EN Kulunvalvontastandardi

SFS-EN 60839-11-1 standardin käytön esteet ja toiminnallisuus-vaatimusten sisällön avaaminen

Turvallisuusjohdon koulutusohjelma

Kehitysprojektin raportti

Petri Sääskilahti

UTC Fire & Security Suomi Oy

Vantaa 1.5.2018

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Vuonna 2013 julkaistiin uusi EN Standardi kulunvalvontajärjestelmistä ja niiden järjestelmä- ja komponenttivaatimuksista. Se korvasi vanhan 1996 julkaistun standardin.

Standardia ei yleisesti käytetä suunnittelussa ja järjestelmien hankinnoissa. Tässä projektityössä selvitetään syitä, miksi näin on. Minkälaisia ongelmia sen käytössä on ja miten sen käyttöä voitaisiin tehostaa.

Projektityössä käsitellään vaatimusmäärittelyiden tavoitteet ja tarvittaessa tarkennetaan niiden sisältöä. Projektityön tavoitteena on auttaa kiinteistöjen omistajia, suunnittelijoita ja konsultteja käyttämään enemmän standardia ja ymmärtämään sen sisältöä.

.

Sisältö

1 Johdanto

Standardi ”sähköiset kulunvalvontajärjestelmät, järjestelmävaatimukset ja komponenttivaatimukset”, on yleiseurooppalainen standardi ja on hyväksytty kaikissa Cenelec komitean jäsenmaissa.

Standardin avulla voidaan määritellä ne kulunvalvontajärjestelmän vähimmäisvaatimukset ja toiminnallisuudet, jotka ovat välttämättömiä kiinteistön turvallisuudelle. Standardissa tarkastellaan toiminnallisuuksia usealla tasolla kiinteistön käyttötarkoituksen ja yrityksen toiminnan mukaan. Kulunvalvontajärjestelmien vaatimukset ovat luokiteltu neljään eri luokkaan.

SFS-EN 60839-11-1standardin käyttö sellaisenaan on käyttäjälle vaativa ja käyttö vähäistä. Suomenkielinen teksti ei kaikilta osin vastaa vakiintuneita termejä kulunvalvontajärjestelmistä. Parhaan tuloksen saa kun vertaa standardin englanninkielistä alkuperäistä tekstiä ja käännöstä. Standardissa on molemmat sekä suomennettu että alkuperäinen englanninkielinen teksti peräkkäin. Tämä toisaalta hankaloittaa dokumentin käyttöä

Standardista on myös vaikea löytää käyttäjälle tärkeitä määrittelyjä, taulukoita on paljon ja niiden painoarvoa on hankala arvioida. Projektityössä selitetään vaatimusmäärittelyjen olennaiset osat. Tämän perusteella käyttäjä painottaa standardista heitä eniten kiinnostavia kohtia. Tilanteesta riippuen käyttäjä voi vaatia koko standardin noudattamista koko järjestelmän osalta tai vaatia noudatettavaksi toiminnallisuuksia, jotka ovat heille erityisen tärkeitä.

2 Projektityön tavoite

Työssä käsitellään erityisesti standardin kulunvalvontajärjestelmän suorituskyvyn toiminnallisia vaatimuksia (Standardin kohta 6). Jokaisen kohdan toiminnallinen tarkoitus selitetään käyttäen vakiintuneita termejä. Työssä sivutaan ympäristöolosuhteita (Standardin kohta 7) ja testausmenetelmiä (Standardin kohta 8), mutta niihin ei esitetä merkittäviä lisäyksiä.

Käsiteltyihin kohtiin esitetään myös parannus- tai lisämäärityksiä.

Projektityön yhtenä tavoitteena on saada standardi tunnetuksi ja lisätä sen käyttöä. Valitettavasti usein turvallisuusjärjestelmiä suunnitellaan ja valitaan vajavaisin määrittelyin. Mikäli standardia hyödynnettäisiin enemmän, varmistettaisiin, että järjestelmä täyttää sille osoitetut vaatimukset.

Tutkimusmenetelmänä on empiirinen tutkimus. Empiirinen tutkimusmenetelmä perustuu havainnointiin ja niistä tehtäviin kokemusperäisiin päätelmiin. (Jyväskylän yliopisto, 2015.)

Projektityön tekijällä on 20 vuoden kokemus sähköisistä turvallisuusjärjestelmistä, joista viimeiset 10 vuotta tekijä on toiminut Lenel OnGuard järjestelmän Suomen teknisenä asiantuntijana ja järjestelmäkouluttajana. Standardin englanninkielinen teksti vastaa teknistä sanastoa, jota käytetään Yhdysvalloissa käytettävissä järjestelmäkuvauksissa ja dokumentaatioissa. Standardin sisältöä voi siten tulkita luotettavasti, vaikka Suomenkielisen tekstin sisältö jää joissain tapauksessa epäselväksi.

