

## CYBERNETICA AS TEGEMISTEST

Ülo Jaaksoo, Monika Oit, Aivar Usk

Cybernetica AS

### PROLOOG

Reede. Osakonna nõupidamine. Selleks, et tellija saaks uue tulemüüri Barrikaad 2 õigeaegselt välis-turule jõuda, on arendustöö tähtaeg viidud äärmiselt lühikeseks. Esmaspäeval tuleb toode tellijale üle anda. Otsustati, et projekti meeskond töötab nädalava-hetusel. Keegi avaldas soovi riigitööle minna. Osa-konnajuhataja lubas projektimeeskonnale nädalava-hetusel suppi keeta.

Veeteede Ametilt on laekunud allkirjastatud leping, mille alusel Cybernetica koordineerib Eesti poolt uue laevaliiklussüsteemi (*Vessel Traffic Management and Information System*) väljaehitamiseks sõlmitud lepingut firmaga Holland Institute of Traf-fic Technology. Aastatepikkused kogemused navi-gatsioonisüsteemide infotehnoloogiliste alamsüs-teemide integreerimise vallas on leidnud tunnustust ja on taas rakendatud meresõiduohutuse riiklike ko-hustuste täitmise seisukohast kriitiliste projektide teenistusse.

Toimuvad läbirääkimised välisinvestoriga, kes plaanib Eestisse ehitada elektroonikatoodete tehase. Arutluse all on koostööleping, millega Cybernetica kohustub tegema vastavat arendustööd. Mõned le-pingu punktid, mis puudutavad intellektuaalset omandit ja Cybernetica toodete turustamist, kutsu-vad ettevõttele ja vajavad muutmist. Leping jääb allkirjastamata.

Tarkvarapaketi DEKLARANT müük läheb endist-viisi hästi.

Mõni päev tagasi esitati Sertifitseerimise Riiklikule Registrile ajatempli teenuse osutaja registreerimis-taotlus. Ettevalmistuseks on juba kulunud mitusada tuhat krooni, mille tagasisaamine vastava teenuse müügist ei ole lähiajal reaalne. Kuid Eesti Asi vajab ajamist, ID-kaardi kasutusvaldkonda tuleb laiendada ning ID-kaardi kasutamine pikaajalise tõestusväärtusega digitaaldokumendi allkirjastamiseks on üks

oluline rakendus. Selleks aga on vaja ajatempli tee-nust.

### AJATEMBELDAMINE

Digitaaldokumendile allkirja andmiseks on vaja luua avaliku ja salajase võtme paarid. Eesti ID-kaardi omanikel on võimalus lasta Sertifitseerimis-keskuses genereerida vastavad võtmed, salvestada salajane võti oma ID kaardil ja hoida avalik võti ser-tifikaadi kujul kõigile asjast huvitatutele kättesaadava Sertifitseerimiskeskuses. Salajase võtmega saab allkirjastada digitaaldokumente ja avaliku võt-mega on võimalik kontrollida, kas allkiri on ehtne.

Võtmete ja sertifikaadi eluiga on reeglina lühem kui seda on dokumendi eluiga. Kui näiteks, salajane võti on lekkinud, siis tuleb võtme paar ja vastav sertifikaat tühistada. Selleks on vaja pöörduda Sertifitsee-rimiskeskuse poole, kes tühistab sertifikaadi ja saadab selle kohta vastava kinnituse. Sertifikaadi tühistamise võimalus tekitab aga uue probleemi – allkirja salgamise probleemi. Oletame, et keegi on allkirjastanud dokumendi, seejärel aga tahtlikult või tahtmatult kaotanud oma ID-kaardi (salajase võtme) ja seejärel teavitanud sellest Sertifitseerimiskeskust. Oletame, et see oli dokument, millele antud allkirja tahab isik salata, st väita, et ta ei ole seda allkirjasta-nud ja kui sellel dokumendil on tema salajase võt-mega moodustatud allkiri, siis seda on kaotatud ID-kaardiga teinud keegi teine. Salgamise vääramiseks on oluline kahe sündmuse – dokumendi allkirjasta-mine ja sertifikaadi tühistamine – järjestus. Juhul kui sertifikaadi tühistamine toimus enne dokumendi allkirjastamist, siis võis seda tõepoolest teha keegi teine ja mitte ID-kaardi omanik ning allkiri on tühi-ne. Kui aga allkirjastamine toimus enne sertifikaadi tühistamist, siis allkiri on moodustatud salajase võtmega, mille hoidmise eest vastutab ID-kaardi omanik, järelikult digitaalallkirja olemasolu eest do-kumendil vastutab ID kaardi omanik.

Kuna salgamise vääramine põhineb dokumendi allkirjastamise ja sertifikaadi tühistamise sündmuse ajalisel järjestusel, siis tõestusväärtusega digitaalallkirja moodustamiseks on ajatempli sissetoomine möödapääsmatu.

Ajatempel on kindla vorminguga elektrooniline andmekogum, mis aitab tõestada või kinnitab mingite sündmuste toimumise ajalisi suhteid, näiteks digitaalallkirja moodustamist ja ajatempli enda moodustamist.

