ZAKLJUČNO POROČILO
O REZULTATIH OPRAVLJENEGA RAZISKOVALNEGA DELA NA PROJEKTU V OKVIRU CILJNEGA RAZISKOVALNEGA PROGRAMA (CRP) »KONKURENČNOST SLOVENIJE 2006 – 2013«

I. Predstavitev osnovnih podatkov raziskovalnega projekta

1. Naziv težišča v okviru CRP:

Učinkovita uporaba znanja za gospodarski razvoj in kakovostna delovna mesta (2)

2. Šifra projekta:

V2-1022

3. Naslov projekta:

Obvladovanje tehničnih in gospodarsko-družbenih vidikov Interneta stvari v slovenskem okolju (OTGDV-ISt)

3. Naslov projekta

3.1. Naslov projekta v slovenskem jeziku:

Obvladovanje tehničnih in gospodarsko-družbenih vidikov Interneta stvari v slovenskem okolju (akronim OTGDV-ISt)

3.2. Naslov projekta v angleškem jeziku:

Managing technical, busines and social implications of Internet of things in Slovene environment

4. Ključne besede projekta

4.1. Ključne besede projekta v slovenskem jeziku:

internet stvari, sistemi RFID, senzorska omrežja, aplikacija novih tehnologij, socio-ekonomski učinki, varnost in zasebnost

4.2. Ključne besede projekta v angleškem jeziku:

internet of things, RFID systems, senzor networks, application of emerging technologies, socio-economical impacts, security, privacy

5. Naziv nosilne raziskovalne organizacije:

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko

5.1. Seznam sodelujočih raziskovalnih organizacij (RO):

Univerza v Ljubljani, Fakulteta za družbene vede

6. Sofinancer/sofinancerji:

Ministrstvo za visoko šolstvo, znanost in tehnologijo

7. Šifra ter ime in priimek vodje projekta:

11077	prof. dr. Denis Trček

Datum: 11. 10. 2011

Podpis vodje projekta:

prof. dr. Denis Trček

Podpis in žig izvajalca:

II. Vsebinska struktura zaključnega poročila o rezultatih raziskovalnega projekta v okviru CRP

1. Cilji projekta:

1.1. Ali so bili cilji projekta doseženi?

- [x] a) v celoti
- [ ] b) delno
- [ ] c) ne

Če b) in c), je potrebna utemeljitev.

Cilji so bili doseženi.

1.2. Ali so se cilji projekta med raziskavo spremenili?

- [ ] a) da
- [x] b) ne

Če so se, je potrebna utemeljitev:

Cilji projekta se med raziskavo niso spremenili.

2. Vsebinsko poročilo o realizaciji predloženega programa dela[1]:

Metodološko je program izhajal iz vzpostavitve referenčnega modela za obvladovanje področij ISt. Ta model je nato kot visokonivojsko izhodišče služil za sistematično vključitev ustreznih področij interneta stvari, vidikov, podajanje ciljev, določanje korakov, sledenje napredku in vrednotenje ter implementacijo korekcij,upoštevaje specifiko in danosti slovenskega prostora, izhajajoč iz statističnih agregatov po gospodarskih sektorjih.

Izhajajoč iz metodoloških osnov je realizacija ciljev kot sledi:

1. Razvit je bil viskonivojski model za proučevanje različnih vidikov interneta stvari;
2. Tehnološki vidiki interneta stvari:
- Identifikacija in predstavitev ključnih tehnologij, med katere spadajo tehnologija RFID, brezžična senzorska omrežja, RFID senzorska omrežja ter tehnologija NFC;
- Pregled pristopov gradnje vmesnih plasti, kjer ugotavljamo, da standardiziranega pristopa ni, pogoste pa so storitveno usmerjene arhitekture ter arhitektura EPCglobal, poleg navedenih pa obstaja precej ad-hoc rešitev;
- Analiza pristopov naslavljanja in odkrivanja naprav, analiza primernosti protokola TCP, ter vplivov na obstoječo omrežno infrastrukturo;
- Pregled obstoječih in porajajočih se standardov za tehnologije interneta stvari, kjer so glavne institucije ETSI, CEN, CENELEC, ISO, ITU ter IETF;
- Oris varnostne problematike ter problemi varovanja zasebnosti:
  i. Identifikacija omejitev naprav in njihov vpliv na zagotavljanje varnosti, predvsem overjanja in zagotavljanja celovitosti;
  ii. Predstavitev obstoječih rešitev in opis njihovih pomanjkljivosti tako za sisteme RFID kot WSN, med katerimi so tudi lastne rešitve nedeterminističnih kriptografskih protokolov;
  iii. Predstavitev mehanizmov za zagotavljanje zasebnosti in identifikacija njihovih pomanjkljivosti;
  iv. Razvit je bil model groženj za naprave interneta stvari, ki je nato apliciran na scenarije uporabe na področjih infrastrukture, gospodarstva, okolja in družbe;
3. Infrastrukturni vidiki:
- Proučitev koncepta inteligentnega prometnega sistema:
  i. Uporaba sistemov RFID v javnem transportu;
  ii. Študija primera nizozemske kartice {\it ov-chipkaart} in ljubljanske {\it Urbane};
- Proučitev koncepta pametnih mest:
  i. Predstavitev projekta Pametnih mest znotraj i2010;
  ii. Primerjava pametnih mest Ljubljane in Amsterdama;
- Ovrednoteni naslednji scenariji uporabe: mestna infrastruktura, javna razsvetljava (primer Osla), avtomatizacija prometa, železnice, ter scenarij pametne bolnice;
4. Gospodarski vidiki:
- Identifikacija ključnih vplivov na gospodarstvo: izboljšana učinkovitost skozi višjo stopnjo avtomatizacije, korenite spremembe v zasnovi nekaterih proizvodnih procesov, mnogi sinergijski učinki ob priključitvi naprav v omrežje, ter predstavitev ugotovitev

[1] Potrebno je napisati vsebinsko raziskovalno poročilo, kjer mora biti na kratko predstavljen program dela z raziskovalno hipotezo in metodološko-teoretičen opis raziskovanja pri njenem preverjanju ali zavračanju vključno s pridobljenimi rezultati projekta.

Evropske komisije o vplivih na gospodarska področja;
- Ovrednoteni naslednji scenariji uporabe: oskrbovalna veriga in logistika, avtomatizacija tovarn, prevoz nevarnih in občutljivih snovi, vseprisotni sistem pozicioniranja, aplikacije v športu ter scenarij pametne garderobne omare;

5. Okoljski vidiki:
- Pregled vplivov IKT ter interneta stvari na porabo električne energije in splošni načini zmanjševanja porabe z uporabo IKT;
- Študija uporabe interneta stvari pri procesu reciklaže;
- Ovrednoteni naslednji scenariji uporabe: pametni koš za samodejno ločevanje odpadkov, pametna hiša, pametni števci, upravljanje reciklaže izdelkov in obvladovanje naravnih nesreč;

6. Vplivi na družbo:
- Opredelitev in analiza vplivov na zasebno življenje:

i. Utrditev pomena percepcije varnosti in varovanja zasebnosti posameznikov za uspešno sprejetje interneta stvari;

ii. Identifikacija ključnih pozitivnih in negativnih vidikov tehnologije RFID;
- Analiza vplivov na širšo družbo;
- Ovrednoteni naslednji scenariji uporabe: podpora starejšim, internet stvari v turizmu ter družabna omrežja;

7. Vplivi na zakonodajo:
- Pregled relevantne obstoječe slovenske zakonodaje;
- Pregled nekaterih ukrepov za sisteme RFID v EU ter ZDA;

8. Prihodnost interneta stvari:
- Identifikacija in oris možnih načinov razvoja v prihodnosti;
- Identifikacija ključnih kazalnikov smeri razvoja;

9. Statistični pregled:
- Uporabe relevantnih tehnologij po različnih področjih na svetovni ravni;
- Ocenjenih številk bodoče prodaje tehnologij na svetovni ravni.

Na koncu velja v zvezi z zadnjo analizo poudariti, da smo morali nekoliko znižati pričakovanja glede statistično podprtih analiz, kajti SURS (in tudi EUROSTAT) metodološko praktično ne zajemata podatkov, ki bi bili relevantni za internet stvari. To predstavlja pomembno področje za nadaljnje raziskave, kjer pa je eno leto (kolikor je trajal naš projekt) resnično prekratek rok (naše izkušnje pri podobnih projektih, ko smo na nacionalnem nivoju zajemali podatke za izboljšanje informacijske varnosti v povezavi z obvladovenjm inovacij,kažejo, da je za topotrebno imeti na voljo vsaj 3 leta).

3. Izkoriščanje dobljenih rezultatov:

3.1. Kakšen je potencialni pomen[2] rezultatov vašega raziskovalnega projekta za:

- ☐ a) odkritje novih znanstvenih spoznanj;
- ☐ b) izpopolnitev oziroma razširitev metodološkega instrumentarija;
- ☒ c) razvoj svojega temeljnega raziskovanja;
- ☐ d) razvoj drugih temeljnih znanosti;
- ☒ e) razvoj novih tehnologij in drugih razvojnih raziskav.

3.2. Označite s katerimi družbeno-ekonomskimi cilji (po metodologiji OECD-ja) sovpadajo rezultati vašega raziskovalnega projekta:

☐ a) razvoj kmetijstva, gozdarstva in ribolova - Vključuje RR, ki je v osnovi namenjen razvoju in podpori teh dejavnosti;

☒ b) pospeševanje industrijskega razvoja - vključuje RR, ki v osnovi podpira razvoj industrije, vključno s proizvodnjo, gradbeništvom, prodajo na debelo in drobno, restavracijami in hoteli, bančništvom, zavarovalnicami in drugimi gospodarskimi dejavnostmi;

☒ c) proizvodnja in racionalna izraba energije - vključuje RR-dejavnosti, ki so v funkciji dobave, proizvodnje, hranjenja in distribucije vseh oblik energije. V to skupino je treba vključiti tudi RR vodnih virov in nuklearne energije;

☒ d) razvoj infrastrukture - Ta skupina vključuje dve podskupini:

- transport in telekomunikacije - Vključen je RR, ki je usmerjen v izboljšavo in povečanje varnosti prometnih sistemov, vključno z varnostjo v prometu;
- prostorsko planiranje mest in podeželja - Vključen je RR, ki se nanaša na skupno načrtovanje mest in podeželja, boljše pogoje bivanja in izboljšave v okolju;

☒ e) nadzor in skrb za okolje - Vključuje RR, ki je usmerjen v ohranjevanje fizičnega okolja. Zajema onesnaževanje zraka, voda, zemlje in spodnjih slojev, onesnaženje zaradi hrupa, odlaganja trdnih odpadkov in sevanja. Razdeljen je v dve skupini:

☒ f) zdravstveno varstvo (z izjemo onesnaževanja) - Vključuje RR - programe, ki so usmerjeni v varstvo in izboljšanje človekovega zdravja;

☒ g) družbeni razvoj in storitve - Vključuje RR, ki se nanaša na družbene in kulturne probleme;

☐ h) splošni napredek znanja - Ta skupina zajema RR, ki prispeva k splošnemu napredku znanja in ga ne moremo pripisati določenim ciljem;

☐ i) obramba - Vključuje RR, ki se v osnovi izvaja v vojaške namene, ne glede na njegovo vsebino, ali na možnost posredne civilne uporabe. Vključuje tudi varstvo (obrambo) pred naravnimi nesrečami.

---

[2] Označite lahko več odgovorov.

3.3. Kateri so **neposredni rezultati** vašega raziskovalnega projekta glede na zgoraj označen potencialni pomen in razvojne cilje?

Neposredni rezultat sta sledeči objavi:
-TRČEK, Denis. Ergonomic trust management in pervasive computing environments - qualitative assessment dynamics. V: YAN, Jingzhi (ur.), LI, Xiaowei (ur.), DEBEVC, Matjaž (ur.), TJOA, A Min (ur.), HU, Bo (ur.). ICPCA10. [S. l.]: IEEE Press, cop. 2010, str. 1-7, graf. prikazi. [COBISS.SI-ID 8074324] - vabljeno plenarno predavanje

-TRČEK D., Computationally supported quantitative risk management for information systems, Performance models and risk management in communications systems, Springer optimization and its applications, vol. 46, New York, Springer, cop. 2011, str. 55-78. [COBISS.SI-ID 8073812]

Neposredni rezultat vključuje tudi praktične senzorske realizacije na področju e-oskrbe in e-zdravstva (že sodelujemo v enem od takih projektov, ki vključuje tako klinične študije kot tudi tehnološko podporo).

In končno - konkretni rezultat je več kot 100 strani dolg dokument, ki obsega tudi celovit in ekstenziven pregled razpoložljive literature (vključno z zakonodajo) na tem področju in lahko služi kot enovit in zadosten dokument za odločevalce, kjer imajo ti vse relevantne vire in stanje "state-of-the-art" dosegljive na enem mestu.

3.4. Kakšni so lahko **dolgoročni rezultati** vašega raziskovalnega projekta glede na zgoraj označen potencialni pomen in razvojne cilje?

Glede na našo ekspertizo bo nadaljevanje s CRP-om omogočenih raziskav vodilo v naslednjih nekaj letih pri razvoju programske rešitve za celovito obvladovanje tveganj v IS, kjer bo vključen internet stvari.

3.5. Kje obstaja verjetnost, da bodo vaša znanstvena spoznanja deležna zaznavnega odziva?

- ☐ a) v domačih znanstvenih krogih;
- ☒ b) v mednarodnih znanstvenih krogih;
- ☐ c) pri domačih uporabnikih;
- ☒ d) pri mednarodnih uporabnikih.

3.6. Kdo (poleg sofinancerjev) že izraža interes po vaših spoznanjih oziroma rezultatih?

Člani konzorcija SALUS, ki se prijavlja na razpis 7OP v novembru tega leta s področja varnosti komunikacijskih sistemov struktur za reševanje in zaščito in kjer bodo senzorska omrežja ter internet stvari igrala pomembno vlogo (člani konzorcija so ugledne organizacije kot npr. Fraunhofer, Casidian / EADS, itd.). Prilagamo info-list.

3.7. Število diplomantov, magistrov in doktorjev, ki so zaključili študij z vključenostjo v raziskovalni projekt?

V okviru projekta sta se odvijali tudi eno magistrsko delo in ena diplomska naloga:

- STARC, Iztok. Zagotavljanje varnosti za okolja omrežnih sistemov radiofrekvenčne identifikacije : magistrsko delo. Ljubljana: [I. Starc], 2011. XII, 202 str., ilustr. http://eprints.fri.uni-lj.si/1494/. [COBISS.SI-ID 8605780]

- ŽVANUT, Primož. Ocenjevanje tveganj v informacijskih sistemih na osnovi teorije omrežij : diplomsko delo. Ljubljana: [P. Žvanut], 2011. 93 f., ilustr. http://eprints.fri.uni-lj.si/1501/. [COBISS.SI-ID 8609364]

4. Sodelovanje z tujimi partnerji:

4.1. Navedite število in obliko formalnega raziskovalnega sodelovanja s tujimi raziskovalnimi inštitucijami.

Formalnega sodelovanja tekom samega projekta nismo zaključili (trajal je le eno leto), smo pa na osnovi CRP-a vzpostavili povezave za konzorcij SALUS, ki se pravkar formalno zapira za prijavo na razpis EU v okviru 7OP.

4.2. Kakšni so rezultati tovrstnega sodelovanja?

Prijava na razpis v okviru 7 OP (glej točko 4.1):
Call identifier: FP7-SEC-2012-1
Date of publication: July 2011
Deadline: 23/November/2011 at 17.00.00
Call topic addressed:
Activity: 10.5 Security systems integration, interconnectivity and interoperability
Area: 10.5.2 Secure Communications
SEC-2012.5.2-1 Preparation of the next generation of PPDR comm. network – CP-FP

5. Bibliografski rezultati[3] :

Za vodjo projekta in ostale raziskovalce v projektni skupini priložite bibliografske izpise za obdobje zadnjih treh let iz COBISS-a) oz. za medicinske vede iz Inštituta za biomedicinsko informatiko. Na bibliografskih izpisih označite tista dela, ki so nastala v okviru pričujočega projekta.

6. Druge reference[4] vodje projekta in ostalih raziskovalcev, ki izhajajo iz raziskovalnega projekta:

Vodja projekta je s področja omenjenega ciljnega raziskovalnega programa sodeloval kot osrednji gost na RTV SLO, oddaja Trikotnik (Življenje z velikimbratom), zasebnost v okoljih vseprisotnega računalništva in interneta stvari - glej http://tvslo.si/predvajaj/zivljenje-z-velikim-bratom/ava2.108024021/.

Glej tudi točko 3.3 - problematika e-zdravja in e-oskrbe.

[3] Bibliografijo raziskovalcev si lahko natisnete sami iz spletne strani:http:/www.izum.si/

[4] Navedite tudi druge raziskovalne rezultate iz obdobja financiranja vašega projekta, ki niso zajeti v bibliografske izpise, zlasti pa tiste, ki se nanašajo na prenos znanja in tehnologije.
Navedite tudi podatke o vseh javnih in drugih predstavitvah projekta in njegovih rezultatov vključno s predstavitvami, ki so bile organizirane izključno za naročnika/naročnike projekta.

V2-1022

Fakulteta za računalništvo in informatiko
Fakulteta za družbene vede

OTGDV-ISt

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Univerza v Ljubljani
Fakulteta za družbene vede

Ciljni raziskovalni program
KONKURENČNOST SLOVENIJE 2006–2013

Obvladovanje tehničnih in gospodarsko-družbenih vidikov interneta stvari v slovenskem okolju

Končno poročilo, različica 1.0

David Jelenc, Eva Zupančič, Denis Trček, Franc Solina in Jaro Berce

12. oktober 2011

Ciljni raziskovalni program
KONKURENČNOST SLOVENIJE 2006–2013

OTGDV-ISt
12. oktober 2011

Obvladovanje tehničnih in gospodarsko-družbenih vidikov interneta stvari v slovenskem okolju

Končno poročilo, različica 1.0

David Jelenc, Eva Zupančič, Denis Trček in Franc Solina

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko
Tržaška 25, 1000 Ljubljana

Jaro Berce

Univerza v Ljubljani
Fakulteta za družbene vede
Kardeljeva ploščad 5, 1000 Ljubljana

Naročnik Javna agencija za raziskovalno dejavnost Republike Slovenije
Tivolska cesta 30, 1000 Ljubljana

Ministrstvo za visoko šolstvo, znanost in tehnologijo
Kotnikova ulica 38, 1000 Ljubljana

Pogodba 1000-10-281022 / V2-1022

Povzetek: Pričujoči dokument povzema raziskovalno in analitično delo na področju interneta stvari raziskovalnih skupin s Fakultete za računalništvo in informatiko in s Fakultete za družbene vede. Raziskovalni projekt je obsegal večplastno preučitev pojava interneta stvari.

Predmet proučevanja se najprej obravnava s tehnološkega vidika, tako da se opiše vse relevantne tehnologije in standarde, ki sestavljajo internet stvari. Predlagamo model za varnostno analizo groženj v internetu stvari, ki ga apliciramo na izbrane scenarije uporabe na različnih področjih. V nadaljevanju obravnavamo infrastrukturni, gospodarski ter okoljski vidik, kjer poleg relevantnih študij vplivov navajamo tudi tipične scenarije uporabe, ki jih ocenimo s predlaganim varnostnim modelom. Vplivi na družbo, kjer posebno pozornost namenjamo percepciji varnosti in zasebnosti, so analizirani tako z vidika posameznika kot z vidika družbe kot celote. Študija obravnava tudi relevantne normativne vidike, kjer predstavimo tako obstoječe slovensko stanje kot stanje na ravni Evropske unije. Raziskava se zaključi z možnimi načini razvoja interneta stvari v prihodnosti, kjer podajamo relevantne kazalnike napredka. V dodatku je podan aktualen statističen pregled in napovedi prodaje relevantnih tehnologij v prihodnje.

Kazalo

Kazalo slik in tabel

Slike

Tabele

1 Uvodno poglavje

V uvodu predstavimo tri ključne pristope k definiranju interneta stvari, predstavimo model za proučevanje različnih vidikov interneta stvari ter napovemo strukturo pričujočega dokumenta.

1.1 Predmet proučevanja

Internet stvari (angl. internet of things), kratko ISt, je nova hitro razvijajoča se paradigma, ki se uveljavlja na področju sodobnih (brezžičnih) telekomunikacijskih tehnologij. V osrčju ideje je množica miniaturnih in primitivnih računskih naprav t. i. stvari (angl. things, objects) – kot so značke RFID (angl. RFID tags), senzorji (angl. sensors), prožilci (angl. actuators), mobilni telefoni in drugi – ki so z uporabo ustreznih naslovnih shem in internetnega omrežja sposobne sodelovati med seboj in okoljem z namenom doseganja skupnih ciljev [1].

Gre torej za sklop tehnologij, ki bodo po mnogih predvidevanjih imele vpliv na veliko vidikov vsakdanjega življenja današnjega človeka. Vplivi se bodo izražali tako v domačem kot na delovnem okolju. Z ISt prihaja čas domotike (angl. domotics), računalniško podprtega bivanja (angl. assisted living), e-Zdravja (angl. e-Health), računalniško podprtega učenja (angl. enhanced learning) in mnogih drugih tehnologij, ki bodo še bolje avtomatizirale industrijske procese, podprle storitve logistike, olajšale obvladovanje poslovnih procesov, omogočile inteligenten transport ljudi in blaga. Tako ni presenetljivo, da je Nacionalni obveščevalni svet ZDA (angl. United States National Intelligence Council, NIC), umestil ISt na seznam *šestih najbolj prebojnih tehnologij* do leta 2025 [2]. NIC predvideva, da bodo do omenjene letnice vsakodnevne stvari (embalaža, pohištvo, dokumenti in druge) zmožne internetne komunikacije. Internet stvari je lahko, v kolikor pride do masovnega sprejetja, podoben katalizator ekonomskega napredka kot je danes *navadni* internet. Hkrati pa NIC opozarja na nevarnosti, ki izhajajo iz te tehnologije, saj pravi, da bo ISt omogočil vsaki *stvari*, da postane vir informacijskih groženj.

V literaturi je mogoče najti različne definicije, kaj internet stvari pravzaprav je. Pojavlja se mnogo različnih interpretacij, ki neredko pustijo bralca v dvomu. Razloge lahko najdemo že kar v besedni zvezi internet stvari, ki

sestoji iz besed *internet* ter *stvari*. Nekatere definicije poudarjajo vidik interneta, druge vidik stvari. Razlike, včasih precejšnje, so posledica različnih zornih kotov različnih deležnikov. Nekateri proučujejo internet stvari z vidika interneta, tj. različnih možnosti povezljivosti, drugi z vidika stvari, tj. objektov, ki se povezujejo. V grobem pa internet stvari pomeni *svetovno omrežje medsebojno povezanih in enolično naslovljenih objektov, ki za komunikacijo uporabljajo standardne protokole* [3]. V takšnem omrežju velikega števila (heterogenih) naprav predstavlja enolično naslavljanje ter predstavitev in hranjenje izmenjanih informacij težak problem. Rešitev tega mnogi vidijo v uporabi semantičnih tehnologij, ki so navdahnile tretji, semantični sklop definicij.

1.1.1 Vidik stvari

Prvi pogledi na ISt so poudarjali vidik stvari. Te so bile večinoma zelo preproste; šlo je le za značke RFID. Izum izraza internet stvari se pripisuje The Auto-ID Labs[1], svetovnem omrežju akademskih raziskovalnih ustanov s področja senzoričnih in RFID tehnologij. Te institucije so v sodelovanju s konzorcijem EPCglobal[2] skušale osnovati arhitekturo za internet stvari [4]. Njihovo delo je bilo osredotočeno na razvoj elektronske kode (angl. electronic product code, EPC) za podporo širjenja omrežij RFID v svetovni trgovini in ustanoviti globalni industrijski standard za omrežje EPCglobal (angl. EPCGlobal Network). Slednji omogoča sledenje objektov skozi celotno oskrbovalno verigo. Gre za pomembno komponento interneta stvari, vsekakor pa ne edino.

Gledano širše, ISt ni zgolj globalni sistem EPC, v katerem so edini objekti značke RFID. Podobno lahko trdimo tudi za njihove alternative, kot npr. je Ubiquitous ID (uID)[3]. Seveda sta vidika sledljivosti in naslavljanja izrednega pomena, vendar je celovita vizija ISt širša. Tako denimo avtorji v [5] še vedno poudarjajo pomembnost tehnologije RFID, vendar omenjajo še brezkontaktno tehnologijo NFC (angl. near field communication, NFC) ter brezžična senzorična omrežja s prožilci (angl. Wireless Sensor and Actuator Networks, WSAN). Tehnologiji NFC in WSAN skupaj z omrežji RFID pojmujejo kot atomarne komponente interneta stvari. Na tem mestu velja omeniti projekt WISP (angl. Wireless Identification and Sensing Platforms) podjetja Intel Labs Seattle[4], kjer razvijajo *stvari*, ki imajo sposobnosti značk RFID, prožilcev (16-bitnih procesorji) in različnih senzorjev.

[1] http://www.autoidlabs.org
[2] http://www.gs1.org/epcglobal
[3] http://www.uidcenter.org
[4] http://seattle.intel-research.net/wisp

V domeno vidika stvari spada tudi koncept *spime* [6]. Gre za angleško skovanko iz besed prostor (angl. space) in čas (angl. time), pomeni pa predmet, ki ga tekom njegove življenjske dobe lahko sledimo v prostoru in času. Čeprav gre za teoretičen koncept, pa lahko najdemo več implementacij med t. i. pametnimi rečmi (angl. smart items). Gre za različne senzorje zmožne (v smislu ISt klasičnega) brezžičnega komuniciranja, pomnjenja in reagiranja ter tudi avtonomnega in proaktivnega obnašanja, prilagajanja okolju in sodelovanja z okolico. Podobno, a bolj splošno so pristopili pri ITU [7], kjer pravijo, da z ISt prehajamo iz klasičnega interneta, kjer imamo *povezljivost kadarkoli in kjerkoli za kogarkoli* v internet kjer bo *povezljivost kadarkoli in kjerkoli za kogarkoli in karkoli.* To je tudi pogled, ki ga lahko zasledimo iz dokumentov Evropske komisije [3], kjer ISt opredeljujejo kot *okolje, kjer imajo stvari identitete in virtualne osebnosti, delujejo v pametnih okoljih ter uporabljajo pametne vmesnike za povezavo in komunicirajo z družabnimi, okoljskimi in uporabniškimi konteksti.*

1.1.2 Vidik interneta

Dodaten poudarek na povezljivosti lahko zasledimo v viziji konzorcija CASAGRAS[5]. Internet stvari po njihovo pomeni *svet, kjer stvari avtomatično komunicirajo z računalniki in med seboj ter zagotavljajo storitve v dobrobit človeštva.* Omenjen konzorcij a) predlaga ISt kot globalno infrastrukturo, ki povezuje virtualni in dejanski svet objektov in b) poudarja pomembnost vključitve obstoječe internetne infrastrukture. Tako bi naj ISt postala podporna arhitektura za porazdeljene storitve in aplikacije [8].

Zveza IP za pametne predmete (angl. IP for Smart Objects, IPSO)[6], osnovana z namenom promocije protokola IP kot glavne omrežne tehnologije za povezovanje pametnih stvari, zatrjuje, da je sklad IP dovolj lahek, tj. računsko nezahteven, da ga je moč uporabljati na pametnih predmetih. Tako poudarjajo, da lahko z integracijo standarda IEEE 802.15.4 [9] ter tehnologije 6LowPAN [10] v sklad protokolov TCP/IP v celoti realiziramo paradigmo ISt.

Načelu zmanjševanja kompleksnosti sklada IP zelo sorodno sledi t. i. Internet-0 [11]. Namen je priti do točke, kjer lahko *usmerjamo pakete IP preko česarkoli* (angl. route IP over anything). V teh krogih velja prepričanje, da je to najboljši način premika iz klasičnega interneta t. i. *interneta naprav* v internet stvari. Tako zveza IPSO kot Internet-0 vidita ISt kot

[5] http://www.rfidglobal.eu
[6] http://ipso-alliance.org

poenostavljen sklad IP protokolov, ki omogoča naslavljanje in dostopnost informacij o predmetih iz vsake lokacije.

1.1.3 Vidik semantike

Semantično usmerjeni pogledi na ISt so posledica dejstva, da bo ISt sestavljala nepredstavljiva množica zelo heterogenih naprav. V tej množici bo predstavitev, shranjevanje, iskanje in organiziranje informacij, ki jih bodo naprave generirale, izjemno težavno. Kot možno rešitev nekateri vidijo semantične tehnologije. Slednje lahko uporabijo različne modelirne tehnike za opis predmetov, iskalne poizvedbe in drugo [12, 13].

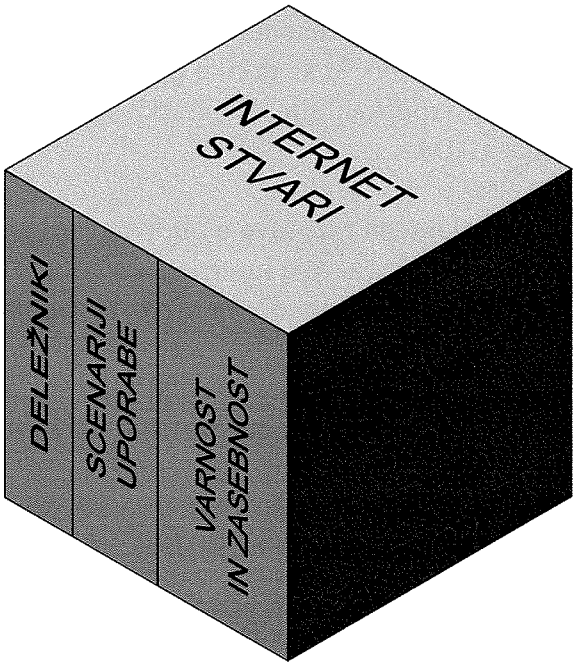
1.2 Model proučevanja

Zapisane definicije in različna pojmovanja interneta stvari pričajo o mnogoterih načinih proučevanja tega pojava. V raziskovalnem projektu Obvladovanje tehničnih in gospodarsko-družbenih vidikov Interneta stvari v slovenskem okolju gledamo na ISt večplastno. Z upoštevanjem dejstva, da je dobro poznavanje tehnologije ključno za celovito analizo tako kompleksnega pojava, najprej analiziramo vse relevantne tehnološke dejavnike. Drugi del raziskave pa se nanaša na uporabo identificiranih tehnologij in analiziranje različnih vidikov pojava internet stvari. Tako posebej analiziramo infrastrukturni, gospodarski, družbeni, okoljski ter zakonodajni vidik. Za vsakega od teh vidikov orišemo nekatere obstoječe in tudi bodoče scenarije uporabe. Za vsakega izmed scenarijev uporabe identificiramo ključne deležnike in podamo analizo groženj. Model proučevanja je grafično prikazan na Sliki 1.

