Väylävirasto
Trafikledsverket

Tasoristeyslaitoksen vaatimusmäärittely

Vesa Ruohomäki (Väylävirasto)
Tomi Lankinen (Proxion)

31.3.2021

Asialista

- Alkusanat
- Ongelman asettelu
- CENELEC EN5012x lyhyesti
- Projektin esittely
  - Mitä tehdään ja miten
  - Aikataulu ja tilanne
- Projektin jälkeen
- Projektissa havaittuja oppeja

Alkusanat

Väylävirasto
Trafikledsverket

- Digirata luento - Pilottihanke tasoristeyksen vaatimusmäärittely CENELEC -standardin mukaisesti elinkaaren hallinnasta RAMS

- Kohteena oleva järjestelmä: TASORISTEYSLAITOS
  - *Noudattaa luonnos vaiheessa olevaa Traficom määräystä*

- Esittäjä: Tomi Lankinen (Proxion Oy)

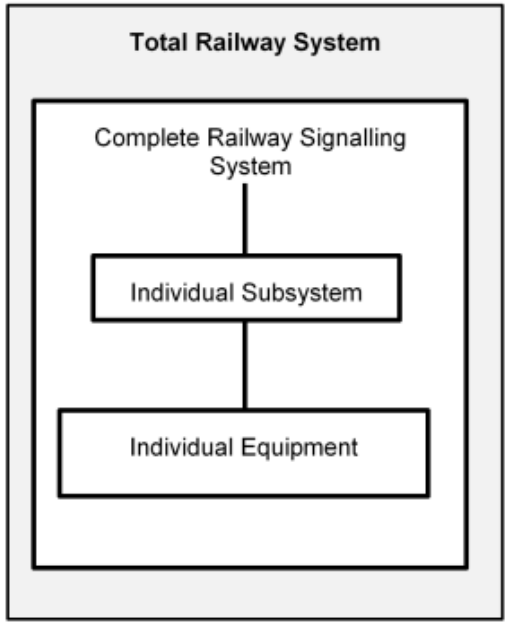
ONGELMAN ASETTELU

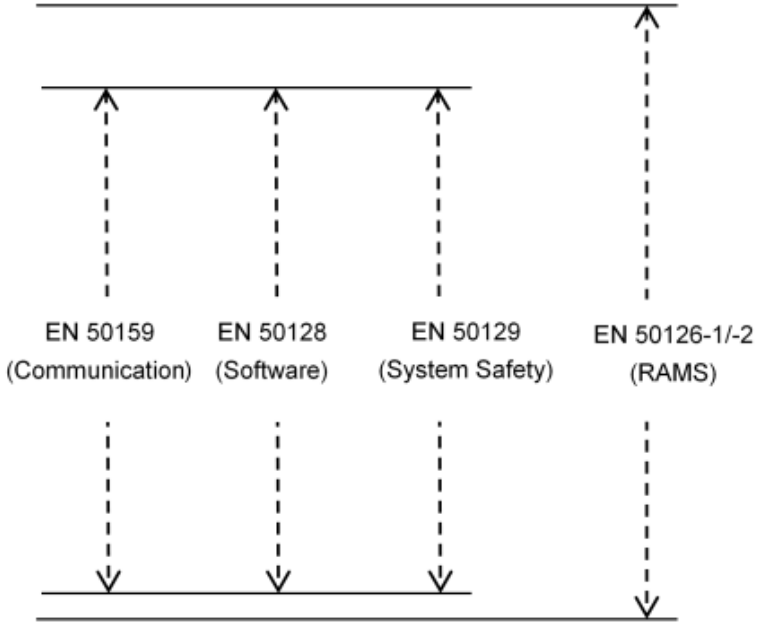
Ongelman asettelu

- Nykyiset varoituslaitoksen tekniset toimitusehdot sekä RATO 6 (varoituslaitos osa) ovat iäkkäitä sisällöltään sekä aika tekniikka sidonnaisia
- Raaseporin onnettomuus jälkeen heräsi tarve saada edullisempia ratkaisuja käyttöön
  - -> tasoristeysvalolaitos on syntynyt tästä lähtökodasta, tasoristeysvalo ei ole kuitenkaan tasoristeyksen varoituslaitos, joten vaatimuksia vähän
- Markkinoille on ollut tunkua uusista teknisistä järjestelmistä, joille ei ole riittäviä vaatimuksia,
- Cenelec standardin (EN 50126 yms.) mukainen toiminta on uupunut niiden tarkoittamalla laajuudella järjestelmän omistajan näkökulmasta

Ongelman asettelu

- Standardit* sisältää koko rautatiejärjestelmää koskevia periaatteita ja vaatimuksia, josta kokonaisuutena vastaa rataverkonhaltija.
- Nykyään Väylävirasto ei ole huomioinut standardissa rataverkon haltijalle kuvattuja tehtäviä (esim. **RAMS politiikka**, **RAM suunnitelma**, **Safety Plan**)
- Standardien mukainen toteutus on osoitettu sopimuksella järjestelmätoimittajan tehtäväksi,
- Väylävirasto ilmoittaa järjestelmältä edellytetyn SIL tason, mutta ei kohdenna sitä mihinkään tasoristeyslaitoksen turvatoimintoon.