Koska standardi on tekijänoikeuksien alainen ja maksullinen tuote, tässä työssä on vähäinen määrä lainauksia standardista Kopiosto Ry opinnäytetyön lupaehtojen mukaisesti. Projektityön täysi hyödyntäminen vaatii siis standardin hankintaa.

3 Standardin nykyinen käyttö

Toisin kuin rikosilmoitinjärjestelmissä, on EN kulunvalvontastandardin hyödyntäminen hankkeiden vaatimusluokituksessa vähäistä. Projektityön tekijä on vain muutamassa hankkeessa kohdannut viittauksia ko. standardiin. Niissäkin vain yleisviittauksella tai korkeintaan luokka 3 vaatimuksiin.

Kulunvalvontajärjestelmien toimittajat eivät myöskään hanki järjestelmälle EN standardin yhteensopivuussertifikaatteja tarkastuslaitoksilta. Sertifikaatit ovat kalliita ja niitä pitäisi päivittää versioittain. Koska sertifikaatteja ei vaadita, vaatimuksenmukaisuus on toimittajan lausuntojen varassa. Tämän lisäksi tilaaja voi pyytää testauspöytäkirjaa standardin määrityksen täyttämisestä.

EN standardin käytöstä on keskusteltu Finanssialan asiantuntijan kanssa, mutta näköpiirissä ei ole, että kulunvalvontastandardin noudattamista vaaditaan esimerkiksi vakuutusehdoissa tai finanssialan yrityksissä. (Aku Pänkäläinen, 2013.)

Mikään laki tai asetus ei vaadi standardin noudattamista turvallisuusjärjestelmien hankinnassa. Myöskään Katakri ei velvoita noudattamaan standardia viranomaiskäytössä olevien tilojen suojaamisessa. (Puolustusministeriö, 2015)

Standardi on kuitenkin ainoa kulunvalvontajärjestelmän määrittelyyn liittyvä yleinen dokumentti, jossa on määritelty keskeiset kohdat toiminnallisuuksille, jotka ovat tärkeitä luokiteltaessa turvallisuustasoja kiinteistön kulunvalvontajärjestelmälle.

4 Standardin eri versiot

Kulunvalvontajärjestelmistä on vuonna 1996 julkaistu standardi EN 50133-1, johon edelleen viitataan hankkeissa. Vuonna 2013 julkaistu EN 60839-11-1 korvaa kuitenkin sen, eikä vanhaa EN 50133 standardia enää tulisi käyttää.

EN 60839-11-1 standardi on vahvistettu 28.10.2013.

Suomenkielisen version päivämäärä on 9.12.2013. Riitatapauksissa ratkaisee englanninkielinen versio.

Suomenkieliseen tekstiin on tehty korjaus 21.8.2015 (AC:2015)

EN 60839-11-1 standardiin on julkaistu korjaus 14.9.2015

Korjaus sisältää tekstin ”Supersedes EN 50133-1:1996 and EN 50133-2-1:2000".

Viimeisin versio joka sisältää molemmat korjaukset on SFS verkkokaupassa pdf dokumentti 1489575930689_6

Standardi on ladattavissa SFS verkkokaupassa. Hinta 119,41 €.

SUOMEN STANDARDISOIMISLIITTO SFS

SESKO ry

https://sales.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID2/6/240870.html.stx

Lisäksi SFS verkkokaupassa on saatavissa englanninkielinen versio.

Standardiin liittyy olennaisena osa 11-2: Sähköiset kulunvalvontajärjestelmät – Soveltamisohjeet (SFS-EN 60839-11-2). Se sisältää järjestelmän

suunnitteluun, asennukseen ja ylläpitoon liittyvät asiat. Tätä standardia ei kuitenkaan käsitellä tässä projektityössä.

5 Standardin hyödyntäminen

5.1 Missä standardia voidaan käyttää?

Standardia voidaan käyttää tarjouspyyntöjen vaatimusmäärittelyssä, yrityksen sisäisessä tilaturvallisuusmäärittelyssä ja hankesuunnittelussa.

Hankemäärittelyssä voidaan esimerkiksi vaatia, että järjestelmän tulee täyttää luokan 4 pakolliset vaatimukset Standardin kohtiin 6.2- 6.7. Sisäisessä määrittelyssä voidaan omat tilat määrittää luokkiin 1-4 ja siten määritellä kulunvalvonnan vähimmäisvaatimukset.

5.2 Mitä standardista puuttuu?

Standardista puuttuu määrittelyjä, joita on hyvä korjata lisätiedoilla. Sellaisenaan se ei käy esimerkiksi kulunvalvontajärjestelmän tarjouspyyntöasiakirjan liitteeksi.

Esimerkiksi salaustekniikoita ei mainita, ei lukijoiden, kulkukorttien eikä siirtoteiden osalta.