Dinamičnost in večplastnost nam pri proučevanju določenih vidikov povzročata, da internet stvari proučujemo tudi izven okvirov modela. Tako je npr. nesmiselno iskati scenarije uporabe na zakonodajnem področju, saj ta vidik zahteva drugačen pristop. Kljub temu se trudimo čim bolj držati zastavljenih smernic proučevanja.

1.3 Struktura dokumenta

V drugem poglavju predstavimo tehnološki pogled na internet stvari. Predstavimo ključne tehnologije, standarde, pristope h gradnji vmesnih pasti, analiziramo relevantne komunikacijske protokole ter poglavje zaključimo z varnostjo in zasebnostjo, kjer predstavimo model groženj, ki se uporablja za ocenjevanje scenarijev uporabe.



Slika 1. Visokonivojski model proučevanja

V tretjem poglavju predstavimo področja uporabe interneta stvari na področju infrastrukture, osvetlimo koncepte pametnih mest in pametnega prometa ter podamo nekatere primerjave slovenskega okolja z nizozemskim. Poglavje se zaključi z navedbo tipičnih scenarijev uporabe.

Četrto poglavje opisuje gospodarske vidike interneta stvari. Najprej predstavimo prognozo učinka interneta stvari na gospodarstvo, nato pa opišemo najbolj pogoste scenarije uporabe.

Peto poglavje zajema vplive interneta stvari na okolje. V njem opišemo, kako lahko internet stvari pomaga slediti paradigmi trajnostnega razvoja, njegov učinek na porabo energije ter načine, kako uporabiti internet stvari pri reciklaži. Poglavje se zaključi z navedbo tipičnih scenarijev uporabe, ki so ocenjeni z modelom groženj.

Šesto poglavje poda analitični pogled na družbeno dinamiko v okolju interneta stvari. Osvetljen je tako vidik posameznika v takšni družbi kot vplivi na družbo kot celoto. Poseben poudarek je namenjen občutku varnosti in zasebnosti posameznika. Tukaj so osvetljeni tako pozitivni kot negativni vidiki tehnologij interneta stvari s stališča posameznika. Tudi to poglavje se zaključi z navedbo tipičnih scenarijev uporabe.

Sedmo poglavje osvetli relevantne zakonodajne vidike. Najprej predstavimo obstoječo slovensko zakonodajo, ki se dotika področja uvedbe ISt, nato pa še nekatere dokumente Evropske unije. Na kratko se dotaknemo tudi reševanja te problematike v ZDA.

Osmo poglavje podaja zaključno razpravo o obravnavani temi. Tukaj predstavimo različne možne načine razvoja interneta stvari v prihodnosti in nekatere kazalnike, preko katerih je mogoče ta razvoj spremljati.

V dodatku je podan aktualen statističen pregled relevantnih tehnologij, ki sestavljajo internet stvari, ter nekatere ocene, kako naj bi se povpraševanje po njih gibalo v bodočnosti.

1.4 Povzetek rezultatov projekta

Na tem mestu na kratko povzemamo ključne rezultate ciljnega raziskovalnega projekta Obvladovanje tehničnih in gospodarsko-družbenih vidikov interneta stvari v Sloveniji. Glavni rezultati so:

1. razvit je bil viskonivojski model za proučevanje različnih vidikov interneta stvari;
2. tehnološki vidiki interneta stvari:
   - identifikacija in predstavitev ključnih tehnologij, med katere spadajo tehnologija RFID, brezžična senzorska omrežja, RFID senzorska omrežja ter tehnologija NFC;
   - pregled pristopov gradnje vmesnih plasti, kjer ugotavljamo, da standardiziranega pristopa ni, pogoste pa so storitveno usmerjene arhitekture ter arhitektura EPCglobal. Poleg navedenih obstaja precej ad-hoc rešitev;
   - analiza pristopov naslavljanja in odkrivanja naprav, analiza primernosti protokola TCP ter vplivov na obstoječo omrežno infrastrukturo;
   - pregled obstoječih in porajajočih se standardov za tehnologije interneta stvari, kjer so glavne institucije ETSI, CEN, CENELEC, ISO, ITU ter IETF;
   - oris varnostne problematike ter problemi varovanja zasebnosti:
     - identifikacija omejitev naprav in njihov vpliv na zagotavljanje varnosti, predvsem overjanja in zagotavljanja celovitosti;

- predstavitev obstoječih rešitev in opis njihovih pomanjkljivosti tako za sisteme RFID kot WSN, med katerimi so tudi lastne rešitve nedeterminističnih kriptografskih protokolov;
- predstavitev mehanizmov za zagotavljanje zasebnosti in identifikacija njihovih pomanjkljivosti;
- razvit je bil model groženj za naprave interneta stvari, ki je nato apliciran na scenarije uporabe na področjih infrastrukture, gospodarstva, okolja in družbe;

3. infrastrukturni vidiki:
   - proučitev koncepta inteligentnega prometnega sistema:
     - uporaba sistemov RFID v javnem transportu;
     - študija primera nizozemske kartice *ov-chipkaart* in ljubljanske *Urbane*;
   - proučitev koncepta pametnih mest:
     - predstavitev projekta Pametnih mest znotraj i2010;
     - primerjava pametnih mest Ljubljane in Amsterdama;
   - ovrednotenje naslednjih scenarijev uporabe: mestna infrastruktura, javna razsvetljava (primer Osla), avtomatizacija prometa, vozni red vlakov, ter scenarij pametne bolnice;
4. gospodarski vidiki:
   - identifikacija ključnih vplivov na gospodarstvo: izboljšana učinkovitost skozi višjo stopnjo avtomatizacije, korenite spremembe v zasnovi nekaterih proizvodnih procesov, mnogi sinergijski učinki ob priključitvi naprav v omrežje, ter predstavitev ugotovitev Evropske komisije o vplivih na gospodarska področja;
   - ovrednotenje naslednjih scenarijev uporabe: oskrbovalna veriga in logistika, avtomatizacija tovarn, prevoz nevarnih in občutljivih snovi, vseprisotni sistem pozicioniranja, aplikacije v športu ter scenarij pametne garderobne omare z osebnim modnim svetovalcem;
5. okoljski vidiki:
   - pregled vplivov IKT ter interneta stvari na porabo električne energije in splošni načini zmanjševanja porabe z uporabo IKT;
   - študija uporabe interneta stvari pri procesu reciklaže;
   - ovrednotenje naslednjih scenarijev uporabe: pametni koš za samodejno ločevanje odpadkov, pametna hiša, pametni števci, upravljanje reciklaže izdelkov in obvladovanje naravnih nesreč;

6. vplivi na družbo:
   - opredelitev in analiza vplivov na zasebno življenje:
     - utrditev pomena percepcije varnosti in varovanja zasebnosti posameznikov za uspešno sprejetje interneta stvari;
     - identifikacija ključnih pozitivnih in negativnih vidikov tehnologije RFID;
   - analiza vplivov na širšo družbo;
   - ovrednotenje naslednjih scenarijev uporabe: podpora starejšim, internet stvari v turizmu ter družabna omrežja;
7. vplivi na zakonodajo:
   - pregled relevantne obstoječe slovenske zakonodaje;
   - pregled nekaterih ukrepov za sisteme RFID v EU ter ZDA;
8. prihodnost interneta stvari:
   - identifikacija in oris možnih načinov razvoja v prihodnosti;
   - identifikacija ključnih kazalnikov smeri razvoja;
9. Statistični pregled:
   - uporaba relevantnih tehnologij po različnih področjih na svetovni ravni;
   - ocena bodoče prodaje tehnologij na svetovni ravni.

2 Tehnološki vidik interneta stvari

Internet stvari je konglomerat, ki bo realiziran z integracijo različnih tehnologij. V tem razdelku predstavimo najpomembnejše. Naš namen ni podrobna predstavitev vsake od tehnologij, temveč njihova umestitev v koncept ISt. Dodatne podrobnosti je moč najti v priloženih referencah.

2.1 Tehnologije identifikacije, zaznavanja in komuniciranja

Karkoli, kjerkoli in preko poljubnega medija (angl. anytime, anywhere, anymedia) je vizija, ki je že dalj časa gonilo napredka v komunikacijskih tehnologijah. V tem pogledu so brezžične tehnologije odigrale ključno vlogo. Število oddajnikov se je skozi leta vztrajno večalo, tako da se danes približujemo razmerju 1:1 [14]. Če k temu pripišemo še tendenco zmanjševanja velikosti, teže, energijske porabe ter cene oddajnikov, vidimo, da se bo to razmerje kmalu drastično obrnilo v korist števila naprav. Tako bo mogoče pritrditi oddajnike na praktično vsak predmet, kar nas pripelje do koncepta ISt.

2.1.1 Tehnologija radio-frekvenčne identifikacije

Pomembno vlogo bo pri tem imela tehnologija radio-frekvenčne identifikacije (angl. radio-frequency identification, RFID). Sisteme RFID sestavljajo čitalniki (angl. reader, interrogator) in značke (angl. tags). Tipično en čitalnik izprašuje več značk [15]. Značke se pritrdijo na različne *stvari*, nato pa se vsaki znački (in posredno tudi vsaki *stvari*) dodeli edinstven identifikator (angl. unique identifier, ID). Stvari so lahko zelo različne in obsegajo vse od (pol)izdelkov v oskrbovalni verigi do živali, v nekaterih primerih pa celo ljudi.

Komunikacijo navadno prične čitalnik, tako da odda ustrezen elektromagnetni signal, s katerim izzove značko. Signal predstavlja poizvedbo o prisotnosti vsem značkam v dometu čitalnika. Značke ujamejo del oddanega signala in kot odgovor sporočijo njihov identifikator. Pri tem je izjemnega pomena, da lahko komunikacija poteka, tudi če čitalnik in značka nista v neposrednem vidnem polju (angl. line-of-sight). Na tak način so sistemi RFID uporabni za nadzor in sledenje stvarem v realnem času in skupaj z uporabo ustreznih zalednih sistemov omogočajo preslikavo realnega v virtualni svet.

Značka RFID je majhen mikročip[7], ki je pritrjen na anteno. Antena se uporablja tako za sprejem signala kot oddajo identifikatorja. Antena in mikročip tako sestavljata značko, ki je največkrat predstavljena kot majhna nalepka. Nekatere značke so lahko izjemno majhne; podjetje Hitachi je razvilo značko dimenzij 0.4 mm × 0.4 mm × 0.15 mm.

Poznamo več vrst značk. Najbolj pogoste so *pasivne značke*. Zanje je značilno, da nimajo lastnega napajanja. Pasivne značke se energetsko oskrbijo s signalom, ki ga odda čitalnik. Signal v anteni značke inducira električni napetost, ki se uporabi za napajanje mikročipa. Ta nato čitalniku pošlje identifikator. Navadno je v takih sistemih dobitek antene (angl. gain), tj. razmerje v moči signala, ki ga je čitalnik sprejel in močjo signala, ki ga je taisti čitalnik oddal, zelo nizek. Ker pa so antene na značkah usmerjene, lahko značke uspešno preberemo na razdalji do več metrov. Prenos informacij lahko poteka v različnih frekvenčnih pasovih; od nizkih (LF) med 124-135 kHz, do ultra visokih (UHF) med 860-960 MHz. Slednje imajo med pasivnimi značkami najdaljši domet.

Druga skupina značk se energetsko oskrbi z baterijami. V tem pogledu ločimo *semipasivne* in *aktivne značke*. Prve z energijo iz baterij oskrbijo mikročip, medtem ko energijo iz signala uporabijo za napajanje oddajnika. Nasprotno pa aktivne značke uporabijo energijo iz baterij tako za krmiljenje mikročipa kot tudi za prenos signala. Aktivne značke imajo med vsemi značkami največji domet, prav tako pa tudi najvišjo ceno. Aktivne značke so lahko, za razliko do pasivnih in semipasivnih, pobudnik komunikacije, medtem ko pri pasivnih in semipasivnih značkah komunikacijo vedno prične čitalnik.

2.1.2 Tehnologija brezžičnih-senzoričnih omrežij

Naslednji pomemben gradnik ISt predstavljajo brezžična senzorična omrežja (angl. wireless sensor networks, WSN). Sicer obstaja tudi možnost kombiniranja sistemov RFID s sistemi WSN. S tem dobimo še boljše načine spremljanja predmetov; poleg njihove lokacije lahko merimo tudi fizikalne količine kot so temperatura, vlaga in drugo. A več o tej tehnologiji v naslednjem podrazdelku.

Brezžično senzorično omrežje sestavlja določeno (običajno veliko) število senzoričnih vozlišč (angl. sensing nodes), ki med seboj brezžično komunicirajo. Posamezna vozlišča beležijo meritve fizikalnih pojavov in jih pošiljajo

[7]Obstajajo tudi značke, ki niso osnovane na mikročipih (angl. chipless tag), a so trenutno še predmet aktivnih raziskav in še niso pogosto uporabljane.

manjšemu številu posebnih ponornih vozlišč (angl. sinks). Slednja posredujejo informacije v zaledne sisteme. Običajno imamo le eno ponorno vozlišče, zato morajo ostala navadna vozlišča tudi znati usmerjati (angl. routing) podatke na poti od vozlišča, ki je meritev opravilo, do ponornega vozlišča.

O senzoričnih omrežjih obstaja obširna znanstvena literatura, ki pogosto naslavlja težave na komunikacijski ravni [16]. Danes večina komercialno dostopnih brezžičnih senzoričnih omrežij uporablja standard IEEE 802.15.4 [9]. Slednji v brezžičnih osebnih omrežjih (angl. wireless personal area networks, WPAN) določa fizično ter del povezovalne plasti (plast za nadzor dostopa do medija [angl. medium access control, MAC]) za naprave z nizko porabo energije ter nizko bitno hitrostjo. Standard IEEE 802.15.4 *ne* določa višjih plasti sklada komunikacijskih protokolov, ki pa so nujne za neposredno povezavo senzoričnih vozlišč v internet. To predstavlja precejšen zalogaj zaradi naslednjih razlogov (povzeto po [1]):

- Omrežja WSN sestavlja veliko število vozlišč. Danes je naslovni prostor IPv4 že izčrpan, tako da je nujna uporaba protokola IPv6, če želimo doseči globalno dosegljivost vsake *stvari*.
- Standard IEEE 802.15.4 predpisuje 127 bajtov kot največjo velikost paketa na fizični plasti. Posledično je največja velikost okvirja na plasti MAC 102 bajta. Če k temu dodamo varnostne mehanizme povezovalne plasti, se lahko velikost okvirja še dodatno zmanjša. Takšne velikosti pa so dejansko premajhne, ko jih primerjamo s tipičnimi velikosti paketov IP.
- Senzorična vozlišča so pogosto v stanju mirovanja (angl. sleep mode), v katerem varčujejo z energijo. V takšnem stanju ne morejo usmerjati paketov, zato je takšen način delovanja za omrežja IP problematičen.

2.1.3 Tehnologija RFID-senzoričnih omrežij

Integracija pasivnih značk RFID ter omrežij WSN je po mnenju nekaterih naslednji logičen korak. Tehnologija zaznavanja kombinirana z možnostjo enolične identifikacije odpira v domeni ISt veliko novih možnosti uporabe [17]. Že v uvodu je bil omenjen projekt platforme za brezžično identifikacijo in zaznavanje (angl. wireless identification and sensing platform, WISP), v katerem sodelujeta Univerza Washington ter podjetje Intel Labs Seattle[8]. Naprave WISP imajo enake značilnosti kot pasivne značke RFID, poleg tega

[8] `http://seattle.intel-research.net/wisp`

Tabela 1. Primerjava karakteristik sistemov RFID, omrežij WSN ter omrežij RSN

	RFID	WSN	RSN
Procesiranje	Ne	Da	Da
Senzorične meritve	Ne	Da	Da
Način komunikacije	Asimetričen	Med vsemi	Asimetričen
Doment [m]	10	100	3
Vir energije	Čitalnik	Baterija	Čitalnik
Čas avtonomije	Neomejen	Do 3 let	Neomejen
Velikost	Izredno majhno	Majhno	Majhno

pa so zmožne še senzoričnega zaznavanja ter računskih operacij. Naprave WISP se energijsko oskrbijo s signalom, ki ga oda čitalnik RFID. Slednjemu se naprava WISP predstavlja kot navadna značka RFID, ki je skladna s standardom EPC Gen1 ali Gen2. Energija se porabi za napajanje 16-bitnega splošnonamenskega procesorja, ki je zmožen opravljati različne računske operacije, kot so vzorčenje in poročanje meritev, zapisovanja na bliskovni pomnilnik (angl. flash) ter opravljati kriptografske izračune. Naprave WISP opremljajo s svetlobnimi in temperaturnimi senzorji ter senzorji za merjenje pritiska, pospeškov in vlažnosti.

Naprave WISP ter ostali podobni gradniki omogočajo gradnjo senzoričnih RFID omrežij (angl. RFID sensor network, RSN). Omrežja RSN sestavlja določeno število vozlišč, tj. značk RFID, ki so dodatno zmožne senzoričnega zaznavanja ter računskih operacij, in čitalnikov RFID. Slednji nastopajo v vlogi ponornih vozlišč ter v vlogi energijskega oskrbovalca značk. V Tabeli 1, ki je povzeta po [18], so podane nekatere karakteristike sistemov RFID, omrežij WSN ter omrežij RSN.

2.1.4 Brezkontaktna tehnologija NFC

V tem sklopu tehnologij je smiselno omeniti tudi brezkontaktno tehnologijo NFC (angl. near field communication) [19]. Tehnologija NFC, v nasprotju s prej predstavljenimi tehnologijami, ni toliko namenjena vseprisotnemu računalništvu (angl. ubiquitous computing), temveč omogoča komunikacijo oz. lajša vzpostavitev komunikacije med stvarmi. Dodatna posebnost te tehnologije je tudi v tem, da mora uporabnik *eksplicitno izraziti željo* po vzpostavitvi povezave.

Tehnologija NFC je dejansko le ovoj okoli tehnologije RFID. Gre torej za čitalnike ter značke z zelo omejenim dosegom; tipično okoli 20 cm. Za vzpostavitev povezave tako potrebujemo čitalnik (ali pisalnik) NFC (angl. NFC

reader, writer) ter značko NFC (angl. NFC tag). Slednja je sestavljena iz integriranega vezja, na katerem so shranjeni podatki, ter antene, preko katere značka komunicira s čitalnikom.

Tehnologija omogoča uporabniku, da zgolj s približanjem dveh naprav izvede intuitivno, varno in brezžično transakcijo, dostopa do digitalnih vsebin oz. v splošnem povezuje elektronske naprave. Gre torej za širok nabor možnih načinov uporabe, ki jih lahko v grobem razdelimo v tri področja; iniciacija storitev (angl. service initiation), komunikacija P2P (angl. P2P communication) ter plačevanje in poverjanje (angl. payment and ticketing).

Iniciacija storitev običajno poteka tako, da uporabnik približa NFC podprto napravo, denimo mobilni telefon, znački NFC, s katere se nato prenese informacija. Navadno gre za kratka besedila kot sta npr. spletni naslov ali telefonska številka. Primer uporabe so t. i. pametni posterji (angl. smart poster), ki oglašujejo vsebine na enak način kot navadni posterji, dodatno pa imajo priložene značke NFC. Uporabnik s približanjem mobilnega telefona sliki na posterju, pod katero je pritrjena značka NFC, na telefon prenese vsebino značke, s katero nato dostopa do dodatnih vsebin o izdelku.

Tehnologijo NFC lahko uporabimo, da poenostavimo (lokalno) komunikacijo med napravami. Če gre za majhno količino podatkov, tj. do 1 kB, se lahko preko radio-frekvenčnih valov prenese kar dejanska vsebina. Bolj pogosto pa se s pomočjo NFC zgolj izmenjajo informacije, s katerimi se vzpostavi zmogljivejša brezžična povezava, npr. Bluetooth ali WiFi, ki se nato uporabi za dejanski prenos vsebine. Primer uporabe komunikacije P2P je prenos slik s fotoaparata na tiskalnik. Tiskalnik in fotoaparat z uporabo tehnologije NFC izmenjata podatke o Bluetooth povezavi, ki se nato samodejno vzpostavi in uporabi za prenos slik.

Zmožnost elektronskega plačevanja in poverjanja je bila ena ključnih silnic pri definiciji NFC standardov. Banke in mobilni operaterji si zelo želijo prenesti (vsa) plačila na mobilne telefone in tudi nekatere raziskave [19] pritrjujejo trditvi, da je tak način plačevanja ljudem blizu. Tako so proizvajalci telefonov spoznali, da potrebujejo komunikacijski standard, ki je združljiv z obstoječimi čitalniki pametnih kartic in ostalimi sistemi v logistiki. Tehnologija NFC bi naj bila *naslednji veliki korak* v elektronskem plačevanju in poverjanju, saj bo omenjeni storitvi mogoče opraviti s poljubno NFC napravo. Pričakovati je, da bodo začetki počasni in da se bodo NFC naprave spočetka uporabljale le za manjše transakcije. Ko pa bo tehnologija dovolj razširjena in med uporabniki sprejeta z zaupanjem, ter ko bo v zadostni meri poskrbljeno za vse varnostne vidike takega poslovanja, pa lahko pričaku-

jemo, da bodo NFC naprave postale elektronske denarnice, ki bodo povsem nadomestile obstoječe bančne kartice.

2.2 Tehnologije vmesne plasti

Vmesno plast (angl. middleware) sestavljajo plasti programske opreme, ki se nahajajo med tehnološko (nizkonivojsko) in aplikativno (visokonivojsko) plastjo. Srednja plast skriva (enkapsulira) podrobnosti in specifike nizkonivojskih tehnologij višjim plastem. Tako se lahko programerji na aplikativni plasti ukvarjajo zgolj z izdelavo namenskih rešitev in se ne obremenjujejo z infrastrukturnimi specifikami. Pomen srednje plasti v zadnjem obdobju narašča, saj so mnogi spoznali dodano vrednost tako pri lažji izdelavi novih kot pri integraciji obstoječih storitev z novimi.

2.2.1 Storitveno usmerjen pristop

Večina pristopov za izgradnjo vmesne plasti v internetu stvari sledi ideji storitveno usmerjene arhitekture (angl. service oriented acrhitecture, SOA). Ta arhitekturni pristop omogoča dekompozicijo kompleksnih in monolitskih sistemov v sisteme, ki so sestavljeni iz preprostih in jasno definiranih komponent. Z uporabo pogostih vmesnikov in standardnih protokolov lahko sestavimo procesni pogled poslovnega sistema tudi na tehnološki ravni. Izvedba poslovnega procesa v SOA je tako sestavljena iz zaporedja manjših storitev, ki odražajo različne akcije predmetov v poslovnem procesu. Tak pristop lajša komunikacijo med posameznimi deli poslovnega sistema in zmanjšuje čas, v katerem se podjetje lahko prilagodi spremembam na trgu [20]. Dodatna prednost storitveno usmerjenega pristopa je tudi v tem, da omogoča ponovno uporabo (angl. reuse) tako strojne kot programske opreme, saj ne zahteva specifične tehnologije za implementacijo.

Kot omenjeno, večina načinov izgradnje vmesne plasti uporablja storitveno usmerjeni pristop. Ker pa v tem času še nimamo široko sprejetega večplastnega arhitekturnega pristopa, mora vsaka od obstoječih SOA implementacij reševati težave z abstrahiranjem funkcionalnosti naprav, povezljivosti med napravami, upravljanja s storitvami ter kompozicijami storitev na svoj način. Posploševanje nas tako pripelje do triplastne arhitekture vmesne plasti [1, 21], ki je prikazana na Sliki 2. Predstavljena vmesna plast skuša zajeti vse omenjene naloge.

Na najvišjem mestu predlagane arhitekture se nahaja plast **aplikacij** (angl. applications), ki izpostavlja vse funkcionalnosti končnemu uporabniku. Dejansko ne gre za del vmesne plasti, ampak ta plast uporablja celotno funkci-

onalnost vmesne plasti. Tukaj lahko programerji z uporabo spletnih storitev in njihovim sestavljanjem relativno enostavno integrirajo porazdeljene sisteme in implementirajo aplikacije, brez da poznajo specifike vsake od številnih in heterogenih naprav, ki sestavljajo internet stvari.

Prvi del vmesne plasti predstavlja **sestavljanje storitev** (angl. service composition). To je pogosti del vmesnih plasti, ki so realizirane s pristopom SOA. Sestavljanje storitev omogoča, da storitve, ki jih ponujajo posamezni predmeti, združujemo v namenske aplikacije. Na tej plasti tako še ne govorimo o napravah (in predmetih) temveč le o storitvah. Pomemben del sestavljanja storitev predstavlja register vseh aktivnih storitev. Tega zagotavlja plast nižje in mora biti ažuren, če želimo uspešno upravljati ter graditi kompleksne storitve. Poslovno logiko in zaporedje izvajanja storitev lahko opišemo z jeziki za opis delovnega toka poslovnih procesov, kot je npr. jezik BPEL (angl. business process execution language). Ti jeziki omogočajo kreacijo poslovnih procesov, ki komunicirajo z zunanjimi entitetami z uporabo spletnih storitev.

Slika 2. Vmesna plast s podplastmi

Na podplasti **upravljanja storitev** (angl. service management) dostopamo do funkcij, ki bi jih naj imela vsaka stvar v ISt in s katerimi upravljamo s stvarmi. Osnovni nabor storitev tako obsega dinamično odkrivanje objektov (angl. object dynamic discovery), nadzor nad stanjem objektov (angl. status monitoring) ter spreminjanje nastavitev storitev (angl. service configuration). Nekateri pristopi sem uvrščajo še mehanizme za nadzor kakovosti storitev (angl. quality of service, QoS), mehanizme za nadzor sočasnosti (angl. lock management) ter nekatere semantične mehanizme, kot so upravljanje s politikami in drugo [22]. Tukaj je tudi implementiran register vseh aktivnih storitev. Zgornja podplast sestavljanja storitev ta register uporablja in z združevanjem atomarnih storitev sestavlja bolj kompleksne.

Plast **abstrahiranja predmetov** (angl. object abstraction) je posledica dejstva, da bo internet stvari sestavljala obsežna množica heterogenih naprav, od katerih bo vsaka ponujala specifičen nabor funkcij in po vsej go-

tovosti imela svoj način dostopanja do teh funkcij. Tako je nastala ideja o dodatni vmesni plasti, ki bi poenotila način dostopa do naprav. Ta plast je jasno odveč za naprave, ki so že povezane v omrežje IP in same poganjajo spletni strežnik s spletno storitvijo. A ker so taki primeri redki, je potreba po abstrahiranju objektov še zelo prisotna. Plast sestoji iz dveh delov, in sicer iz vmesnika in iz komunikacijskih podplasti. Preko vmesnika dostopamo do naprave z uporabo standardnih spletnih storitev. Komunikacijske podplasti pa realizirajo metode spletnih storitev, tako da prevajajo klice metod v ukaze, ki jih razumejo naprave. V tej luči so nekateri že uspeli vgraditi (okrnjeno) različico sklada protokolov TCP/IP (npr. TinyTCP, mIP, lwIP) v različne naprave [23]. Omenjeni skladi tako omogočajo internetno povezavo z vgrajenimi napravami preko vtičnic (angl. socket). Na naprave se lahko namesti spletni strežnik, ki z uporabo spletnih storitev zagotavlja funkcije plasti abstrahiranja predmetov. Drugačen, a bolj pogost, pristop k abstrahiranju predmetov pa je uporaba posrednika (angl. proxy) [24]. Slednji poganja spletni strežnik s spletnimi storitvami in pretvarja spletne zahteve v specifične jezike in ukaze, ki jih nato po drugem (navadno manj zahtevnem) komunikacijskem protokolu pošilja napravam.

Iz opisanih načinov realizacije plasti abstrahiranja predmetov vidimo, da lahko predmete na dva različna načina povežemo v omrežje internet, in sicer neposredno in posredno. Neposredni način zahteva, da je vsaka stvar zmožna komuniciranja v omrežju IP, posredni pa zahteva uporabo posrednika. Ta je običajno računsko zmogljivejša naprava, ki je zmožna komunicirati po protokolu TCP/IP in je v omrežje internet tudi povezana. Za predmete tako opravlja nalogo omrežnega prehoda (angl. gateway), predmeti pa s posrednikom komunicirajo po manj zahtevnem protokolu. Neposredni način omogoča, da ima vsaka stvar svoj edinstven naslov IP, s čimer postane globalno naslovljiva, medtem ko lahko pri posrednem načinu povezave globalno naslovimo le posrednika. Ugotovljeno ima vpliv na analizo varnostnih vidikov kot bomo videli v nadaljevanju.

2.2.2 Omrežje EPCglobal

Pri obravnavi vmesne plasti v ISt je potrebno omeniti tudi omrežje EPCglobal (angl. EPCglobal Network). Omrežje EPCglobal je globalna infrastruktura z namenom zajemanja, obdelave in izmenjave podatkov (zajetih s tehnologijo RFID) med vsem akterji oskrbovalne verige. Omrežje je osnovano na standardu za elektronsko kodo (angl. electronic product code, EPC) – edinstveni označevalni shemi za označevanje predmetov – ter ostalih sorodnih standardih. V nasprotju s klasičnim povezovanjem med posameznimi akterji je omrežje EPCglobal zasnovano za čim večjo stopnjo prilagodljivo-

sti obremenitvam (angl. scalability), saj se v prihodnosti pričakuje skokovit porast količine podatkov. Arhitekturni pregled omrežja podaja standard EPCglobal Architecture Framework [4].