**Standardit = rautatien RAMS standardit CENELEC EN 50126 jne.*

Projektin tavoite ja laajuus

- Tärkeimmät tavoitteet:
  - Tuottaa FIR kaltainen vaatimuskokoelma tasoristeysten turvalaitteista.
  - Määritellä tasoristeyslaitoksilta vaadittavat turvatoiminnot ja niiltä vaaditut turvallisuuden eheyden tasot.
  - Määritetään eritasoiset vaatimukset järjestelmän varustelun mukaan keskittyen toiminnallisuuksiin
  - Selvitys muutostarpeista muihin Väyläviraston ohjeisiin
- Vaatimusten laajuus:
  - kaikki tasoristeyksistä tienkäyttäjien varoittamiseen liittyvät tekniset laitteistot mekaanisia laitteita (esim. liikennemerkit, portaalit) lukuun ottamatta
- Työssä on keskitytty Linjalaitoksiin

Mutta, mitäs nykyisille vaatimuksille tapahtuu? Joutaako ne roskakoriin?

CENELEC EN5012x LYHYESTI

CENELEC EN5012x standardit

- EN 50126
  - Osa 1 - Yleinen RAMS prosessi
  - Osa 2 - Järjestelmien turvallisuus
- EN 50128 - Ohjelmistot
- EN 50129 - Turvallisuuteen liittyvän järjestelmän hyväksyntä
- EN 50159 - Turvallisuuteen liittyvä tiedonsiirto

CENELEC EN5012x lyhyesti

- Esittää rautatiellä toimijoille RAMS* hallinnan periaatteet, velvoittavia vaatimuksia sekä esimerkkejä mm. asiakirjoista ja käytetyistä parametreista
- EN 50126 on rautatielle kirjoitettu standardi sisältäen mm. toiminnallisen turvallisuuden hallinnan periaatteet (safety management)
- Standardi esittää RAMS vaatimusten määrittelyn ja osoituksen prosessit, joilla edesautetaan toimijoiden yhteistä ymmärrystä RAMS hallinnasta *(yhteinen kieli sidosryhmien kesken)*
- Järjestelmälähtöisyys, mahdollistaa RAMS hallinnan arvioinnin yksinkertaisissa ja monimutkaisissa toteutuksissa.
- Standardin noudattaminen tukee myös EU tavoitteita yhtenäisestä Rautatiemarkkinasta

RAMS = Realiability, Availability, Maintainability, (functional) Safety*

CENELEC EN5012x lyhyesti

- Standardit täydentää organisaatioiden yleisiä laadun- ja turvallisuuden hallinnan sekä suorituskyvyn menettelyitä (esim. ISO 9001)
- Standardi sisältää:
  - Rautatien RAMS-osatekijät ja niiden vaikutus rautatiejärjestelmän suorituskykyyn, riskien hallinnan periaatteet
  - Yleiset vaatimukset RAMS hallinnalle, elinkaarimalli, organisaatiot, standardin soveltaminen, dokumentointi, V&V, ISA
  - RAMS elinkaarimalli (konseptoinnista käytöstä poistoon)
  - Turvallisuuden perustelu (safety case)
- Informatiiviset liitteet mm.
  - RAMS suunnitelma, RAMS parametrit, riskimatriisi, standardin ja EU 2008/57/EC (YTE) olennaisten vaatimusten yhteneväisyyden

RAMS

- Standardit ja niiden vaatimukset kohdistuvat pääasiassa neljän eri osatekijän hallintaan: **luotettavuuteen (R)**, **käytettävyyteen (A)**, **kunnossapidettävyyteen (M)** ja **turvallisuuteen (S)**.
  - R - <toimilaitteen> kyky suoriutua annetussa ajassa ja rajoissa ilman vikaantumista
  - A - <toimilaitteen> kyky suorittaa vaadittu toiminto annetussa ajassa ja rajoissa
  - M - <toimilaitteen> kyky palauttaa järjestelmä toimintakuntoiseksi
  - S - vapaus ei-hyväksyttävistä riskeistä
- Osatekijät käsitellään standardeissa yleensä kahtena erillisenä kokonaisuutena: RAM ja S.