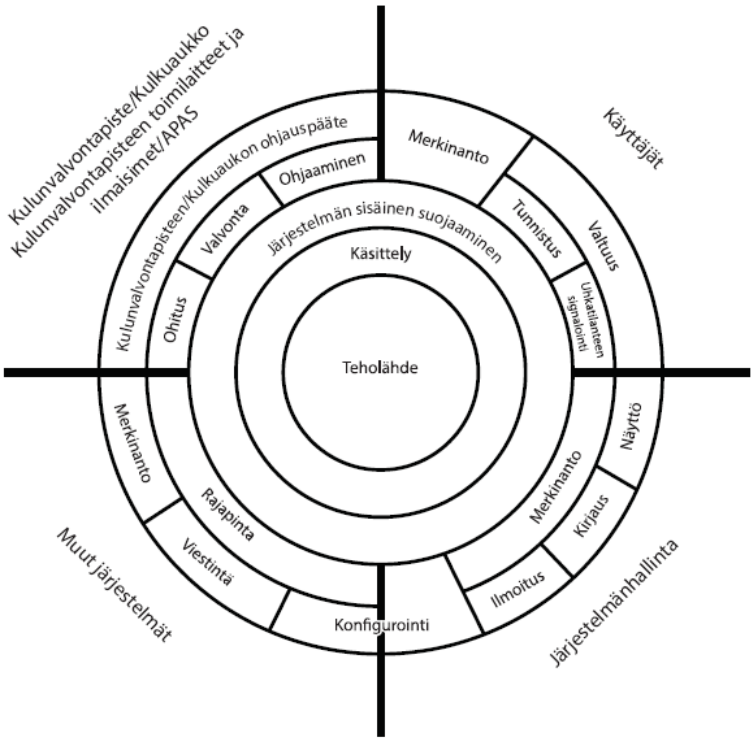
On erityisen tärkeää määritellä mitä kulkukorttiteknologiaa käytetään, esim. DesFire EV2. Muuten koko järjestelmän suojaustaso heikkenee oleellisesti. On huomattava, että teknologia on kehittynyt viidessä vuodessa merkittävästi. Samoin aikaisemmin turvallisena pidetyt teknologiat on murrettu.

6 Standardin vaatimusten käsittely

6.1 Käsitemallit

Standardissa kulunvalvontajärjestelmä on jaettu toiminnallisesti eri lohkoihin: käsittely (A), viestintä (B), konfigurointi (ohjelmointi) (C), kulunvalvontapisteen ohjauspääte (D), tunnistus (E), merkinanto (F), uhkatilanteen signalointi (G), rajapinnat muihin järjestelmiin (H), järjestelmän sisäinen suojaus (I), teholähde (J), käyttöliittymä (K):

Suorituskyvyn määrityksissä (Standardin kohdat 6) on käsitelty vaadittavat toiminnallisuusvaatimukset luokittain. Lohkokaaviossa (Kuva2) toiminnallisuudet on merkitty kirjaimin. Kuitenkaan standardissa ei viitata näihin numeroituihin lohkoihin. Taulukosta (Taulukko 1) voidaan hakea lohkoon liittyvä toiminnallisuusvaatimus.

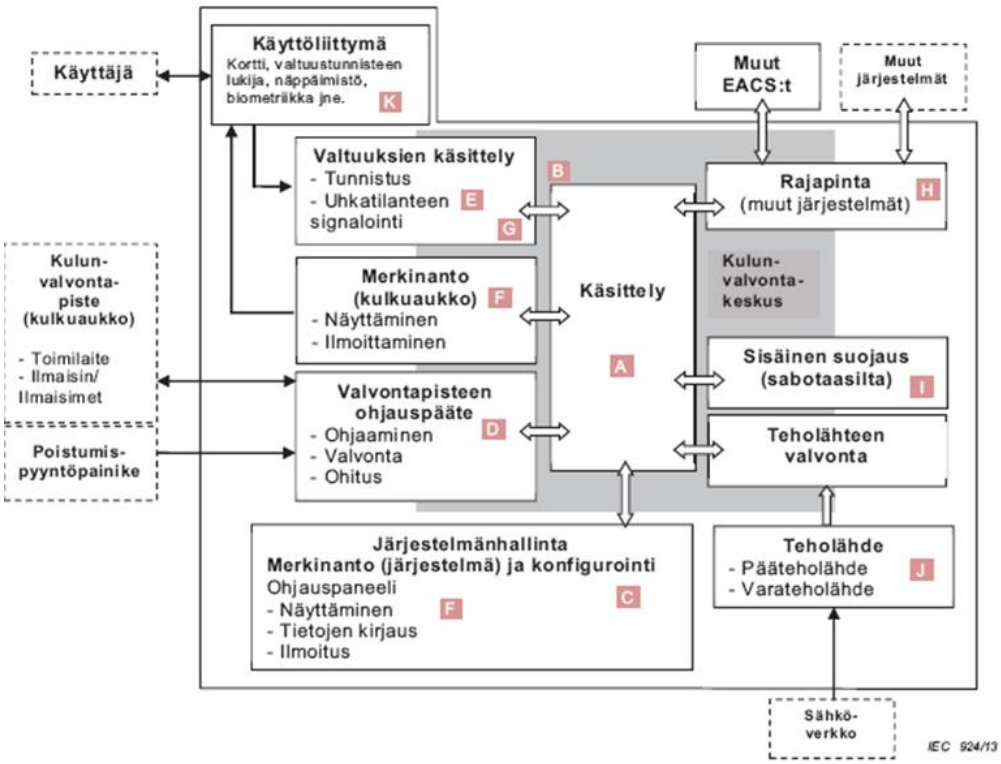


Kuva 1 Käsitteet kehämallissa (Suomen Standardoimisliitto SFS, 2013, 42)