Danes so nekatera podjetja že uspešno implementirala interne RFID rešitve. Težava je v tem, da so načini zajemanja in shranjevanja podatkov med podjetji, ki imajo takšne sisteme, med seboj slabo združljivi, če sploh. Omrežje EPCglobal največ obljublja ravno v tem segmentu, saj uvaja poenotenje omenjenih procesov. Glavne komponente omrežja so imenski strežnik ONS (angl. object naming service, ONS), register storitev EPCDS (angl. EPC discovery service) ter informacijski sistem EPCIS (angl. EPC information service). Imenski strežnik ONS se uporablja za lociranje informacijskega sistema proizvajalca izdelka, medtem ko se register storitev EPCDS uporablja za pridobitev naslovov vseh informacijskih sistemov, ki vsebujejo podatke o izdelku s konkretno kodo EPC. Tipičen primer uporabe omrežja je podan v nadaljevanju.

Proizvajalec na izdelek pritrdi značko RFID, ki je opremljena z edinstveno kodo EPC. Kreacija izdelka in izdaja kode EPC se prijavita v strežnik ONS, dodatne informacije o tem izdelku pa se zabeležijo v proizvajalčev sistem EPCIS. V register EPCDS se pošlje obvestilo, da proizvajalčev EPCIS vsebuje informacije o izdelku s konkretno kodo EPC. Ko izdelek zapusti okolje proizvajalca, se to zabeleži v proizvajalčev EPCIS. Na prihodu v naslednjo lokacijo v oskrbovalni verigi, denimo k razpečevalcu na široko, se v razpečevalčev EPCIS zabeleži čas prihoda in hkrati, podobno kot je storil proizvajalec, sporoči v EPCDS, da sedaj tudi razpečevalčev EPCIS vsebuje podatke o tem izdelku. Na podoben način postopajo vsi ostali akterji v oskrbovalni verigi; v lastne informacijske sisteme EPCIS zapisujejo pomembne poslovne dogodke in hkrati ob prvem takem vnosu o tem obvestijo register EPCDS.

Ko želi nek akter v oskrbovalni verigi, lahko tudi končni kupec, pridobiti informacije o izdelku, pošlje poizvedbo, ki vsebuje kodo EPC, na imenik ONS. Ta mu vrne lokacijo proizvajalčevega EPCIS, iz katerega se pridobijo dodatne informacije. Če pa denimo želi akter pridobiti informacije o transportu skozi oskrbovalno verigo, se poizvedba posreduje na register EPCDS. Ta kot rezultat vrne seznam naslovov EPCIS vseh deležnikov oskrbovalne verige, ki vsebujejo podatke o iskanem izdelku. Oba opisana postopka sta za iskalca informacij povsem transparentna.

Kritike omrežja EPCglobal so v največji meri usmerjene v implementacijo imenskega strežnika ONS. Ta je implementiran hierarhično kot del sheme domenskih strežnikov DNS. Koda EPC se pretvori v veljavni naslov URL z

domeno `onsepc.com`, ki se nato razreši z uporabo strežnikov DNS. Na primer koda EPC `urn:epc:id:sgtin:0614141.112345.400` se pretvori v naslov `112345.0614141.sgtin.onsepc.com`. Imenik ONS lahko tako razumemo kot podsistem domenskega strežnika, s čemer ONS podeduje vse znane omejitve domenskih strežnikov. Med glavnimi so v praksi omejena redundanca in pojav kritičnih točk odpovedi (angl. single point of failure). Upravljanje s korenskim ONS je bilo leta 2004 zaupano družbi VeriSign[9].

Pomembno je poudariti, da omenjen standard zgolj definira vmesnike in poizvedovalne mehanizme, ne definira pa dejanskih implementacij komponent. Implementacija je tako prepuščena podjetjem samim, ki se lahko odločijo bodisi za storitveno usmerjen pristop bodisi za kaj drugega.

2.2.3 Nekateri drugi pristopi

V skupino pristopov realizacije vmesne plasti, ki niso osnovane na principu SOA, sodi projekt Fosstrak[10]. Raziskovalci v tem projektu so se ukvarjali z upravljanjem aplikacij, ki temeljijo na uporabi tehnologije RFID. Rezultat projekta je odprtokodna infrastruktura, ki implementira vmesnike iz standardov omrežja EPCglobal. Infrastruktura ponuja storitve za diseminacijo, agregacijo in filtriranje podatkov, omogoča zapisovanje na značke, prožnje čitalnikov RFID z eksternimi senzorji, omogoča upravljanje z napakami in nastavitvami omrežja, interpretacijo podatkov, deljenje poslovnih RFID dogodkov, storitve poizvedovanja in register storitev ter mnogo drugih [25]. Dostop do vseh omenjenih funkcij je omogočen na aplikacijski plasti.

Podobna ideja vmesne plasti za sisteme RFID je predstavljena v [26]. Vmesna plast je razdeljena v tri funkcionalna področja; značka RFID, fizična lokacija ter upravitelj scen (angl. scenic manager). Značka omgoča identifikacijo posameznih objektov, fizična lokacija pa je določena z lokacijami čitalnikov. Upravitelj scen kombinira zaznavanje značk z lokacijami čitalnikov in skrbi za proženje ustreznih aplikacij.

Naslednji v vrsti pristopov, ki ne sledijo načelom SOA, je projekt e-SENSE[11]. Raziskovalci v njem zajemajo ambientalno inteligenco z uporabo brezžičnih senzoričnih omrežij. Predlagajo arhitekturo, ki je razdeljena v štiri logične podsisteme, in sicer: aplikacije, upravljanje, vmesna plast ter podsistemi za povezovanje. Vsak podsistem je sestavljen iz različnih protokolov in nadzornih entitet, ki ponujajo širok nabor storitev in funkcij drugim podsiste-

[9] `http://www.verisign.com`
[10] `http://www.fosstrak.org`
[11] `http://www.ist-e-sense.org`

mom. Celotni sklad podsistemov je implementiran tako na senzoričnih kot na ponornih vozliščih, pri čemer imajo senzorična vozliča zreduciran nabor funkcij. Za raziskovalce v projektu e-SENSE je naloga vmesne plasti zgolj vzpostavitev in vzdrževanje infrastrukture, medtem ko se informacije iz vozlišč obdelujejo porazdeljeno in se lahko rezultat po potrebi prenese nazaj na izvorno senzorično vozlišče. Ostale funkcije iz arhitekture na Sliki 2 so pripisane drugim podsistemom.

Cilj projekta UbiSec&Sens[12] je bil definirati celovito arhitekturo za srednja in velika senzorična omrežja. Poseben poudarek je bil dan varnostnim vprašanjem, saj so hoteli zagotoviti okolje za poganjanje zaupanja vrednih in varnih aplikacij. Vmesna plast v tej arhitekturi se v glavnem osredotoča na a) varno in dolgoročno beleženje okoljskih podatkov po posameznih regijah (TinyPEDS); b) na funkcije, ki posameznim vozliščem v omrežju zagotavljajo deljenje pomnilniških kapacitet (TinyDSM); in c) implementaciji porazdeljenega hranjena in zbiranja podatkov (DISC) v omrežjih WSN.

2.3 Tehnologije povezovanja v internet

Internet stvari bo vseboval izjemno veliko število vozlišč. Takšna množičnost potrebuje ustrezne mehanizme naslavljanja, če želimo naprave naslavljati iz poljubnih lokacij. Dejstvo, da bodo ISt sestavljale procesno, pomnilniško in energijsko omejene naprave, predstavlja dodaten vidik, ki ga je potrebno upoštevati pri povezavi v omrežje. In nenazadnje, veliko število v omrežje priključenih naprav lahko konkretno spremeni obnašanje omrežja samega. V tem razdelku skušamo osvetliti omenjene vidike.

2.3.1 Naslavljanje in odkrivanje naprav

Trenutno še uporabljamo internetni protokol IPv4. Ta ima (le) 32-bitni naslovni prostor, ki pa je praktično že izčrpan. Zato je smiselno, da bo ISt uporabljal novejše politike naslavljanja. Že prej smo omenili, da je bil protokol IPv6 predlagan za integracijo v sklad protokolov za naprave z nizko bitno hitrostjo in nizko porabo energije (6LowPAN). Omrežni naslovi v IPv6 imajo 128 bitov, kar pomeni, da je možnih približno 10^{38} različnih naslovov. V tem kontekstu pogosto naletimo na prispodobo, ki pravi, da IPv6 omogoča več naslovov, kot je peska na Zemlji. Takšna množičnost odstrani bojazen, da bi prostih naslovov kdajkoli zmanjkalo.

[12] `http://www.ist-ubisecsens.org`

Ideja interneta stvari je v tem, da se vsakemu naslavljanja vrednemu predmetu dodeli svoj 128-bitni IPv6 naslov. Ker pa imajo značke po standardu EPCglobal lahko 64-96 bitni identifikator, potrebujemo rešitve za naslavljanje značk RFID v protokolu IPv6. Tako denimo avtorji v [27] proučujejo načine integracije značk RFID v omrežja IPv6. Druga skupina raziskovalcev predlaga neposredno kombiniranje enoličnih RFID identifikatorjev v IPv6 naslove. Predlagajo, da se spodnjih 64 bitov naslova IPv6 uporabi za naslavljanje značke RFID, zgornjih 64 bitov pa za naslavljanje prehoda (angl. gateway) med sistemom RFID in omrežjem. V tem primeru bi prehod deloval kot posrednik, ki za vsako sporočilo iz sistema RFID v omrežje internet sestavi paket IP. Kot izvorni naslov IPv6 navede konkatenacijo 64-bitnega naslova prehoda in 64-bitnega naslova značke, vsebina paketa (angl. payload) pa vsebuje dejansko sporočilo. Analogno prehod pri prejetem paketu uporabi spodnji del naslova, da identificira naslovljeno značko.

Omenjenega pristopa ni mogoče uporabiti, če je naslov značke dolg 96 bitov. V takem primeru je potrebno uporabiti dodaten omrežni element – agenta za upravljanje z naslovi (angl. address management agent) [28]. Ta skrbi za preslikavo poljubno dolgega identifikatorja RFID v 64-bitni naslov, ki se nato uporabi na enak način kot je opisano v prejšnjem primeru. Agent mora zato vzdrževati ažurno tabelo preslikav med naslovi IP in naslovi RFID.

Tukaj je potrebno omeniti, da omenjene rešitve ne podpirajo mobilnosti, saj delujejo s predpostavko, da je vsaka značka dosegljiva le skozi specifičen, vnaprej določen prehod. V kolikor pa se značke premikajo, potem potrebujemo ustrezne sisteme za podporo mobilnosti. Takšni sistemi bodo sestavljeni iz velikega števila podsistemov z zelo različnimi karakteristikami. Nekaj mehanizmov za podporo mobilnosti že obstaja [29], a bo potrebno njihovo ustreznost v domeni ISt še preveriti; zlasti vidike stopnje prilagodljivosti obremenitvam ter podprtosti širokemu naboru heterogenih naprav. Omenimo, da je visoka stopnja prilagodljivosti obremenitvam lažje dosegljiva z uporabo domačega agenta (angl. home agent), kot je denimo mobilni IP [30], kot pa z uporabo rešitev, ki se uporabljajo v celičnih omrežjih. Mobilni IP namreč ni centraliziran, kar je z vidika visoke prilagodljivosti obremenitvam pomembno.

Pri naslavljanju je še pomemben vidik odkrivanja naslovov. V klasičnem internetu se naslov IP pridobi s pošiljanjem poizvedbe na domenski strežnik DNS (angl. domain name server). Ta zagotavlja preslikavo domenskega naslova v naslov IP. V ISt bo komunikacija potekala med oz. z napravami in ne le s strežniki. Zato se v ISt uvaja koncept imenskega strežnika ONS (angl. object name service), katerega naloga je, da poveže referenco na opis

predmeta z identifikatorjem predmeta [4]. Tako imenik ONS preslika enolični identifikator RFID, denimo kodo EPC, v naslov URL (angl. uniform reference locator), ki kaže na vir dodatnih informacij o predmetu. Posebnost ISt je v tem, da mora imenik ONS delovati v obe smeri, tj. omogočati mora poiskati dodatne informacije iz identifikatorja predmeta in obratno. Slednje zagotavlja storitev OCMS (angl. object code mapping service), katere implementacija je zelo zahtevna. Karakteristike takšnega mehanizma so podane v [31], kjer avtorji predlagajo pristop P2P z namenom izboljšanja prilagodljivosti obremenitvam.

2.3.2 Neprimernost protokola TCP

Internet stvari bo po mnenju avtorjev v [1] prinesel spremembe tudi v skladu protokolov na transportni plasti. Glavne naloge transportne plasti so zagotavljanje zanesljivosti med izvorom in ponorom povezave ter krmiljenje zamašitev (angl. congestion control). V skladu protokolov TCP/IP se na transportni plasti za zagotavljanje zanesljivosti uporablja protokol TCP (angl. transmission control protocol). Ta je po mnenju omenjenih raziskovalcev neprimeren za okolje ISt zaradi naslednjih razlogov:

1. **Vzpostavitev povezave.** Protokol TCP je povezavno usmerjen protokol, ki vsako sejo začne s posebnim postopkom vzpostavitve povezave, s t. i. tristranskim rokovanjem (angl. threeway handshake). To je za domeno interneta stvari nepotrebno, glede na to, da bo večino komunikacij predstavljala izmenjava majhnih količin podatkov. Tristransko rokovanje bi pri takem načinu komuniciranja porabilo preveč časa in drugih kapacitet, saj je ob vzpostavitvi povezave potrebno opraviti nekatere netrivialne izračune.

2. **Krmiljenje zamašitev.** Protokol TCP zagotavlja krmiljenje nad zamašitvami v povezavi. To utegne v domeni ISt povzročiti performančne težave, saj bo večina povezav brezžičnih, kar se je v preteklosti že izkazalo kot težavno za protokol TCP [32]. Če pa upoštevamo, da bo količina prenesenih podatkov na sejo zelo majhna, je krmiljenje zamašitev dejansko odvečno, saj se bo celotna seja zaključila takoj po prenosu prvega paketa in njegovi potrditvi.

3. **Kontrola pretoka.** Protokol TCP zahteva, da končni vozlišči uravnavata kontrolo pretoka tako, da začasno hranita podatke v medpomnilniku (angl. buffer). Izvorno vozlišče mora pomniti vsak poslan podatek, za katerega še ni dobilo potrdila o prejemu, zato da ga lahko v primeru izgube ponovno pošlje. Ponorno vozlišče uporablja medpomnilnik

za shranjevanje in pravilno razvrščanje prejetih podatkov, da jih lahko uredi in servira aplikacijski plasti. Upravljanje s takšnim medpomnilnikom zahteva zadostno količino razpoložljivega pomnilnika, kar bo neredko težko izpolniti.

Posledično je protokol TCP v najboljšem primeru neoptimalen, v najslabšem pa neprimeren za transportni protokol v internetu stvari. Do danes še ni bilo predlaganih rešitev za ta problem.

2.3.3 Vplivi na obstoječo omrežno infrastrukturo

Internet stvari bo internet, v katerem bo količina miniaturnih naprav korenito presegala količino (danes klasičnih) uporabnikov interneta, tj. uporabnikov osebnih računalnikov priključenih v internet. Skokovit porast v številu internetnih vozlišč bo definitivno imel vpliv na obnašanje in delovanje samega omrežja.

Trenutno je izredno težko odgovoriti na vprašanje, kakšne bodo karakteristike prometa, ki ga bodo generirale (pametne) stvari povezane v internet. Ta težava je vse prej kot zanemarljiva, saj je poznavanje obremenitev omrežij ključno za načrtovanje omrežne infrastrukture ter protokolov. Edino, kar zanesljivo vemo, je to, da so karakteristike prometa v omrežjih WSN močno odvisne od scenarijev uporabe omrežja [33]. Težava nastane, ko postanejo vozlišča omrežij WSN integralni del interneta – kot veleva osnovna ideja interneta stvari. V tem primeru omrežje prenaša velike količine podatkov, ki jih generirajo pametne naprave, ki so bile zasnovane za zelo različne namene in imajo zelo različne karakteristike. Če k temu prištejemo še to, da so veliki in porazdeljeni sistemi RFID še precej v povojih, vidimo, da praktično nimamo nobenih otipljivih podatkov, s katerih bi lahko sklepali o bodočih obremenitvah omrežja internet.

Po drugi strani pa je poznavanje bremen omrežij nujno potrebno za ponudnike internetnih storitev (angl. internet service provider, ISP). Brez znanja o dinamiki bremen ne morejo načrtovati infrastrukturnih sprememb ter zagotavljati zadostne stopnje kakovosti storitev (angl. quality of service, QoS). Do danes poznamo le nekatere mehanizme zagotavljanja kakovosti v omrežjih WSN [34], sistemi RFID in sistemi RSN pa so v tem pogledu so še praktično popolnoma neraziskani.

2.4 Obstoječi in porajajoči se standardi

Že med predstavljanjem gradnikov in tehnologij povezovanja je bilo omenjenih več standardov. Nekateri so že dokončani, nekateri pa so trenutno še na nivoju osnutka. V tem razdelku povzamemo vse že omenjene standarde in poleg njih navajamo še nekaj novih.

Internet stvari je kompleksna in heterogena tvorba in kot taka potrebuje prispevke širokega kroga ljudi, tako iz raziskovalne domene kot od predstavnikov industrije. Med najpomembnejše spadajo različne sekcije organizacije Auto-ID Lab, Evropska komisija in ostale evropska standardizacijska telesa (ETSI, CEN, CENELEC), njihovi mednarodni ekvivalenti (ISO, ITU) in drugi standardizacijski organi in konzorciji (IETF, EPCglobal). Veliko se pričakuje od delovne skupine M2M (angl. machine-to-machime, M2M) iz Evropskega standardizacijskega instituta za telekomunikacije (angl. European Telecommunications Standards Institute, ETSI) in od nekaterih delovnih skupin pri Internetni delovni skupini (angl. Internet Engineering Task Force, IETF), kot sta 6LoWPAN ter ROLL.

Manjše težave se kažejo na področju tehnologije RFID, saj je standardiziranje razdrobljeno v dve področji; določanje frekvenčnih pasov in protokolov za komunikacijo med značko in čitalnikom, ter določanje formata podatkov za zapis na značke in etikete. Glavni organi pri tem so EPCglobal, ETSI in ISO. EPCglobal[13] je podružnica mednarodne neprofitne organizacije za standardizacijo, GS1. Njena glavna naloga je podpora globalnemu sprejemu edinstvenega identifikatorja na vsaki znački – elektronski kodi izdelka EPC (angl. electornic product code, EPC) – in ostalim sorodnim industrijskim standardom. Eden od glavnih rezultatov so izdana priporočila za EPCglobal Architecture Framework [4], katerega smo podrobneje opisali v razdelku 2.2.2.

Evropska komisija je glede standardizacije na področju RFID storila velik korak naprej z vzpostavitvijo Neformalne delovne skupine za implementacijo tehnologije RFID (angl. Informal working group on the implementations of the RFID), ki je sestavljajo ključni deležniki, ki morajo biti seznanjeni s tehnologijo RFID v splošnem, direktivami o varovanju podatkov in priporočili za tehnologijo RFID. Sem spadajo predstavniki iz industrije, standardizacijskih teles, civilne družbe, organizacij za varovanje podatkov in drugi.

[13] `http://www.epcglobalinc.org`

Eden od teh deležnikov je Evropski odbor za standardizacijo[14] (angl. European Committee for Standardization, CEN), ki se ukvarja s prehodom sistemov RFID v internet stvari. Med njihovimi delovnimi skupinami (angl. working group, WG) so za ISt najbolj relevantne WG 1-4 BARCODES, WG 5 RFID in Globalni forum standardizacije za interoperabilnost tehnologije RFID (angl. Global RFID Interoperability Forum for Standards, GRIFS). Slednji je dvoletni projekt, ki ga koordinirajo GS1, ETSI in CEN, s ciljem definirati standarde za fizične objekte (čitalniki, značke, senzorji), komunikacijsko infrastrukturo, frekvenčni spekter uporabe tehnologije RFID in obvladovanje varnosti in zasebnosti [35].

Mednarodna organizacija za standardizacijo[15] (angl. International Standards Organization, ISO) se osredotoča bolj na tehnološka vprašanja, kot je denimo definiranje frekvenčnega spektra, modulacijskih shem in protikolizijskih protokolov.

Bolj fokusiran na idejo interneta stvari kot celoto je Evropski standardizacijski institut za telekomunikacije[16] (angl. European Telecommunications Standards Institute, ETSI). ETSI je ustanovil tehnološki odbor za izvajanje dejavnosti v smeri standardizacije sistemov M2M in senzoričnih omrežij z vidika interneta stvari. Glavne naloge omenjenega odbora so razvoj in vzdrževanje arhitekture za M2M po protokolu IP in krepitev raznih postopkov standardizacije M2M, kot so integracija senzoričnih omrežij, naslavljanje, lociranje, zagotavljanje kakovosti, obvladovanje varnostnih vidikov, upravljanje in nadzor ter definicija programskih in strojnih vmesnikov [36].

Pri IETF najbolj izstopata že omenjeni delovni skupini 6LoWPAN in ROLL. 6LoWPAN [10] definira nabor protokolov za integracijo senzoričnih vozlišč v omrežja IPv6. Osnovni nabor protokolov v skladu z 6LoWPAN je že dorečen in na tržišču že lahko najdemo nekatere zgodnje komercialne implementacije. Druga pomembna delovna skupina pri IETF je ROLL [37]. Ta se ukvarja z usmerjanjem po izgubnih omrežjih z nizko porabo energije (angl. Routing Over Low power and Lossy networks, ROLL). Nedaven rezultat dela omenjene skupine je osnutek protokola RPL. Ta bo osnova za usmerjanje prometa po omrežjih z visoko stopnjo izgube ter z nizko porabo energije kot je 6LoWPAN, ki še potrebuje dodatne prispevke, da bo v celoti dokončan.

Iz opisanega jasno izhaja, da bo standardizacija interneta stvari integralni del standardizacije bodočega interneta. Slednje je nedavno izjavila skupina

[14] http://www.cen.eu
[15] http://www.iso.org
[16] http://www.etsi.org

Tabela 2. Najbolj relevantni standardi

Naziv	Namen
V razdelku obravnavani standardi	
EPCglobal	Integrirati tehnologije RFID in elektronske kode za podporo sledenju izdelkov skozi oskrbovalno verigo
GRIFS	Definirati standarde za RFID, da bo prehod iz lokalnih aplikativnih RFID rešitev v internet stvari čim lažji
M2M	Definirati učinkovite ter cenovno ugodne rešitve za komunikacijo M2M, da bodo ISt in vse sorodne tehnologije čim hitreje zaživele
6LoWPAN	Integrirati energijsko šibkih naprav (IEEE 802.15.4) v omrežje IPv6
ROLL	Definirati protokole za usmerjanje v energijsko šibkih ter izgubnih omrežjih
Še nekateri drugi standardi	
NFC	Definirati nabor protokolov za dvosmerno komunikacijo bližnjega polja
Wireless Hart	Definirati protokole za samo-organizujoče in samo-popravljive mrežne arhitekture za naprave IEEE 802.15.4
ZigBee	Omogočiti izdelavo zanesljivih, cenovno ugodnih, energijsko šibkih in brezžičnih naprav za nadzor in krmiljenje

evropskih raziskovalnih in razvojnih projektov interneta stvari[17] (angl. cluster of European R&D projects on the internet of things, CEPR-IoT) [38]. Vredno je tudi omeniti, da je v literaturi mogoče zaslediti tesno sodelovanje med različnimi standardizacijskimi telesi, globalnimi interesnimi skupinami in zavezništvi. Čutiti je pripravljenost na sodelovanje vseh deležnikov z namenom, da bi dosegli *pravi* internet stvari [38].

Kratek pregled vseh omenjenih (in še nekaterih drugih) standardov je podan v Tabeli 2.

2.5 Varnost in zasebnost

Internet stvari bo naletel na odpor in ne bo široko sprejet, v kolikor ne bo prisotnega zadostnega zaupanja, da vse omenjene tehnologije ne bodo posegale v zasebnost posameznikov. Ko je leta 2004 italijansko podjetje Benetton napovedalo, da bo poskusno opremilo celotno serijo oblačil z značkami RFID, je bil odziv potrošnikov jasen. Organizirali so množična zborovanja in proteste[18], ki so na koncu omenjeno podjetje (v ekonomskem smislu) prisilili, da se je v celoti odpovedalo ideji uporabe tehnologije RFID. Opisan primer je jasen pokazatelj, da je pri obravnavi interneta stvari potrebno po-

[17] http://www.rfid-in-action.eu/cerp
[18] http://www.boycottbenetton.com

sebno pozornost namenjati varnostnim vprašanjem in vprašanjem varovanja zasebnosti.

2.5.1 Informacijska varnost

Beseda varnost ima v vsakdanjem življenju različne pomene. V računalništvu se pod besedo varnost najpogosteje razume koncept informacijske varnosti. Tega organizacija ISO opredeljuje kot *zmožnost ohranjanja zaupnosti, celovitosti in razpoložljivosti informacij, poleg tega pa tudi ohranjanje drugih lastnosti, kot so verodostojnost, neovrgljivost in zanesljivost* [39].

Zagotavljanje varnosti v internetu stvari je težavno iz več razlogov. Najprej, večina na predmete pritrjenih naprav je večji del časa nenadzorovana, kar pomeni, da so te naprave zelo dojemljive za fizične napade. Drugič, večina poznanih in preverjenih mehanizmov za zagotavljanje varnosti zahteva izvajanje računsko zahtevnih operacij, ki pa jih naprave interneta stvari, za katere praviloma velja, da so procesno, pomnilniško, komunikacijsko in energijsko omejene, ne zmorejo izvesti. Tu si nasproti stojita dve silnici. Prva teži k nizkemu številu logičnih vrat v napravah, saj morajo biti naprave stroškovno upravičljive, dodatno število vrat pa naprave draži. Druga silnica pa pravi, da bo cena naprav v prihodnosti padla, kar pomeni, da bo mogoče v napravo pri nespremenjeni ceni vgraditi več logičnih vrat in ji s tem povečati kapacitete. Tretja težava pri zagotavljanju varnosti pa je v tem, da je večina komunikacije med napravami brezžičnih, s čimer postane prisluškovanje (angl. eavesdropping) na komunikacijskemu kanalu relativno enostavno.

Največje težave predstavlja zagotavljanje overjanja in podatkovne celovitosti. Overjanje se v klasičnem internetu zagotavlja z uporabo ustrezne infrastrukture in strežnikov, ki uporabnike overi z izmenjevanjem različnih sporočil. Primer takšnega mehanizma je infrastruktura javnih ključev (angl. public key infrastructure, PKI), ki povezuje javne ključe uporabnikov z njihovimi identitetami. Takšne rešitve niso primerne za naprave interneta stvari, saj zahtevajo izvedbo kompleksnih računskih operacij in večkratnega zaporednega izmenjavanja sporočil. Slednje najbolj omejuje pasivne značke RFID, medtem ko vozlišča omrežij WSN malo manj.

Za omrežja WSN obstajajo rešitve za overjanje vozlišč [40]. Njihova pomanjkljivost je v tem, da so vse osnovane na način, pri katerem so le ponorna vozlišča povezana v omrežje internet, ostala vozlišča pa uporabljajo ponorna vozlišča kot prehode. Ponorna vozlišča so zadolžena za overjanje drugih, navadnih vozlišč, kar pomeni, da lahko v nekem omrežju ponorna

vozlišča overijo le tista navadna vozlišča, ki so del istega omrežja WSN. V internetu stvari se pričakuje drugače, namreč da bo vsako vozlišče zmožno povezave v internet, kar pomeni, da je potrebno overiti tudi takšna vozlišča, ki so lahko (v osnovi) del drugega omrežja WSN. V takem scenariju omenjene rešitve odpovejo. Obstajajo tudi analogni poskusi za tehnologijo RFID, a so, kot opisuje [41], tudi zelo omejene.

Celovitost zagotavlja, da v kolikor pride do nedovoljenega spreminjanja podatkov, sistem spremembo zazna. Zagotavljanje celovitosti v internetu stvari je težavno zaradi dveh razlogov, in sicer (i) naprave v internetu stvari so večino časa nenadzorovane, kar pomeni, da je napadalcu relativno preprosto pridobiti fizični dostop do njih, in (ii) brezžične komunikacije omogočajo lažje prisluškovanje in posledično tudi spreminjanje podatkov, ko potujejo po omrežju [42]. Zaščita zoper napade iz točke (i) so mehanizmi za zaščito pomnilnika na značkah. Tako imajo npr. značke po standardu EPCglobal Class-1 Gen2 pomnilnik zaščiten z geslom. Podobne rešitve obstajajo tudi za omrežja WSN [43]. Pred napadom iz točke (ii) se zavarujemo z uporabo shem HMAC (angl. key-hash message authetication code) [44], ki temeljijo na uporabi deljene skrivnosti med značko in čitalnikom. Ta skrivnost se uporabi pri izračunu enosmerne zgoščevalne funkcije nad vsebino sporočila.

Glavna težava je v tem, da je trenutno še praktično vsaka od predlaganih varnostnih rešitev vsaj v nekem pogledu pomanjkljiva. Gesla za zaščito pomnilnika so tipično prekratka in ne nudijo zadostnega varovanja. Dodatno težavo predstavlja upravljanje s tovrstnimi gesli, saj bodo značke in gesla v ISt tipično dodeljena v različnih organizacijah. Po drugi strani pa vse varnostne rešitve vsebujejo kriptografske prijeme. Ti temeljijo na izvajanju energijsko, procesno, pomnilniško in komunikacijsko zahtevnih izračunov in so kot take neprimerne za domeno ISt. Od tu potreba po t. i. lahkih kriptografskih rešitvah. Nekatere so že bile predlagane za sisteme RFID; npr. lahka simetrična kriptografija [45, 46] in nedeterministični kriptografski protokoli [47], ki so rezultat dela naše raziskovalne skupine. Podobne lahke rešitve obstajajo tudi za omrežja WSN [40].

