoittuvuuksien ja tunnisteiden päivitykset. Tunnistepäivityksillä päivitetään tunnettujen haavoittuvuuksien kuvauksia, joita poimitaan merkkijonovertailun avulla verkkoliikenteestä. Laitteiden päivityssyklit ja nopeudet vastata erilaisiin nollapäivän hyökkäyksiin vaihtelevat laitevalmistajakohtaisesti. Haluttaessa suojautua nollapäivän hyökkäyksiä vastaan tulee päivitykset ottaa käyttöön välittömästi niiden julkaisun jälkeen. Tunnisteiden testaus ennen käyttöönottoa on välttämätöntä ennen tuotantoon ottoa. Huolellisella tunnisteiden testauksella voidaan minimoida palvelukatkokset. [14, s. 26 - 31.]

3.5 Markkinakatsaus

IDPS-markkinat nykypäivänä ovat jatkumo vanhemmasta IDS (intrusion Detection System) -teknologiasta. IDPS-laitteet sisältävät samat ominaisuudet, mutta merkittävimpinä edistysaskelina ovat erilaiset tunnistustekniikat. Heuristiset ominaisuudet haavoittuvuuksien tunnistuksessa vievät tekniikkaa eteenpäin. Markkinoilla olevat IDPS-laitteet jakautuvatkin karkeasti neljään ryhmään; markkinajohtajiin, haastajiin, pikku pelureihin ja visionääreihin.

Gartnerin vuonna 2008 tekemän markkinatutkimuksen mukaan laitepohjaisten tunkeutumisenestolaitteiden nelikenttäanalyysi jakautui kuvan 22 mukaisesti.



Kuva 22. IDPS-laitevalmistajien nelikenttäanalyysi [15]

Palomuurivalmistajat ovat olleet hitaita tarjoamaan palomuuri-integroituja IPS-ominaisuuksia. Tästä johtuen IPS-yksittäislaitemarkkinat ovat kasvaneet erityisen voimakkaasti viime vuosina. Yritysten uusiessa tulevaisuudessa ensimmäisen sukupolven IPS-laitteita, tulevat palomuuri-integroidut tuotteet kasvattamaan markkinaosuuttaan entisestään.

Hyökkäyksien luonne on muuttunut viime vuosina. Yrityksiin kohdistettuja haittaohjelmahyökkäyksiä on yhä enemmän. Näiden estäminen vaatii paremman mekanismin kuin vain tunnisteisiin perustuvan havainnoinnin. Laite-

valmistajat tulevatkin panostamaan tämän tyyppisten haavoittuvuuksien estämiseen tulevaisuudessa yhä enemmän. Nollapäivän hyökkäykset ovat myös kasvaneet räjähdysmäisesti. Erilaisten selainhaavoittuvuuksien kautta tunkeudutaan yrityksiin yhtä useammin. Gartner arvioikin, että vain noin 10 % yrityksistä ottaa käyttöön nollapäivän tunnisteet välittömästi. Yritysten vertaillessa IDPS-tuotteita, merkittävin paino tulisikin olla tunnistekuvausten laadussa ja tarkkuudessa. Laadukkaat tunnisteet mahdollistavat nopean suojautumisen nollapäivän hyökkäyksiä vastaan.

Tulevaisuudessa IDPS-teknologia tulee kehittymään entisestään, ja merkittävänä edistysaskeleena tulee olemaan DLP (Data Loss Prevention) -tekniikka. Tekniikka mahdollistaa arkaluontoisen informaation säilyttämisen yrityksen sisällä. Mahdollisten tuote- ja tekniikkaan liittyvien liikesalaisuuksien vuotaminen ulkomaailmaan voidaan estää DLP:llä. Komplikaatioita tekniikan käyttöönotossa voi joidenkin tuotteiden ja lakien osalta olla esimerkkinä mm. lex Nokia. Suomessa käyttäjätietoja saa tutkia hyvin rajallisesti, ja nekin tapahtuvat yleensä rikostutkinnallisista syistä poliisin toimesta.

Salattu verkkoliikenne on ongelma IDPS-laitteille. Salauksen vuoksi, ja erityisesti SSL-tekniikan suosio sovelluksissa tuottaa ongelmia havainnointilaitteille. Laite ei pysty purkamaan salattua verkkoliikennettä, jolloin yhteyden sisällä tapahtuvaa liikennöintiä ei voida tutkita eikä haavoittuvuuksia näin pystytä havaitsemaan.

Tuotteiden hinnat tulevat tulevaisuudessa elämään ja laskemaan entisestään IPS-ominaisuuksien vakiinnuttaessa paikkaansa tietoverkossa. Markkinoiden vertailu on hyvinkin vaikeaa tuotteiden erilaisten ominaisuuksien ja hinnoittelujen vuoksi. IDPS-markkinat ovat kasvaneet tasaiseen tahtiin, ja odotettavaa onkin, että maailmanlaajuisesti markkinat hipovat jo 2 miljardia dollaria vuoteen 2011 mennessä. [15.]