Lohkojen ja vaatimusmäärittelyn vastaavuus:

Taulukko 1

Toiminnallisuusvaatimukset standardissa	Kuvan lohko
6.2 Kulunvalvontapisteen ohjauspäätteen vaatimukset	D
6.3 Ilmoittaminen ja merkinanto	F
6.4 Tunnistus	E
6.5 Uhkatilanne	G
6.6 Ohitus (valvomosta)	K, D
6.7 Viestintä	A
6.8 Sisäinen suojaus	I
6.9 Teholähde	J



Kuva 2 Käsitemallit (Suomen Standardoimisliitto SFS, 2013, 44)

6.2 Luokittelu

Standardin sisältämä tilaluokitus perustuu kiinteistön käytön vaatimaan turvallisuustasoon. Tämä on karkea jako 1-4 luokkaan, mutta asettaa vaatimustason järjestelmälle todennäköisesti oikealle tasolle.

Vaikka ei ole välttämätöntä asettaa luokkaa 4 jokaiselle osa-alueelle vaatimuksesi, kulunvalvontajärjestelmä on kuitenkin kokonaisuus, jolloin vaatimusmäärittely koskee koko järjestelmää. Jos käytetään erillisiä järjestelmiä eri kiinteistöissä, voidaan käyttää eri tasoja eri järjestelmissä.

Nykyaikaiset kulunvalvontajärjestelmät skaalautuvat usean eri käyttäjän ja kiinteistöjen kokonaisuuksiksi. Siksi hallinnallisesti on hyvä käyttää yhtä ohjelmisto- ja hallintajärjestelmää koko yrityksen osalta mikäli se on mahdollista.

7 Standardin toiminnallisuusvaatimusten käsittely

7.1 Luokittelumetodologia ja toiminnallisuudet – Suojaustasojen lukumäärän määrittäminen

Luokkien jako noudattaa tilan suojaustarpeen vaatimuksia riskitason, tiloissa säilytettävän tiedon, tunkeutujan osaamisen (motiivin) ja esimerkkien perusteella.

Luokat 1-2 ovat matalan turvallisuuden kohteita. Näissä ei yleensä käytetä hyväksi standardin vaatimusmäärittelyjä. Järjestelmät tehdään käytännössä sähköurakoinnin yhteydessä.

Luokka 3 käsittää suurimman osan suunnittelua ja määrittelyä vaativista kohteista, joiden hankkeissa yleensä on turvasuunnittelija mukana.

Luokka 4 on korkean tason kohteita, joissa turvajärjestelmien suunnittelussa on eniten hyötyä standardin määrittelyistä. Näissä kohteissa käyttäjä itse määrittelee järjestelmän ominaisuuksia ja valvoo toteutusta testein.

Tässä projektityössä keskitytään erityisesti luokan 4 korkean luokan turvallisuutta vaativiin kohteisiin ja niiden pakollisiin vaatimuksiin.

Taulukko 2 Luokkien jaottelu (Suomen Standardoimisliitto SFS, 2013, 45)

Luokka	1	2	3	4
Riskitaso	Matala	Matala tai kohtalainen	Kohtalainen tai korkea	Korkea
Käyttö	organisatoriset seikat, vähäarvoisen omaisuuden suojaus	organisatoriset seikat, vähäarvoisen tai kohtalaisen arvokkaan omaisuuden suojaus	ei juuri organisatorisia seikkoja, kohtalaisen arvokkaan tai hyvin arvokkaan liike-omaisuuden suojaus	pääasiassa hyvin arvokkaan kaupallisen tai elintärkeän infrastruktuurin suojaus
Tunkeutujien/ Hyökkääjien taito/ tietämys	vähäiset taidot, vähäinen kulunvalvontajärjestelmien tuntemus, ei valtuustunniste- tai IT-teknologioiden tuntemusta vain vähän varoja käytettävissä hyökkäyksiin	kohtalaiset taidot, kohtalainen kulunvalvonta-järjestelmien tuntemus, vähäinen valtuustunniste- ja IT-teknologioiden tuntemus vähän tai kohtalaisesti varoja käytettävissä hyökkäyksiin	hyvät taidot, hyvä kulunvalvonta-järjestelmien tuntemus, kohtalainen valtuustunniste- ja IT-teknologioiden tuntemus kohtalaisesti varoja käytettävissä hyökkäyksiin	erittäin hyvät taidot, erittäin hyvä kulunvalvonta-järjestelmien tuntemus, hyvä valtuustunniste- ja IT-teknologioiden tuntemus suuret varat käytettävissä hyökkäyksiin
Tyypillisiä esimerkkejä	hotelli	toimistot, pienet liikeyritykset	teollisuus, hallinto, finanssiala	erittäin arkaluonteiset alueet (sotilaskohteet, hallinto, tutkimus- ja kehitysosastot, elintärkeät tuotantoalueet)

7.2 Kulunvalvontapisteen ohjauspäätettä koskevat vaatimukset

Kohdassa määritellään oven aukiohjauksen ajat, valvonnat, eri kulkusäännöt ja tilatietojen valvonnat.