Standardien tavoitteet

- Standardien tavoite on luoda hyvät puitteet sille, että **RAMS-osatekijät tulevat huomioiduiksi riittävällä tasolla järjestelmän koko elinkaaren ajan** aina konseptin luomisesta käytöstä poistoon saakka.
  - Toisin sanoen, tavoitteena on, että
    - järjestelmän vaatimusmäärittely on tarkoitettuun käyttöön soveltuva ja riittävän kattava
    - järjestelmä täyttää sille asetetut vaatimukset koko sen elinkaaren ajan
- Tavoitteisiin pyritään antamalla toimintamalleja sekä muita vaatimuksia RAMS-asioiden hallintaan.
- Standardit **eivät** määrittele varsinaisia RAMS-vaatimuksia.

Tavoitteisiin pyrkiminen

- Pohjimmiltaan standardit pyrkivät tavoitteeseensa (eli turvallisen, aiottuun käyttöön soveltuvan ja vaatimusten mukaisen järjestelmän saamiseksi) **pidentämällä järjestelmässä esiintyvien virhetoimintojen esiintymisväliä**.
  - Ei ole olemassa järjestelmää, joka toimisi ikuisesti ilman virhetoimintoja.
  - Virhetoimintojen esiintymisväliin voidaan kuitenkin vaikuttaa.

- Virhetoimintojen syyt jaetaan kahteen eri luokkaan:
  - **systemaattiset virheet** (systematic failures)
  - **satunnaiset viat** (random faults)

Systemaattiset viat / virheet

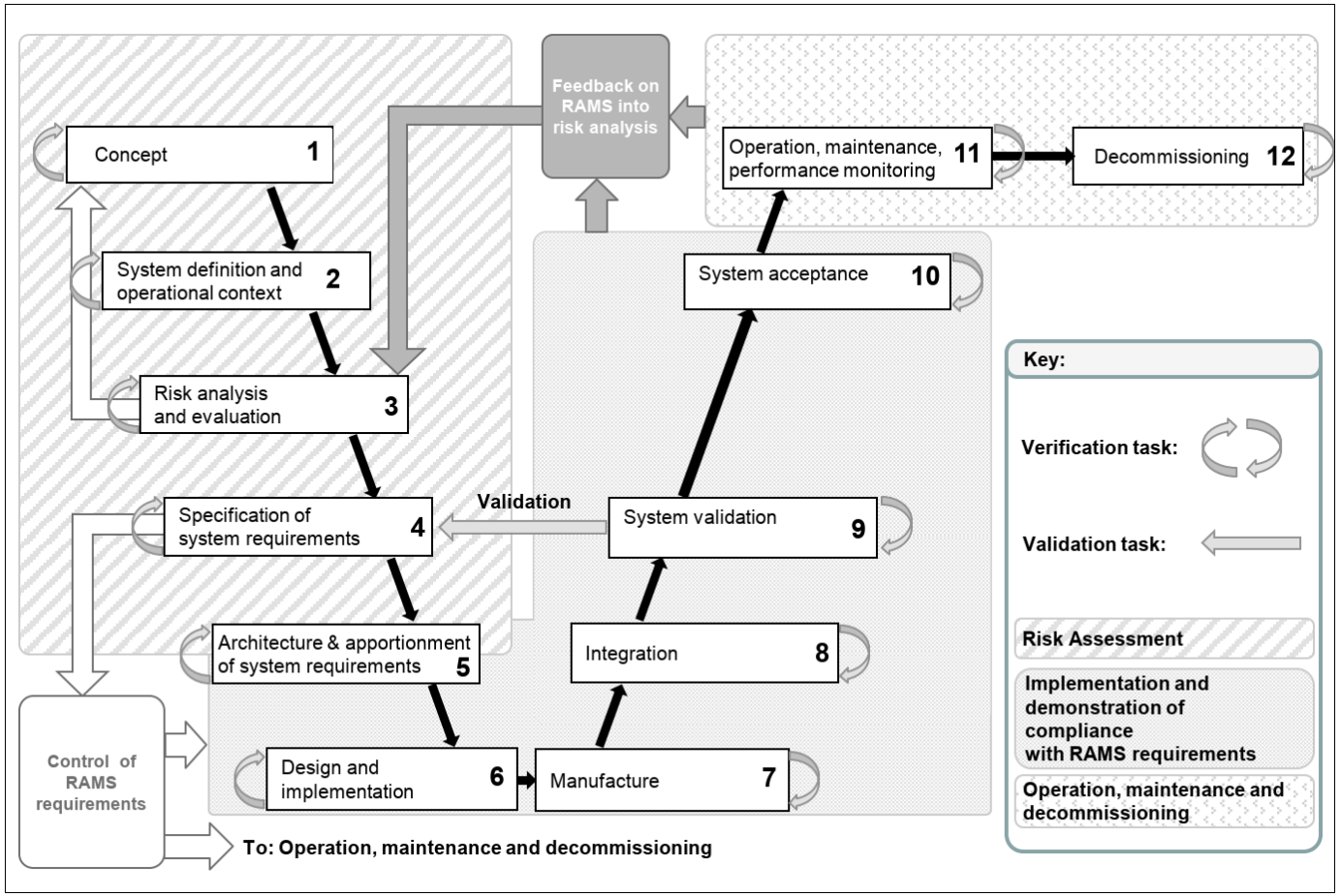
- Systemaattiset virheet ovat yleisesti **ihmisten tekemiä virheitä** järjestelmän eri elinkaaren vaiheissa.
- Esimerkkejä systemaattisista virheistä, jotka voivat johtaa virhetoimintoihin:
  - Vaatimusmäärittely on tulkinnanvarainen
  - Koodari tekee virheen
  - Akselinlaskijan asennus tehdään väärin
    - laitevalmistajan ohjeita ei noudateta
    - ohjeet ovat virheelliset tai puutteelliset
    - ei ole saatu koulutusta
- Järjestelmässä oleva systemaattinen virhe ilmenee aina, kun tietyt ehdot ja/tai olosuhteet toteutuvat.
- Eri menetelmillä (esim. testaamisella) voidaan löytää virheitä, mutta käytännössä ei ole mahdollista varmistaa, että järjestelmässä ei ole laisinkaan systemaattisia virheitä.
- Systemaattisia virheitä pyritään vähentämään **laadullisilla vaatimuksilla**, joita noudattamalla virheiden määrän oletetaan pysyvän hyväksyttävällä tasolla.