4 ESTO JA HAVAINNOINTI KÄYTÖNVALVONTAJÄRJESTELMISSÄ

Käytönvalvontajärjestelmien laitteiden poistoajat ovat yleensä hyvinkin pitkiä, ja niihin liittyvät tietotekniset hankinnat tulee suunnitella pitkälle aikavälille. Vanhoihin järjestelmiin voi olla vaikeaa istuttaa modernia IDPS-ympäristöä, sillä verkkotekniikka on vanhaa, liitännät erikoisia ja protokollat laitevalmistajakohtaisia. Uusittavien järjestelmien kanssa tilanne on toinen. Näihin voidaan hyvin saumattomasti ottaa käyttöön uusi IDPS-järjestelmä. SCADA-verkoissa tunkeutumisenesto- ja havainnointitekniikkaa käyttöön ottaessa kannattaa suunnitella järjestelmän käyttöönottoa myös muun tietoverkon käyttöön. Näin saadaan tehokkaasti hyödynnettyä IDPS-laitteiden tarjoamia palveluita läpi koko organisaation verkon.

Yleensä IDPS-järjestelmien käyttöönotoilla pyritään takaamaan liiketoiminnan jatkuvuutta erilaisissa poikkeustilanteissa, eikä sijoitetun pääoman tuottoa laitteelle suoraan voi laskea. Laskelmat perustuvat säästettyyn työaikaan, ja nopeuteen reagoida poikkeustilanteissa. Työaikasäästöt saadaan laitteiden ns. virtuaalipäivitys-ominaisuuksilla suojauduttaessa nollapäivän hyökkäyksiä vastaan. Vaikka IDPS-laitteisto mahdollistaa sovellusten ja haavoittuvuuksien virtuaalipäivityksen, ei tule unohtaa sovellusten todellisen päivittämisen tarvetta.

Tunkeutumisenesto- ja havainnointijärjestelmien käyttöönottoon SCADA-verkoissa tulee suhtautua kriittisesti. Protokollakuvausten saatavuus vaihtelee eri laitevalmistajien kesken. Nykypäivän laitevalmistajat eivät tarjoa kuvauksia läheskään kaikkiin käytettyihin protokolliin. Laitteista saatavat todelliset hyödyt tulee kunkin yrityksen selvittää hyvissä ajoin ennen käyttöönottoprojektin aloitusta.

4.1 IDPS-laitteiden tuki käytönvalvontajärjestelmien protokollille

IDPS-laitevalmistajien tuki käytönvalvontaprotokollille on hyvin rajattua. Laitevalmistajien välillä voi ilmetä huomattavia eroja tuetuista protokollista ja niiden kuvauksista, esim. DNP3-protokolla on kehitetty suoraan IEC101-protokollan 60870-5-liikennöintimallien pohjalta, mutta ei ole varmuutta, että tätä DNP3:lle kirjoitettua protokollakuvausta voidaan hyödyntää IEC104-protokollakuvauksen sijaan. IEC:n standardoimat 101 ja 104 protokollat ovat vallitsevia pohjoismaissa, valitettavasti kuitenkin näiden protokollakuvauksien tarjonta on hyvin rajallista IPS-laitteille.

IDPS-laitteissa tuettuna onkin vain yleisimmät protokollat, kuten ICCP, DNP3 ja Modbus. Useimmista markkinajohtajien laitteista löytyvät kuvaukset em. protokolliin. Markkinoilla on myös pienempiä laitevalmistajia, näitä ei esim. Gartnerin tutkimuksessa ole vertailtu lainkaan. Pienemmiltä laitevalmistajilta voi löytyä kuvauksia myös vähemmän käytetyille protokollille, kuten ELCOM-90 ja IEC 61850/UCA.

Taulukkoon 1 on kerätty vertailevaa tietoa yleisimmistä SCADA-protokollista. Osaan laitteista on asennettavissa protokollakuvaukset kolmannen osapuolen ohjelmoimina.

Taulukko 1. Laitevalmistajat ja niiden tukemat yleisimmät SCADA-protokollat [18]

Laitevalmistaja	DNP3	Modbus	ICCP/TASE.2	IEC 60870-5-101	IEC 60870-5-104	IEC 61850	ELCOM-90
TippingPoint	x	x	x	-	-	-	-
Industrial Defender	x	x	x	-	-	x	-
CheckPoint	-	-	-	-	-	-	-
IBM Proventia	x	x	x	-	-	-	-
Juniper	*x	*x	*x	-	-	-	-
McAfee	*x	*x	*x	-	-	-	-
Cisco Systems	*x	*x	*x	-	-	-	-
Sourcefire	*x	*x	*x	-	-	-	-

Tuki kolmannen osapuolen kautta	*x
Natiivi tuki protokollalle	x

Muiden organisaatioiden kirjoittamia kuvauksia voidaan ladata IDPS-laitteeseen, jolloin protokollakuvaukset voidaan saada hyödynnettyä eksoottisimpienkin protokollien osalta. Taulukossa on vertailtu Digital Bond -organisaation kehittämiä protokollakuvauksia. Tuettuihin protokolliin liittyvät ominaisuudet on hyvä varmistaa vielä laitevalmistajalta ennen hankintoja.