Suurin osa vaatimuksista on yleisesti käytössä kaikissa kulunvalvontajärjestelmissä. Luokkaan 4 vaaditaan kuitenkin ajastettu APB, pehmeä ja kova APB sekä kahden miehen sääntö. Näitä ei ole enää peruskulunvalvontajärjestelmissä, mutta ovat tärkeitä ominaisuuksia kun valvotaan kaksisuuntaisilla ovilla varustettuja tiloja, kuten konesaleja.

Taulukko 2 Standardin sivut 50 ja 52

A 1-5 Oven aukiolon ja ohjauksen vaatimukset.

B 5-19 Kulkusuuntien, kaksipuoleisten ovien sekä takaisinpaluun (APB; Anti Pass Back) vaatimukset

C 20-23 Oven aukiolon ajan valvonta

D 24 Signaalit

Pakollisia vaatimuksia on 13 kpl luokassa 4.

7.3 Ilmoittamista ja merkinantoa koskevat vaatimukset

Kohdassa määritellään järjestelmän ilmoitukset sallitusta ja hylätyistä kuluista. Ilmoitukset tehdään paikallisesti ovella, yleensä lukijan ledeillä ja summerilla.

Järjestelmän ohjelmisto tulee näyttää kaikki tapahtumat, niiden syyt sekä kirjata tapahtumat lokiin (tietokantaan) myöhempää raportointia varten. Lisäksi määritellään milloin hälytykset kirjataan ja kuitataan.

Vaatimuksissa on merkittävä määrä ja kaikkien täyttäminen osalla järjestelmillä on vaativaa. Kaikkien kenttälaitteiden tulisi mm. raportoida virtalähteen vikatilanteesta sekä lukijan yhteyden katkeamisesta, jolloin lukija tulisi olla kytketty OSDP liitännällä. Wiegand liitäntäisissä lukijoissa ei ole yleensä merkinantoa yhteyden katkeamisesta.

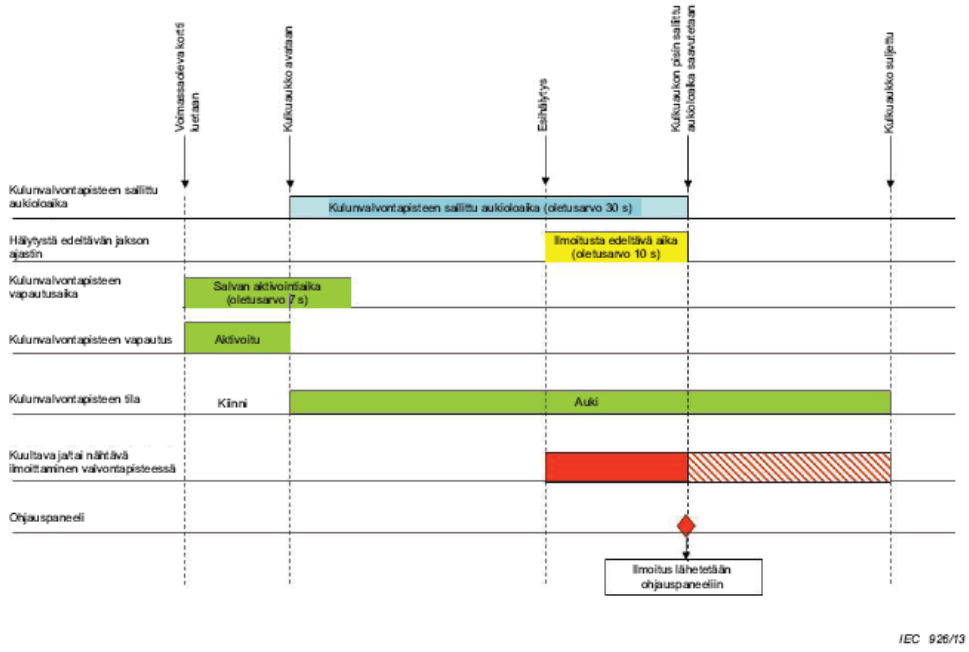
Tapahtumien käsittelyssä on luokassa 4 useita kohtia, jotka vaativat ohjelmistolta kehittynyttä tapahtumien kirjausominaisuuksia. Hälytykset pitää kuitata ja tapahtumaan pitää jäädä tieto kuka kuittasi ja milloin.

Taulukko 3 Standardin sivut 52, 54 ja 56.