Kõige lihtsam moodus on selline, kus nii allkirjastamise hetkel kui sertifikaadi tühistamise hetkel pöördutakse ajatempliserveri poole, mis vaatab kella ja vastab päringule, lisades ajatempliserverile saadetud allkirjale ja tühistamiskinnitusele ajanäidu. Selle meetodi üheks oluliseks puuduseks on see, et me peame ajanäiduellikat täielikult usaldama.

Tegelikult ei huvita meid üldse absoluutne aeg, vaid võimalus tõestada, et üks bitijada eksisteeris ajalisel enne mingit teist bitijada. Matemaatikas on tuntud kollisioonivabad räsifunktsioonid, mis teisendavad suvalise pikkusega bitijadad mingi kindla pikkusega bitijadadeks, räsiks. Kollisioonivaba räsifunktsiooni on väga raske pöörata, st teisendatud bitijadast lähtebitijada saamine on peaaegu võimatu. Selgub, et kollisioonivabad räsifunktsioonid võimaldavad ajatempleid niimoodi kokku linkida, et iga ajatempel sisaldab eelmisena väljaantud ajatempli ja mõne varem välja antud ajatempli räsi. Viimaste aastate teoreetiline uurimistöö, mis on toimunud Ahto Buldase juhtimisel, ongi suunatud efektiivsete linkimisskeemide väljatöötamisele ja nende omaduste uurimisele [1,2,3].

## SÜSTEEMIDE INTEGRATSIOONIST

Kuidas optimeerida Balti mere rasketes keskkonnatingimustes töötava navigatsioonitule automaatika-, side- ja positsioneerimissüsteemi toitva akumulaatori laadimisrežiimi selliselt, et aastaid hoolduseta töötama määratud akumulaatori vahetus uue vastu toimuks optimaalsel ajahetkel, ilma et rahvusvahelisel mereteel paiknev objekt ootamatu toitekatkestuse tõttu töövõime kaotaks, kuid samas kasutataks ära kogu akumulaatori ressurs?

Kui täpselt õnnestub ennustada võimsa tuletorni lambi jääkressurssi plinkimiskarakteristiku ja tööaja alusel ning millised oleks vastava elueamudeli ülejäänud võimalikud olulised sisendid?

Milline on pooljuht-valgusdiodide (Light Emitting Diodes, LED) optimaalne paigutus poitule kiirguris, mis tagaks tule küllaldase nähtavuskauguse ka soolases mereudus ja linnatulede taustal, jättes seejuures komponentide arvu ja voolutarbe sellisele tasemele, mis võimaldaks toodet maailmaturul konkurentsivõimelise hinnaga müüa?

Millistest materjalidest valmistada suurte temperatuurikõikumistega välitingimustes töötava, kliendi poolt nõutava pika elueaga toote korpuse erinevad komponendid ning kuidas tagada ühekorruga löögi- ja veekindlus, remonditavus ja komponentide piisav jahutus?

Kuidas organiseerida tõrkekindlat kauginfovahetust seirekeskuse ja piiratud toitevooluga autonoomse sardsüsteemi (poitule) vahel ning viimase kohtvõrgus minimaalse energiakuluga?

Selliseid ja sarnaseid väljakutseid esitab alatihti meie süsteemi- ja tootearendusprojektide argipäev, saades meie inseneriteadust viljelevalt meeskonnalt nii mõnelgi juhul vastuseks ka patendikõlbuliku lahenduse. Käesolevaks hetkeks on navigatsioonisüsteemide osakonnal käes kaks kasuliku mudeli tunnistust, kolm taotlust on hetkel töötluses.

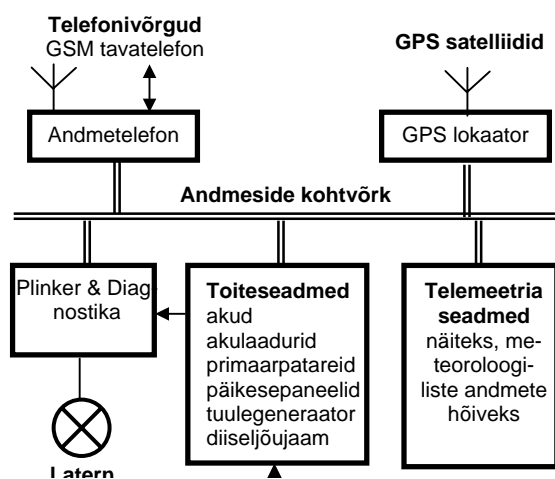
Ühena 72-st Rahvusvahelise Meremärgistuse ja Tuletornide Assotsiatsiooni (IALA) tööstusliikmest oleme keskendunud eelkõige merenavigatsioonisüsteemide temaatikale, kusjuures tegevusvaldkond ulatub lähteuringutest, tootearendusest, tootmistegusest ja süsteemide integreerimisest projektijuhitise ning nõustamis- ja koolitusteenusteni. Mahuka arendustöö tulemusena on valminud seiretarkvarast ja navigatsioonivahendite riistvarast koosnev hajutatud mitmetasandiline Navigatsioonimärkide seire- ja juhtimissüsteem, mis pärast kasutuselevõttu Eesti Veeteede Ametis aitab ööpäevaringselt tõsta meresõiduohutuse taset Eesti vastutusallas, võimaldades samaaegselt ka kokkuhoidu personalikulude arvelt.