Toistaiseksi tarjonta protokollakuvauksista on rajallista, ja tulevaisuudessa laitevalmistajat varmasti nojaavatkin kolmansien osapuolten kirjoittamiin kuvauksiin, etenkin kapean markkina-alueen sovellusprotokollien osalta. Protokollakuvauksien tarkkuus voi vaihdella merkittävästi ohjelmoijien välillä, ja kuvauksiin tuleekin suhtautua varauksella. [18.]

4.2 Vaatimusmäärittelyt

Määrittelyt ovat merkittävin vaihe uuden laitteiston hankinnassa. Vaatimusmäärittelyillä yritys kuvaa yksiselitteisesti ja selkeästi vaatimuksensa järjestelmälle, muodostaen teknisen toteutuksen ja toiminnallisuuden reunaehdot. Määrittelyiden laatiminen on haastavaa, sillä on tunnettava tekniikan tuomat mahdollisuudet ja rajoitukset, sekä selvitettävä yrityksen tarpeet perusteellisesti.

Valmistajavaatimukset

Valmistajan on oltava kansainvälisesti arvostettu, tunnettu ja sellainen, jonka markkinaosuus on huomattava. Tuotteiden elinkaaripolku engl. *road map* ja lisensointi on pystyttävä kuvaamaan ylätasolla. Ongelmatilanteita varten on laitevalmistajan tarjottava pääsy ylläpitämäänsä tietämyskantaan engl. *knowledge base*. Jos valmistaja toimii partneriverkoston kautta, on sillä oltava hyvät kanavat Suomessa tai vähintään samalla aikavyöhykkeellä.

Toimittajavaatimukset

Toimittajan tulee tarjota tukea vika- ja ongelmatapauksissa. Toimittajan kanssa on kirjoitettava tukisopimus, josta ilmenee vasteajat, tuen laatu ja kohde. Tukisopimuksen on hyvä sisältää rikkoontuvien laitteiden varalaitesopimukset, jolloin saadaan uusi laite rikkoontuneen tilalle mahdollisimman nopeasti. Lisäksi toimittajan on kyettävä tarjoamaan käyttökoulutusta ylläpitäjille.

Tukea tarjoavan toimittajan henkilöstön osaaminen on tarvittaessa pystyttävä todentamaan. Aikaisempi kokemus SCADA-verkoista ja niihin liittyvistä tunkeutumisenesto ja havainnointijärjestelmien käyttöönottoprojekteista on eduksi.

Laitteistovaatimukset

SCADA-ympäristöissä liikennemäärät jäävät järjestelmästä riippuen suhteellisen pieniksi. Merkittävin painoarvo tulee olla laitteiden saatavuudessa. Yhden linjaan kytketyn IDPS-laitteen tai muun komponentin rikkoutuminen ei saa aiheuttaa koko järjestelmään palvelukatkosta. Teknisesti laitteet tulee olla kahdennettavissa. Laitteiden tulee olla myös linjaan kytkettävissä, jolloin haavoittuvuudet voidaan estää aktiivilaitteessa reaaliaikaisesti.

Haavoittuvuuskuvauksien tarkkuus ja laadukkuus on oltava ensiluokkaista käytönvalvontaprotokollien osalta. Virhenegatiivisten osuus on pystyttävä minimoitava laitteiden säätömahdollisuuksilla. Säätöominaisuudet tulee olla skaalautuvat käytettäessä hybridiympäristöä, jotka hyödyntävät isäntä-, verkko- ja poikkeavuusanalysointimekanismeja.

Tunkeutumisenesto- ja havainnointilaitteiden tulee tarjota suojaa myös verkon muille haavoittuville komponenteille, kuten työasemille ja palvelimille. Järjestelmästä voi löytyä osia, joita ei ole mahdollista päivittää normaalin päivitys-syklin mukaisesti näitä ovat mm. käyttöjärjestelmä- ja viruspäivitykset. IDPS-laitteen virtuaalipäivitys, eli tunnistepohjaisten haavoittuvuus- ja viruskuvausten käyttö tulee olla mahdollista.

Laitteiden on tuettava kolmansien osapuolien protokollakuvauksia. Näitä kehittelevät erilaiset organisaatiot, joiden toiminta on yleensä enemmän tai vähemmän kaupallista. Kolmansien osapuolien kuvaukset on ohjelmoitu yleensä avoimen lähdekoodin alustaa käyttäen, mutta voidaan integroida useimpien laitevalmistajien tuotteisiin. Kuvausten avulla voidaan tulevaisuudessa saada tuki myös useimmille pohjoismaissa käytetyille käytönvalvontaprotokollille.

Teollisuusympäristöissä laitteita joudutaan sijoittelemaan vaativiin olosuhteisiin, ja olosuhteet voivat aiheuttaa laitevikoja normaalia useammin. Hankintavaiheessa on kiinnitettävä huomiota laitteiden fyysisiin ominaisuuksiin. [13, s. 261 - 270.]

Operointivaatimukset

Tuotteen on tarjottava keskitetty hallintaympäristö standardeilla suojatuilla ylläpitoprotokollilla. Hallintapolitiikat ym. säännöstöt tulee olla ladattavissa keskitetystä järjestelmästä kullekin kohdelaitteelle. Hallintaympäristön tulee olla skaalautuva tulevaisuuden tarpeisiin. Sensoreiden lukumäärä voi kasvaa, jolloin niiden liittäminen hallintaympäristöön on oltava mahdollista myös tulevaisuudessa.