2.5.2 Zasebnost

Zasebnost (angl. privacy) je pravica posameznika ali skupine, da varuje in skriva svoje *osebne podatke* in preprečuje drugim, da vstopajo v njegov *osebni prostor* [48]. Pravica do zasebnosti predstavlja eno temeljnih pravic in je kot taka močno zakoreninjena v načelih demokratičnih družb. To je tudi glavni razlog, zakaj pri širokem sprejetju ideje interneta stvari prihaja

do mnogih zadržkov. Slednji so vsekakor dobro osnovani, saj ISt prinaša oblike zbiranja in obdelave (osebnih in drugih) podatkov, kot jih do sedaj nismo poznali. Z vidika posameznika bo postalo praktično nemogoče, da osebno nadzira zbiranje in razkrivanje osebnih podatkov. Dodaten dejavnik predstavlja padanje cen shranjevanja podatkov (angl. cost of information storage), tj. cen podatkovnih nosilcev na enoto količine podatkov, ki se danes že približuje 0,001 €/MB. To pomeni, da bodo zbrani podatki z vidika trajanja življenja posameznika hranjeni praktično v nedogled.

Internet stvari tako predstavlja veliko novih groženj zasebnosti, kot jo poznamo danes. Dodaten dejavnik pri vsem tem je t. i. *pasiven način oddajanja* podatkov. Danes, v klasičnem internetu, uporabniki razkrivajo podatke tako, da aktivno vnašajo vsebine na razna družabna omrežja in druge spletne strani. V internetu stvari pa uporabniki delijo osebne podatke, tudi če ne uporabljajo storitev – podatki se zbirajo in obdelujejo avtomatizirano, tudi če uporabniki tega ne želijo in navadno celo brez njihovega vedenja.

Varovanje zasebnosti v internetu stvari mora zato potekati tako, da lahko *uporabniki nadzirajo, kateri osebni podatki se zbirajo, ter da vedo, kdo jih zbira ter kdaj in kje. Zbrani podatki se morajo uporabijo le za namen neposredne podpore storitvi, zaradi katere so bili zbrani, in smejo se hraniti le toliko časa, dokler je to za zagotavljanje omenjene storitve potrebno* [1]. Scenarij uporabe, ki takšna priporočila upošteva, je denimo pametna hiša, ki sledi stanovalcem v njej in glede na to uravnava osvetlitev in ogrevanje hiše. Če je sledilni sistem namenjen zgolj varčevanju z energijo, potem ustrezna politika varovanja zasebnosti zahteva, da sledilni sistem ne beleži lokacije vsakega posameznika posebej, temveč operira le z agregiranimi vrednostmi, kot je npr. število stanovalcev v posameznem prostoru. Poleg tega morajo biti vsi stanovalci o sledenju obveščeni in se z njim strinjati. Zbrani podatki o posameznem stanovalcu se morajo pobrisati takoj, ko stanovalec zapusti hišo.

Omenjena priporočila je mogoče uveljaviti normativno, tehnološko ali z obema pristopoma hkrati, tj. normativno in tehnološko. V tem razdelku si bomo ogledali le nekatere tehnološke pristope. Nadzor nad zbiranjem in uporabo podatkov zahteva rešitve, ki so odvisne od vrste podpornih tehnologij; pogledali si bomo nekatere rešitve za omrežja WSN ter sisteme RFID.

Ko govorimo o senzoričnih omrežjih postane problem nadzora nad zbiranjem podatkov praktično nerešljiv. Denimo, da imamo senzorsko omrežje kamer, ki pokriva nek prostor in zajema slike obiskovalcev. Omrežje kamer zajema slike tudi, če obiskovalci tega ne želijo, in edini način, kako se lahko

posameznik zajetju slike izogne, je, da tega kraja sploh ne obišče. Nekatere rešitve sicer predlagajo *zameglitev* zajetih podatkov, tj. popačenje zajetih slik do te mere, da so zajeti podatki še vedno uporabni za podporo storitvam, a hkrati ne dovolj natančni za identifikacijo oseb [49] ali da sistem sporoča le približne podatke (npr. lokacijo) iz zajetih slik [50]. Nobena od rešitev ni posebej dobra, saj postavi celotno skrb za varovanje zasebnosti na zbiratelja podatkov.

V sistemih RFID je problem dvoplasten. Najprej, za pričakovati je, da bo večina značk pasivnih, kjer je čitalnik vedno pobudnik komunikacije. Ker se pasivne značke vedno odzovejo pozivu čitalnika, temu načinu overjanja pravimo vsiljeno overjanje (angl. enforced authentication). Večina rešitev zahteva, da značke izvedejo postopke za overjanje čitalnikov, kar pomeni izvajanje kompleksnih operacij, kar je v mnogih primerih nesprejemljivo. Na tem področju so obetavni že omenjeni nedeterministrični kriptografski protokoli, saj večji del računskega bremena prenesejo na čitalnik in zaledne sisteme [47]. Druga plast problemov v sistemih RFID pa predstavlja prisluškovanje na komunikacijskem kanalu. Slednje se rešuje z uporabo (lahkih) šifrirnih shem. Šifriranju navkljub pa lahko napadalec na podlagi ponavljajočega odziva še vedno ugotovi prisotnost določene značke in identiteto nosilca. To se rešuje bodisi z uporabo že omenjenih nedeterminističnih kriptografskih protokolov, ki omogočajo, da značka vrača različne odgovore, a čitalnik ve, da gre za isto značko, ali z uporabo posebnih čitalnikov, ki oddajajo *popačen* signal, ki ima obliko psevdo-šuma [51]. Značka signal modulira in vrne odgovor, ki je prav tako popačen, a ga zna overjen čitalnik, ki ima informacijo o popačenju signala, popraviti in prebrati. Zlonamerni čitalniki te informacije nimajo, zato prestreženega odziva značke ne znajo popraviti.

Tehnološke rešitve, ki bi zagotavljale, da se zbrani podatki uporabijo zgolj za namen, zaradi katerega se zbirajo, ne obstajajo. Takšne rešitve so v domeni normativnega urejanja. Obstajajo pa tehnološke rešitve, ki v imenu posameznika in v skladu z njegovimi navodili avtomatično komunicirajo z ostalimi napravami in deklarativno dovoljujejo (ali zavračajo) zbiranje podatkov. Ena od takšnih rešitev je diskretna škatla (angl. discreet box) [52]. Gre za program, ki je del vmesne plasti, v katerem uporabnik nastavi svojo politiko deljenja podatkov, program pa se vedno, ko uporabnik pride v situacijo, da je zajem podatkov možen, samodejno odloči ali je zajem podatkov skladen s politiko, in če je, zajem odobri. Kot rečeno, gre za enega od zgodnjih poskusov in na tem področju se pričakujejo še dodatni prispevki.

Za zasebnosti je pomemben tudi koncept digitalnega pozabljanja (angl. digital forgetting) [53]. S padanjem cene shranjevanja podatkov dobivamo čedalje večje kapacitete za hrambo. Od tu prihaja potreba po rešitvah, ki bi periodično uničevala podatke, ki se ne potrebujejo več, saj namen, zaradi katerega so bili zbrani, ni več aktualen. V prihodnosti razvite rešitve bi morale podpirati takšno funkcionalnost pozabljanja.

2.5.3 Model groženj

Obstaja veliko načinov, kako lahko nepridipravi napadejo gradnike interneta stvari in ogrozijo posameznika v več pogledih. V literaturi lahko zasledimo mnogo klasifikacij tovrstnih napadov na naprave; nekateri ločijo po načinu napada, denimo fizični, aktivni in pasivni napadi [47, 54], drugi obravnavajo predvsem napade na komunikacijski ravni, kjer pogosto ločijo napade po plasteh sklada komunikacijskih protokolov [55, 56].

V tej študiji uporabljamo drugačen pristop, in sicer bomo namesto napadov obravnavali namerne grožnje napravam interneta stvari. Grožnje predstavljajo možne vzroke za pojav neželenih incidentov, tj. izkoriščanja različnih nepopolnosti v napravah. Tveganje je posledica nastopa groženj in je po standardu ISO/IEC 27000:2009 opredeljeno kot kombinacija verjetnosti nastopa neželenih incidentov ter posledic nastopa takšnih incidentov. Uporabili bomo pristop iz [57], kjer je tipologija namernih groženj po ISO/IEC 27005:2008 aplicirana na omrežne sisteme RFID. Model groženj je prirejen, tako da obsega tudi omrežja WSN. Predstavljen je v Tabeli 3.

Model groženj bomo v nadaljevanju uporabili pri analizi varnostnih vidikov scenarijev uporabe na različnih področij obravnave interneta stvari. Zanimali nas bodo neposredno napadi na značke RFID, njihovo komunikacijo s čitalniki, senzorična vozlišča, usmerjanje v njih ter vplivi napadov na zmožnost zagotavljanja storitev v internetu stvari. Pri tem se bomo omejili na napade, ki so posledica človeškega dejavnika in so namerni. Model napadov je zato potrebno razumeti splošno, saj ga je možno aplicirati tudi na scenarije uporabe, ki jih v tem poročilu ne obravnavamo. Imena groženj so povzeta po slovenskem prevodu standarda ISO/IEC 27000:2009, zato pri nekaterih, manj opisnih imenih groženj, v opombah navajamo angleški izvirnik.

Vse omenjene grožnje se lahko tako v omrežjih RFID kot v omrežjih WSN v internetu stvari izvedejo še na dodaten način, in sicer oddaljeno. Če so osnovni gradniki globalno naslovljivi lahko napadalec marsikateri napad izvede preko interneta. Primer takšnih groženj je denimo nepooblaščeno po-

Tabela 3. Model groženj, napadov in učinkov na internet stvari

Grožnja	Primer napada	Učinek napada
Kraja	Začasna odtujitev značke za pridobitev tajnega ključa, ponareditev značke in pretvarjanje za pridobitev zaupne informacije.	Zaupnost in celovitost storitve nadzora dostopa
Razkritje[a]	Razkritje napake algoritma za izračun tajnega sejnega ključa komunikacije značke in čitalnika, ki se uporablja za sistem nadzora fizičnega dostopa ustanove.	Celovitost storitve nadzora dostopa
Nepooblaščeno poseganje	Vpis podatka na značko, ki vsebuje zlonamerno kodo. Podatek se preko čitalnika posreduje zaledju, kjer se izvede injekcija ukaza SQL.	Celovitost podatkovne baze
Odkritje položaja	Sledenje položaju sovražnih bombnikov na podlagi ranljivosti značke RFID.	Zaupnost vojaške naloge in celovitost človeških življenj
Nepooblaščena uporaba opreme	Namestitev virusa na značko, zaradi katerega čitalnik dobi vedno drugačen odziv kode EPC, ki vodi v odpoved storitve vodenja poslovnih procesov.	Celovitost storitve vodenja procesov
Okvara podatkov[b]	Vnos deformiranega niza kode EPC za onemogočenje storitve sledenja predmetov poštnih pošiljk.	Razpoložljivost storitve sledenja predmetov
Nezakonita obdelava podatkov	Nezakonito spremljanje potovanja imetnikov kartice zaupanja v urbanem središču preko javne mreže čitalnikov za namen ciljnega trženja.	Zasebnost posameznika
Poneverba podatkov	Vnos veljavne kode EPC z namenom ponareditve izvirnosti izdelka.	Celovitost storitve preprečevanja ponaredkov
Poneverjanje pravic	Napadalec zasleduje lastnika avtomobila s ključem RFID. S pomočjo komunikacijskega releja poveča doseg komunikacije ključa – značke RFID in čitalnika – avtomobilsko ključavnico. Njegov pajdaš ukrade avtomobil.	Celovitost storitve nadzora dostopa
Zavrnitev storitve	Uporaba zlonamernega vozlišča (angl. sinkhole) za motenje usmerjevanja v omrežjih WSN.	Razpoložljivost storitve merjenja
Prisluškovanje	Oddaljen dostop do usmerjevalnih vozlišč ISt za nezakonito pridobivanje podatkov navad uporabnikov.	Zasebnost uporabnika v pametnem domu

[a] Angl. disclosure
[b] Angl. corruption of data

seganje v zapis vsebin značk RFID ali upravljanje s posameznimi vozlišči senzorskih omrežij. Takim grožnjam je potrebno nameniti dodatno pozornost, saj jih je ravno zaradi oddaljenega načina izvedbe veliko težje zaznati.

2.6 Akcijska vodila in smernice

V tem delu smo obravnavali tehnološke vidike interneta stvari. Videli smo, da je trenutno še precej tehnoloških vprašanj, zlasti na področju varnosti ter zasebnosti, odprtih. Zato ocenjujemo, da bi bilo za razvoj interneta v slovenskem okolju (in tudi na splošno) ugodno, da se sprejmejo ukrepi, ki:

- spodbujajo in podpirajo raziskave tako na področju razvoja tehnologij vmesne plasti interneta stvari in komunikacijskih protokolov za računsko omejene naprave kot tudi rešitve za zagotavljanje varnosti ter varovanja zasebnosti v okoljih RFID, WSN, RSN in NFC;
- spodbujajo in podpirajo industrijske iniciative, ki so usmerjene v istovrstne rešitve kot so omenjene v zgornji alineji, pri čemer je potrebno, da so rešitve skladne z relevantnimi že obstoječimi (kot tudi porajajočimi se) standardi, kjer je to mogoče.

Glavno vlogo pri tem bi morala imeti pristojna ministrstva, predvsem ministrstvo pristojno za znanost in tehnologijo ter ministrstvo pristojno za gospodarstvo.

3 Vplivi na infrastrukturo

V tem razdelku najprej opredelimo pojem infrastrukture, nato pa obravnavamo vpliv interneta stvari nanjo. Predstavimo nekatere aktualne in pretekle raziskovalne projekte ter predstavimo nekaj izbranih scenarijev uporabe, ki jih ovrednotimo s predlaganim modelom groženj.

3.1 O infrastrukturi

Pojem infrastrukture zajema osnovne fizične in organizacijske strukture, ki so potrebne za delovanje družbe in organizacij [58]. Navadno pod tem pojmom razumemo raznovrstne tehnične strukture, ki podpirajo družbo: ceste, vodovodna omrežja in zbirnike za vodo, kanalizacijske jaške, električna omrežja, telekomunikacijska omrežja ipd. Infrastruktura je torej skupek fizičnih in organizacijskih komponent in med seboj sorodnih sistemov, ki zagotavljajo bistvene proizvode in storitve, ki omogočajo, vzdržujejo ali celo izboljšujejo bivanjske življenjske pogoje [59].

S funkcionalnega vidika infrastruktura omogoča proizvodnjo blaga in storitev, njihovo razpečavo na trge ter tudi druge družbeno zavedne storitve, kot so šolski sistem in bolnišnice. V vojaškem smislu pa se infrastruktura navezuje na zgradbe in stalne objekte, ki podpirajo nastanitev in delovanje vojaških sil [60].

V tej luči so tehnologije in storitve interneta stvari uporabne na vsakem izmed različnih področij infrastrukture. V nadaljevanju tako podrobneje opišemo inteligentni prometni sistem ter pametna mesta.

3.2 Inteligentni prometni sistem

Inteligentni prometni sistemi so napredne aplikacije, ki uporabljajo informacijske in komunikacijske tehnologije za promet in zagotavljanje inovativnih storitev pri načinih prevoza in upravljanja prometa. Kažejo se kot nujni za zmanjševanje porabe energije in okolju prijaznejši promet, hkrati pa imajo velik potencial za učinkovitejšo uporabo vseh načinov prevoza, za zmanjšanje zastojev v cestnem prometu, zmanjšanje prometnih nesreč in emisij CO_2 povezanih s prometom. Pri tem ne gre le za cestni promet, z in-

teligentnimi aplikacijami se srečuje tudi železniški, pomorski in zračni promet.

Inteligentni prometni sistemi torej prispevajo k razvoju trajnostne mobilnosti za državljane in gospodarstvo: z izboljševanjem uspešnosti regij, predvsem urbanih področij, z izboljševanjem trgovinske dejavnosti med regijami in na notranjem trgu Evropske unije, ter s povečevanjem zaposlenosti. Konkreten projekt na področju inteligentnih prometnih sistemov je projekt Evropske unije *EasyWay*[19], katerega cilji so doseči pozitiven učinek na pretok prometa, doseči višjo varnost v prometu in zmanjšanje negativnih učinkov na okolje. Aktivnosti projekta se raztezajo skozi sedemletno obdobje (2007-2013), s tem pa stremijo k cilju trajnostnega razvoja do leta 2020. Do sedaj izpeljane aktivnosti so: vzpostavitev nadzornih sistemov, omrežij za komunikacijo, centrov za nadzor prometa in informacije o prometu, sporočilne table, sistemi za zaznavanje prometnih nezgod in navigacijo avtomobilov. Ti medsebojno povezani sistemi naj bi nudili storitve za evropske državljane z namenom povečanja varnosti v zmanjševanju pogostosti prometnih nesreč, povečanje mobilnosti, zmanjševanju gostote prometa in trajnostnega razvoja na področju zmanjševanja izpustov CO_2.

3.2.1 Tehnologija RFID v javnem prevozu

Nizozemska je leta 2005 začela z uvajanjem kartice *OV-chipkaart*[20] – enotne kartice za javni promet – ki bo počasi nadomestila vse druge oblike plačevanja in papirnatih vozovnic za potovanje po Nizozemskem z uporabo javnega prevoza (vlak, avtobus) in s potniškim prometom v mestih (avtobus, tramvaj, podzemna železnica, ...). Kartica, velikosti bančne kartice, vsebuje čip, kamor naložimo kredit v evrih za plačevanje sprotnih voženj ali pa nanjo shranimo, na primer, sezonsko vozovnico za vlak. Obstajajo tri vrste kartic: osebna, anonimna in za enkratno uporabo. Osebna kartica z imenom, priimkom in fotografijo uporabnika omogoča tudi pregled potovalnih podatkov in kredita prek spleta. Nalaganje kredita na kartico ali nakup vozovnic je možen na za to namenjenih avtomatih ali pri blagajnah na postajališčih, uporablja pa se ob vstopu in izstopu na prevozno sredstvo, kjer je nameščen terminal za odčitavanje kartice. Kartica uporablja Phillipsovo *Mifare* tehnologijo za brez-kontaktne pametne kartice, ki se uporabljajo po vsej Evropi v transportne namene in dostop do institucij, ter delujejo po principu RFID.

V tem trenutku je uporaba kartice obvezna oziroma edini način plačevanja za prevoz z avtobusom, metrojem in tramvajem v dveh mestih, Amsterdam

[19] http://www.easyway-its.eu
[20] http://www.ov-chipkaart.nl

in Rotterdam. Ostale vrste plačila ne veljajo več. Kartica pa tudi klasične vozovnice se še lahko uporabljajo po celi nizozemski prometni mreži avtobusov in na nacionalnih železnicah, v regiji Amsterdama pa celo za hitri trajekt. Prednosti kartice so predvsem integracija uporabe različnih prevoznih sredstev, cenovne ugodnosti glede na npr. dan v tednu, ter zmanjšanje izogibanju plačilom. Ni znano, koliko časa bo trajalo, da se bo uporaba *OV-chipkaart* kartice kot edinega in poenotenega načina plačevanja za javni promet razširila na celotno Nizozemsko, vendar nekateri predvidevajo še vsaj pet let.

V Sloveniji je mestna občina Ljubljana aprila 2009 začela z uporabo enotne mestne kartice *Urbana*[21], in sicer najprej na področju mestnega potniškega prometa. Kar se tiče prometa, je tehnologija, uporaba, plačilo in vrste kartic zelo podobna nizozemski *OV-chipkaart* kartici, z razliko v tem, da je trenutno omejena na uporabo na mesto Ljubljana in samo na avtobusni promet. Poleg tega pa se z *Urbano* lahko plačuje vožnjo z vzpenjačo in parkirnino na nekaterih parkiriščih, v nadaljevanju pa bo mogoče plačati tudi storitve v knjižnicah. Kasneje bo *Urbano* mogoče uporabiti tudi ob obisku muzejev, športnih zavodov in kulturnih prireditev.

Glavna razlika je torej, da je nizozemska kartica namenjena transportu, medtem ko je *Urbana* mestna kartica, katere uporaba naj bi se razširila na javne institucije. Pozitivna stran plačevanja za prevoz v Ljubljani pa je, da omogoča tudi alternativo: plačevanje s telefonom prek Monete. Novejših podatkov o tem, ali se bo plačevanje z *Urbano* razširilo tudi na železniški promet, ni bilo zaslediti, vendar pa bi bila to dobra poteza za integracijo različnih prevoznih sredstev po vzoru Nizozemske, za povezanost Slovenije in za odpiranje možnosti za nove cenovne ugodnosti, ki bi spodbudile uporabo železniškega prometa in zmanjšale problem zgoščevanja prometa v prestolnici.

3.3 Pametna mesta

Pametna mesta (angl. smart cities) je izraz, ki se uporablja za mesta, ki stremijo k pametni ekonomiji, mobilnosti, okolja, ljudi (intelektualni in socialni kapital), bivanja (pametni domovi) in upravljanja. Mesta in urbana področja se srečujejo z izzivom kako investirati v inovacije mreže IKT, da bi s tem izboljšali kvaliteto in učinkovitost svojih storitev ter infrastrukture, ki bi vodila v nastanek pametnih mest.

[21] `http://www.jhl.si/holding/urbana`

Pametna mesta so korak dlje od uporabe pametnih mestnih ali potovalnih kartic in združujejo ta element mesta še z ostalimi elementi; ne gre le za pametni prevoz ampak za celotno delovanje mesta kot prek IKT povezanega ekosistema, kar vodi v trajnostni razvoj in izboljšuje kvaliteto življenja meščanov in obiskovalcev.

3.3.1 Projekt pametnih mest znotraj i2010

Evropska unija sicer nima specifičnega projekta pametnih mest, obstajajo pa različne iniciative, ki so podprte s strani EU, npr. *SmartCities*[22] za regijo Severnega morja. Zaslediti pa gre tudi delovanje in ukrepe na področju razvoja pametnih mest v delovnem programu za konkurenčnost in inovacije (angl. Competitiveness and Innovation Framework Programme, CIP), kateri se ukvarja predvsem z IKT politikami [61]. Opisani delovni program spada pod iniciativo i2010 za razvoj informacijske družbe.

Cilj projekta CIP je široka implementacija odprtih platform za dostop do internetnih storitev v mestih. Te platforme naj bi pomagale inovacijskemu ekosistemu pospeševati nastanek pametnih mest in zagotoviti kvalitetne in trajnostne storitve za meščane in poslovanje. Konkretni cilji so:

- **Odprta uporabniška inovacija za bodoče internetne storitve.** Primer odprtih inovacij so *Living Labs*, ekosistemi oziroma raziskovalni koncepti, ki so integrirani v mesto in povezani na evropski ravni, spodbujajo uporabnika k inovacijskemu procesu in javno-zasebna partnerstva v smislu poslovnih modelov in omrežij.
- **Povezana pametna mesta.** Omrežje mest bo podpiralo prenos znanja, izkušenj in najboljših praks med mesti, s fokusom na pametno življenje (urbano načrtovanje pametnih domov in bivanjskih prostorov), zelene digitalne agende (načrtovanje infrastrukture za nizkoogljično ekonomijo), izboljšano vpletenost meščanov kot soustvarjalcev in potrošnikov storitev, ter odprte pametne platforme, ki omogočajo internetne storitve za meščane, turiste, podjetja in javno upravo.
- **Inovativne internetne storitve.** Te naj bi temeljile na uporabi mobilne tehnologije, širokopasovne povezave, naprednih protokolov (npr. IPv6), tehnologiji RFID, multimodalnih vmesnikih, 3D tehnologijah in tako naprej. Govorimo torej o internetu stvari, ki je z visoko družbeno vrednostjo nujen element za nastanek in delovanje pametnih mest [61].

[22] `http://www.smart-cities.eu`

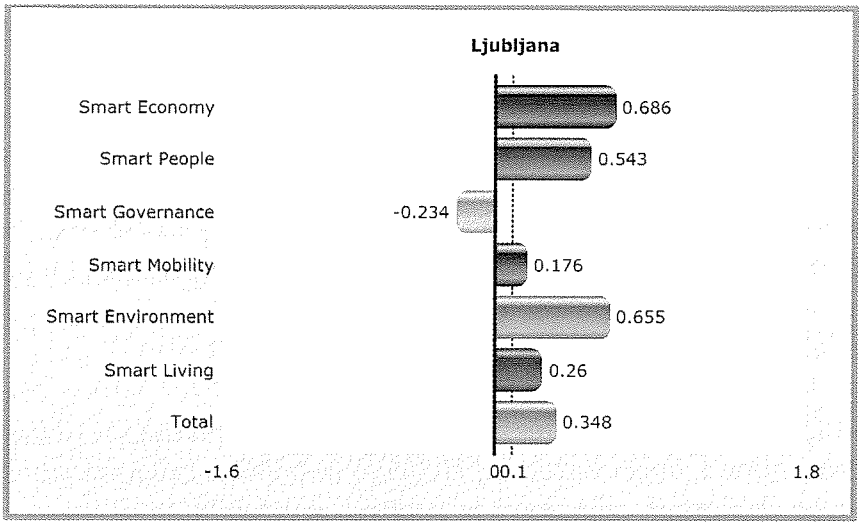
3.3.2 Primerjava Amsterdama z Ljubljano

Amsterdam je znano kot eno vodilnih pametnih mest v Evropi. Projekt *Amsterdam Smart City* označuje sodelovanje med prebivalci mesta, podjetji in upravo, predvsem pa se osredotoča na varčevanje z energijo in inovativne tehnologije. Poskuša stimulirati spremembe v vedenju prebivalcev, saj le-ti bistveno pripomorejo h klimatskim in energijskim programom, katerih cilj je zmanjšanje emisij CO_2 tako na nivoju Amsterdama, kot na nacionalnem in evropskem nivoju.

Leta 2009 in 2010 so začeli s financiranjem projektov, ki se ukvarjajo s področji dela, bivanja, mobilnosti in javnega prostora. Na primer, testni projekt *West Orange*, s področja pametnega bivanja, se ukvarja z implementacijo sistemov za upravljanje energije po domovih, s katerimi želi osveščati ljudi o porabi energije in doseči zmanjšanje porabe v domovih. S sistemom je mogoče daljinsko nadzorovati (npr. z mobilnim telefonom) posamezne aplikacije, pokaže pa tudi porabo energije za vsako posamezno aplikacijo (npr. pralni stroj). Cilj je seveda zmanjšanje izpustov CO_2. Poleg tega je cilj v projektih pametnega bivanja tudi izmenjava znanj, za kar sta odgovorni iniciativi *Amsterdam Open* s spletno platformo za izmenjavo znanj med prebivalci in strokovnjaki, kar vodi v soustvarjanje politik in reševanje problemov v mestu, ter *Apollon Living Lab* za čezmejno sodelovanje in izmenjavo znanj s strani različnih deležnikov; industrije, akademije idr. Projekt *Apollon* se ukvarja predvsem z izdelki IKT in storitvami IKT, kot so e-zdravje, energetska učinkovitost, e-proizvodnja in e-participacija. V programu *Amsterdam Smart City* zasledimo veliko število posameznih projektov – v povezavi z zasebno kot tudi z javno sfero – ki se ukvarjajo s skoraj vsakim področjem implementacije *pametnega* v pametna mesta.

Projekt *Ljubljana, pametno mesto* na enem mestu povzema vse *aktivnosti, ki so usmerjene k boljši kakovosti življenja in boljšim urbanim storitvam z uporabo naprednih tehnologij in okoljsko sprejemljivih ukrepov. Skupni cilj s prebivalci mesta je, da s premišljenim in prijaznim ravnanjem iz Ljubljane naredijo zeleno, pametno mesto* [62]. Za razliko od Amsterdamskega projekta se projekt Ljubljane osredotoča le na okoljski vidik, v povezavi s tem pa na izpeljavo institucionalnih ukrepov mestnih oblasti in okoljsko odgovornega ravnanja posameznikov. Spremembe potekajo na štirih področjih, zrak, voda, zemlja in energija. Na področju Ljubljanskega potniškega prometa uvaja okolju prijazne avtobuse za zmanjšanje emisij CO_2, izvaja projekt *Civitas Elan* za povečanje deleža in kakovosti javnega prevoza (sem sodi tudi pametna mestna kartica) ter za povečanje kolesarskega prometa. Zagotavlja tudi kakovost vodnega omrežja, manjše svetlobno onesna-

ževanje z varčnimi žarnicami, ločevanje odpadkov, večanje zelenih površin itd. Projekt vodi mestna občina, ki deluje na področjih svoje pristojnosti in se za enkrat ne povezuje z drugimi (zasebnimi) podjetji, kar pa bi v prihodnosti lahko prineslo veliko izboljšav in poslovnih priložnosti. Kar lahko sklepamo iz povedanega je, da se projekt Ljubljana ne angažira na ravni interneta stvari, kateri označuje temelj pametnega mesta, projekt pa se tudi ne ukvarja s povezavo na ravni IKT. Tu je potrebno omeniti, da v primeru Ljubljane uporaba imena pametno mesto po kriterijih evropske skupnosti ni ravno ustrezna, saj ne presega okoljskega vidika. Vendar pa obstaja iniciativa *European Smart Cities*, ki preučuje srednje velika evropska mesta prav z vidika indikatorjev pametnih mest in se ukvarja s perspektivo razvoja teh mest. Kot pojasnjuje projekt, imajo manjša mesta (v primerjavi z metropolami, kot je Amsterdam), manjšo kritično maso, vire in kapacitete za organizacijo projektov. To obrazloži, zakaj se v Ljubljani (še) niso lotili projektov povezovanja v internet stvari na višji ravni. Kljub tej pomanjkljivosti pa se Ljubljana po modelu pametnih mest, ki ga uporablja opisana iniciativa, uvršča na 17. mesto izmed sedemdesetih srednje velikih evropskih mest po sledečih kriterijih[23] (Slika 3).



Slika 3. Ljubljana kot pametno mesto po različnih kriterijih

Kot vidimo, Ljubljana zaostaja za drugimi mesti le pri e-vladi (angl. governance), najbolj napreden pa je razvoj pri ekonomiji (indikatorji fleksibilnost trga dela, produktivnost, mednarodna vpetost, ...) in pri okolju (indikatorji onesnaženje, zaščita okolja, privlačnost naravnih pogojev, ...). Mesto Ljubljana ima torej velik potencial, da postane pametno mesto v smislu povezanih pametnih elementov, vendar pa bo potrebno vlaganje v razvoj pove-

[23] Razlaga indikatorjev `http://www.smart-cities.eu/model.html` (7. 2. 2011)

zav prek IKT ter predvsem osveščanje in vključevanje državljanov v procese upravljanja.