Satunnaiset viat

- **Satunnaisella vialla** tarkoitetaan komponentin/laitteen odottamatonta vikaantumista.
  - On odotettavissa, että jokainen laite vikaantuu joskus, mutta tarkkaa ajankohtaa ei ole mahdollista ennakoida.
- Satunnaisten vikojen esiintymistaajuus pyritään saamaan hyväksyttävälle tasolle **määrällisillä vaatimuksilla**.
- Vikojen esiintymistaajuuteen ja niiden vaikutuksiin voidaan vaikuttaa laite- ja komponenttivalinnoilla sekä arkkitehtuurisilla ratkaisuilla

Elinkaarimalli

- Standardi määrittelee järjestelmälle viitteellisen elinkaarimallin
- Kullekin elinkaaren vaiheelle on määritelty tehtäviä/vaatimuksia
- Mallia voi mukauttaa, kunhan viitteellisen mallin vaatimukset tulevat huomioiduksi kokonaisuudessaan
- Valittu elinkaarimalli kuvataan esim. RAM-suunnitelmassa ja/tai Safety Planissa



Viite: EN 50126-1, figure 7

Eikö vaatimuksen kirjaaminen ole aika suoraviivaista tekemistä?

Mihin me siinä tarvitaan RAMS elinkaarimallia ja kaikkea ”turhaa” dokumenttia?

Eikö vaatimuksen kirjaamisessa ole aika helppoa ehkäistä systemaattiset virheet?