Ylläpitotunnukset tulee jaotella käytön ja organisaation mukaan roolipohjaisesti. Käyttäjätunnusten tulee olla henkilökohtaisia ja yhteiskäyttöisten tunnusten käyttöä on rajoitettava. Hallintaympäristön on tuettava roolipohjaisia käyttäjäryhmiä, joissa kullekin käyttäjäryhmälle on tarvittaessa eri käyttöoikeudet. Laitteissa tulee olla mahdollisuus käyttää myös ulkopuolista käyttäjätietokantaa, jota vasten käyttäjien tunnistus voidaan suorittaa.

Hallintaympäristön tulee tukea IDPS-laitteiden ryhmäasetuksia, jolloin ylläpitotoimet voidaan tehdä ryhmäkohtaisesti kullekin laiteryhmälle. Hallintajärjestelmästä on saatava muokattavissa olevat raportit tapahtumista ja muista tapahtuneista loukkauksista. Käytettäessä ylemmän tason valvontaratkaisua on IDPS-hallintaympäristön kyettävä lähettämään tapahtumat eteenpäin ylätason valvontajärjestelmälle.

Haavoittuvuustunnisteiden päivitykset tulee voida automatisoida, jolloin saadaan nopea suoja nollapäivän haavoittuvuuksia vastaan. Päivityksistä tulee löytyä myös palautusominaisuus, jolloin voidaan nopeasti palauttaa toimivan järjestelmän asetukset ongelmatilanteissa. Lisäksi laitteisiin kohdistuvien järjestelmä- ja haavoittuvuuskuvausten päivitysten seuraaminen on oltava mahdollista. Laitteistosta tulee saada järjestelmä- ja konfiguraatiovarmistukset kerättyä säännöllisin väliajoin.

4.3 Tunkeutumisen havainnointi- ja estojärjestelmän toteuttaminen

IDPS-järjestelmän käyttöönotto tulee toteuttaa projektiluontoisesti. Projektiorganisaation tehtävä on huolehtia projektin etenemisestä, tavoitteiden saavuttamisesta ja vastuiden määrittelystä. Projektiorganisaatioon on hyvä kuulua asiakas, tässä tapauksessa SCADA-järjestelmän omistaja, laitetoimittaja ja IDPS-palveluntuottaja. Projektin tarkoituksena on tuottaa vaatimusmäärittelyiden mukainen tunkeutumisenesto- ja havainnointijärjestelmä käytönvalvontajärjestelmään.

4.3.1 Esiselvitykset

Uusittavien SCADA-järjestelmien suunnittelu tulee aloittaa jo käytönvalvontajärjestelmän hankinta- ja suunnitteluvaiheessa. IDPS-palveluntuottajan osallistuminen projektikokouksiin tässä vaiheessa on tärkeää. Näin kaikki projektiin osallistuvat tahot saavat tiedon suunnitellusta toteutuksesta. Vanhojen järjestelmien kanssa joudutaan käynnistämään selvitykset alusta, ja kokoamaan projektiorganisaatio uudelleen.

Selvitykset aloitetaan tapauksesta riippumatta SCADA-järjestelmän arkkitehtuurista ja IDPS-järjestelmän vaatimusmäärittelyistä. Arkkitehtuuriselvityksen yhteydessä tulee selvittää myös järjestelmän toiminta pääpiirteittäin. Kerätään lista palvelimista, verkkolaitteista, käyttöjärjestelmistä ja muista oleellisista komponenteista. Komponenttilistan lisäksi on kartoitettava käytettävät tietoliikenneyhteydet ja protokollat. Näin saadaan kokonaiskuva, jonka avulla on helpompi hahmottaa järjestelmän toiminnallisuus. Kartoitus toimii IDPS-arkkitehtuurisuunnittelun pohjana.

Ylemmän tason arkkitehtuurikuvan avulla selvitetään kuinka SCADA-järjestelmä liittyy yrityksen muuhun tietoliikenneverkkoon. Syvyyssuuntaisen suojautumisen periaate ilmenee selkeästi ylätason kuvasta. Mikäli suojautumismallia ei ole käytetty, ja siihen halutaan siirtyä, voidaan käyttöönottaa palomuureja sujausvyöhykkeiden rajoilla. Rajoja ovat mm. Internet, toimistoverkko, laitosverkko, SCADA-verkko ja ala-asemaverkko. Suunnittelua tehdessä on pidettävänä mielessä, että liiketoiminnan kannalta tärkein ja suojattavin kohde on suojausarkkitehtuurin ytimessä.

Jo esiselvitysvaiheessa tulisi tutustua markkinoilla oleviin IDPS-laitevalmistajiin, ja aloittaa alustavat neuvottelut toimittajien kanssa. Neuvotteluiden pohjana toimii vaatimusmäärittely. Ylläpidollisiin tekijöihin tulisi kiinnittää huomiota tässä vaiheessa. Se helpottaa käyttöönottoa, kun suunnitelmat raportoinnin, päivitysten ym. hallinnollisten tehtävien osalta on saatu valmiiksi.