A 1–4 Ilmoitukset paikallisesti ovella

B 5–47 Ilmoitukset valvomossa (monitorointisovelluksessa)

Pakollisia vaatimuksia on 38 kpl luokassa 4 ja numeroarvoja 3 kpl.



Kuva 3 Ajastusmalli (Suomen Standardoimisliitto SFS, 2013, 44)

7.4 Tunnistusta koskevat vaatimukset

Kohdassa asetetaan järjestelmän kellon ja tarkkuuden vaatimuksia, jotka eivät yleensä ole ongelmallisia. Kenttälaitteiden tulisi päivittää aika palvelimelta automaattisesti.

Kulkuoikeustasojen vähimmäismäärät, aikaohjelmien ja poikkeuspäivien määrät ovat pieniä, ne eivät riitä suuriin järjestelmiin. Näihin tilaajan tulisi lisätä luvut oman harkinnan mukaan, esimerkiksi kulkuoikeuksien määräksi 64 tai 128 kpl, 255 aikaohjelmaa ja 128 poikkeuspäivää.

Hylättyjen kulkujen tai väärän PIN-koodin tulee poistaa kulkuoikeudet, mikä on luokassa 4 pakollista. Lisäominaisuutena voisi lisätä oven lukitseminen määräajaksi. Biometristen tunnisteiden osalta, vaatimusmäärittely on käytännössä lukijoista riippuvainen tieto.

Lukijoiden ja kulkukorttien ominaisuuksiin ei standardissa oteta riittävästi kantaa. Vaikka lukijat ovat erillisiä ja usein eri valmistajan tuotteita, ovat ne olennainen osa kulunvalvontajärjestelmää. Vaatimusmäärittelyssä ottaa kantaa lukijoihin ja kulkukorttien teknologiaan. 125 kHz (Prox) lukijoita tai kortteja ei tulisi käyttää enää missään järjestelmässä niiden helpon kopioitavuuden takia.

Kaikissa luokan 4 kohteissa on käytettävä vahvaa salausta kortin ja lukijan välillä. Tämän hetkinen teknologia on Mifare DesFire EV1-2. Tai vastaava teknologia kuten HID SEOS tai Lecig.

Tunnisteen tiedon siirto lukijasta kuluvalvontapäätteeseen, pitää olla mahdollista salata standardilla tavalla, kuten OSDP v2. Muuten mahdollistetaan kulkukortin numeron selvittäminen kaapeloinnista.

Taulukko 4 Standardin sivut 58 ja 60

A 1–12 Kulkuoikeustasot

B 13–27 Tunnistuslaitteet

Pakollisia vaatimuksia on13 kpl luokassa 4 ja numeroarvoja 4 kpl.

7.5 Uhkatilanteen signalointia koskevat vaatimukset

Uhkatilanteella tarkoitetaan tilannetta, jossa tunkeutuja pakottaa kortinhaltijan avaamaan oven käyttäen omaa tunnistetta. Tilanteessa käyttäjän pitäisi viestittää uhkatilanteesta valvomoon. Tämä tehdään käyttämällä PIN-koodia muutettuna, niin että ovi aukeaa normaalisti. Valvomo saa samalla uhkatilanteesta hälytyksen.

Standardissa uhkakoodin vaatimukset ovat riittävällä tasolla. Tähän voi tarvittaessa lisätä vaatimuksen, jossa ovikohtaisesti määritellään, ettei ovi aukea uhkakoodilla.

Taulukko 5 Standardin sivu 62

1-3 Uhkakoodin käsittely

Pakollisia vaatimuksia on 3 kpl luokassa 4.

7.6 Ohitusta koskevat vaatimukset

Ohituksella tarkoitetaan oven avausta etäohjauksella käyttöliittymän avulla tai muun järjestelmän toimesta. Pakollisena on mahdollistaa hätäjärjestel-

mien, kuten paloilmoittimen ohjaus poistumisteiden oville. Tätä voi tarkentaa vielä, että ohjaus tulee tapahtua palvelimen tilasta riippumatta. Ohjaus kytketään suoraan kenttälaitteiden sisääntuloon ja se ohjelmoidaan avaamaan poistumisreittien ovet automaattisesti.

Taulukko 6 Standardin sivu 62

1-7 Ohitusta koskevat vaatimukset

Pakollisia vaatimuksia on 2 kpl luokassa 4.

7.7 Viestintää koskevat vaatimukset

Viestinnällä tarkoitetaan sitä miten yhteyskatkokset laitteiden ja palvelimen välillä on varmistettu ja miten yhteyskatkokset vaikuttavat järjestelmään. Standardi määrittelee myös milloin yhteydet tulee salata.

Standardi ei ota kantaa mitä tasoa viestinnän salaus tulisi olla. Kohteen turvallisuustason mukaisesti tulisi mainita mikä on salaustapa IP, sarjaliikenne, lukijaliitäntöjen ja lukijoiden osalta. Esimerkiksi TSL, AES 128, AES 256, OSDP V2 ja DesFire EV1-2. Ilman tarkennusta, salaus voi jäädä heikoksi.