3.4 Izbrani scenariji uporabe

Na tem mestu predstavljamo nekaj izbranih scenarijev uporabe interneta stvari v infrastrukturne namene. Poleg že opisanih pametnih mest in pametnega prometa podajamo še nekaj novih.

3.4.1 Infrastruktura mesta

Stavbe, pločniki, prevozna sredstva, ceste, tiri, semaforji, postajališča in druga infrastruktura so opremljeni s senzorji [1]. Zaledni sistem zbira podatke o stanju infrastrukture in jih posreduje ostalim namenskim sistemom.

V središču mesta imamo opravke in želimo čim bližje parkirati. Aplikaciji za parkiranje sporočimo lokacijo, kjer imamo opravke. Sistem pošlje poizvedbo senzorjem, ki merijo stanje parkirišč (zasedeno / prosto) v bližini želene lokacije in predlaga pot do ustreznega prostega parkirišča. Če na voljo ni prostega parkirišča, sistem predlaga oddaljeno parkirišče v bližini avtobusne postaje, kamor bo v kratkem prispel avtobus, ki vozi do centra mesta. V mestu se zadržimo dlje časa kot smo načrtovali in bliža se čas prometne konice. Kar pa sploh ni več problem, saj semaforji spremljajo promet in prilagodijo svoje delovanje, tako da je pretok prometa čim večji in ni zastojev.

Glavni namen pametne mestne infrastrukture je, da izboljša kakovost bivanja meščanov in obiskovalcev mesta. Poleg tega prinaša prek IKT povezana mestna infrastruktura dodatne ekonomske prednosti. Senzorji pošiljajo podatke o stanju objektov sistemu za vzdrževanje. Na podlagi analize stanja teh podatkov mestna občina učinkovito planira vzdrževalna dela in načrtuje gradnjo novih objektov.

Ključni uporabniki so **občine, javni prevoz, prebivalci in obiskovalci mest, podjetja za vzdrževanja, gradbena podjetja** in drugi. Analiza izbranih varnostnih groženj za ta scenarij obsega:

- **Nezakonita obdelava podatkov.** Napadalec zbira podatke, kdaj, kako in katere storitve uporablja obiskovalec mesta. Z analizo podatkov preuči njegove življenje navade. Pri naslednjem obisku mesta mu aplikacija za iskanje parkirnih mest npr. predlaga prosto parkirno me-

sto, ki je "po naključju" zraven restavracije s kitajsko hrano, ki jo dotični uporabnik aplikacije obožuje.

- **Nepooblaščena uporaba opreme.** Na senzorje, ki spremljajo količino prometa, je nameščen virus. Sistem, ki uravnava promet in upravlja delovanje semaforjev, dobi napačne podatke in zato na napačnih mestih poveča pretok. Dokler napaka ni odpravljena, prihaja od velike gneče in zastojev na cestah.
- **Nepooblaščeno poseganje.** Napadalec spremeni delovanje semaforjev, luči, prihode vlakov, ipd. Spremembe pri delovanju mu omogočajo popoln nadzor nad pretokom prometa in ljudi. Z usmerjanjem prometa in množice ljudi lahko načrtno povzroči kaos v mestu in / ali izvede teroristični napad.

3.4.2 Javna razsvetljava

Obcestne luči in ulične svetilke so opremljene s senzorji in brezžično komunicirajo s strežnikom, ki upravlja delovanje razsvetljave[24]. Zaledni sistem v realnem časa zbira podatke o vremenskih razmerah, količini prometa, stanju na ulicah in podatke o stanju luči. Glede na trenutne razmere sistem vključi dodatne luči ali pa do določene stopnje zasenči nekatere luči. Zaledni sistem lahko svetilkam posreduje frekvenco utripanja, kar lahko služi kot dodatna signalizacija in usmerjanje v primeru prometnih nesreč. Za vsako svetilko sistem lahko spremlja podatke o napetosti električnega toka, porabljeni energiji, številu ur, ko žarnica sveti, morebitnih napakah, ki so se pojavile, itd. Glede na zbrane podatke se izdela načrt menjave žarnic in ostalih vzdrževalnih pregledov, pri čemer kontrolni obhodi niso več potrebni. Glavne prednosti na tak način vodene javne osvetljave so: manj porabljene energije in posledično s tem manjši stroški ter večja skrb na okolje, nižji stroški vzdrževanja, večja prometna varnost, manjše svetlobno onesnaževanje in izboljšano mestno okolje. Prednosti avtomatične javne razsvetljave v potrjuje pilotni projekt iz Osla, kjer so namestili sistem 120[25] pametnih cestnih svetilk [63]. Po šestih mesecih spremljanja podatkov je bil prihranek energije več 70% v primerjavi s porabo energije pri starih svetilkah.

Ključni deležniki so **distributerji električne energije, podjetja za vzdrževanje javne razsvetljave, udeleženci v prometu** in **občine**. Analiza varnostnih vidikov za ta scenarij obsega:

[24]Primer: `http://www.echelon.com/solutions/streetlight/default.htm`
[25]Mesto Oslo sicer upravlja skupaj več kot 250 000 luči.

- **Zavrnitev storitve.** Napadalec onesposobi sistem, ki pošilja navodila posameznim cestnim svetilkam. Lahko pride do popolnega mrka.
- **Nepooblaščena uporaba opreme.** Napadalec v sistem za upravljanje luči namesti virus. Luči se prižigajo in ugašajo v zaporedju, ki povzroča neprijetna občutke in zmanjšuje koncentracijo voznikov, ki se peljejo vzdolž migetajočih luči.

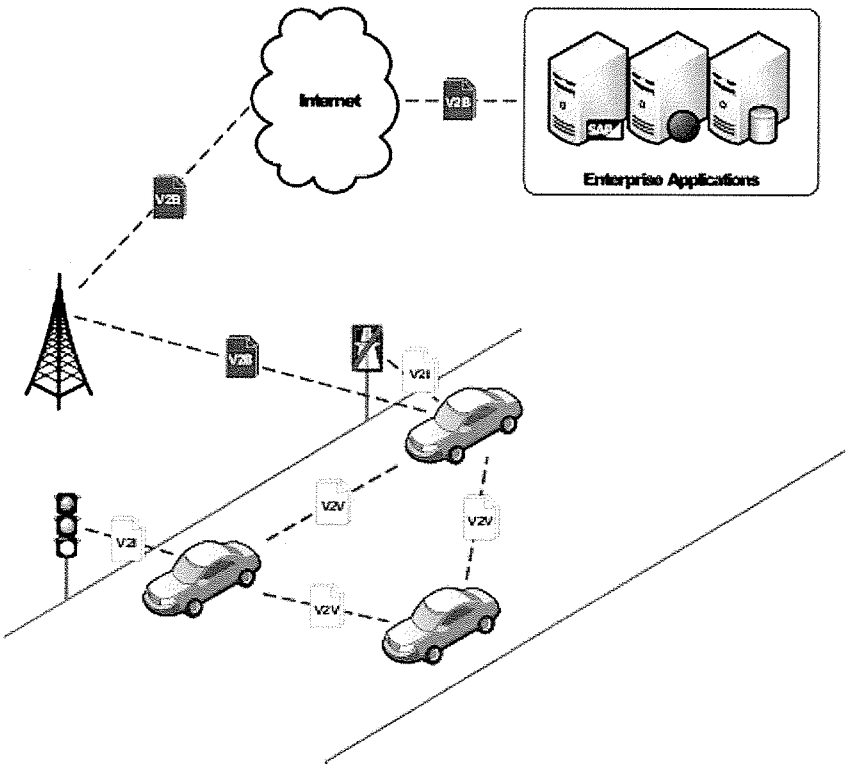
3.4.3 Avtomatizacija prometa

Vozila in cestna infrastruktura [64, 65] so opremljeni s senzorji, ki zaznavajo razmere na cestah in stanje vozila – spolzkost cestišč, tlak v pnevmatikah, gostoto prometa, oddaljenost do drugega vozila, poslabšano vidljivost zaradi megle, ipd. Vozila so povezana z internetom, kar jim omogoča komunikacijo z drugimi vozili (angl. vehicle-to-vehicle communication, V2V), komunikacijo s cestno infrastrukturo (angl. vehicle-to-infrastructure communication, V2I) in dostop do široke palete dodatnih storitev zabavno-informativne narave (angl. vehicle-to-business communication, V2B), kot je prikazano na sliki 4. Avtomobil med vožnjo zazna, da je cestišče zaprto, kar povzroča gnečo. Sporočilo z geografsko lokacijo zaprtega cestišča odpošlje vozilom, ki se približujejo temu predelu. Navigacijski sistem v približujočih se avtomobilih upoštevajo sprejeto informacijo in vozilo preusmerijo na drugo pot. Avto, ki je obstal v gneči se nenadoma pokvari. Vozilo avtonomno pokliče servisni center, ki se nato oddaljeno poveže nanj in diagnosticira okvaro. Če napake ni možno daljinsko odpraviti, se na kraj, kjer je avto obstal, pripelje serviser z rezervnim delom in popravi avto. V primeru nesreče avtomobil pokliče reševalno postajo[26]. Poleg diagnostike avta posreduje tudi podatke o tem, kaj prevaža (ljudi, blago, strupene kemikalije in drugo), da lahko reševalni center pravilno in učinkovito ukrepa.

Vozilo je popravljeno in nadaljuje svojo pot. Kmalu zatem zazna prazen tank, zato v omrežje pošlje poizvedbo o bližnjih bencinskih postajah. Vozniku poleg informacij o oddaljenosti do postaje sporoči tudi cene bencina, ponudbo kosil v restavraciji na postajališču in druge dodatne vsebine.

Glavni namen avtomatizacije in povezanosti vozil – govorimo o t. i. *internetu vozil* (angl. internet of vehicles) – je izboljšanje prometne varnosti. Poleg tega internet vozil poveča pretok prometa in voznikom olajša vožnjo. Popolna avtomatizacija bo pomenila, da se vozila premikajo samostojno, brez

[26]Ukrep, po katerem bodo naša vozila samodejno klicala reševalce ter jim javila lokacijo nesreče je sprejela tudi Evropska unija:`http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm`



Slika 4. Inteligentni prometni sistem, vir Miche et al

šoferja. Ideja vozil brez voznika je smiselna pri uvedbi robotskih taksijev [1]. Le-ti zajemajo informacije o prometu in delujejo v skupini. Pot posameznega taksija se dinamično spreminja glede na dane pogoje in zahteve strank, tako da celotna veriga taksijev čim bolj učinkovito zagotovi prevoze strank.

Pogosti uporabniki in ponudniki opisane storitve so **proizvajalci vozil, podjetja za vzdrževanje cest, javna prevozna sredstva, taksi službe, šoferji** in drugi. Analiza groženj po predlaganem modelu groženj:

- **Nepooblaščeno poseganje.** Na določenem odseku ceste potekajo obnovitvena dela in cestni odsek je na tem delu nevaren za vožnjo. Center za obveščanje vozil hrani podatek o nevarnem odseku. Navigacijski sistem v vozilu načrtuje pot in centru za obveščanje pošlje poizvedbo o zaprtih in nevarnih cestiščih. Napadalec v sistemu centra za obveščanje spremeni podatke o nevarnih odsekih in tako je vozilo usmerjeno na nevarno cestišče. Voznik je vajen, da ga sistem pravočasno in pravilno obvesti o vseh nevarnosti in preprekah na cesti in je posledično manj pozoren na vožnjo. Na nepričakovano nevarnost bo slabo reagiral, pri čemer so posledice lahko tudi smrtne.

- **Okvara podatkov.** Napadalec prestreže sporočilo o oddaljenosti do drugega objekta, ki ga senzor posreduje glavnemu sistemu vozila in spremeni podatke. Obstaja nevarnost, da voznik, ki je vajen pomoči pri parkiranju ali avtomatskega parkiranja, brez pravih podatkov o oddaljenost do drugih objektov ne bo zmožen samostojno parkirati avtomobila. Ali pa – med hitro vožnjo po avtocesti ne bo znal sam presodit, kakšna je primerna varnostna razdalja. Tehnologija, ustvarjena v dobri veri z namenom, da bo v pomoč in korist uporabnikom, začne delovati v škodo uporabnikom[27].

- **Nepooblaščena uporaba opreme.** Napadalec deformira delovanje senzorjev, tako da merilci hitrosti beležijo nižjo hitrost od predvidene. V primeru nesreče zaradi neprilagojene hitrosti izvedenci analizirajo zgodovinske podatke, ki jih shranjuje avtomobilski sistem. Ugotovijo, da je en izmed avtomobilov vozil prehitro, drugi (s ponarejenimi podatki) pa je vozil po predpisih. Zavarovalnica vozniku drugega vozila izplača škodo, prvemu pa ob naslednjem zavarovanju prišteje kazenske točke.

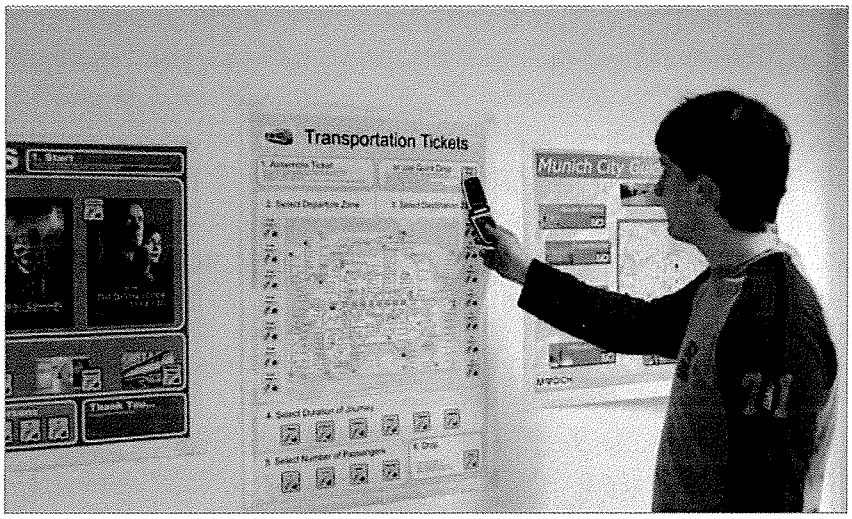
3.4.4 Vozni red vlakov

Vozni redi vlakov [1, 66] so označeni z značkami NFC in se nahajajo na železniški postaji ter na drugih lokacijah v mestu. Uporabnik na voznem redu poišče informacije o odhodu vlakov proti želenem cilju, kot prikazuje slika 5. Z mobitelom, ki ima vgrajen čitalnik NFC, se približa mestu, kjer je nameščena značka NFC. Sproži se transakcija in uporabniku se posredujejo dodatne informacije, kot so na primer cena vozovnice, število prostih sedežev na vlaku, postanki na poti, morebitna zamuda, možnost spalnega vagona, ipd. Uporabnik prek telefona neposredno kupi vozovnico in rezervira sedež ob oknu. S tem se izogne vrsti pri prodajnem okencu ali avtomatu, hkrati pa dobi podatke, veljavne v danem trenutku.

Ključni deležniki pri tem scenariju so **potniki, podjetja za upravljanje železniške infrastrukture, ponudniki železniškega potniškega prometa**. Analiza varnostnih vidikov z modelom groženj:

- **Okvara podatkov.** Napadalec spremeni zapis na znački NFC v lastno korist oz. korist naročnika – na primer taksi službe. Uporabnika, ki bo želel pridobiti podatke o prostih sedežih na določenem vlaku, preusmeri na taksistovo spletno stran, kjer se mu ponudi *posebna enkratna*

[27] Primer bloga z pomisleki o tem, kdaj in kako tehnologija poneumlja ljudi in nam začne škodovati: `http://scifisophie.wordpress.com/2011/03/11/34/`



Slika 5. Vozni red vlakov, označen z značkami NFC, vir Broll et al

priložnost. Naiven uporabnik se bo zaradi tega odločil raje za prevoz s taksijem. Ne-naiven uporabnik v izjemni naglici, ki v danem trenutku ne bo imel možnosti na drug način pridobiti informacij o vlaku in nakupu karte, pa je lahko primoran sprejeti dano (z nepooblaščenim dejanjem vsiljeno) ponudbo taksi službe.

3.4.5 Pametna bolnica

Pametna bolnica [1, 64, 67, 65] je izdatno opremljena z značkami RFID. Označeni so medicinski pripomočki, zdravniki in medicinske nosijo t. i. *pametne značke* (angl. smart badge), bolnik ob prihodu v bolnico dobi zapestnico z vgrajeno značko RFID, ravno tako so elektronsko označene tudi vse njegove kartoteke, označena so zdravila, vrečke krvi, itd. Pametna bolnica ima nameščene tudi čitalnike RFID. Le-ti so nameščeni na vhodu, v vsaki operacijskih sobi, v ambulantah, čakalnicah in na drugih strateških mestih.

Ko bolnik vstopi v bolnišnico, je jasno identificiran in sistem zbere podatke o njegovih preteklih zdravljenjih. Zmanjša se verjetnost, da bi bolniku zaradi napačne identifikacije predpisali napačna zdravila ali ga zdravili na njemu škodljiv način [67]. Prav tako se s pametnimi značkami označi novorojenčke [68], da ne pride do zamenjav[28].

Označeni medicinski pripomočki pripomorejo k nižjemu številu napak med operacijami; denimo označene vrečke krvi zmanjšajo število napačnih transfuzij [69, 70], boljše sledenje pa zmanjša število operacij, pri katerih ki-

[28] `http://www.wnd.com/?pageId=45542`

rurgi v telesu operiranca pozabijo kakšen pripomoček[29] [30] [31] [32], kar je danes neredko dokumentirana napaka [71].

Z označevanjem medicinskih pripomočkov se zmanjša tudi število kraj leteh. V podatkih iz raziskave [72] je bilo leta 2005 v enajstih bolnišnicah v Veliki Britaniji ukradenih za več ko 155 000 EUR materiala.

Poleg tega nameščena tehnologija spremlja pretok bolnikov, delo osebja in zasedenost kapacitet. Na podlagi izmerjenih podatkov vodstvo bolnišnice optimizira delovne procese, izboljša oskrbo pacientov in v splošnem izboljša kakovost storitev.

Ključni deležniki so **bolnišnice, zdravniki, medicinske sestre, negovalci, pacienti, dobavitelji medicinske opreme**. Analiza izbranih varnostnih groženj za opisan scenarij:

- **Kraja.** Zdravnik po končanem delu svojo značko pusti na delovni halji, ki jo obesi v ambulanti, ter gre domov. Medinska sestra vzame zdravnikov pametno značko in jo pošlje ponarejevalcu, ki iz značke razbere tajni ključ, ki zdravniku omogoča dostop do sobe z zaupnimi dokumenti. S ponarejeno značko lahko medicinska sestra nepooblaščeno dostopa do zaupnih informacij in dragih medicinskih pripomočkov.
- **Nezakonita obdelava podatkov.** Osebje bolnišnice zaradi optimizacije delovnih procesov spremljajo, kje se nahajajo. Iz podatkov razberejo tudi druge podatke, ki niso relevantni za izboljšanje delovnih tokov – s kom hodijo na kosilo, s kom se pogosteje družijo, kdaj gredo na stranišče, itd., s čimer je ogrožena njihova zasebnost.
- **Okvara podatkov.** Napadalec zve, da se v bolnišnici nahaja vpliven politik. Niz elektronske produkte kode, ki označuje zdravila, ki so mu predpisana, zamenja z nizom EPC, ki označuje zdravila z nasprotnim učinkom. Dostava zdravil do pacienta je avtomatizirana glede na predpis v elektronski kartoteki pacienta. Politik dobi zdravila, ki za njegovo zdravstveno stanje lahko smrtonosna.

[29] http://www.dailystrength.org/health_blogs/teamds/article/surgical-sponge-left-in-patient-during-surgery

[30] http://www.spanglaw.com/Surgical-Errors-and-Post-Surgical-Complications/Foreign-Objects-Left-in-Body.shtml

[31] http://legalmedicine.blogspot.com/2010/06/something-left-inside-during-surgery.html

[32] http://www.nursinghomesabuseblog.com/medical-malpractice/never-event-6-foreign-objects-left-in-during-surgery

3.5 Akcijska vodila in smernice

Glede na obravnavane scenarije uporabe in analizo vplivov interneta stvari na področju infrastrukture predlagamo naslednje akcijske korake:

- finančna spodbuda malim in srednje velikim podjetjem (angl. small and medium enterprises, SMEs), saj gre pri uvedbi interneta stvari za infrastrukturne namene za tehnologijo, ki je obvladljiva za mala in srednje velika podjetja;
- spodbuda domačim ponudnikom na področju razvoja in implementacije rešitev za t. i. pametno infrastrukturo; med drugim tudi z ustrezno zakonsko regulativo, ki bo pri naročilih omogočala prednost slovenskim ponudnikom pred tujimi.

Ključni igralci: mestne občine, Ministrstvo za promet, Ministrstvo za gospodarstvo, Ministrstvo za visoko šolstvo, znanost in tehnologijo, Ministrstvo za notranje zadeve.

4 Vplivi na gospodarstvo

Integralni del interneta stvar je tehnologija RFID, za katero bi lahko rekli, da v tem času doživlja drugo pomlad, tokrat na gospodarskem področju. Danes skušajo podjetja najti rešitve RFID na različnih nivojih poslovanja z različnimi nameni: bodisi izboljšati učinkovitost procesov v distribucijskih centrih, izboljšati strategije nabave, kot je denimo uvesti dobavo v pravem času (angl. just in time), zmanjšati število ponaredkov na trgu in še marsikaj drugega. Zdi se, da bo tehnologija RFID postala podobno revolucionarna, kot je bila IKT v osemdesetih in devetdesetih letih prejšnjega stoletja. Druge tehnologije interneta stvari so v analizah in ekonomskih prognozah precej zapostavljene, kar je verjetno posledica manjše uporabe v primerjavi s tehnologijo RFID. Kljub temu pa v nadaljevanju zapisano velja tudi za senzorična omrežja ter ostale tehnologije.

4.1 Predvideni ekonomski učinki

Danes je težko podati sistemsko in zanesljivo oceno celotnega vpliva tehnologije RFID na gospodarstvo. Razlog je predvsem v tem, da jo podjetja sprejemajo z različno intenzivnostjo, kar pomeni, da je uporaba razpršena po celotnem gospodarskem spektru, poleg tega pa je v večini primerov še na dokaj začetni stopnji. Zato študije, ki se ukvarjajo z napovedovanjem ekonomskih učinkov, temeljijo na različnih predpostavkah in izkušnjah, ki izhajajo iz merjenja učinkov tehnologije IKT [73].

Raziskovalci v študiji [73] ugotavljajo, da bo tehnologija RFID imela velike vplive zlasti zaradi naslednjih treh razlogov; (i) tehnologija bo omogočila izboljšavo učinkovitosti v mnogo procesih, ki so se do sedaj izvajali ročno, saj bo omogočila visoko stopnjo avtomatizacije, (ii) zaradi povečane transparentnosti, zanesljivosti in točnosti bo tehnologija RFID nekatere procese korenito spremenila in (iii) pojavili se vodo sinergijski učinki, ko bodo v omrežje tehnologije RFID vstopili dodatni omrežni elementi in uporabniki. Na tem mestu omenimo omrežje EPCglobal, ki smo ga opisali v poglavju 2.2.2 in ki ga nekateri interpretirajo kot sam internet stvari.

Rezultati omenjene študije kažejo, da se bodo glavni vplivi izražali v povečani stopnji produktivnosti. Ta bo posledica višje stopnje transparentnosti in bolj natančnih podatkov o dogajanju v oskrbovalni verigi, zamenjave roč-

nega dela z avtomatiziranim ter dodatne zmožnosti oddaljenega zaznavanja in sledenja izdelkom. Poleg tega bo tehnologija RFID imela konkretne vplive na zaposlovanje, saj bo na eni strani zmanjšala potrebo po nizko kvalificiranih kadrih, ki jih bo nadomestila avtomatizacija, in po drugi strani povečala zahteve po visoko izobraženih kadrih, ki bodo potrebni za vzdrževanje takšnih sistemov in izvajanje analiz nad zbranimi podatki. Tehnologija RFID ponuja možnosti razvoja novih izdelkov in storitev, ki lahko podjetjem ne samo pomagajo izboriti si boljši položaj na trgu, temveč celo odprejo povsem nove trge. V splošnem lahko pričakujemo, da bo tehnologija RFID povečala raven produktivnosti in v končni fazi tudi povečala rast BDP držav.

4.2 Gospodarski vidik znotraj Evropske unije

Po ugotovitvah Evropske komisije [74] se komponente interneta stvari kažejo na sledečih gospodarskih področjih:

- Uporaba pametnih mobilnih telefonov, ki uporabljajo brezkontaktno tehnologijo NFC (angl. near-field communication, NFC). Namen tovrstne komunikacije je, na primer, pridobivanje dodatnih informacij o izdelkih – o alergenih.
- Uporaba enotne serijske številke na farmacevtskih izdelkih (črtna koda), ki omogoča preverjanje vsakega izdelka, preden ga dobi pacient. Opisano zmanjšuje možnosti ponaredb in napak pri izdajanju zdravil. Možna aplikacija tega pa je uporaba takega pristopa sledljivosti pri potrošniških izdelkih za prepoznavanje ponarejanja in nevarnih izdelkov, kjer bi Evropa lažje ukrepala.
- Uporaba v energetskem sektorju za merjenje porabe električne energije. Omogoča pridobivanje podatkov o porabi potrošnikov v realnem času in daljinsko spremljanje električnih aparatov.
- Uporaba v logistiki, predelovalni dejavnosti in maloprodaji. *Inteligentni predmeti* olajšujejo izmenjavo informacij in povečujejo učinkovitost proizvodnega cikla.

4.3 Izbrani scenariji uporabe

V nadaljevanju predstavljamo nekatere tipične scenarije uporabe interneta stvar na področju gospodarstva. Tipično je na tem mestu govora o upravljanju oskrbovalne verige in izboljševanju proizvodnih procesov, mi pa dodajamo še nekatere manj znane.

4.3.1 Oskrbovalna veriga in logistika

Izdelki so opremljeni z značkami RFID, ki omogočajo spremljanje lokacije izdelkov v vsakem trenutku [1, 65, 75]. Upravljanje oskrbovalne verige se v veliki meri avtomatizira. Zaledni sistem za upravljanje oskrbovalne verige spremlja stanje v skladišču – kateri in koliko izdelkov je na zalogi ter avtomatično naroči novo pošiljko. Spremlja, kje se nahaja tovornjak z naročeno pošiljko. Prav tako spremlja, kateri artikli so na policah v trgovini in dinamično pošilja manjkajoče izdelke iz skladišča v trgovino. Za vsak izdelek je natanko znano, kje v trgovini se nahaja. Tehnologija interneta stvari omogoča aplikacije, kot so vodenje in pomoč kupcu v trgovini glede na njegov nakupovalni seznam, avtomatično plačevanje glede na vsebino vrečke, ki jo odnese iz trgovine in podobno. Tehnologija RFID v oskrbovalni verigi omogoča nadzor nad vsakim korakov v oskrbovalni verigi in s tem pripomore k optimizaciji naročil in avtomatizaciji celotnega procesa. Korak več od opisanega omogoča omrežje EPCglobal, ki dodatno ponuja možnost končnemu kupcu, da tudi on poizveduje o izdelku.

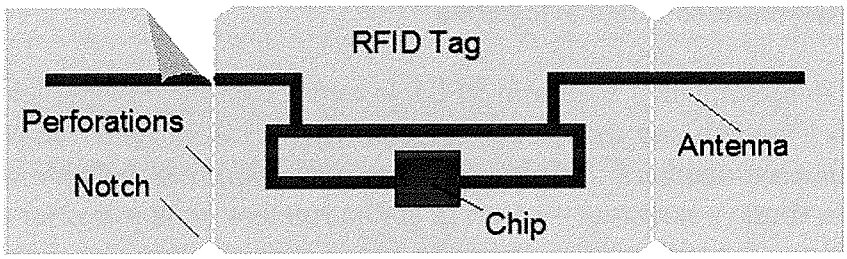
Odziv kupcev po uvedi RFID označevanja v trgovski verigi Wal-Mart[33] nakazuje, da se kupci zavedajo, da je z uvedbo značk RFID lahko ogrožena njihova zasebnost[34]. Podjetje IBM je razvilo značko Clipped Tag [76], ki predstavlja rešitev za problem zasebnosti strank. Značka Clipped Tag je zasnovana tako, da lahko uporabnik enostavno odstrani antenski del, kot je prikazano na sliki 6. Z odstranjenim antenskim delom se radij branja omeji na en centimeter, kar omogoča kupcu, da vsaj delno obvaruje svojo zasebnost. To rešitev omenja tudi Evropska komisija [77], ko govori o pravici potrošnika, da utiša čipe (angl. silence of the chips). Sicer drži, da se tveganje ob taki znački zmanjša, vendar s tem dejanjem do tedaj *pametni* predmet, ki je del interneta stvari, postane navaden predmet, ki z internetom nima več stika, kar pomeni, da praktično izgubi del vrednosti za domačega uporabnika.

Ključni deležniki pri tem scenariju so **tovarne, trgovci, prevozniki, distributerji, kupci, skladišča**. Analiza varnostnih vidikov z modelom groženj:

- **Nezakonita obdelava podatkov.** Stranka kupi izdelek, ki je označen z značko RFID. Ob nakupu artikla značke ne odstrani ali pa še vedno aktivirano značko odstrani in vrže v smeti. Napadalec nezakonito spre-

[33] http://www.walmart.com

[34] http://www.dailyfinance.com/blog/2010/07/26/wal-marts-plan-to-use-smart-rfid-tags-sparking-privacy-concerns/



Slika 6. Zgradba značke Clipped Tag, vir Moskowitz et al

mlja, kakšne izdelke uporablja kupec in zbrane podatke uporabi bodisi za namene ciljnega trženja bodisi sledenje ali druga zlonamerna dejanja.

- **Nepooblaščeno poseganje.** Napadalec na značko RFID vpiše podatek, ki se preko čitalnika posreduje zalednemu delu sistema. Vpisani podatek vsebuje zlonamerno kodo, ki spremeni zapise v podatkovni bazi. Sistem za vodenje oskrbovalne verige deluje napačno.
- **Poneverba podatkov.** Kupec prekopira podatke iz veljavne značke RFID, ki označuje izdelek z nizko ceno in jih shrani na ponarejeno značko RFID, s katero je označen drag izdelek. Izdelek kupi po (nepooblaščeno pridobljeni) ceni, nižji od prodajne.