Riskianalyysit

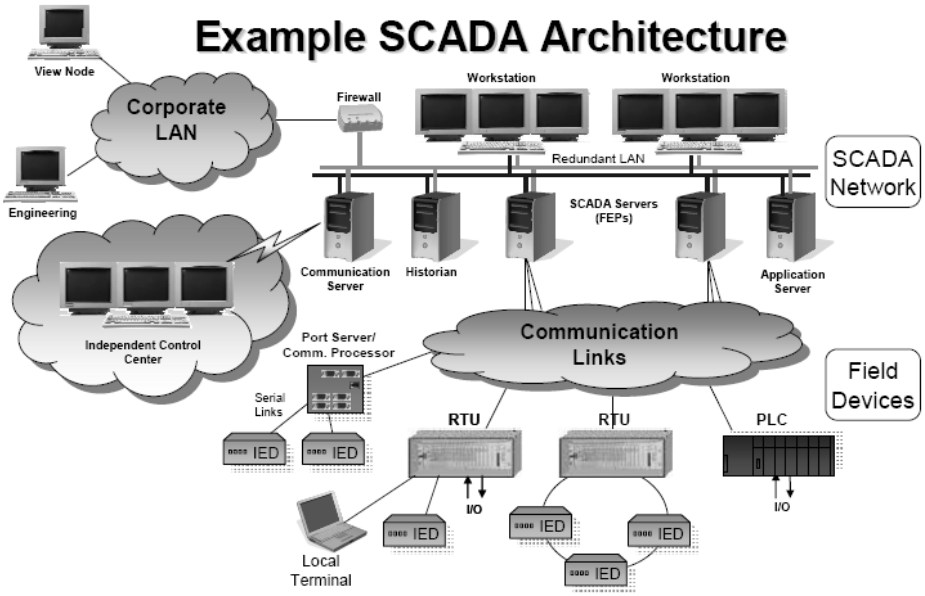
Oleellista IDPS-laitteiden kannalta on niiden sijoittelu. Sijoittelu määrittää käytettävän tekniikan ja suorituskykyvaatimukset laitteistolle. Sijoittelun suunnittelua voidaan helpottaa tekemällä SCADA-järjestelmän tietoliikenneyhteyksistä riskikartoitus. Riskikartoituksessa tulee analysoida uhka ja uhkaan liittyvä tunkeutumisen todennäköisyys ja vaikutus. Analyysi suoritetaan kaikkien SCADA-järjestelmään liittyvien tietoliikenneyhteyksien osalta. Lopputuloksena saadaan dokumentti kriittisimmistä yhteyksistä ja komponenteista, joista tunkeutuminen järjestelmään voisi tapahtua. Riskianalyysissä on hyvä tarkastella myös olemassa olevien prosessien soveltuvuutta IDPS-järjestelmän ylläpitoon ja hallintaan.

4.3.2 Arkkitehtuuri

Arkkitehtuurisuunnittelussa tulee käyttää kartoituksen palvelin- ja komponenttilistaa. Palvelimien osalta listasta selviää käytettävä käyttöjärjestelmä ja palvelinalusta. Isäntäperusteisessa tekniikassa on palvelinkäyttöjärjestelmään asennettava erillinen ohjelma, joka tutkii paikallisesti prosesseja ym. resursseja. Näin tunkeutuminen voidaan havaita jo palvelinkäyttöjärjestelmässä. Verkkoperusteisessa tekniikassa analysoidaan SCADA-verkon liikennettä verkkotasolla. Verkkotasolla voidaan suorittaa tunnisteisiin perustuvaa havainnointia ja estää haitallinen liikenne pääsemästä verkkoon. Samalla tasolla voidaan analysoida myös verkon käyttäytymistä ja havaita poikkeavuuksia liikennevuosta. Kokonaisvaltaisesti suojauduttaessa on hyvä turvautua jopa kaikkiin kolmeen tunnistustekniikkaan.

Yleensä käytönvalvontajärjestelmien valvonta- ja palvelinkeskuksissa on kaksi lähiverkkoa, jotka varmentavat toinen toisiaan. Tällä tavoin laitevalmistajat pyrkivät takaamaan järjestelmän korkeamman saatavuuden. Järjestelmäarkkitehtuurista saattaa kuitenkin löytyä heikkouksia, yksittäiset aktiivilaitteet ja niitä vastaavat solmupisteet on hyvä selvittää, sekä kahdentaa tarpeen mukaan.

SCADA-verkkojen välillä on kuitenkin reititettävä verkkoliikennettä, joka tuo mukanaan vaatimukset liikenteen rajoittamiselle ja monitoroinnille. Palomuureissa tulisi pyrkiä hyödyntämään tunkeutumisenesto- ja havainnointitekniikoita sekä niiden tuomia muita tietoturvaominaisuuksia mahdollisuuksien mukaan. Kuvassa 23 on SCADA-verkkoarkkitehtuuri, josta on havaittavissa kaikki oleelliset komponentit järjestelmän toiminnallisuuden kannalta.