PROJEKTIN ESITTELY

Projektin esittely

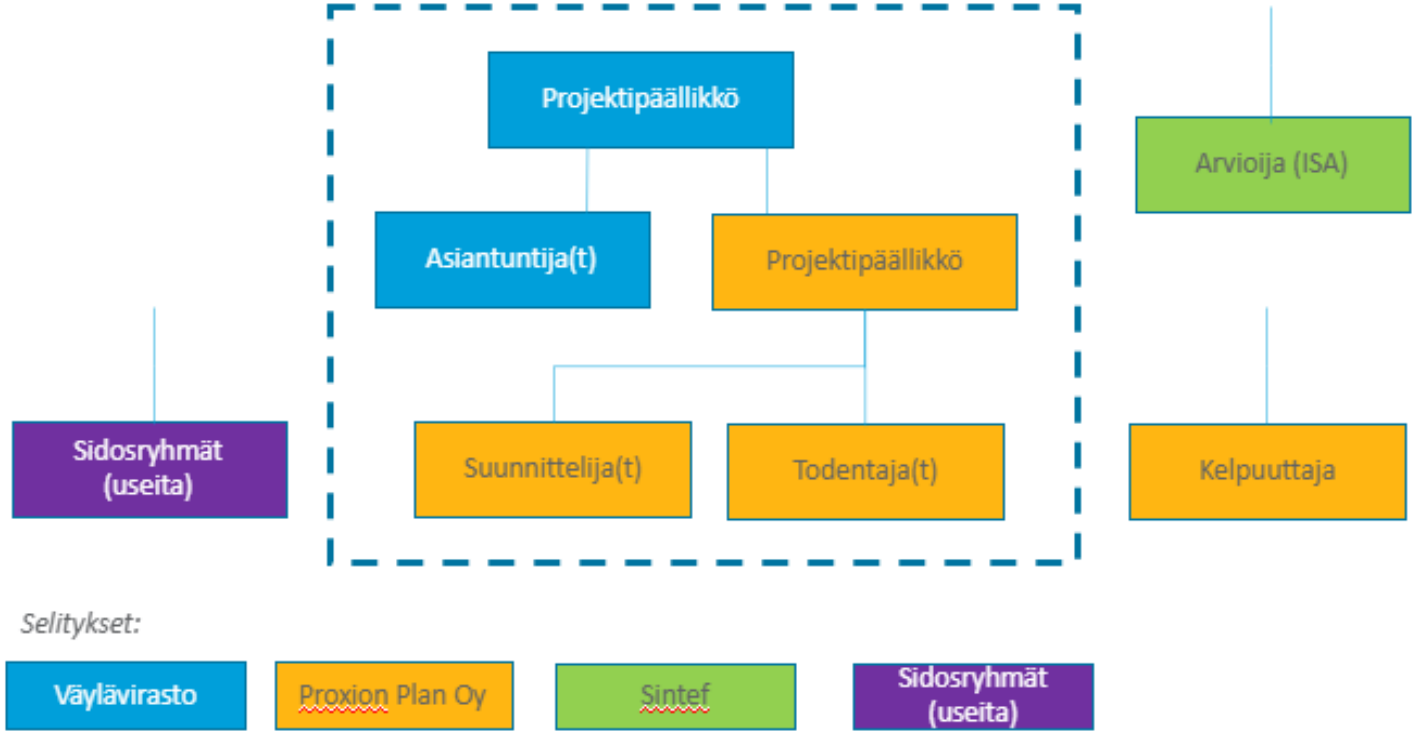
- Projekti toteutetaan Väyläviraston RTJJ* mukaisesti, jota täydennetään standardien ** mukaisilla prosesseilla.
- Järjestelmälle on laadittu menettelykuvaukset, jotka asettavat raamit ja toimintamallit elinkaarimallin mukaisten tehtävien suoritukselle. *(myös ehkäistään systemaattisia virheitä)*
- sisältä mm. seuraavat tiedot:
  - Järjestelmän elinkaarimalli
  - RAMS hallinnan menettelyt ja tehtävät elinkaarimallin mukaisesti
  - Järjestelmän teknisen tiedon dokumentointi (mm. versioiden hallinta)
  - Turvallisuus ja riskienhallinnan periaatteet, menettelyt
  - Vaatimusten hallinnan menettelyt ja vaiheet
  - Muutosten hallinnan menettelyt
  - Tarkastus ja todentamisen suunnitelma

** RTJJ = Rautatietoimintojen turvallisuusjohtamisjärjestelmä*

*** Standardit = CENELEC EN 5012x sarja*

Projektiorganisaatio

- Proxion toimii suunnittelukonsulttina sekä koordinaattorina,
- Väylävirasto katselmoi, kommentoi, linjaa, tekee suuret päätökset, hyväksyy lopputuotteet
- Todentaja tarkastaa tuotokset sekä elinkaaren vaiheet
- Validoija kelpuuttaa vaatimusmäärittelyn
- EN ISA arvioi kokonaisuuden
- Sidosryhmät kommentoivat tuotoksia, osallistuvat riskityöpajoihin