4.3.2 Avtomatizacija tovarn

Delovna obleka in orodje delavcev v tovarni so opremljeni z značkami RFID[35]. Ko delavec vstopi v tovarno, senzorji preverijo, ali je ustrezno zaščiten. Orodje delavca se nato avtomatično prilagodi glede na delo, ki je tisti dan predvideno za delavca. Delavec lahko vstopa na določena območja tovarne glede na njegovo usposobljenost in opremo, ki jo nosi. Če se na nevarnem območju nahaja oseba, ki ni ustrezno zaščitena, se sproži alarm.

Z značkami RFID so označeni tudi proizvodni deli [1]. Ko jih pripeljejo v tovarno, čitalnik RFID prebere lastnosti dostavljenih delov in sistem preveri, ali so originalni. Dostavljeni deli so avtomatično razporejeni na prava mesta v skladišču. Sistem spremlja stanje zaloge in v pravem času naroči novo pošiljko.

Naprave v tovarni so brezžično povezane in medsebojno sodelujejo [64]. Poleg tega so naprave in stroji opremljeni s senzorji, ki spremljajo pogoje delovanja. Če so tresljaji pri montaži določenega dela preveliki, proizvodnja ustavi. Nenehno spremljanje delovnih pogojev omogoča stalen nadzor

[35] `http://www.ict-sensei.org/Sensei_090422/`, zgodba Worker in a Plant

kakovosti. Če se določena naprava pokvari, se ustavijo tudi vse tiste naprave, ki so odvisne od delovanja pokvarjenega stroja. Naloge v delovnem procesu se avtomatično prerazporedijo, tako da je škoda zaradi okvare naprave, čim manjša. Sistem za spremljanje in upravljanje naprav obenem vodji obrata pošlje sporočilo, da je prišlo do nepredvidenega dogodka. Vodja proizvodnje, lahko na daljavo spreminja nastavitve naprav in delavcem dodeli druge naloge. Sistem za spremljanje in nadzor mu prav tako omogoča, da v vsakem trenutki spremlja stanje naprav, pogoje v tovarni, količino proizvedenih izdelkov, napredovanje pri izvrševanju delovnih nalog, ipd. Proizvodnja je z opisano avtomatizacijo in možnostjo spremljanja delovnih procesov v vsakem trenutku poveča, obenem pa je zagotovljena tudi ustrezna kakovost.

Ključni deležniki pri tem scenariju so **tovarne, delavci, proizvajalci in serviserji delovnih strojev, proizvajalci delovne opreme**. Analiza varnostnih vidikov z modelom groženj:

- **Poneverba podatkov.** Napadalec v značko RFID, ki označuje pomemben rezervni del, vnese veljavno kodo EPC, ki označuje rezervni del, izdelan pri ugleden proizvajalcu. Proizvod je nevede sestavljen iz ponarejenih delov, ki ne dosegajo predpisane kakovosti. Problem je posebej navzoč v letalski industriji [65], saj je vzrok za vsaj 28 nesreč letno[36] uporaba ponarejenih delov.
- **Zavrnitev storitve.** Napadalec glavnemu sistemu v tovarn pošlje preveliko število zahtev, kar onemogoči upravljanje glavnega sistema z napravami v tovarni. Napadalec lahko na daljavo ustavi celotno proizvodnjo.

4.3.3 Prevoz nevarnih in občutljivih snovi

Podjetje za prevoz nevarnih materialov, kot so radioaktivne snovi, kemikalije, eksplozivi, vnetljive snovi, strupi in podobno, z značkami RFID označi embalažo, v kateri snovi iz proizvodnega obrata dostavi v laboratorije, tovarne, vojaške postojanke in druge relevantne lokacije [42, 1, 78, 65]. Podjetje lahko spremlja lokacijo, kje se material nahaja, stanje zalog, prevzem materiala in druge aktivnosti, pomembne pri upravljanju oskrbovalne verige. Oskrbovalna veriga z nevarnimi snovni se od klasične oskrbovalne verige razlikuje v tem, da je poleg same lokacije izdelkov potrebno tudi natančno spremljati pogoje, v katerih se snovi nahajajo. Senzorji glavnemu

[36] http://www.ctv.ca/CTVNews/CTVNewsAt11/20020306/ctvnews848463/

sistemu pošiljajo podatke o temperaturi, vlagi in tresljajih. Kupec pošiljko zavrne, v kolikor je bila dobavljena snov izpostavlja neprimernemu okolju in zato ni več ustrezna za nadaljnjo uporabo. Sistem spremlja lokacijo različnih nevarnih snovi in kemikalij in sproži alarm, v kolikor zabojnika kemikalij, ki bi ob stiku lahko povzročila eksplozijo, prideta preblizu drug drugemu.

Ključni deležniki pri tem scenariju so **podjetja za prevoz nevarnih snovi, laboratoriji, vojska, plinarne**. Analiza varnostnih vidikov z modelom groženj:

- **Odkritje položaja.** Napadalec odčita kodo značke RFID, s katero je označen zabojnik za prevoz nevarne snovi in nato sledi lokaciji zabojnika. Če gre za zelo občutljivo snov, lahko že z majhnimi spremembami v okolici (npr. rahel tresljaj) povzroči eksplozijo. Eksplozija tovornjaka na strateški lokaciji ni splet nesrečnih okoliščin, ampak posledica dobro načrtovanega napada, izpeljanega na podlagi zlorabe značk RFID in ustreznega poznavanja kemikalij.
- **Nepooblaščeno poseganje.** Napadalec spremeni zapis v podatkovni bazi, ki označuje ime kemikalije. Vojska naroči kemikalijo za razvoj novega kemičnega orožja. Zaradi zlonamerno spremenjenega zapisa v podatkovni bazi, v vojaško skladišče dostavijo drugo kemikalijo. Dostavljena kemikalija ob stiku s snovmi, ki so že shranjene v skladišču, povzroči eksplozijo, ki uniči celo vojaško bazo.
- **Okvara podatkov.** Podatki o temperaturi, ki jih senzorji pošiljajo glavnemu sistemu so zlonamerno spremenjeni. Kupec pred plačilom preveri, kakšna je bila temperatura v kamionu med prevozom določene kemikalije. Glede na (neprave) podatke iz senzorjev so bile kemikalije na neprimerni temperaturi, kar zmanjša verjetnost, da bodo vsi nadaljnji kemijski postopki uspešno izpeljani. Kupec je pripravljen sprejeti pošiljko le za polovično ceno, ki pa je posledica nepooblaščenega dejanja.

4.3.4 Vseprisotni sistem pozicioniranja

Tehnologija vseprisotnega pozicioniranja omogočajo lociranje objektov, kjerkoli se ti nahajajo. Razlika med vseprisotnimi sistemi pozicioniranja in trenutnimi globalnimi sistemi pozicioniranja, kot so denimo ameriški GPS, kitajski BD2 ali evropski Galileo, je v tem, da se mora objekt sledenja pri slednjih nahajati na odprtem prostoru, tako da med lokacijsko napravo in navigacijskim satelitom ni ovir. Vseprisotni sistemi pozicioniranja pa delujejo tudi v zaprtih prostorih, kjer omenjena zahteva ni izpolnjena. Takšni

sistemi bodo v zaprtih prostorih realizirani z uporabo razpoložljive infrastrukture, med katerimi bodo pogoste naprave interneta stvari, kot so tehnologija RFID in brezžična senzorska omrežja.

S takšnim sistemom lahko realiziramo scenarij iskanja predmetov, kjer imajo praktično vsi (pomembni) predmeti (avtomobilski ključi, očala, denarnica in drugi) pritrjeno značko RFID[37] [1]. Če uporabnik nekega predmeta ne najde, uporabi aplikacijo, ki beleži mesta, kjer se je predmet nazadnje nahajal. Aplikacija spremlja lokacijo predmeta in uporabniku pošlje sporočilo, če zazna, da je drag predmet neavtorizirano zapustil omejeno območje, denimo da ob odhodu stranke iz prodajalne prodajalno zapusti tudi denarnica prodajalca. Na tem mestu velja omeniti, da se je skovanka *internet stvari* prvič pojavila leta 1999 ravno pri takšnem scenariju uporabe. Takrat je Kevin Ashton iz Auto-ID Labs z značkami RFID opremil več *zanimivih reči*, po prostoru namestil čitalnike, jih povezal z računalniškim sistemom in ta sistem uporabil za iskanje predmetov.

Ključni deležniki pri tem scenariju so vsi uporabniki, ki potrebujejo storitev lociranja predmetov tako **podjetja** kot **gospodinjstva** in **javne ustanove**. Analiza varnostnih vidikov z modelom groženj:

- **Nepooblaščena uporaba opreme.** Potrebno je zagotoviti, da ima iskalec predmetov zadostne pravice, da predmet išče. V nasprotnem primeru postane takšen sistem le pripomoček za poklicne tatove in način nedovoljenega sledenja posameznikom bodisi s strani vladnih ustanov bodisi kriminalcev.
- **Okvara podatkov.** Napadalec v značko vnese deformiran niz elektronske produktne kode. Predmeta sistem ne prepozna več in javi napako, ko uporabnik aplikaciji za iskanje predmetov pošlje povpraševanje o lokaciji danega predmeta.
- **Poneverba podatkov.** Napadalec spremlja imetnika prenosnega računalnika, ko zapušča poslovno stavbo podjetja in posname veljavno sporočilo, ki se na izhodu prenese med čitalnikom in značko, ki označuje prenosnik. Naslednji dan napadalec vzame prenosnik in na izhodu pošlje prestreženo sporočilo. Sistem ne zazna prevare in lastnik prenosnika ni obveščen o kraji.

4.3.5 Aplikacije v športu

[37] http://www.loc8tor.com/uk/

Uporabnik se odloči, da se bo začel ukvarjati s športom, zato se vpiše v bližnji fitnes center. Ob vpisu mu aplikacija za izdelavo športnih treningov predpiše dolgoročni program za osebno vadbo. Klubska kartica fitnes centra, ki jo prejme ob vpisu, vsebuje značko RFID, po kateri naprave v fitnesu prepoznajo imetnika kartice in nastavijo težavnost, čas in način vadbe, ki ustreza njegovemu programu. Naprave spremljajo napredek in zdravstvene parametre uporabnika ter te podatke pošiljajo aplikaciji, ki njegov vadbeni program po potrebi sproti spreminja, da se doseže optimalen učinek [1]. Senzorji na napravah hkrati spremljajo, ali je prišlo do nesreče in v tem primeru sprožijo alarm, ki pokliče zdravniško pomoč. V lepem vremenu želi uporabnik vadbo na fitnes napravah združiti s športnim udejstvovanjem v naravi. Uporabnik nosi športne čevlje z vgrajenimi senzorje, ki spremljajo število narejenih korakov, čas teka, hitrost tekača, dolžino in vzpone na pretečeni progi in podobno[38] [39]. Fitnes aplikacija spremlja njegove tekaške aktivnosti in jih združi s podatki o vadbi v fitnesu, ter tudi drugih športnih aktivnostih uporabnika (npr. kolesarjenju, plavanju, smučanju, ...). Tehnologija interneta stvari vsakemu posamezniku za malo denarja omogoča posebej njemu prilagojeno športno vadbo, spremljanje napredka in optimizacijo treninga glede na dosežke.

Ključni deležniki pri tem scenariju so **posamezniki, fitnes centri, športniki, športni trenerji, proizvajalci fitnes naprav, proizvajalci športne obutve, oblačil in druge opreme**. Analiza varnostnih vidikov z modelom groženj:

- **Odkritje položaja.** Senzorji v športnih čevljih spremljajo in sproti izrisujejo traso tekača. Podatke o trenutni lokaciji tekača dobi nepooblaščena oseba, s čimer je ogrožena tekačeva zasebnost in varnost.
- **Nepooblaščena uporaba opreme.** Napadalec deformira delovanje aplikacije za osebno športno vadbo. Uporabnik aplikacije sledi zahtevam, ki pa zanj niso primerne, zato lahko pride do nesreče zaradi preobremenitve. Uporabnik aplikacij, ki lahko vplivajo na njegovo zdravje ali lahko celo ogrožajo njegovo življenje, se mora zavedati, do katere meje lahko dopusti aplikacijam in tehnologiji interneta stvari, da upravljajo z njegovim delovanjem. Prepoznati mora mejo, ko aplikacija za uporabnika ni več pripomoček, ki mu lajša življenje, ampak uporabnik (ne da bi se tega zavedal) dopusti, da je suženj aplikacije in da le-ta manipulira z njim.

[38] http://www.apple.com/ipod/nike/
[39] http://nikerunning.nike.com/nikeos/p/nikeplus/en_US/plus/

4.3.6 Pametna garderobna omara z osebnim modnim svetovanjem

Pametna garderobna omara ima na vratih vgrajen čitalnik, ki prebere vsebino značke na obleki, ki jo damo v omaro ali vzamemo iz nje [79, 80]. Garderobna omara tako *ve*, katere obleke so v danem trenutku shranjene v omari in lastnosti le-teh, npr. kje je bil kos oblačila kupljen, kakšne barve in velikosti je, iz kakšnega materiala itd. Uporabnik zjutraj zažene aplikacijo za pomoč pri oblačenju. Pametna omara predlaga kose oblačil, ki se barvno ujemajo in ustrezajo vremenu ter aktivnostim, zabeleženim v njegovem koledarju - npr. poslovni sestanek, športni izlet, ... Po napornem dnevu se uporabnik omare vrne domov in ker mu je čez dan zmanjkalo časa za nakupovanje, zažene aplikacijo za nakup novih oblačil. Pametna omara mu glede na trenutno vsebino omare predlaga nove kose oblačil, ki jih bo lahko kombiniral s trenutnimi kosi, ki ustrezajo modnemu slogu uporabnika in upoštevajo vnesene cenovne omejitve. Lastnik omare želi (za posebno priložnost) kupiti novo srajco, ki jo bo oblekel k rjavim hlačam in moderni zeleni jakni. Aplikacija iskanje oblačil omeji na take srajce, ki se skladajo z izbranima kosoma oblačil. Uporabnik lahko še bolj omeji iskanje (npr. želi, da se nova srajce prilega tudi k temno zelenim hlačam). Uporabnik lahko srajce, ki mu jih ponudi aplikacija, takoj kupi prek spleta. Poleg tega sistem za uporabnika na spletu poišče tudi modne dodatke (npr. usnjeno torbico, pas, čevlje), ki ustrezajo novim kombinacijam oblačil. Uporabnik lahko tudi te neposredno naroči prek interneta ali pa jih shrani na nakupovalni seznam in jih naroči kasneje. Ko je imetnik pametne omare v bližini trgovine, kjer prodajajo izdelke iz njegovega nakupovalnega seznama, mu aplikacija pošlje sporočilo o tem. Lastnik pametne omare si oblačilo ogleda v trgovini in ga morda kupi.

Ključni deležniki pri tem scenariju so **individualni kupci, trgovci z oblačili in modnimi dodatki, podjetja za trženje**. Analiza varnostnih vidikov z modelom groženj:

- **Razkritje.** Napadalec javno objavi seznam oblačil, ki jih vplivna oseba hrani v omari, s čimer močno ogrozi njeno zasebnost.
- **Nezakonita obdelava podatkov.** Aplikacije za pomoč pri oblačenju in nakupovanju novih oblek, uporabljajo podatke o tem, kaj se v omari nahaja, kakšen je življenjski slog uporabnika omare, kateri izdelki so mu všeč, ipd. Ponudnik tovrstnih aplikacij mora uporabniku zagotoviti, da bo podatke uporabil izključno za namene, s katerimi se je uporabnik strinjal.

4.4 Akcijska vodila in smernice

Glede na opisane gospodarske prednosti in priložnosti, ki jih prinaša internet stvari, predlagamo naslednje akcijske korake:

- finančna spodbuda malim in srednje velikim podjetjem (angl. Small and medium enterprises, SMEs) pri razvoju novih storitev in produktov, ki temeljijo na tehnologijah interneta stvari;
- uvedba ustreznih zakonskih regulativ, s katerimi se omogoči prednost domačim ponudnikom.

Ključni igralci: Ministrstvo za gospodarstvo, Ministrstvo za visoko šolstvo, znanost in tehnologijo.

5 Vplivi na okolje

Tehnologija RFID omogoča tudi podporo trajnostnemu razvoju s poudarkom na zmanjšanju energetske porabe in učinkoviti reciklaži. Na tem mestu velja opredeliti, kaj pomeni termin trajnostni razvoj: Trajnostni razvoj zadovoljuje potrebe sedanjega človeškega rodu, ne da bi ogrozili možnosti prihodnih rodov, da zadovoljijo svoje potrebe [81].

Z razvojem računalniške tehnologije in njeno naraščajočo prisotnostjo v gospodinjstvih, narašča tudi poraba energije, vezana na sektor IT. Tovrstni sistemi pa namreč predstavljajo tudi znatno energetsko obremenitev (v 2008 je namreč delovanje IKT predstavljalo 8% celotne porabe električne energije), pogosto omrežja delujejo neprestano [82]. S stališča okoljske politike je to problematično in vse več truda se vlaga v varčno rabe energije tudi v IT sektorju. Hlavacs in drugi [82] navajajo primer zelo požrešne tehnologije velikih strežnikov, katerih cena porabe energije že dosega ceno same strojne opreme.

Razumljiva smer razmišljanja je v zmanjšanju števila hkrati delujočih naprav ter tovrstnem zmanjšanju cene energije v IKT. Avtorji prav tako predlagajo skupno omreženo delovanje domačih računalnikov, kjer bi se delovanje le enega skušalo čim bolj izkoristiti in preko neizkoriščenih kapacitet ostalih računalnikov posameznega gospodinjstva vzpostaviti sistem, kjer bi slednji prešli v stanje hibernacije in na ta način zmanjšali rabo električne energije. Mattern in drugi [83] kličejo k vzpostavitvi *zelene IKT*, ki se že odražajo v prvih poskusih regulacije toplote procesorjev, zahteve delovanja velikih podatkovnih centrov in podaljševanje življenjske dobe baterijsko podprtih naprav.

Mattern in drugi [83] ponujajo sistematični pregled dejavnikov in posledic vpeljave IKT v področje ravnanja z viri:

- Premik od neusahljivih zalog do redkih virov; viri so v moderni dobi postali redka dobrina, ki povzročajo politične krize ali celo vojne. Industrijsko razvitim državam zaradi velike porabe teh virov primanjkuje, zato se okoriščajo na račun držav v razvoju.
- Od regulacije k deregulaciji. Evropa uvaja nove in nove mere, ki bi odprle trg z energijo, četudi je ta v našem prostoru še zmeraj precej zaprt.

Z zakonskimi prijemi skušajo vpeljati na energetski trg vpeljati nove ponudnike, a žal ostaja ta trg precej monopolističen.

- Od centralizirane ponudbe do distribuirane rabe.
- Od nadzora do sodelovanja.
- Od rabe energije do pametne in varčne porabe; številni obnovljivi viri so še vedno dokaj neprimerljivi konvencionalnim ponudnikom energije.

5.1 Zmanjšanje porabe

Leitner in dr. [84] ocenjujejo, da se za vsak kilovat energije, ki se porabi za delovanje omrežij RFID lahko z učinkovito rabo drugih naprav, ki temelji na teh sistemih RFID, prihrani celo do 10 kilovatov. Z zavedanjem okoljske problematike, medijsko izpostavljenimi problemi globalnega segrevanja, emisije toplogrednih plinov in tudi e-odpadkov in na drugi strani razvojem in vse širšo rabo informacijsko-komunikacijskih tehnologij se vse več vlaga v IKT kot podporo učinkovitejše rabe in zmanjšanje rabe naravnih virov, s tem predvsem se nanašajo predvsem na učinkovitejšo rabo energije z znatno boljšim izkoristkom.

Smer razvoja IKT kot vir ohranjevanja okolja lahko izboljšuje energijsko učinkovitost na dveh ravneh: učinkovito rabo energije (angl. energy efficiency) in zmanjšanje rabe energije (angl. energy conservation). Kot primer slednjega navajamo delo od doma, kar izniči stroške potovanja na delovno mesto ali pa podpora vzdržnem ravnanju z viri v domačem okolju [83]. Pri tem se izpostavlja tudi vloga interneta stvari oziroma tehnologij RFID.

Ozadje vpeljave ISt predstavlja več kot tretjino (37%) rabe energije, ki pripada zasebnim uporabnikom [83], zatorej je pričakovan klic po tehnoloških rešitvah, ki bi vodile k učinkovitejši rabi energije. Tovrstno, učinkovito rabo virov pa omogočajo t.i. pametna bivanjska okolja. Le-ta Hlavacs in drugi [82] opredeljujejo kot povezavo večjega števila omreženih aparatov, inteligentnih pripomočkov in senzorjev, ki skupaj s domačim računalnikom tvorijo domače omrežje. Medtem ko se v podjetjih varčevanje z energijo nanaša predvsem na avtomatizacijo in optimizacijo poslovanja podprto s klasičnimi IKT, je to v domačem okolju znatno težje. Klasične mere varčne rabe pogosto niso primerne, oziroma ne pridejo do dejanskega izraza/uporabe. Na tem mestu se izkaže vseprisotno računalništvo s senzorji zaznave, cenejšo brezžično komunikacijo, povezavo s svetovnim spletom, ki končno omogoča varčevanje z energijo tudi brez neposredne vpletenosti uporabnika.

Nekateri zanimivi primeri vpletenosti tehnologij za ohranjanje okolja so: avtomatizirana zaznava aktivnosti v posameznem domovanju, ki v komunikaciji s klimatsko napravo prilagodi delovanje dejanskem stanju oziroma potrebam. Podobno se lahko pametni domovi poslužujejo interneta stvari, posebnih pametnih metrov, ki se lahko po potrebi preklopijo na cenejši vir energije, če je le ta na voljo [83]. Napredni tehnologiji navkljub, po možni optimizaciji in avtomatizaciji sistemov pametnega doma vedno ostaja omejitev človeškega faktorja, ostaja namreč vprašanje posameznikove zavzetosti, pripravljenostjo za morda minimalno izgubo udobja in spremembe, ki bi nadalje onemogočila neizkoriščeno porabo energije. Tako višanje cen energije kot tudi skrb za trajnostni razvoj sta ob razvoju obsežnih infrastrukturnih sistemov in procesov omogočali optimizacijo čim nižje porabe energije.

Mattern in drugi [83] navajajo možnosti simulacij, optimizacije in nadzora, kar pride do izraza že pri zasebnih porabnikih. Na drugi strani v industrijski rabi RFID tehnologije pogosto olajšajo odločitve in omogočajo optimizacijo proizvodnih procesov kot tudi posameznih delov oskrbovalne verige ali zbiranje podatkov iz okolja. Navedeni primeri se pogosto obrestujejo na obeh ravneh, za zasebne ali gospodarske subjekte, saj cena energije v zadnjem obdobju opazno narašča, zato je povsem verjetna tudi nadaljnja potreba in razvoj za tehnološko podprte rešitve za ohranjanje okolja.

IKT lahko z avtonomno optimizacijo naredi veliko pri prihranku energije in pri spreminjanju družbenih vzorcev. Predvsem slednje je težko doseči, vendar moramo kljub morda deloma nezadovoljivim prvim rezultatom, ki so lahko posledica neustreznih metod motiviranja in vključevanja kupcev, vztrajati pri njih. Treba je razumeti, da tudi če so prihranki le nekaj odstotni, je energija, ki je ne naredimo, ker je ne potrebujemo, še vedno najcenejša in najbolj okolju prijazna. Pri uporabi teh sistemov je očitna še posredna prednost: ljudje, ki se pogosto ukvarjajo z vprašanjem porabe, bodo bolj verjetno upoštevali okoljsko problematiko, ko bodo kupovali nov TV, avto ipd. [83]

5.2 Uporaba pri reciklaži

Višja kvaliteta življenja je povezana z večjo potrošnjo dobrin in storitev ter posledično z višanjem porabe virov, onesnaževanjem in okoljsko degradacijo [85]. Internet stvari in brezžična tehnologija se lahko uporabljata za izboljšanje efektivnosti številčnih nacionalnih programov za varovanje okolja, npr. pri nadzoru izpušnih plinov vozil (pozitiven vpliv pri ohranjanju čistega zraka), za zbiranje materialov, primernih za reciklažo, za pomoč pri ponovni uporabi elektronskih naprav, reciklažo elektronskih odpadkov (s

sistemi RFID lahko identificiramo komponente računalnika, mobilnega telefona in drugih naprav, ki so primerne za ponovno uporabo in s tem znižamo količino e-odpadkov). RFID lahko tudi pomaga podjetjem pri oskrbovalni verigi tako, da lahko bolj uspešno sledijo in upravljajo z inventarjem in s tem znižajo nepotrebne zahteve pri transportu in uporabo goriva [86].

Označevanje dobrin je za industrijo in okolje izrednega pomena, saj bi se lahko uporabljalo za ločevanje odpadkov. V osemdesetih in devetdesetih letih so se številni raziskovalci iz področja okoljske problematike začeli ukvarjati s trajnostnim razvojem tehnologije, ekonomskih sistemov in okolja. Poudarjali so tehnološki napredek industrijske družbe pri bolj učinkoviti izrabi materialov in produktov. Graedel in Alenby [87] sta leta 1995 razvila koncept industrijskega ekosistema, pri katerem se odpadki enega sektorja skoraj v celoti uporabijo v drugih sektorjih. Seveda uresničitev teh idej še danes ostaja težavna naloga, saj je zbiranje, ločevanje in upravljanje z odpadki zelo težavno in drago [88].

Uporaba značk pri recikliranju oz. pri ponovni uporabi surovin je še v povojih. Običajno gre vse še vedno na skupno smetišče ali pa se odpadke ločuje ročno kot npr. reciklaža elektronskih produktov. Uporaba RFID značk npr. na baterijah lahko naredi ločevanje baterij, ki so primerne za recikliranje, bolj poceni in učinkovito. RFID na zdravju škodljivih produktih (npr. kemikalijah) lahko identificira vsebino in sporoči, kako in kam ta odpadek zavreči [88].

RFID značke so lahko namenjene tudi kot spodbude; kadar vemo za kateri proizvod gre (ali je zdravju škodljiv, ali se ga da predelati ipd.), lahko preverjamo človeško ravnanje z njimi. Pomembno je narediti programe, ki nagrajujejo pravilno recikliranje ter kaznujejo napačno uporabo. Podobna, vsem znana spodbuda je tudi plačevanje manjših vsot pri vračanju steklenic. Da ti principi delujejo, mora biti značka prisotna na proizvodu, ko je ta prodan, ostati pritrjena vse svoje življenje, industrija predelave pa jo mora bit sposobna tudi prebrati [88].

Binder in drugi [85] opisujejo dva različna sistema uporabe tehnologije RFID, ki bi pripomogla k skrbi za okolje. Prvo je oblikovanje pametnega koša za smeti, ki optimizira proces ločevanja odpadkov v gospodinjstvih in podjetjih in ga v naslednjem razdelku podrobneje analiziramo. Drugo je avtomatizacija na koncu cevi, ki se osredotoča na potencial izboljšanja ločevanja odpadkov v sežigalnicah in je predstavljena v nadaljevanju.

Vsaka sežigalnica bi morala biti opremljena s posebno napravo, ki loči vrečke za smeti od dejanskih odpadkov. Vreče se avtomatsko odprejo, odpadki pa so ločeni v večjem bobnu, kjer se material loči na podlagi štirih različnih velikosti delcev. Recikliranje poteka v treh predelih; z magneti v prvi vrsti ločijo pločevinke. Ves ostali material gre v naslednji predel, kjer je prisotna antena, ki prebere značke RFID. Slednja prepozna tipe preostalih odpadkov in sporoči, ali je potrebno dodatno ročno ločevanje. V prvem primeru se podatki vrnejo na začetek, kjer se jih lahko ločuje ročno, v drugem primeru pa gredo ostanki v sežig.

Pri značkah RFID seveda obstajajo tudi omejitve, izpostavlja se predvsem interferenca in območje branja podatkov. Čeprav značke delujejo odlično pri papirju in plastiki, se pojavlja problem pri kovinah, ki spreminjajo elektro-magnetsko polje, znotraj katerega značka deluje. Na območje branja pa vplivajo številni faktorji, npr. moč in velikost antene, sistema frekvenc in velikost značke [88].

5.3 Izbrani scenariji uporabe

V tem razdelku predstavljamo nekatere izbrane scenarije uporabe interneta stvari v domeni recikliranja, varčne porabe energije ter varovanja pred nesrečami. Scenarije ovrednotimo v skladu z modelom proučevanja.

5.3.1 Pametni koš za samodejno ločevanje odpadkov

Vsak potrošnji izdelek je opremljen z značko RFID, na kateri je zapisana ID številka izdelka. Pametni koš za samodejno ločevanje odpadkov je sestavljen iz različnih zabojnikov (za steklo, plastiko, kovine, idr.), ampak ima le en vhod. Na vhodu koša za smeti je nameščen čitalnik. Ko uporabnik izdelek vrže v koš, čitalnik prebere ID izdelka in se prek interneta poveže na podatkovno bazo, v kateri so zapisane dodatne informacije o izdelku – vsebina, material, teža, rok trajanja, ipd. Glede na vrsto izdelka in lokalna pravila za ločevanje odpadkov, pametni koš izdelek usmeri v ustrezen zabojnik. Imetniku pametnega koša se ni potrebno izobraževati o pravilnem ločevanju, a kljub temu pripomore k večji reciklaži izdelkov in posledično čistejšemu okolju. Poleg tega pametni koš obvesti komunalno službo, kdaj ga bo potrebno izprazniti. Pobiranje smeti se optimizira in stroški storitve se zmanjšajo.