Kuva 23. SCADA-järjestelmäarkkitehtuuri [20]

Arkkitehtuurikuvassa 23 on kommunikaatiolinkit päätetty suoraan FEP (Front End Processor) -palvelimille. Todellisuudessa yhteydet on hyvä eriyttää palvelimista, jolloin RTU ym. kenttäyhteydet päätetään omaan valvottuun palomuurisegmenttiin. Samaa ajattelumallia tulisikin soveltaa kaikkien ulkoisten yhteyksien osalta. Järjestelmän kannalta merkittävimmät palvelimet ovat yhteys-, historia-, kommunikaatio- ja sovelluspalvelimet. Näissä kohteissa on suositeltavaa käyttää isäntäperusteista tunnistusta muiden tunnustustekniі-

koiden lisäksi. Käytettäessä erillistä linjaan kytkettyä IDPS-laitetta, on suositeltavaa sijoittaa se palomuurilla suojattavien segmenttien eteen.

Mikäli käytönvalvontaprotokolla on esimerkiksi IEC104, ei yleisimmistä IDPS-laitteista löydy kuvauksia protokollaan ja protokollakuvausten tuomat suojausominaisuudet ovat tässä tapauksessa mitättömät. IDPS-laite voi kuitenkin suojata SCADA-komponentteja muilla tietoturvaominaisuuksilla. Palvelimissa on usein monia varusohjelmia, joiden päivityksistä ei huolehdita aktiivisesti. Virtuaali-päivitysominaisuudet ovat tässä tapauksessa hyödyllisiä, ne suojaavat SCADA-verkkoa nollapäivän hyökkäyksiltä. Tunnistepäivityksillä voidaan suojata verkkoa myös tunnetuilta viruksilta ja käyttöjärjestelmähaavoittuvuuksilta.

Yrityksellä voi olla useita SCADA-verkkoja, ja hallintalaitteiston tulisi kyetä palvelemaan useampien verkkojen IDPS-laitteita. Tämän vuoksi hallintalaitteisto tulee sijoittaa olemassa olevaan laajempaan hallintaverkkoon, eikä ainoastaan SCADA-verkon sisäpuolelle.

Käytönvalvontajärjestelmän ulkopuolelta suoraan sisään tulevat yhteydet tulisi minimoida. Suositeltavaa on muodostaa yhteydet käytönvalvontajärjestelmästä ulospäin. Yhteyksien toteutusperiaatteena tulisikin käyttää juuri tähän pohjautuvaa ajattelumallia, kuitenkin siten, että suorat Internet-yhteydet estetään täysin järjestelmän sisältä.

4.3.3 Tuotteen valinta ja hankinta

Projektin aloitusvaiheessa, alustavissa neuvotteluissa laitetoimittajien kanssa, on saatu jo jokin näkemys markkinoilla olevista teknologioista ja laitevalmistajista. Jos kaikki laitevalmistajat ovat kyvykkäitä toimittamaan määrittelyiden mukaisen konseptin, on valintaperusteissa käytettävä muita metodeja. Voidaanko esim. nykyiseen palomuurien tai muiden laitteiden hallintaympäristöön lisätä hankittavat IDPS-laitteet. Näin voidaan vähentää hankintakustannuksia huomattavasti. Samoin henkilöstöllä voi olla osaamista vanhan ympäristön ylläpidosta, näin suurimmilta koulutuksilta voidaan välttyä. Luultavammin myös vanha hallintaympäristö on liitetty osaksi ylläpito- ja hallintaprosesseja, jolloin käyttöönotto helpottuu.

Tuotteen lopullinen valinta perustuu vaatimusmäärittelyn reunaehtoihin. Hankintaan tulee soveltaa kunkin yrityksen omia hankintasäädöksiä ja lakeja.

4.3.4 Käyttöönotto

Laitteiden asennus ja käyttöönotto voidaan hankkia ”avaimet käteen” -periaatteella. Kaikilla laitetoimittajilla ei välttämättä ole tarvittavaa SCADA osaamista, joten yrityksen omia resursseja tullaan joka tapauksessa tarvitsemaan. Omia resursseja sitoo myös se, että asennuksen suorittava yritys ei voi integroida järjestelmää ylläpidollisiin prosesseihin. Integrointi on jokaisen yrityksen tehtävä itse. Toteutettaessa IDPS-järjestelmää itsenäisesti, on hyvä sopia tukikanavat kuntoon ennen asennusten aloittamista. Ennalta määritetyllä tukiorganisaatiolla taataan nopea vasteaika käyttöönoton yhteydessä ilmenevissä ongelmatilanteissa.

Tuotannossa olevan käytönvalvontajärjestelmän käyttökatkot tulee minimoida ja IDPS-järjestelmän käyttöönoton aiheuttamat katkokset on oltava hallittuja. Järjestelmä tuleekin ensin testata testiympäristössä, joka mukailee mahdollisimman paljon tuotannossa olevaa järjestelmää. Huolellisesti suunniteltu testaus onkin käyttöönoton merkittävin vaihe. Testeissä suurimmat ongelmat saattavat esiintyä isäntäperusteisen tekniikan agenttien asennuksessa ja käyttöönotossa. Palvelinohjelmistot ovat monimutkaisia ja lähes ainoa asiantuntemus on ohjelmistotoimittajalla. Suositeltavaa on rajoittaa muiden ohjelmistojen toimintaa palvelimella, ja jättää SCADA-järjestelmän sovellukset ilman tarkempaa tutkimista. Tämä takaa SCADA-ohjelmistokomponenttien toimivuuden ensisijaisesti.