Kohdassa on myös itsensä kumoava rivi, jossa palvelinyhteyden katketessa ei määritellä minimitoimintoja. Todetaan vain, että toiminnot jotka toimivat ilman palvelinyhteyttä pitää toimia.

Tässä tulee lisäksi määritellä että laitteiston keskusyksikön (kontrollerin) tulee säilyttää vähintään kulkuoikeudet sekä aikaohjelmat, mikäli yhteys palvelimeen katkeaa. Lisäksi laitteen tulisi automaattisesti lähettää katkoksen aikana tapahtuneet toiminnot palvelimelle.

Kohdassa on lueteltu vaadittavat ominaisuudet ja viitataan numeroarvoihin taulukkoon 3, riviin 38 enimmäisviiveeseen sekä taulukkoon 7 riviin 9 viestintäyhteyden katkeamisen havaitsemiseen.

7.8 Järjestelmän sisäistä suojausta koskevat vaatimukset

Sisäiseen suojaukseen kuuluu järjestelmän laitteiden mekaaninen suojaus ja murtamisen havaitseminen, tiedonsiirron salaaminen ja palautuksen eheys katkoksien jälkeen.

Järjestelmän on palauduttava tietoliikennekatkoksesta tai tehonmenetyksestä ilman että tietoa menetetään.

Vaatimukset komponenttien kotelointiin on, että ne ovat riittävästi suojattuja ja murtaminen havaitaan.

PIN koodien käytössä on vaatimuksia, joita useimmat järjestelmät eivät tue, kuten nousevan tai laskevan numerosarjan annon esto. Uniikin numeron anto sen sijaan on yleensä tuettuna.

Tässä kohdassa otetaan kantaa kulkukortin ja lukijan väliseen salaukseen luokissa 3 ja 4. Kuten aikaisemmissa kohdissa, varsinaiseen salausteknologiaan ei oteta kantaa, vaan se on määriteltävä erikseen.

Taulukko 7. Standardin sivut 66 ja 68.

A Estäminen 1-25

B Havaitseminen ja raportointi 25-28

Pakollisia vaatimuksia on 20 kpl luokassa 4 ja numeroarvoja 3 kpl.

7.9 Teholähdettä koskevat vaatimukset

Vaatimuksissa määritellään tehonlähteiden varmistus ja toiminta-aika sähkökatkoksessa. Nämä arvot voivat olla suuremmat tilankäytön tarpeista riippuen.

Taulukko 8. Standardin sivu 70.

Tehonlähde 1-4

Pakollisia vaatimuksia on 3 kpl luokassa 4 ja numeroarvoja 1 kpl.

7.10 Ympäristöolosuhteita ja sähkömagneettista yhteensopivuutta (häiriönsietoa) koskevat vaatimukset

Ympäristöolosuhteiden määritys ja testaus perustuu IEC 62599-1 standardiin eikä niitä käytännön olosuhteissa voida testata. Tärkeää on todeta että laitteet ja koteloinnit ovat sijoitettu valmistajan määrittelemällä tavalla ja vastaavat ympäristön vaatimuksia. Esimerkiksi kotelointiluokka on oikea. Yleensä kulunvalvontaelektroniikkaa pois lukien lukijat, ei tule sijoittaa ulkotiloihin.

Sähkömagneettisten häiriösuojauksine osalta, valmistaja vastaa CE and EMC merkinnöillä niiden standardinmukaisuudesta.

8 Testausmenetelmät

Standardi sisältää mittavan luettelon testeistä, jotka tehdään jokaiselle toiminnallisuusvaatimukselle. Tämä vastaa toimittajan ja tilaajan yhdessä tekemää FAT (Factory Acceptance Test) prosessia.

Jos standardin testausmenetelmät otetaan käyttöön, on tehtävä Excel tai vastaava taulukko, jossa on kirjattu jokaisen testin sisältämä vaatimus suorituskykytaulukosta. Sellaisenaan testiluettelo ei ole käyttökelpoinen, koska testi viittaa taulukkoon ja tekijä joutuisi hakemaan tiedot erikseen.

Taulukossa on lisäksi eriteltävä mihin tilaluokitukseen (1-4) järjestelmä on tarkoitus hyväksyä. Taulukkoon kirjataan testin tulos ja poikkeamat.

Vain harva turvallisuusjärjestelmä testataan luovutuksen yhteydessä. Syyt ovat yleensä ajallisia ja taloudellisia. FAT prosessi voi järjestelmästä riippuen kestää päiviä ja kustannus on tuhansia euroja.

Toisaalta jos järjestelmään investoidaan satoja tuhansia euroja, vaatimusten mukaisuuden tarkistaminen testausmenettelyllä on perusteltua. Se antaa tilaajalle varmuuden että toimitettu järjestelmä täyttää sille annetut määreet. Testauksen vaatiminen jo tarjouspyyntövaiheessa, asettaa toimittajat samaan asemaan ja testauksen kustannukset sisällytetään projektin hintaan.