Tänapäevane poi- või majakasüsteem on suhteliselt keerukas elektronmoodulite kompleks, milles võib sisalduda mitu üksteisest sõltumatult töötavat mikroprotsessorjuhitavat plokki, mis vahetavad omavahel andmeid kohtvõrgu vahendusel. Mitte iga süsteemi tarvis pole kogu vajaminevat funktsionaalsust tagavaid valmismoduleid võimalik sisse osta, samas pole ka kogu juhtsüsteemi loomine nullist alates otstarbekohane, seetõttu tuleb süsteemi optimaalse hinna saavutamiseks enamasti teha mitmeid

otsuseid – kas luua vajaminev sõlm ise või omandada sobiv ostutoode ja integreerida see loodavasse süsteemi.

Funktsionaalsete moodulite elektrilise ja konstruktiivse ühildatavuse kõrval nõuab süsteemide projekteerimisel ja integreerimisel märkimisväärset tähelepanu ka informatiivne külg – pole sugugi haruldased juhtumid, kus innovatiivse toote turule paisanud nimekas firma võib olla mõnda standardit tavatult tõlgendanud ja seade üritab “rääkida” teises järjekorras baitidega kui võiks standardit tundes eeldada. Sarnaste ootamatuste õigeaegne tuvastamine eeldab lisaks heale õnnele ka läbimõeldud testimisplaani. Ka peab olema välistatud kogu süsteemi tõrge mõne alamsüsteemi kapriisuse tõttu, mis vastutusrikaste süsteemide, nagu radarsüsteemi või ka võimsa tule torni automaatikasüsteemi puhul, nõuavad kriitiliste moodulite dubleerimist.

Joonis 1 annab ülevaate tulemärgi (tule torni või poitule) tüüpilisest lokaalsüsteemist, mille RS485-põhine kohtvõrk on sisuliselt avatud vajalikkude funktsionaalsust tagavate moodulite lisamiseks. Tänu sellele on võimalik loodud arhitektuuri taaskasutada ka muude ülesannete lahendamiseks: laterna plinkimist juhtiv moodul – plinker – on programmeeritav vajaliku juhtfunktsiooni täitmiseks, mõõte- ja juhtmooduleid võib vastavalt vajadusele lisada.



Joonis 1.  
Tulemärgi automaatikasüsteem.

Sidemoodul (“andmetelefon”) võimaldab objekti seiret, kaughaldust ja -juhtimist. Tänapäevases variandis on ka GPS positsioneerimis- ja süsteemse aja hoidmise funktsioonid viidud sidekontrolleri tasemele.

Kasutaja suhtleb sellise süsteemi komponentidega personaalarvuti vahendusel, mis seirekeskusena ka kogub ja analüüsib sõlmede olekuinfot. Loodud arhitektuur võimaldab mõningaste muudatuste järel rakendamist ka teistes seire- ja kaugjuhtimisülesannete lahendamist nõudvates valdkondades.

## EPILOOG

Esmaspäev. Vaatamata nädalavahetusel tehtud pingelisele tööle uus toode – Barrikaad 2 – ei saanud ikkagi valmis. Töö alustamisel võetud riskid osutusid liiga suureks. Tellijaga alustati uusi läbirääkimisi teemal, kuidas toimida edasi.

Ajatempliserver töötab, nõutud formaalsused on täidetud ja Cybernetica on esimene täievoliline registreeritud ajatempliteenuse osutaja Eestis. Juba on Cyberneticas välja töötatud tehnoloogia äratanud rahvusvahelist huvi.

Cybernetica arendusosakondades on 58 töötajat, sealhulgas 11 teaduste doktorit. Kaks neist, Jan Villemson ja Peeter Laud, kaitsesid oma doktoritöö tänavu.

Cybernetica AS on ISO 9001:2000 kvaliteedisertifikaati omav rahvusvaheliselt evalveeritud teadus- ja arendusasutus.

## KASUTATUD KIRJANDUS

1. Ansper, A., Buldas, A., Laud, P., Saarepera, M., Willemson, J. Improving the availability of time-stamping services. The 6th Australasian Conference on Information Security and Privacy – ACISP'2001, Sydney, Australia, July 2-4, 2001. LNCS 2119. Springer-Verlag, 2001, 360-375.
2. Buldas, A., Laud P. New linking schemes for digital time-stamping. The 1st International Conference on Information Security and Cryptology – ICISC'98. Seoul, Korea, 18–19 December 1998, 3–14.
3. Buldas, A., Laud, P., Lipmaa, H., Villemson, J. Time-stamping with binary linking schemes. Krawczyk, H. (ed.). Advances in Cryptology – CRYPTO '98, NCS 1462. Springer-Verlag, 1998, 486-501.