Suunnittelu, todennus, kelpuutus

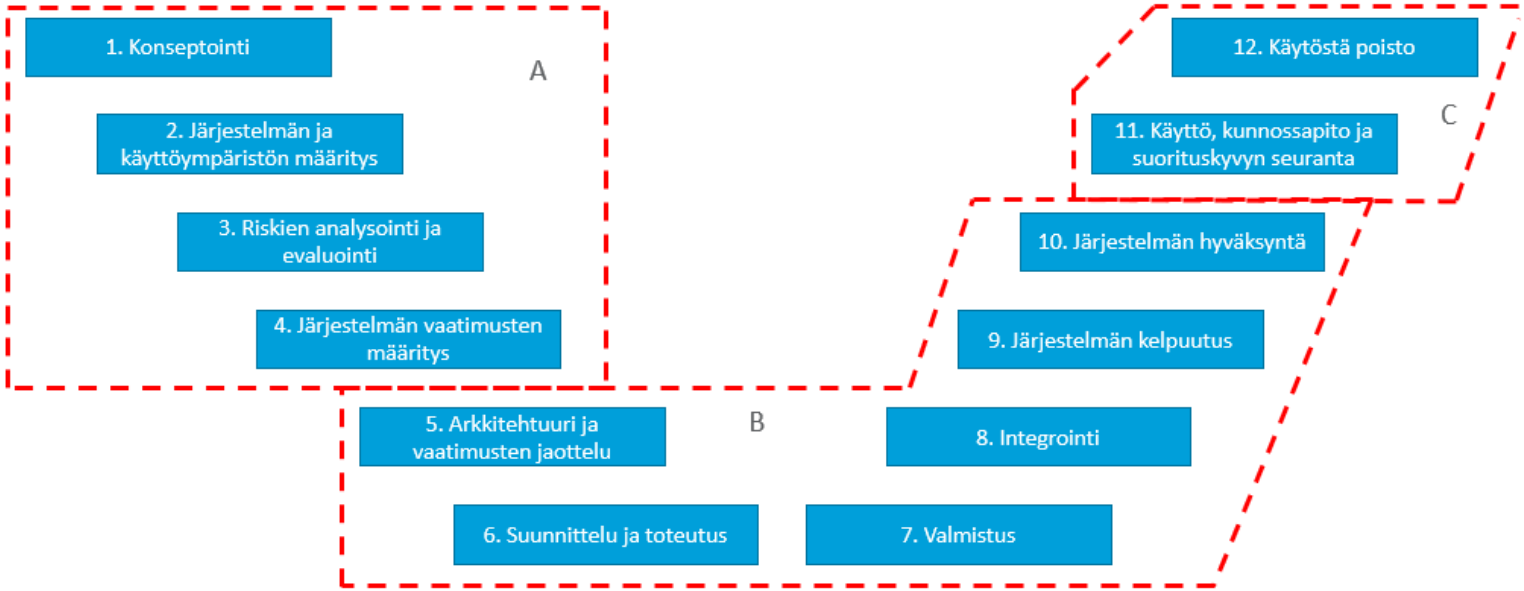
- Suunnittelun tehtävät
  - Laatia vaatimusmäärittelyt, tuottaa "tarinaa" vaatimusten taustalle
  - "tarina" luodaan CENELEC prosessin ja Väyläviraston ohjeiden mukaan
- Todentamisen tehtävät
  - Onko yksittäiset tuotokset ymmärrettäviä, vaatimusten mukaisia, sisältääkö ne oikeat tiedot
  - Onko työvaiheet (~elinkaaren vaiheet) tehty ohjeiden mukaan
  - *Systemaattisten virheiden havaitsemista*
- Kelpuutuksen tehtävät
  - Onko todentaminen tehty suunnitelman mukaisesti?
  - Toteuttaako vaatimusmäärittelyn mukainen järjestelmä halutun lopputuloksen?
  - *Systemaattisten virheiden havaitsemista*

Arviointi

- Arvioijan tehtävät
  - Onko määrittelyssä noudatettu CENELEC standardia?
  - Onko tekijät olleet päteviä heille osoitetuissa tehtävissä?
  - Onko toimintamallit olleet soveltuvia?
  - *Systemaattisten virheiden havaitsemista*
  - Arviointi perustuu määrittelyn aikana luotuihin asiakirjoihin (turvallisuus perustelua ei ole laadittu)
  - Laatii arviointilausunnon työn päätteeksi.

Projektin esittely

- Projekti käynnistyi syksyllä 2020 ja päättyy kesällä 2021.
- Missä ollaan menossa?



A = järjestelmän määrittely
B = järjestelmän suunnittelu ja toteutus
C = järjestelmän käyttö ja käytöstä poisto