Testausvaiheessa on testiympäristössä hyvä asettaa käyttöön kaikki laitteiden tarjoamat suojaukset. Mikäli testausvaiheessa havaitaan ongelmakohtia, on tässä vaiheessa helppo lähteä poistamaan suojauksia systemaattisesti, kunnes järjestelmän normaalitoiminta palautuu. Testiympäristöstä siirryttäessä tuotannon asennukseen on suojaukset pidettävä yhtenäisinä, jotta vältytään turhilta tietoturva-aukoilta. Testauksen aikana tulee IDPS-laitteiden säätöominaisuuksilla pyrkiä minimoimaan virhenegatiivisten osuus liikenteestä. Tästä yleensä seuraa virhepositiivisten tapahtumien kasvu, joka työllistää ylläpitäjiä.

Asennuksen jälkeen tulee IDPS-järjestelmä integroida osaksi yrityksen ylläpitoprosesseja. Järjestelmä pysyy relevanttina hankintavaiheen jälkeen vain hetken jonka jälkeen se rapistuu, mikäli integrointia ei tehdä. Laitteita on valvottava, kehitettävä ja huollettava. Niiden elinkaaresta on pidettävä huolta, jotta järjestelmä palvelee organisaatioita mahdollisimman pitkään.

5 YHTEENVETO

Työssä tutustuttiin nykyaikaisten käytönvalvontajärjestelmien komponentteihin, arkkitehtuuriin ja liikennöintiprotokolliin. Lisäksi tutkittiin markkinoilla olevien tunkeutumisenesto ja havainnointilaitteiden soveltuvuutta infrastruktuuria ylläpitävien käytönvalvontajärjestelmien käyttöön. Työn ohella tuotettiin Helsingin Energialle IDPS-laiteympäristön vaatimusmäärittelyt ja järjestelmän käyttöönoton toteutussuunnitelma.

Käytönvalvontajärjestelmiin kohdistuvat tietoturvauhat ovat samanlaisia kuin muissakin tietoverkoissa. Kohdistetut hyökkäykset infrastruktuuria ylläpitäviin järjestelmiin ovat lisääntyneet tietoverkkojen verkottumisen myötä yhä enemmän. Järjestelmät eivät ole suljettuja kuten voidaan kuvitella, ja tietoa on pystyttävä siirtämään eri käyttäjien ja järjestelmien välillä saumattomasti. Nykypäivän toteutukset vaativatkin suunnitelmallista palomuurisegmentointia ja liikenteen suodatusta tietoverkkojen välillä. Tietomurroilta voidaan välttyä henkilöstön tietoturvakoulutuksella sekä huolellisella arkkitehtuurisuunnittelulla. Lisäksi ottamalla käyttöön erilaisia teknisiä tietoturvalaitteita, voidaan pienentää riskejä. Tietoturvalaitteiden tarjoamia ominaisuuksia tulee hyödyntää mahdollisimman monipuolisesti, jotta voidaan vastata nykypäivän tietoturvahaasteisiin.

Markkinoilla olevien tunkeutumisenesto- ja havainnointilaitteiden tarjoamiin SCADA-protokollakuvauksiin tulee suhtautua varauksella. Käytönvalvontajärjestelmät ovat niin liiketoimintakriittisiä, että protokollakuvausten tarjoama todellinen hyöty jää vähäiseksi, jos verrataan liiketoiminnalle kohdistuvaa riskiä protokollakuvausten käytöstä. Samoin Pohjoismaissa yleisesti käytössä oleviin protokolliin ei löydy kuvauksia, jolloin varsinaisesta SCADA-protokollatuesta saatavat hyödyt jäävät olemattomaksi. Kolmansien osapuolten kirjoittamien protokollakuvausten ansiosta voidaan tulevaisuudessa saa-

da protokollatuki myös Pohjoismaissa käytetyille SCADA-protokollille, mikäli laitevalmistajat mahdollistavat näiden lisäämisen laitteisiin.

IDPS-laitteet kuitenkin tarjoavat muilla tietoturvaominaisuuksillaan huomattavia parannuksia käytönvalvontaverkkojen tietoturvan kohottamiseksi. SCADA-järjestelmien laitteiden päivittämisestä ei aina huolehdita aktiivisesti, ja tunkeutumisenesto- ja havainnointilaitteet tarjoavatkin erityisesti tähän ongelmaan ratkaisun virtuaalipäivitysominaisuuksilla. IDPS-laitteiston käyttöönotto ei yksistään poista tietoturvariskejä. Virtuaalipäivitysten lisäksi on käytönvalvontajärjestelmän komponenttien todellisista päivityksistä huolehdittava säännöllisesti. Julkaistut haavoittuvuudet sovelluksissa ym. komponenteissa tulee päivittää, ja myös laitetoimittajien on ymmärrettävä nämä seikat. Tulevaisuudessa laitevalmistajat luultavasti integroivatkin järjestelmien asennusvaiheessa omia tunkeutumisenhavainnointi- ja estojärjestelmiä SCADA-verkkoihin.