9 Johtopäätökset

Projektityössä tekijä perehtyi perusteellisesti standardin SFS-EN 60839-11-1 sisältöön. Jokaista standardin kohtaa arvioitiin sekä kokemusperäiseen tietoon että kulunvalvontajärjestelmien tekniseen dokumentaatioon perustuen. (United Technologies Corporation, 2017). Standardin käyttökelpoisuutta arvioitiin ja syitä siihen, miksi sitä ei käytetä suurissakaan hankkeissa säännöllisesti.

Tekijä perehtyi standardiin jo sen ollessa lausuntokierroksella. Odotuksia oli sen laajasta käyttöönotosta turvallisuusjärjestelmien suunnittelussa heti julkaisemisen jälkeen. Alan toimijat eivät kuitenkaan saaneet standardista riittävästä tietoa, se myös koettiin hankalasti tulkittavaksi, eikä siitä muodostunut vaatimuksenmukaisuusdokumenttia edes julkishallinnon kohteissa.

Standardi on kuitenkin kulunvalvontajärjestelmien suorituskykyä mitattaessa erinomainen työkalu. Sen käyttö vaatii perehtymistä, kuten muutkin standardit. Tämän projektityön tarkoituksena on madaltaa kynnystä tutustua standardiin ja lisätä sen käyttöä vaativissa hankkeissa.

Tekijä suosittelee standardin käyttöönottoa julkishallinnon sekä korkean turvallisuuden kohteissa. Yhteismitallisena EN standardina se asettaa sekä kotimaiset, että ulkomaiset toimittajat samalle tasolle. Kun hankkeessa vaaditaan myös testausmenettely standardin mukaisesti tai FAT prosessina, tilaaja varmistaa järjestelmän olevan suunnitelman mukainen.

Jatkotoimenpiteenä projektityölle tulisi tehdä testausmenettelyn taulukointi, joka mahdollistaa testausten suorittamisen tehokkaasti ja tuottaa myös testauspöytäkirjan.

Lisäksi standardista SFS-EN 60839-11-2 (Sähköiset kuluvalvontajärjestelmät. Soveltamisohjeet. Julkaistu 18.5.2015) tulisi tehdä vastaava selvitys. Tässä standardissa on ohjeet suunnitteluun, sekä sallitut poikkeukset tässä

projektiyössä käsiteltyihin vaatimuksiin. Tätä standardia käytetään harvoin hyväksi suunnittelutoimistojen tai turvallisuuskonsulttien toimeksiannoissa. Myöskään yritykset eivät käytä standardia riskienhallinnassa tai suunnittelussa.

Soveltamisohjeiden standardi on paremmin jäsennelty ja käyttökelpoisempi kuin järjestelmä ja komponenttivaatimuksien standardi. Samaan suuntaan toivoisi tämän projektityön kohteena olevan standardin kehittyvän tulevaisuudessa.

10 Muut kulunvalvontajärjestelmien hankintaan ja asennukseen liittyvät ohjeet

Muita kulunvalvontamäärittelyyn liittyviä ohjeita on Katakri (*1), joka on haastatteluun ja arviointiin perustuva tietoturvallisuustason määrittely-dokumentti. Samoin Vahti (*2) joka on julkishallinnon tietoturvallisuuteen keskittyvä ohjeistus. Molemmissa otetaan kantaa järjestelmien suojaukseen ja tiedon hallintaan.

ST-kortistossa (*3) on saatavissa ohjekirja, joka määrittelee kulunvalvonta-järjestelmän perustiedot ja toteutusperiaatteet. Se ei kuitenkaan ota kantaa eri luokituksiin.

***1. Katakri**

Puolustusministeriö

Tietoturvallisuuden auditointityökalu viranomaisille

Verkkojulkaisu:
https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

***2. Vahti**

Valtionvaraministeriö

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto.

Verkkojulkaisu:

https://www.vahtiohje.fi/web/guest

***3. Kulunvalvonta- ja murtoilmaisujärjestelmät. ST-käsikirja 11**

Sähköinfo

Saatavissa verkkokaupassa: http://kauppa.sahkoinfo.fi/product/1306

Lähdeluettelo:

Jyväskylän yliopisto. 2015. Tutkimusstrategiat.

Verkkojulkaisu:

https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/empiirinen-tutkimus

Puolustusministeriö. 2015.Katakri

Tietoturvallisuuden auditointityökalu viranomaisille

Verkkojulkaisu:
https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Suomen Standardoimisliitto SFS, 2013. SFS-EN 60839-11-1

SESKO ry

Saatavissa verkkojulkaisuna:

https://sales.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID2/6/240870.html.stx

United Technologies Corporation. 2017. Lenel Systems International, DOC-925-EN-US_CSI-Format_OnGuard_7.3_AE_Specification

Saatavissa Lenel Systems asiakkaiden ja konsulttien käyttöön.

Henkilölähde

Aku Pänkäläinen, 2013. Keskustelu Pänkäläinen/Sääskilahti EN Kulunvalvontastandardista 4/2013

Finanssiala Ry