Vaatimusten määrittely prosessina

Tiedon jalostuminen

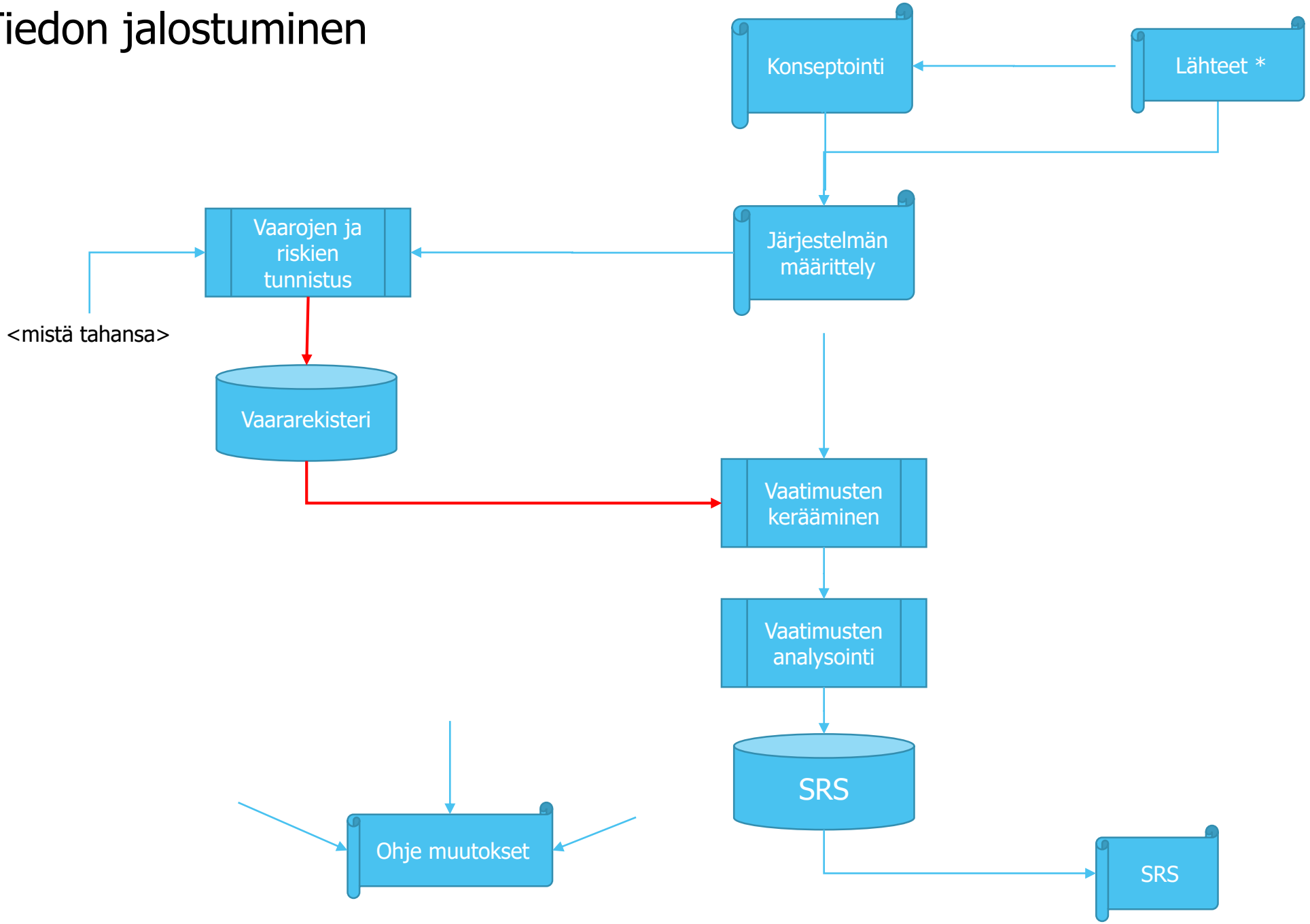
- Järjestelmän suunnittelutieto on dokumentoitu eri asiakirjoihin, joissa mm.
  - Kuvataan kohteena oleva järjestelmä, sen käyttötarkoitus ja toimintaympäristö,
  - Kuvataan liittyvät säädökset, lait, määräykset ja ohjeet
  - Määritetään järjestelmän käyttötapaukset, toiminnot ja toimintatilat
  - Esitetään tasoristeyslaitostyypit
  - Määritetään järjestelmän rajapinnat* sekä käytön edellytykset
- Järjestelmän riskitietoisuus dokumentoidaan järjestelmän Vaararekisteriin (TURI)

➔ kaikki tämä toimii lähtötietona järjestelmän vaatimusmäärittelylle

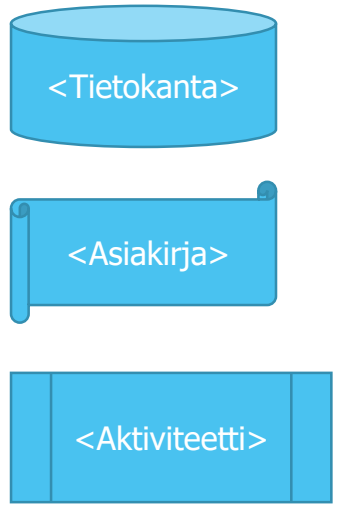
- Järjestelmän vaatimukset kirjataan Väyläviraston Jira tietokantaan, josta julkaistaan Väyläviraston ohjeluetteloon erillinen ”snapshot” hankintoja varten

**Rajapintamäärittelyssä pysytään toiminnallisuudessa*

Tiedon jalostuminen



Selitteet:



<Riskitieto>

<suunnittelun tieto>

* Sidosryhmien toiveet, tarpeet, lait, määräykset yms.