Vaatimusmäärittelyiden tärkeys aloitusvaiheessa on merkittävä, ja siihen tulee panostaa huomattavasti. Se määrittelee teknisen toteutuksen ja toiminnallisuuden reunaehdot koko IDPS-laitteistoarkkitehtuurille, ja määrittelyt voidaan tehdä hyvinkin moniulotteisesti. Asennus ja käyttöönotto tulee suorittaa projektimaisesti ja integroida projektin päätteeksi ylläpito- ja hallintaprosesseihin.

Tietoverkkojen monimutkaisuuden ja verkottumisen myötä onkin vain ajan kysymys milloin infrastruktuuria ylläpitävä järjestelmä joutuu tietomurron kohteeksi Suomessa. Tulevaisuudessa yritysten on määriteltävä entistä tiukemmat vaatimukset järjestelmätoimittajille, joiden on myös kyettävä vastaamaan yritysten vaatimuksiin. Tunkeutumisenesto- ja havainnointijärjestelmien käyttöönotolla voidaan pienentää käytönvalvontajärjestelmiin kohdistuvia riskejä.

VIITELUETTELO

[1] Suomen Automaatioseura Ry, Teollisuusautomaation tietoturva. *Verkottumisen riskit ja niiden hallinta*. Helsinki: Suomen Automaatioseura Ry Turvallisuusjaosto. 2005

[2] Viestintäministeriö. *Haavoittuvuudet 2008* [verkkodokumentti, viitattu 14.9.2008]. Saatavissa: http://www.cert.fi/haavoittuvuudet.html

[3] Shaw, William T, *Cybersecurity for SCADA Systems*. Tulsa, Oklahoma: PennWell Corporation. 2006.

[4] University of Illinois, Illinois Security Lab. *IEC 61850 - Communication Networks and Systems in Substations* [verkkodokumentti, viitattu 13.10.2008]. Saatavissa: http://seclab.uiuc.edu/docs/iec61850-intro.pdf

[5] University of Illinois, Illinois Security Lab. *Overview of TASE.2/ICCP* [verkkodokumentti, viitattu 13.10.2008]. Saatavissa: http://seclab.uiuc.edu/docs/iccp-intro.pdf

[6] DNP User Group. *A DNP3 Protocol Primer* [verkkodokumentti, viitattu 20.10.2008]. Saatavissa: http://www.dnp.org/About/DNP3%20Primer%20Rev%20A.pdf

[7] DNP User Group. *Overview of the DNP3 Protocol* [verkkodokumentti, viitattu 20.10.2008]. Saatavissa: http://www.dnp.org/About/Default.aspx

[8] Electronic Systems Group, Department of Electrical Engineering, Indian Institute of Technology. *Comparison of protocols used in remote monitoring: DNP 3.0, IEC870-5-101 & Modbus* [verkkodokumentti, viitattu 27.10.2008]. Saatavissa: www.ee.iitb.ac.in/~esgroup/es_mtech03_sem/sem03_paper_03307905.pdf

[9] SINTEF Energy Research, *ELCOM-90 documentation, report list* [verkkodokumentti, viitattu 5.11.2008]. Saatavissa: http://www.sintef.no/upload/Energiforskning/Energisystemer/ELCOM%2090-2.pdf

[10] SINTEF Energy Research, *Securing Elcom-90 with TLS* [verkkodokumentti, viitattu 5.11.2008]. Saatavissa: http://www.sintef-norge.no/upload/Energiforskning/Energisystemer/ELCOM%2090.pdf

[11] Modbus-IDA, *Modbus application protocol specification V1.1b* [verkkodokumentti, viitattu 5.11.2008]. Saatavissa: http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

[12] Modbus-IDA, *Modicon Protocol Reference Guide* [verkkodokumentti, viitattu 5.11.2008]. Saatavissa: http://www.modbus.org/docs/PI_MBUS_300.pdf

[13] Earl, Carter – Jonathan, Hogue. *Intrusion Prevention Foundamentals*. USA, Indianapolis: Cisco Press. 2006.

[14] National Institute of Standars and Technology, *Guide to Intrusion Detection and Prevention Systems (IDPS)* [verkkodokumentti, viitattu 26.11.2008]. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[15] Gartner Inc., *Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08* [verkkodokumentti, viitattu 16.2.2009]. Saatavissa: http://mediaproducts.gartner.com/reprints/tippingpoint/154849.html

[16] University of Maryland, *Waterfall model* [verkkodokumentti, viitattu 14.3.2009] Saatavissa: http://www.cs.umd.edu/class/spring2003/cmsc838p/Process/waterfall.pdf

[17] fcSovelto ITILv3-Kurssi, *ITILv3 Foundation*. Helsinki: fcSovelto. 2009.

[18] Digital Bond, *SCADA IDS Signatures* [verkkodokumentti, viitattu 16.3.2009]. Saatavissa: http://www.digitalbond.com/wiki/index.php/SCADA_IDS_Signatures

[19] U.S Department of Energy, *Networked Embedded Control for Cyber Physical Systems* [verkkodokumentti, viitattu 23.3.2009]. Saatavissa: http://www.truststc.org/scada/papers/paper34.pdf