Ključni deležniki pri tem scenariju so **gospodinjstva, komunalna podjetja, hoteli, restavracije, podjetja, šole**, in drugi. Izbrane grožnje varnosti in zasebnosti za ta scenarij uporabe:

- **Prisluškovanje.** Tehnologija RFID omogoča branje na daljavo, zato lahko prehrambeno trgovsko podjetje brez fizičnega stika s košem za smeti spremlja, kakšni odpadki so bili odvrženi v koš. Podjetje iz vrste odpadkov razbere prehranjevalne navade odjemalca, zanj ustvari oglaševalsko strategijo in ga zasipa z reklamami, informacijami o posebej zanj prirejenih akcijah in posebnih ponudbah ter drugim nezaželenim (in zavajajočim) gradivom. S tovrstnim prisluškovanjem je ogrožena zasebnost uporabnika.
- **Nepooblaščena uporaba opreme.** Na čitalnik, ki je nameščen na vhodu koša za smeti, napadalec namesti virus, ki spremeni pravila za ločevanje smeti. V zahodnem svetu se že uvajajo kazni za napačno ločevanje odpadkov. Imetniku z virusom okuženega pametnega koša grozi, da bo plačal globo za napačno ločevanje odpadkov.
- **Zavrnitev storitve.** Napadalec uporabi motilni signal in s tem prepreči delovanje koša za smeti. Uporaba pametnega koša za smeti je onemogočena in imetnik mora smeti ločevati ročno.

5.3.2 Pametna hiša

Pametna hiša[40] [1, 63, 65, 89, 90] je opremljena s senzorji in prožilci, ki spremljajo dogajanje v hiši in okolici. S senzorji merimo fizikalne pojave, kot so temperatura, vlaga in drugo. Tako se gretje, klimatizacija in osvetljava samodejno uravnavajo glede na vremenske razmere in glede na potrebe in prisotnost stanovalcev. Sistem pametne hiše spremlja cene elektrike in v terminu, ko je cena elektrike najvišja izklopi hladilnik – za časovno obdobje, ki nima negativnih učinkov na izdelke, ki so shranjeni v njem. Gospodinjski aparati in druge naprave, se samodejno izključijo, če niso v uporabi. Če hiša na primer zazna, da v hiši ni nikogar in je TV vključen, ga avtomatsko izključi. Ker so naprave povezane z internetom, lahko na daljavo spremljajo njihovo stanje in upravljamo z njimi. Ko žarnica pregori, hišni sistem prek spleta naroči novo žarnico in skrbniku hiše pošlje e-pošto, s katerim le-ta potrdi naročilo. Po napornem dnevu v službi, si stanovalka pametne hiše na poti domov zaželi skodelico kave. Prek mobilne naprave pošlje sporočilo kavnemu avtomatu. Ko pride domov s svojim mobilnim telefonom odpre vhodna vrata[41] in v kuhinji jo že čaka sveže skuhana kava. Stanovalci pametne hiše lahko nepretrgoma spremljajo in analizirajo porabo energije, vode

[40] http://homeseer.com/index.html

[41] http://www.racunalniske-novice.com/novice/dogodki-in-obvestila/odpiranje-hisnih-vrat-z-mobilnikom.html?MLSa96c83ab4736529e0c83f7d314cda6ef

in drugih prvin. Zaradi samodejnega uravnavanja pa je poraba v pametni hiši že od začetka nižja.

Ključni deležniki pri tem scenariju so **gospodinjstva, podjetja za distribucijo električne energije, proizvajalci ter uvozniki senzorjev in prožilcev, prodajalci in serviserji delilnikov toplote**, idr. Analiza varnostnih vidikov z modelom groženj:

- **Nepooblaščeno poseganje.** Senzorska vozlišča podatke o izmerjenih fizikalnih količinah pošiljajo posebnemu ponornemu vozlišču. Napadalec poslani podatek prestreže in ga spremeni. Zaledni sistem dobi napačne podatke o temperaturi, vlagi, svetlobi in drugih količinah. Na primer – poveča se gretje, čeprav je v hiši dovolj toplo, luči cel dan svetijo in pralni stroj se vklopi, čeprav ni poln. Poraba elektrike se močno poveča, naprave v hiši se zaradi pregretja in nepravilnega upravljanja pokvarijo.
- **Okvara podatkov.** V zaledni sistem pametne hiše se naloži zlonamerna programska koda, ki TV po en minuti vedno izklopi – ne glede na to, ali pametna hiša pred TV zazna gledalce ali ne. Stanovalcem je onemogočeno nemoteno gledanje TV.
- **Poneverjanje pravic.** Stanovalec hiše pametni hiši pošlje sporočilo, da bo izjemoma prej prišel iz službe in naj se vklopi gretje. Napadalec prestreže sporočilo o ukazu in ponaredi pravice, s katerimi kasneje nepooblaščeno pošilja zahteve pametni hiši in jo oropa.

5.3.3 Pametni števci

Stanovalci večstanovanjskih in drugih stavb z najmanj štirimi posameznimi deli morajo od 1. 10. 2011 dalje imeti vgrajene delilnike stroškov toplote. K temu jih obvezujeta 94. člen Energetskega zakona [91] in Pravilnik o načinu delitve in obračunu stroškov za toploto v stanovanjskih in drugih stavbah z več posameznimi deli [92]. Glavna prednost in namen vgradnje delilnikov stroškov in pametnih števcev (angl. smart metering) je zmanjšanje porabe in s tem povezanih stroškov za ogrevanje in pripravo tople vode [64, 63, 89].

Ključni deležniki pri tovrstnih scenarijih uporabe so **podjetja za dobavo in distribucijo električne energije, podjetja za dostavo in montažo delilnih naprav, stanovalci v večstanovanjskih zgradbah, eko in okoljski skladi** in drugi. Pri analizi varnostni izstopa predvsem naslednja grožnja:

- **Nezakonita obdelava podatkov.** Iz prebranih vrednosti merilcev se lahko v nekaterih primerih restavrira precej natančna slika dogajanja v okolju merjenja. Tako so raziskovalci iz visokofrekvenčnih podatkov pametnega števca za električno energijo uspeli enoznačno določiti, kateri TV program ali DVD gledajo člani družine na domačem TV zaslonu [93]. Podjetje za distribucijo električne energije poleg podatkov o porabljeni energiji, ki jih potrebuje za obračun, dobi tudi podatke, s katerimi lahko določi navade uporabnikov. Tako dobi natančnejšo sliko porabe in lahko spremeni obračunski cenik. Zasebnost uporabnikov, ki uporabljajo pametne števce, je ogrožena.

5.3.4 Upravljanje reciklaže izdelkov

Izdelki so preko značk RFID označeni z enoličnim identifikatorjem in povezani z informacijskim sistemom. Enolični identifikator in izdelek sta nerazdružljiva, zato je možno spremljati trenutni status in celotno zgodovino izdelka – od zibelke do groba (angl. from cradle to grave). Ko se produktu izteče življenjska doba, sistem lastniku produkta pove, kakšne so možnosti za okolju prijazno recikliranje oziroma uničenje le-tega. S tovrstnim sledenjem produktov se poveča količina zbranega materiala za reciklažo, predvsem odpadne embalaže in zmanjša se količina zavrženih električnih in elektronskih naprav, t. i. e-odpadkov (angl. e-waste). Sledenje izdelkov na njihovi življenjski poti omogoča delovanje programov nagrajevanja za okolju prijazno delovanje z odpadki – primer takega programa so t. i. reciklirne banke (angl. recycle bank)[42]. Reciklirna banka spremlja količino zbranih odpadkov za reciklažo in ostala okolju prijazna dejanja stranke. Klienti z okolju prijaznimi dejanji pridobivajo točke, ki jim prinesejo nagrade v obliki popustov in praktičnih izdelkov.

Ključni deležniki pri tem scenariju so **gospodinjstva, podjetja, komunalna podjetja, reciklirne banke, deponije, proizvodnji obrati, podjetja za reciklažo**, idr. Izbrane grožnje varnosti in zasebnosti za scenarij reciklaže:

- **Nezakonita obdelava podatkov.** Kiberkriminalci nezakonito pridobivajo podatke s prisluškovanjem komunikaciji med enoličnim identifikatorjem izdelka in informacijskim sistemom. Podatke o posameznikih, na kakšen način in katere izdelke določen uporabljajo, posreduje tržnim podjetjem. Le-ta iz posredovanih informacij razberejo življenjske navade posameznika in jih uporabijo za ciljno oglaševanje. Alternativno

[42] http://www.recyclebank.com

lahko kiberkriminalci zbrane podatke prodajo policiji ali podobni ustanovi, ki tovrstne podatke potrebuje pri različnih preiskavah.

- **Okvara podatkov.** Napadalec deformira niz, ki enolično označuje izdelek, s čimer je sledenje izdelku onemogočeno. Reciklirne banke ne morejo nagrajevati svojih klientov. Celoten koncept spremljanja izdelka in kasnejšega uničenja in reciklaže na podlagi zbranih podatkov je s tem onemogočen.

5.3.5 Obvladovanje naravnih nesreč

Reševalna služba dobi klic, da je prišlo do razlitja nevarnih tekočin ali plinov. Na teren pošljejo mikro zračna vozila brez posadke (angl. micro unmanned aerial vehicles, MUAV) [94]. Vozila so opremljena z lahkim mobilnim senzorskim sistemom, s katerim spremljajo področje in stopnjo onesnaženosti. Vozila so med sabo brezžično povezana in si preko zalednega sistema sporočajo geo-informacije, podatke o pregledanem območju in sprejetih ukrepih za reševanje. Reševanje naravnih nesreč z mikro vozili ima v primerjavi s pošiljanjem gasilcev in ostalih reševalnih enot na onesnažena področja številne prednosti. Reševalno osebje ni direktno podvrženo nevarnim razmeram, ki ogrožajo njihovo zdravje. Vozila na kraj nesreče pridejo hitreje kot posadke z reševalnim osebjem ter strokovnjaki za jedrsko, biološko in kemično zaščito. Meritve niso omejene smo na talne meritve na področjih, kjer je omočen dostop z avtomobilom, ampak se koncentracija nevarnih snovi lahko izmeri v vseh smereh širitve. Na podlagi obsežnejših informacij in širšega območja opazovanja so možne natančnejše napovedi širjenja nevarnih snovi in pravočasna morebitna evakuacija prebivalstva.

Ključni deležniki pri tem scenariju so **reševalne službe, gasilci, strokovnjaki za jedrsko, biološko in kemično zaščito, inženirji zračnih plovil, strokovnjaki za komunikacijske sisteme** idr. Izbrane grožnje varnosti in zasebnosti za ta scenarij uporabe:

- **Nepooblaščena uporaba opreme.** Napadalec na senzorje, ki odčitavajo podatke o stanju onesnaženosti namesti virus, ki deformira podatke, ki jih senzorji pošiljajo drugim senzorjem in zalednemu sistemu. Zaradi napačnih podatkov sistem predvidi ukrepe, ki ne ustrezajo dejanskemu stanju. Obvladovanje naravnih nesreč je neuspešno. Reševanja in odprava posledic traja bistveno več časa, kot bi sicer, pri velikih nesrečah so ogrožena človeška življenja.

- **Okvara podatkov.** Napadalec deformira identifikatorje senzorjev. Komunikacija med senzorji je s tem onemogočena in podatki o stanju razlitja oz. druge vrste onesnaženosti niso pravilno posredovani. Obvladovanje naravnih nesreč z brezžično povezanimi mikro vozili popolnoma odpove, kar privede do dolgoročnih gospodarskih in družbenih posledic.
- **Zavrnitev storitve.** Podatki zaradi motilnega signala ne pridejo do sistema. Podobno kot v prejšnjih dveh primerih, naravne nesreče ni moč rešiti s predlaganim sistemom mikro zračnih vozil in je nujno imeti v pripravljenosti usposobljeno človeško reševalno ekipo.

5.3.6 Ostali ekološki primeri

Kot priznava Direktorat za Informacijsko družbo Evropske komisije [74] je moč tehnologije RFID vpeti v varovanje okolja na več ravneh: omogočanje sledenja transporta in hranjenja okolju škodljivih snovi, posredovanje ključnih informacij iz okolja v primeru nesreč in izboljšanje varnosti pri transportu. Velike izgube, ki bi jih lahko omilili z uporabo sistemov RFID se nahajajo tudi v predelavi lesa, s tehnologijami RFID pa bi lahko vzpostavili sistem prepoznavanja specifikacij lesa in vpliv okolja na slednjega, s čimer bi se zmanjšal odpad skozi pregled tekom celotne oskrbovalne verige. Z nadomeščanjem aktualnih črtnih kod s sistemi RFID bi tako pridobili cenejšo, robustnejšo in različnim vremenskim pogojem prilagojeno, razgradljivo tehnologijo z obširnimi ugodnostmi za okolje, ne nazadnje tudi s preprečevanjem nelegalnega izseka in prodaje lesa, npr. tropskega. Primer, ki nam je najbližje so moderni avtomobili, katerih regularni delež vloge elektronike je 30%, pri vrstah prestižnejših avtomobilov pa že 60%. Novejši avtomobili že sami po sebi predstavljajo omrežno središče. Funkcije znotraj avtomobilu so med seboj natančno povezane in s tem omogočajo cel spekter zmogljivosti, od preprečevanja prometnih nesreč, sistemi RFID obenem omogoča nadzor nad prometnimi gnečami in hkrati zmanjšanje emisij ogljika.

Drugi pogled, ki priča o možnosti omejitve izpušnih plinov, ki jih prinaša promet, je predvsem učinkovitejši javni transport. Slednjega bi se lahko s pomočjo nadzornih sistemov prilagodilo potrebam. Tako taksiji kot tudi javni avtobusni prevoz bi se lahko povezali na širši elektronsko voden sistem, s čimer bi lahko zmanjšali neefektivnost časa porabljenega za čakanje, klic, nakup in neefektivno in onesnažujočo vožnjo avtobusov ali taksijev. S pomočjo sistemov GPS bi lahko posamezni ponudnik javnega prevoza oddajal svojo lokacijo in razpoložljivost. Uporabnik lahko prek mobilne aplikacije preveril razpoložljivost in prejel informacijo o javnem prevozu ipd. Podobne aplikacije že omogoča spletna stran Telargo za napovedovanje pri-

hodov avtobusov v Ljubljani[43]. Tovrstne aplikacije bi lahko z nadaljnjimi izpopolnitvami vpeljane v druga slovenska mesta. Pri povezavi med ponudniki taksi prevozov in uporabniki pa je še relativno veliko prostora za razvoj elektronsko podprte organizacije prevozov med uporabnikom in ponudnikom.

Promet se izpostavlja kot pogost vir onesnaževanja in kot tak potreben implementacije tovrstnih tehnologij, ki bi maksimirale njegovo učinkovito porabo energije, ne dvomiva pa tudi, da bo v prihodnosti vpeljava tehnologij RFID vse bolj pogost v naših domovih in vzpostavitev pametnih domov naša realnost.

5.4 Akcijska vodila in smernice

Pri uvedbi interneta stvari kot orodja za podporo pri zmanjšanju porabe energije, učinkoviti reciklaži in drugih ukrepih za čistejše okolje, predlagamo naslednje:

- uvedba subvencij za državljane, ki bodo v namen okolju prijaznega obnašanja investirali v produkte ali storitve, ki temeljijo na paradigmi interneta stvari.

Ključni igralci: Ministrstvo za okolje in prostor, Ministrstvo za gospodarstvo, Ministrstvo za visoko šolstvo, znanost in tehnologijo.

[43] http://bus.talktrack.com

6 Vplivi na družbo

Internet stvari bo vplival na veliko področji našega življenja. V tem razdelku so osvetljeni različni družbeni vidiki. Pomemben poudarek je dan percepciji varnosti tehnologije, različnim učinkom tehnologije RFID, vplivom na širšo družbo ter nekaterim scenarijem uporabe.

6.1 Vplivi na zasebno življenje

Predvideni vplivi interneta stvari na posameznikovo življenje so naslednji [65]:

- Internet stvari ter njegove aplikacije in storitve bodo imeli velik vpliv na neodvisno življenje posameznikov. Predvsem je tu vidik starejše populacije, ki bo lahko s pomočjo različnih senzorjev obvladovala stabilno **zdravstveno stanje**. Z uporabo tehnoloških stvari, ki bi regulirale in spremljale pacientovo zdravje, bi tako hitreje odkrili, če je karkoli narobe s pacientom.
- Gradnja inteligentnih stavb oziroma **pametnih domov**, bi pripomogla k temu, da se računalniški brezžični sistem poveže s senzorji, ki merijo na primer vlažnost in temperaturo zraka, svetlost, in tako prilagaja celotno gretje oziroma hlajenje stavbe. Senzorji bi lahko reagirali tudi na aktivnosti človeka v stavbi in mu pripomogli v primeru, ko bi naletel na kakšno težavo. Namen interneta stvari je v prihodnosti omogočiti najbolj ekonomično porabo vseh razpoložljivih virov energije v domovih in tako omogočiti bolj udobno bivanje ljudi v njem.
- V medicini bodo s pomočjo **implantacije brezžičnih naprav v telo človeka** kos različnim boleznim in mu tako pripomogli k bolj varnemu obvladovanju le-teh.
- Ljudje se bodo zaradi tehnologij interneta stvari v okolju počutili bolj varne, saj bodo brezžične identifikacijske naprave uvedene na različnih področjih z namenom **povečanja varnosti**. Eno od področji je okoljski nadzor potresov, cunamijev, poplav. Drugi primer je varovanje in opazovanje nepravilnosti na stavbah, kot je uhajanje plina, vode, ognja, vandalizma. Tretja pa je osebna raven, ki se nanaša na varovanje pred ropi, plačilni sistem in podobno.

- Internet stvari bo omogočil zlitje različnih telekomunikacijskih tehnologij ter ustvaril nove servise in tako še bolj **povezal posameznike** (NFC, Bluetooth, WLAN, GPS, ...).

6.1.1 Potrebe po varnosti in zasebnosti

Internet stvari obljublja revolucijo v računalniški in komunikacijski tehnologiji. Prav tako ponuja revolucijo v načinu, kako živimo ter potencialno zagotavlja inteligentno podporo na vseh področjih našega življenja. Nov razvoj v tehnologiji RFID in brezžičnih senzorjih pomeni, da je še več stvari lahko medsebojno povezanih, še več stvarem lahko sledimo in jih naredimo pametne, v upanju, da za korist družbe [95].

Eden od najpomembnejših izzivov pri prepričevanju uporabnikov za sprejetje novih tehnologij je varovanje podatkov in zasebnost. Zaskrbljenost glede zasebnosti in varstva podatkov je zelo razširjena, zlasti ker lahko senzorji in pametne oznake sledijo uporabnikovemu gibanju, navadam in trenutnim preferencam. Vidna in stalna izmenjava podatkov med stvarmi in ljudmi ter med stvarmi in drugimi stvarmi bo prišla do neznanih lastnikov in izvirov teh podatkov. Sam obseg in zmogljivosti nove tehnologije bodo samo še povečali ta problem [7].

Zaskrbljenost javnosti in aktivne pobude s strani potrošnikov že ovirajo komercialne preizkuse tehnologije RFID. Za spodbujanje bolj razširjenega sprejetja tehnologij, na katerih temelji internet stvari, je potrebno ohraniti načela soglasja, zasebnosti in varnosti podatkov. Poleg tega varovanje zasebnosti ne sme biti omejeno na tehnične rešitve, ampak mora zajemati tudi zakonodajna, tržna in družbeno-etična vprašanja. Če ne obstajajo skupna prizadevanja vlade, civilne družbe in akterje v zasebnem sektorju za varovanje teh vrednot, bo razvoj interneta stvari lahko oviran, če ne celo preprečen [7].

Kot navaja Weber [96] internet stvari, nastajajoča globalna na internetu temelječa tehnična arhitektura, ki omogoča menjavo blaga in storitev v globalnih dobavnih verižnih omrežjih, vpliva na varnost in zasebnost udeleženih strani. Iz tega razloga je potrebno določiti ukrepe, ki zagotavljajo arhitekturno odpornost na napade, verodostojnost podatkov, nadzor dostopa in zasebnost strank.

6.1.2 Zahteve, povezane s tehnologijo interneta stvari

Kot je omenjeno ima opisana tehnična arhitektura interneta stvari vpliv na varnost in zasebnost udeleženih zainteresiranih deležnikov. Zasebnost vključuje tako prikrivanje osebnih informacij kot tudi sposobnost za nadzor, kaj se s temi informacijami dogaja. Pravica do zasebnosti se v tem primeru upošteva kot temeljna in neodtujljiva pravica [96].

Uporabnikom dodelitev oznak predmetom ne sme biti znana, hkrati pa tudi ne sme biti zvočnih ali vizualnih signalov, ki bi pritegnili pozornost uporabnika tega predmeta. Tako je mogoče uporabnikom slediti brez njihove vednosti; na ta način bo uporabnik pustil svoje podatke ali vsaj sledi v kibernetskem prostoru. Problem ni več samo država, ki se zanima za zbiranje ustreznih podatkov, ampak tudi zasebni akterji, kot so marketinška podjetja [96].

Kjer gre za poslovne procese je potrebna visoka stopnja zanesljivosti. V literaturi so tako opisane naslednje zahteve o varnosti in zasebnosti, ki jih bodo morala zasebna podjetja, ki uporabljajo tehnologijo interneta stvari, vključiti v svoj koncept upravljanja tveganj, ki urejajo dejavnosti na splošno [96]:

- **Odpornost na napade.** Sistem mora preprečevati nezavarovane točke in se mora prilagoditi na vozlišče napak.
- **Podatki za preverjanje verodostojnosti.** Pridobljeni naslovi in informacije o predmetu morajo biti avtentični.
- **Nadzor dostopa.** Skrbniki informacij morajo biti sposobni izvajati nadzor nad zagotovljenimi podatki
- **Zasebnost stranke.** Sprejeti je potrebno ukrepe, da lahko samo skrbnik informacij na podlagi opazovanja sklepa o uporabi sistema, ki je povezan z določeno stranko.

6.1.3 Percepcija (ne)varnosti

Varovanje zasebnosti v računalniških okoljih je zahteven problem, ki v domeni interneta stvari dobi še nove razsežnosti. Te smo opisali v razdelku 2.5.2, kjer smo tudi zapisali, da je do sedaj bilo razvitih že več pristopov, vendar so vsi vsaj v nekem pogledu pomanjkljivi, kar definitivno vpliva na percepcijo varnosti omenjene tehnologije. Uspešno izvedeni napadi in nove

potencialne možnosti zlorabe tehnologije RFID so pripeljale do tega, da nekateri značke RFID imenujejo kar vohunski čipi (angl. spy chips)[44]. Ozer [97] tako navaja primere prestrezanja podatkov tehnologije RFID, ki posegajo v zasebnost posameznika:

- IO Active, podjetje iz Seattla, je leta 2007 demonstriralo, kako enostavno je prestrezanje in kloniranje informacij, ki so zapisane v vstopnih karticah v javne ali privatne stavbe. Z napravo v velikosti mobilnega telefona so prestregli podatke mimoidočih in jih kasneje uporabili za vstop v različne stavbe.
- V letu 2006 so s pomočjo čitalnika RFID vrednega 500 dolarjev vdrli v britanske e-potne liste navkljub šifriranju s trojnim DES. Kot pravi Albrecht [98] je bila podobna zgodba s sodobnimi potnimi listi; varnost podatkov je na zelo nizkem nivoju tudi v Nemčiji in na Češkem, kjer so z lahkoto prestregli osebne podatke na omenjenem potnem listu.
- Naslednji primer je vdor raziskovalcev z MIT v kreditne kartice s čipi RFID kot je npr. American Express, kjer so pridobili osebne podatke lastnikov kartic.
- Prestrezanje podatkov VeriChipa, ki ga vstavijo v človeka za razne zdravstvene namene.
- Prestrezanje podatkov na karticah za gorivo in karticah oziroma ključih za avtomobile. Avtomobili, ki delujejo s pomočjo ključev in vsebujejo čip RFID ne vžgejo brez tega čipa; raziskovalci iz Johns Hopkins University so leta 2005 z lahkoto dešifrirali podatke. Na podoben način delujejo tudi tatovi avtomobilov, ki s pomočjo naprave vredne nekaj sto dolarjev dešifrirajo tako kode avtomobilskih ključev kot tudi kartic za gorivo.
- V Združenih državah Amerike so v uporabi vozniška dovoljenja, ki se jih zaradi RFID da preveriti na daljavo. To pomeni, da v primeru, ko se ameriški državljan približa meji ga lahko že od daleč zaznajo preko antene, kjer se nato cariniku na zaslonu pokaže slika in osebni podatki voznika. Ko voznik pride do meje je postopek prečkanja poenostavljen in se v hitrejšem času sprosti promet preko meje. Takšna vozniška dovoljenja z vgrajenim čipom so sicer prostovoljna, vendar se tudi tu postavi vprašanje zasebnosti in varnosti podatkov imetnika tega vozniškega dovoljenja. Nekdo lahko prestreže te podatke s pomočjo določene naprave in tako prebere vse podatke imetnika vozniškega dovoljenja [98].

[44] http://www.spychips.com

V ZDA je leta 2006 oddelek Department of Homeland Security Data Privacy in Integrity Advisory Committee zapisal, da RFID identifikacijski dokumenti omogočajo neavtoriziran dostop do informacij in da se te informacije lahko ponovno uporabi za druge namene brez vednosti ali dovoljenja posameznikov. Takšni sistemi RFID imajo torej potencial, da dovolijo razširitev nadzora nad posamezniki brez njihove vednosti ali dovoljenja [97].

6.1.4 Negativni vidiki tehnologije RFID

Ozer [97] opozarja, da se s tem, ko je v dokumentih vgravirana nezavarovana tehnologija RFID povečuje nadzor nad posamezniki in jim onemogoča pravico do svobode govora oziroma anonimnosti. Prav izguba anonimnosti in zasebnosti vodi v zmanjšano udeležbo pri svobodnem izražanju mnenja in bolj previdne vsakodnevne aktivnosti posameznikov. Posamezniki se v najslabšem primeru ne bi udeleževali političnih protestov v zavedanju, da bi se lahko njihova identiteta in dejanja nekje beležila.

Drug aspekt, ki ga omenja Ozer [97] se nanaša na posameznikovo svobodo oziroma človeško dostojanstvo. S tem je mišljeno, da ljudje ne bi smeli biti označeni kot produkti. Pod človeško vrlino spada pravica do svobode. Označevanje ljudi bi torej moralo vsekakor biti predmet široke razprave na vseh ravneh družbe.

Potem je tu še problem osebne in javne varnosti. S tem, ko se prestreže informacije na identifikacijskih dokumentih lahko pride do različnih zlorab informacij, ki lahko škodujejo imetniku tega dokumenta. Zato je pomembno za posameznike, da ohranijo kontrolo nad razkazovanjem svojih osebnih podatkov. Vendar ravno uporaba tehnologije RFID v identifikacijskih dokumentih ogroža to sposobnost ohranjanja kontrole [97].

Negativna stran, ki jo prinaša tehnologija RFID in kot pravi Ozer [97], je tudi v kloniranju in spoofingu. Kloniranje se nanaša na to, da se prestreženi podatki shranijo na novo kartico, spoofing pa se nanaša ne pošiljanje radijskega signala s pridobljenimi informacijami kar preko prenosnika. Osnova tehnologije RFID nima dovolj tehnološke zaščite, ki je potreba za zaščito pred vdori. Tako torej ni mogoče preveriti ali je npr. potni list tudi avtentičen. Tehnologija je torej omogočila, da se hitro preverja posameznike na kontrolnih točkah na letališčih ali mejah kjer se izvede le vizualni pregled. S tem pa se spodkopava kritična domača mejna kontrola in učinkovitost policistov.

Posebno v ZDA, kjer masovno uporabljajo številko SSN (angl. social security number) lahko zaradi prestrezanja podatkov pride do kraje identitet, kjer se lahko zmanjša finančna varnost posameznikov. V današnjem času se takoj prekliče vse račune in ostale dokumente v primeru, da se izgubi denarnica. Pri tehnologiji RFID pa ne moremo vedeti kdaj prihaja do zlorabe podatkov zato se tudi težko zavarujemo. Kot že enkrat omenjeno je mogoče vdreti v kreditne kartice. Če so torej osebni podatki, številka računa ali katerikoli drugi podatki vpisani na RFID čip in niso primerno tehnološko varovani, se pridobljene informacije lahko uporabljajo za neprimerne namene [97].

V povezavi s tehnologijo RFID se postavlja tudi vprašanje državljanskih svoboščin in zasebnosti potrošnikov. Ozer navaja dva primera, ki sta sporna za kršitev teh svoboščin. Prvi primer je sledenje (angl. tracking), kjer lahko kdorkoli s pomočjo čitalnika RFID prestreza podatke na daljavo, kjerkoli se oseba nahaja. Prav s tem dejanjem se močno omejuje pravico do zasebnosti te osebe. Drugi primer pa je profiliranje (angl. profiling), ki se nanaša na uporabo tehnologije RFID na osebnih in identifikacijskih dokumentih. To profiliranje omogoča, da se o posamezniku ustvari slika njegovih privatnih dogajanj ter predvidevanje o njegovih prihodnjih aktivnostih. Ustvari se velika baza podatkov o posamezniku, ki omogoča državi ali komu drugemu vpogled tako v dejavnosti posameznika kot tudi v njegovo zdravstveno stanje. Primer profiliranja uporabljajo tudi v zabaviščnih parkih, kjer otrokom dodelijo zapestnice s čipom RFID, da jih lahko starši lažje najdejo, hkrati pa tudi za ugotavljanje, katere atrakcije so najbolj zanimive za obiskovalce.

6.1.5 Pozitivni vidiki tehnologije RFID

Vse večja popularnost in uporabnost tehnologije RFID pa za posameznika prinaša tudi mnoge prednosti. Pogostost uporabe se vidi na primer v trgovinah, kjer gre za sledenje določenim izdelkom, na športnih dogodkih, v knjižnicah, vlakih, letališčih, avtobusnih postajah, kjer se preko radijskih frekvenc zazna kraj in čas gibanja imetnika te tehnologije [98].

V porastu je ponudba mobilnih telefonov, ki vsebujejo čipe RFID – natančneje tehnologijo NFC, ki deluje na principu, da mobilni telefon približamo določeni napravi in v hipu opravimo rezervacijo brez da bi vtipkali katerokoli številko. Na takšen način se rezervira na primer koncertne karte, hotelske sobe, letalske vozovnice itd., ker so v telefonu shranjeni podatki kreditne kartice, kar omogoča takojšnjo transakcijo denarja [98].

Potem so tu še zdravstvene kartice, potni listi, označevanje živine, ki pripomorejo k temu, da se lažje in predvsem hitreje zazna osebo ali predmet s

tovrstno tehnologijo. Posamezniki nimajo toliko opravka z izpolnjevanjem raznih obrazcev in vključevanjem v postopke plačila, saj so vsi podatki že podani in jih poseben čitalnik lahko prebere brez posredovanja lastnika kartice [98].