SRS = Järjestelmän vaatimusmäärittely

Vaatimusten määrittely prosessina

- Prosessin vaiheet:
  - Vaatimusten kerääminen useasta eri lähteestä (raakavaatimukset)
  - Vaatimusten analysointi (ajattelutyö)
  - Vaatimusten dokumentointi
  - Vaatimusten validointi

- Projektin toimintamalli:
  - Proxion kerää raakavaatimukset tietokantaan
  - Proxion analysoi vaatimukset, tunnistaa ristiriitoja, ongelmia, puutteita, epäselviä vaatimuksia
  - Analysoinnin tulokset katselmoidaan sidosryhmien kesken
  - Proxion dokumentoi analysoinnin perusteella vaatimukset Jira tietokantaan
  - Proxion validoi vaatimukset

Muutamista lopputuotteista s.7 mukaisesti

Järjestelmän vaatimusmäärittely

- Dokumentoidaan Väyläviraston Jira tietokantaan, jossa ylläpidetään. Hankintoja varten tehdään ”snapshot” osaksi hankinta-asiakirjoja.
- Säilyy dokumentoitu tieto vaatimusten käsittelystä ja muutoksista
- Hyödynnetään mahdollisimman paljon nykyisiä vaatimuksia, mutta ne pitää analysoida ja osittain kirjoittaa uudestaan

- Tämän hetkinen tilanne:
  - Jira projekti perustettu
  - Vaatimusten kirjausohje käynnissä
  - Vaatimusten analysointi käynnissä
  - Vaatimusten kirjaus on alkamassa huhtikuun alussa
  - Vaatimukset tarkastamatta ja validoimatta

Turvatoimintojen määritys (S vaatimukset)

- Tunnistetaan turvatoimintojen tarve (Vaarojen kartoitus)
- Määritetään turvatoiminnot sekä niiden THR -> voidaan muuttaa SIL tasoksi

- Tämän hetkinen tilanne:
  - Prosessin määritys käynnissä
  - Turvatoiminnot määrittämättä
  - Turvallisuuteen liittyvät vaatimukset määrittämättä

Eritasoiset vaatimukset järjestelmän varustelun mukaan

- Vaatimusmäärittelyssä huomioidaan varustelun näkökulmasta eritasoiset järjestelmät ja luodaan näille vaatimukset.
- Työssä on tarkoitus rajoittaa mahdollisimman vähän teknisiä toteutuksia keskittyen toiminnallisuuksiin

- Tämän hetkinen tilanne:
  - Järjestelmätyypit on tunnistettu
  - Vaatimusten tarkempi erottelu on käynnissä

Selvitys muutostarpeista muihin Väyläviraston ohjeisiin

- Erillinen selvitys on käynnissä, täydennetään projektin aikana
  - Tunnistetaan muutostarpeet muissa Väyläviraston ohjeissa, jotta jatkossa ohjeet ovat yhtenevä ja eheä kokonaisuus
  - Ohjeiden päivitys työ ei sisälly tähän toimeksiantoon
- Selvitys julkaistaan lopputuotteena

PROJEKTIN JÄLKEEN

Mitä materiaalille tapahtuu projektin päätyttyä?

- Järjestelmän elinkaarimalli toimii viitekehyksenä myöhemmille elinkaaren vaiheille
- Uudet tasoristeyksiin tehtävät turvalaiteratkaisut tulee päivittää nyt laadittuihin asiakirjoihin + arvioitava muutosten vaikutus
- Jatkossa järjestelmän vaatimusmäärittelyä ylläpidetään Jira tietokannassa

PROJEKTISSA HAVAITTUJA OPPEJA

Mitä on opittu?

- Uusien toimintamallien tunnistaminen, määrittäminen, katselmointi ja ihmisten perehdytys vie aikaa (perehdytyksessä ollaan osittain epäonnistuttu)
- Työ on pääsääntöisesti dokumenttien lukemista ja kirjoittamista, kommunikointia, viestintää
- Asiakirjoissa käytetty yksityiskohtaisuuden taso on herättänyt paljon keskustelua, on ollut haastavaa tunnistaa rajaa mikä on tarpeeksi, mikä liikaa
- Työn rajaus on todella tärkeää
- Tarvittujen avainhenkilöiden roolitus ja vastuut on erittäin tärkeä määrittää
- Projekti edellyttää jokaiselta vahvaa sitoutumista menettelyiden mukaiseen työskentelyyn
- Tarkan aikataulun laatiminen ja sen mukainen toiminta on ollut vaikeaa

Väylävirasto
Trafikledsverket