Hayles [99] pa predstavlja nekoliko drugačen pozitivni vidik obravnavanih tehnologij. Omenja zapestnice, ki se uporabljajo za sledenje gibanja zapornikov, ki so v hišnem priporu, ki na nek način pripomorejo k večji varnosti družbe, saj je oseba pod stalnim nadzorom.

6.1.6 Vpliv tehnologije RFID v prihodnosti

Ozer [97] opozarja, da uporaba tehnologije RFID v osebnih identifikacijskih dokumentih v kombinaciji z povečanim javnim nadzorom ljudi s pomočjo kamer lahko pomeni, da lahko vlada z večjo verjetnostjo potrdi identiteto posameznika, ki pride v bližino kamere. To pomeni, da se lahko pridobi posameznikove podatke o njegovih avtomobilih, policijskih prekrških, zaposlenosti, potovalnih in nakupovalnih navadah, DNK itd. Na tem mestu bi bilo potrebno z ustrezno pravno podlago zavarovati posameznike in posledično celotno družbo.

Če se bo množično razširila uporaba RFID v osebnih dokumentih, bo zelo težko narediti te dokumente varne pred zlorabami. Največji uspeh za preprečevanje zlorab pri uporabi tehnologije RFID je odvisen od vzdrževanja varnostnih sistemov. Zato bi morale države čim več sredstev vlagati v kakovostno izdelavo le-teh [97].

Tehnologija RFID prinaša tudi veliko dobička proizvajalcem. Kot pravi Ozer [97] Američani ne plačujejo za RFID samo z davki ampak tudi s posledično izgubo zasebnosti, osebne in finančne varnosti. Naslednji problem je zloraba moči nekaterih držav. Posebno po izbruhu terorističnih napadov v ZDA si države prilaščajo pravico, da nadzorujejo vse in se ne ozirajo dosti na osnovne zakone o posameznikovi zasebnosti. Tehnologija RFID je torej lahko le še dodatna možnost preko katere se lahko izvaja ta nadzor. Potem je tu še dodatna ovira, ki se nanaša na kaznovanje tistih, ki zlonamerno prestrezajo podatke. Težava je predvsem v tem, da tehnologije RFID ne obvestijo imetnika, da se njegove informacije berejo in uporabljajo v zlonamerne namene; tako tudi napadalci ostajajo zakriti [97].

6.2 Vplivi na širšo družbo

Legoland je že razvil aplikacijo, s pomočjo katere lahko sledimo gibanju otrok po zabaviščnem parku. Po eni strani naj bi ta sistem zagotavljal večjo varnost otrok in pomagal staršem hitreje najti otroka, če se ta izgubi. Po drugi strani se lahko osebje zabaviščnega parka prilagodi povpraševanju obiskovalcev na točno določenih lokacijah, kjer v nekem trenutku nastane gneča. In še bi lahko naštevali primere uporabe novih tehnologij interneta stvari, ki jih bomo lahko v prihodnosti občutili končni uporabniki.

Iz zgoraj navedenih primerov postane jasno, da so vplivi, ki jih bodo nove tehnologije povzročila s prodorom v vsakdanjo rabo, izjemni in težko je predvideti do katere mere bodo prodrli v pore družbe. Predpostavlja se, da bo vedno več doslej neodvisnih aplikacij med seboj povezanih s podatki in informacijami o posameznikih, ki bodo omogočale celostno servisiranje uporabnika in na ta način še dodatno prispevale h kakovosti življenja. Ob tem pa številni opozarjajo, da je potrebno prioritetno obravnavati vprašanje zasebnosti in varovanja osebnih podatkov, saj se bodo z razmahom interneta stvari informacije o osebnih podatkih lahko začele množično zbirati in povezovati. Evropska komisija izpostavlja, da bi moral biti razvoj interneta stvari usmerjen predvsem v interes končnih uporabnikov/posameznikov in spodbujati pozitivne učinke na kvaliteto življenja, ne pa izključno v korist privatnega komercialnega sektorja za ustvarjanje profita s pomočjo zbranih podatkov o končnih uporabnikih.

Evropska direktiva navaja, da je potrebno posebno pozornost nameniti varovanju zasebnih podatkov, zaradi same narave tehnologije RFID, ki je vseprisotna in nevidna. Zato pravi, da bi moralo biti načelo spoštovanja zasebnosti in varovanja osebnih podatkov vgrajeno v sam razvoj aplikacij RFID, še preden bodo le-te široko sprejete in množično uporabljane s strani končnih uporabnikov [100].

Po mnenju Evropske komisije je pomembno, da podjetje, ki ima v lasti aplikacijo RFID na vidnem mestu jasno navede

- naziv in naslov podjetja,
- namen aplikacije,
- kateri podatki se bodo z aplikacijo zbirali in obdelovali, še posebej, če gre za osebne podatke, in ali bo aplikacija spremljala tudi lokacijo čipov,
- povzetek ocenjenih učinkov na varovanje podatkov in zasebnosti,

- če obstajajo, morajo biti navedena tudi možna tveganja zasebnosti in ukrepi, ki jih lahko posameznik zavzame, da ta tveganja zmanjša.

Poleg tega bi moral vsak proizvajalec na čitalnik namestiti prepoznavni znak, ki uporabniku sporoča, da izdelek vsebuje tehnologijo RFID. Ta znak mora vsebovati tudi kontaktne podatke o lastniku čitalnika, ki uporabniku zagotavljajo vir informacij, kjer se lahko dodatno pozanimajo o informacijski varnosti pri uporabi aplikacije. Poleg tega mora trgovec, ki prodaja tovrstne izdelke, uporabniku ponuditi možnost, da mu na licu mesta in brez proti-plačila čip odstrani ali deaktivira. Uporabnik pa ima pravico, da preveri ali je bila deaktivacija uspešna in čip ne oddaja več signala [100].

Pomembno je torej, da se mere varovanja zasebnosti vzpostavijo in opredelijo vzporedno s samim razvojem interneta stvari in da so preventivni ukrepi integrirani v same aplikacije. Pravočasno je potrebno predvideti možne nevarnosti za poseganje v zasebnost končnih uporabnikov in določiti ukrepe oziroma sankcije za morebitne zlorabe. Zagotoviti moramo ustrezno sigurnost in zasebnost preden bo tehnologija povsem razvita in bo postala del našega vsakdanjega življenja.

6.3 Izbrani scenariji uporabe

Na tem mesu predstavljamo nekatere izbrane scenarije uporabe interneta stvari, ki imajo vpliv na različna družbena področja, kot je denimo podpora starejšim občanom, uporaba v turizmu zdravstvu in drugo.

6.3.1 Podpora starejšim

Domovi starejših ljudi in ljudje sami so opremljeni s senzorji [75, 65]. V tleh so nameščeni senzorji, ki zaznajo padec osebe in pokličejo pomoč. Senzorji v postelji merijo, ali se oseba premika. Pametno stranišče[45] preverja urin in pošilja podatke v laboratorij zdravstvenega doma. Škatla za prvo pomoč in shranjevanje zdravil spremlja jemanje zdravil [79, 101]. Če je oseba pozabila vzeti zdravilo, jo pošlje sporočilo. Ko začne zdravil primanjkovati, pametna škatla za prvo pomoč pošlje sporočilo zdravniku, ki v naslednjih dneh obišče bolnika na domu. Ljudje nosijo obleke, v katerih so vgrajeni senzorji, ki spremljajo njihovo telesno temperaturo, utrip srca in dihanje. Ljudje s težavami s srcem, imajo implantiran kardioverter defibrilator, ki se samodejno vključi. Ob tem obvesti zdravnika, ki ustrezno ukrepa glede nadaljnje

[45] http://articles.cnn.com/2005-06-28/tech/spark.toilet_1_toilet-toto-bathroom?_s=PM:TECH

pomoči. Uporabljena tehnologija izboljša (ali celo reši) življenje ostarelih; še posebej tistih, ki živijo sami in nimajo družine, ki bi skrbela zanje.

Danes smo v zahodnem svetu priča staranju populacije in tako postaja skrb za starejše vse bolj pomembna. Zato so tovrstni scenariji v velikem družbenem interesu. Med tipične uporabnike tako sodijo **ostareli in bolni, zdravniki, negovalci** precejšen interes utegnejo imeti tudi **zavarovalnice**. Izbrane grožnje varnosti in zasebnosti za ta scenarij uporabe:

- **Nezakonita obdelava podatkov.** Podatki o zdravstvenem stanju posameznikov se smatrajo kot zaupni in razkritje teh podatkov nepooblaščenim ne predstavlja le kršitev omenjene zaupnosti, temveč je lahko celo življenjsko nevarno za uporabnika storitve, saj omogoča potencialnemu napadalcu oddaljen vpogled v zdravstveno stanje žrtve.
- **Nepooblaščeno poseganje.** Napadalec za značko, ki označuje škatlico z zdravili vnese zlonamerno kodo. Ob naslednjem jemanju zdravil, čitalnik prebere značko in podatek posreduje zalednemu sistemu. Tam se izvede zlonamerna koda, ki količino preostalih zdravil nastavi na največ, kar je možno. Če jemalec zdravil ni sam pozoren na to, da bo zmanjkalo zdravil, lahko brez zdravil ostane v usodnem trenutku.
- **Zavrnitev storitve.** Napadalec prepreči dostop podatkov, ki jih posredujejo senzorji, do glavnega sistema. Podatek iz senzorja, ki je izmeril nenadno upočasnitev utrip srca, ne pride do glavnega sistema in zdravniška pomoč ni obveščena o nujnem primeru.

6.3.2 Internet stvari v turizmu

Scenarij uporabe se prične, ko turist prispe v mesto. Na svojem telefonu ima naložen zemljevid mesta, vendar se po zemljevidu prek mobitela težko orientira, težkih vodičev z zemljevidi pa tudi ne želi nosit. Ustavi se na informacijski točki in povpraša po velikem papirnatem turističnem zemljevidu, kakršne ponavadi hrani med spominki iz potovanj. Na informacijski točki mu ponudijo papirnati turistični zemljevid, opremljen z značkami NFC [1, 102]. Med ogledi se mu ena od znamenitosti zdi še posebej zanimiva. Mobilni telefon usmeri proti ikoni na pametnem zemljevidu, ki označuje dotično znamenitost. Sproži se interakcija in turistu se na ekranu mobilnega telefona izpišejo dodatne informacije o znamenitosti. Nato nadaljuje z ogledi in pozno popoldne postane lačen. Mobilni telefon, na katerem ima naložene aplikacije za iskanje bližnjih restavracij[46], usmeri proti trgu, kjer se nahaja.

[46] Primer: `http://www.augmentedplanet.com/2010/05/pizza-hut-goes-ar`

Na zaslonu se izriše trg, ki so mu dodani smerokazi do bližnjih restavracij. Medtem ko čaka, da mu postrežejo s kosilom, zažene mobilno aplikacijo[47], ki mu glede na njegove želje predlaga načrt potovanja in ogled znamenitosti za preostanek večera. Aplikacija poleg tega posodobi njegovo pot in označi mesta, kjer se je ta dan zadrževal. Turist potrdi dodajanje fotografij k označeni poti in prijateljem pošlje vabilo, naj spremljajo njegovo potovanje. Po kosilu nadaljuje z ogledi in se zvečer vrne v hotel. S pomočjo internetne tehnologije je izkoristil dan v najboljši meri, saj ni porabil veliko časa za iskanje turističnih atrakcij in listanje po vodičih. Pred spanjem potrdi rezervacijo sedeža na vlaku in naslednji dan nadaljuje s potovanjem.

Ključni deležniki pri tem scenariju so **turisti, hoteli, restavracije, turistične točke** in drugi. Izbrane grožnje varnosti in zasebnosti za ta scenarij uporabe:

- **Nepooblaščeno poseganje.** V kolikor ni ustrezno zaščitena vsebina značk NFC na zemljevidu, lahko napadalec vnese zlonamerno vsebino. Ta preusmeri turistov telefon na spletni naslov, iz katerega se naloži virus, s katerim lahko napadalec denimo pridobi nadzor nad telefonom, sledi turistu, mu ukrade denar in podobno.
- **Odkritje položaja.** Turist se na različnih lokacijah po mestu poveže na splet in dostopa do želenih storitev. Dokler uporablja aplikacijo, prek katere deli utrinke iz potovanja s prijatelji, in sam eksplicitno označuje mesta, kjer se nahaja, s tem ni težav. Težave nastopijo, ko če se turistu nepooblaščeno sledi.
- **Prisluškovanje.** Napadalec prisluškuje komunikaciji med značko NFC in čitalnikom. Na podlagi pridobljenih podatkov, analizira, kje se turist nahaja in kaj so njegovi interesi. Glede na zbrane podatke ponudnik turističnih storitev izdela ponudbo, ki ustreza zanimanjem turista in ga zasipa z reklamnimi SMS sporočili.

6.3.3 Družabna omrežja

Ljudje za komunikacijo in ohranjanje stikov s prijatelji in znanci uporabljajo družabna spletna omrežja. Prek družabnih omrežij ljudi iz njihove mreže poznanstev informirajo o dnevnih aktivnostih – kje, kdaj in s kom se nahajajo, kaj počnejo, kako se počutijo, itd. Vsakodnevni pripomočki, ki jih ljudje uporabljajo, so povezani na internet in zapise o aktivnostih samodejno

[47] Primer: `http://www.mtrip.com`

posodabljajo glede na okoliščine [1]. Družabnih omrežij ne uporabljajo več samo ljudje, ampak namesto njih tudi predmeti[48] [49] [50].

Tpični deležniki pri tem so **mladi, proizvajalci elektronskih naprav, ponudniki spletnih omrežij**. Izbrana analiza varnostnih groženj zavzema naslednje vsebine:

- **Prisluškovanje.** Napadalec legalno spremlja sporočila, ki jih oseba objavlja na spletih družabnih omrežjih in jih uporabi za lastne koristi. Percepcija zasebnosti se spreminja[51] in za dostop do osebnih podatkov niso več potrebne *klasične*, tj. nelegalne metode prisluškovanja za pridobivanje zasebnih podatkov. S spremenjeno percepcijo zasebnosti se tako tudi spremeni meja, ko posameznik meni, da je njegova zasebnost ogrožena.
- **Nezakonita obdelava podatkov.** Podjetja za trženje uporabijo podatke, pridobljene na spletu: informacije o starosti, stanu, zaposlitvi, ipd., ki jih ljudje objavljajo na svojih profilih v družbenih omrežjih, sporočila, prek katerih obveščajo svoje prijatelje o svojih aktivnosti, zanimive misli, komentarje na druge objave, itd. Glede na sporočila o geolokaciji, ki jih objavljajo z internetom povezane naprave na osebnih profilih v družabnih omrežjih, lahko analitiki ugotovijo kje, kdaj, s kom, na kakšen način in kako se ljudje družijo med sabo. V splošnem so osebni podatki o ljudeh postali zelo vroče blago. Vse bolj pogosta so podjetja, ki po spletu iščejo informacije o posameznikih (angl. information brokering) – na primer starost, premoženje, družinsko drevo, vrednost hiše, itd. – in jih prodajajo[52] [53] [54].

6.4 Akcijska vodila in smernice

Pri obravnavi različnih družbenih vidikov interneta stvari smo videli, da je percepcija varnosti tehnologije prav tako pomembna kot dejanska varnost sama. Zaupanje dovolj širokega kroga ljudi v tehnologije interneta stvari

[48] http://www.bbc.co.uk/blogs/technology/2009/06/things_that_tweet.html

[49] http://www.telegraph.co.uk/science/science-news/6156291/The-house-that-Twitters.html

[50] http://news.bbc.co.uk/2/hi/technology/8113914.stm

[51] http://www.smh.com.au/technology/technology-news/facebook-fear-schooldays-could-be-most-damaging-of-your-life-20110325-1ca1o.html

[52] http://www.spokeo.com

[53] http://www.answers.com/topic/choicepoint-inc

[54] http://www.lexisnexis.com

je nujen pogoj za njeno širitev. Zato ocenjujemo, da bi za razvoj interneta stvari bilo ugodno, da se sprejmejo ukrepi, ki:

- spodbujajo in podpirajo ozaveščanje ljudi tako glede interneta stvari na splošno kot tudi varnostnih vprašanj in vprašanj zasebnosti v internetu stvari;
- omogočajo sistematično zbiranje podatkov relevantnih za študije vidikov interneta stvari. Takšni podatki so osnova za dajanje ocen o (ne)varnosti naprav kot tudi osnova za načrtovanje varnostnih protiukrepov, s čimer se krepi percepcija varnosti. Statistične raziskave, podane v dodatku tega poročila, so narejene na svetovni ravni, saj na državni takšnih podatkov nimamo.

Glavno vlogo pri ozaveščanju javnosti bi morale imeti univerze ter raziskovalni inštituti, medtem ko se pri izdelavi metodologije pričakuje prispevek s strani Statističnega urada.

7 Vplivi na zakonodajo

Na tem mestu obravnavamo zakonodajni vidik interneta stvari. Najprej podamo pregled obstoječe slovenske zakonodaje na tem področju, v nadaljevanju pa predstavimo nekatere direktive Evropske unije ter primere iz Združenih držav Amerike.

7.1 Obstoječa slovenska zakonodaja

Obstoječo zakonodajo bomo predstavili na podlagi končnega poročila iniciative Coordinating European Efforts for Promoting the European RFID Value Chain (CE RFID) [103], katere namen je izboljšanje pogojev za konkurenčnost tehnologije RFID in njen nadaljnji napredek v Evropi ter izboljšati politično okolje v prid tehnologije RFID na evropskem nivoju. Iniciativa je bila financirana s strani Evropske komisije znotraj 6. okvirnega programa. V Sloveniji imamo trenutno šest zakonov, ki obsegajo področje RFID tehnologije in jih predstavljamo v nadaljevanju.

7.1.1 Zakon o varstvu osebnih podatkov

S tem zakonom se določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice (v nadaljnjem besedilu: posameznik) pri obdelavi osebnih podatkov. [104]

Varstvo podatkov je glavna skrb pri uveljavi tehnologije RFID in vseh možnih aplikacij, ki jih ta prinaša. Sicer v večini primerov tehnologija RFID ne vključuje uporabo osebnih podatkov in ne zbuja varnostnih vprašanj, vendar v nekaterih primerih prihaja do procesiranja osebnih podatkov, tako da obstaja tveganje odkritja teh podatkov in njihovega posredovanje neželenim strankam [105].

7.1.2 Zakon o elektronskih komunikacijah

Ta zakon ureja pogoje za zagotavljanje elektronskih komunikacijskih omrežij in za izvajanje elektronskih komunikacijskih storitev, ureja zagotavljanje univerzalne storitve, upravljanje radiofrekvenčnega spektra, izrabo številskega prostora (oštevilčenje), določa pogoje za omejitev la-

stninske pravice, določa pravice uporabnikov, ureja delovanje omrežij in storitev v izrednih stanjih, ureja zaščito tajnosti in zaupnosti elektronskih komunikacij, ureja reševanje sporov med subjekti na trgu elektronskih komunikacij, ureja pristojnosti, organizacijo in delovanje Agencije za pošto in elektronske komunikacije Republike Slovenije (v nadaljnjem besedilu: agencija) kot neodvisnega regulativnega organa ter pristojnosti drugih organov, ki opravljajo naloge po tem zakonu, in ureja druga vprašanja, povezana z elektronskimi komunikacijami. [106]

Tehnologija RFID, podobno kot pri prejšnji točki, spada na področje elektronskih komunikacij, predvsem v smislu mrež in storitev.

7.1.3 Zakon o telekomunikacijah

Ta zakon ureja prenos informacij v telekomunikacijskih omrežjih, pogoje za opravljanje javnih telekomunikacijskih storitev in obratovanje javnih telekomunikacijskih omrežij, ureja izdajanje dovoljenj za opravljanje telekomunikacijskih storitev, določa pogoje in postopek za uporabo radiofrekvenčnega spektra, pogoje za medsebojno povezovanje omrežij in priključevanje uporabnikov, ureja zagotavljanje univerzalnih telekomunikacijskih storitev, določa pogoje za uporabo telekomunikacijskih številk ter pogoje za uporabo radijske in terminalske opreme, ureja ustanovitev, organizacijo in delovanje Agencije za telekomunikacije in radiodifuzijo Republike Slovenije (v nadaljevanju: agencija) kot neodvisne organizacije urejanja ter pristojnosti organov, ki opravljajo druge upravne naloge po tem zakonu, določa naloge Sveta za telekomunikacije, določa pravice in obveznosti operaterjev telekomunikacijskih storitev in njihovih uporabnikov ter ureja druga vprašanja, povezana s telekomunikacijami. [107]

Tehnologija igra ključno vlogo pri razvoju rabe RFID, zato je nujna tehnološka podlaga, da lahko RFID uspe v širšem smislu. Obstajati mora skupna in uravnovešena radio-frekvenčna baza znotraj Evrope [105].

7.1.4 Zakon o industrijski lastnini

(1) Ta zakon določa vrste pravic industrijske lastnine po tem zakonu in postopke za podelitev in registracijo teh pravic, sodno varstvo pravic in zastopanje strank v postopkih po tem zakonu.

(2) Pravice industrijske lastnine po tem zakonu so patent, dodatni varstveni certifikat, model, znamka in geografska označba.

(3) Ta zakon prenaša v pravni red Republike Slovenije določbe Direktive št. 98/44/ES Evropskega parlamenta in Sveta z dne 6. julija 1998 o pravnem varstvu biotehnoloških izumov (UL L št. 213, z dne 30. 7. 1998, str. 13), Direktive št. 98/71/ES Evropskega parlamenta in Sveta z dne 13. oktobra 1998 o pravnem varstvu modelov (UL L št. 289, z dne 28. 10. 1998, str. 28), Prve direktive 89/104/ES z dne 21. decembra 1988 o približevanju zakonodaje držav članic v zvezi z blagovnimi znamkami (UL L št. 40, z dne 11. 2. 1989, str. 1) in Direktive 2004/48/ES Evropskega parlamenta in Sveta z dne 29. aprila 2004 o uveljavljanju pravic intelektualne lastnine (UL L št. 195, z dne 2. 6. 2004, str. 16). [108]

Tukaj gre predvsem za regulacijo v smislu patentne rabe, saj tehnologija RFID prinaša obilo novosti, ki bodo potrebovale pravno zaščito.

7.1.5 Zakon o varstvu okolja

Ta zakon ureja varstvo okolja pred obremenjevanjem kot temeljni pogoj za trajnostni razvoj in v tem okviru določa temeljna načela varstva okolja, ukrepe varstva okolja, spremljanje stanja okolja in informacije o okolju, ekonomske in finančne instrumente varstva okolja, javne službe varstva okolja in druga z varstvom okolja povezana vprašanja. [109]

Zakonska podlaga za varovanje okolja je nujna, saj vemo da lahko nove tehnologije kot je RFID, povzročijo nezaželene učinke v okolju [105]. Dejstvo je, da je varovanje okolja prioritetno.

7.1.6 Zakon o varstvu pred ionizirajočimi sevanji in jedrski varnosti

(1) Ta zakon ureja varstvo pred ionizirajočimi sevanji z namenom, da se zmanjša škoda za zdravje ljudi in radioaktivna kontaminacija življenjskega okolja zaradi ionizirajočih sevanj zaradi uporabe virov ionizirajočih sevanj (v nadaljnjem besedilu: vir sevanja) do najmanjše možne mere, in se hkrati omogoči razvoj, proizvodnja in uporaba virov sevanj in izvajanje sevalnih dejavnosti. Za vir sevanja, ki je namenjen pridobivanju jedrske energije, zakon ureja izvajanje ukrepov jedrske varnosti in, če gre za uporabo jedrskega blaga, tudi posebnih ukrepov varovanja.

(2) Ta zakon določa tudi organizacijo po tem zakonu pristojnih upravnih organov in inšpektorjev ministrstva, pristojnega za zdravje, in ministrstva, pristojnega za okolje. [110]

Tehnologija RFID temelji na uporabi elektromagnetnih tokov in radiofrekvenčnega sevanja, zato je pomembno, da se zakonsko zavaruje vse uporabnike teh tehnologij, pred nezaželenimi učinki.

7.2 Potencialni učinki na zakonodajo

Pri predstavitvi morebitnih vplivov na zakonodajo se bomo naslonili na končno poročilo CE-RFID iniciative, ki vsebuje analize in priporočila pri uvajanju tehnologije RFID.

Glavna skrb pri sistemih RFID je predvsem varstvo podatkov. Na tem mestu je potrebno poudariti, da mora slediti Direktivi o zaščiti posameznikov pri obdelavi osebnih podatkov [111]. Obstoječa zakonodaja pokriva varstvo podatkov po principu nevtralnosti tehnologije in strinjanja posameznikov. V tem smislu je torej zakonodaja dovolj fleksibilna, da lahko sledi razvoju tehnologije RFID. Strokovnjaki, ki so sestavili to poročilo še pravijo, da bi zakon nov zakon, ki bi obravnaval samo tehnologijo RFID, napravil več škode kot koristi in bi tako onemogočil nadaljnji razvoj te tehnologije. Naslednja stvar, ki bi jo bilo treba vzeta pod drobnogled je zakonodaja glede varstva okolja. Direktivi WEEE [112] in ROHS [113] predpisujeta ravnanje z odpadno električno in elektronsko opremo. Stvar je v tem, da tehnologija RFID kot taka ne pade v kategorijo električnih in elektronskih naprav, pač pa tehnologija, ki je z njo povezana. Na tem mestu bi lahko pričakovali kakšne spremembe prej omenjenih direktiv in v tem smislu tudi dopolnila v nacionalni zakonodaji. Nenazadnje moramo pogledati na področje varovanja zdravja. Tukaj gre predvsem za spremljanje rabe tehnologije in njenih vplivov na človeka. Tako, da lahko na tem področju še pride do sprememb, saj je razvoj tehnologije zelo nepredvidljiv [105].

Zgoraj omenjeni učinki na zakonodajo so samo potencialni in mogoče celo do neke mere pristranski glede na izvajalce tega poročila. Kljub vsemu pa je iniciativo podprla tudi EU.

7.3 Ukrepi povezani s tehnologijo RFID v Evropski uniji

Evropska unija skuša na različne načine pristopiti k reševanju tematike RFID tehnologije [55] [56] [57]. Pri vprašanjih z varnostjo podatkov Evropski komisiji pomagajo različni strokovnjaki, ki z različnimi študijami pomagajo pri oblikovanju novih ukrepov. EU tudi stalno spodbuja debato med interesnimi skupinami, ki jih ta tehnologija zadeva. Ne nazadnje pa skuša čim bolje sodelovati z Azijo in ZDA, da bi lahko na podlagi njihovih izkušenj čim bolj uspešno pristopili k rešitvi problema. Evropska unija je k reševanju problema pristopila nekoliko kasneje kot recimo ZDA, saj je bilo šele v letu 2006 prvič sproženo vprašanje tehnologije RFID. V letu 2006 je sledilo veliko delavnic na katerih so skušali doseči konsenz glede glavnih točk pri implementaciji tehnologije. Na podlagi teh delavnic so sledila različna posvetovanja. Nato pa je v oktobru 2006 sledila javna konferenca o tehnologiji RFID. Do sedaj se je zgodilo veliko podobnih dogodkov (konference, seminarji, poročila, delavnice).

V glavnem obstajata dve evropski direktivi, ki sicer ne obravnavata tehnologije RFID neposredno vendar imata nanjo vplivata. To sta Data protection Directive [111] in ePrivacy Directive [114]. V splošnem obe direktivi obravnavata varstvo osebnih podatkov. Rečemo lahko, da se v na nivoju Evropske unije stvari sicer premikajo, vendar je vse še precej v zametkih in na nivoju dogovorov[58].

Evropska komisija se zaveda vprašanj varnosti in zasebnosti v zvezi s tehnologijo RFID in internetom stvari. V priporočilu (12. maj 2009) o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah, podprtih s tehnologijo RIFD [100], je Evropska komisija pozvala države članice, naj zagotovijo smernice za načrtovanje in delovanje aplikacij RFID na zakonit, etičen ter družbeno in politično sprejemljiv način, ob spoštovanju pravice do zasebnosti in zagotavljanju varstva osebnih podatkov. Priporočilo navaja ukrepe, ki jih je treba sprejeti za uvedbo uporabe RFID, z namenom zagotoviti, da se nacionalna zakonodaja uskladi z direktivami EU o varstvu podatkov (95/46, 99/5 in 2002/58). Države članice morajo zagotoviti, da industrija v sodelovanju z ustreznimi zainteresiranimi stranmi civilne družbe razvije okvir za ocenjevanje vpliva na varstvo zasebnosti in varstvo podatkov

[55] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/740&format=HTML&aged=1&language=SL&guiLanguage=en

[56] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/952&format=HTML&aged=1&language=SL&guiLanguage=en

[57] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462&format=HTML&aged=1&language=SL&guiLanguage=en

[58] http://ec.europa.eu/information_society

(PIA). Industrija in interesne skupine civilne družbe so v procesu vzpostavljanja zahtevanega okvira PIA do konca leta 2009. Cilji PIA so namenjeni ugotavljanju posledic uporabe aplikacij na varstvo zasebnosti in varstvo podatkov; da se ugotovi, ali je upravljavec sprejel ustrezne tehnične in organizacijske ukrepe za zagotovitev ustrezne zaščite in dokumentiranje ukrepov, izvedenih v zvezi z ustrezno zaščito, in služi kot podlaga za PIA poročilo, ki se lahko predloži pristojnim organom pred uvedbo aplikacije. Verjetno bi moral okvir služiti za določitev skupne strukture in vsebine poročil. Zlasti opis uporabe aplikacij RFID in področja; pomembne so predvsem tiste aplikacije, ki urejajo ravnanja, odgovornosti, analiziranje in reševanje. Poleg tega so nosilci dejavnosti zadolženi za izvajanje presoje posledic uporabe na varstvo osebnih podatkov in zasebnosti ter sprejemanje ustreznih tehničnih in organizacijskih ukrepov za zagotovitev varstva osebnih podatkov in zasebnosti, in osebo, ki je imenovana za pregled ocen ter ustreznosti tehničnih in organizacijskih ukrepov. Poleg tega so države članice pozvane, naj podprejo Evropsko komisijo pri opredeljevanju tistih aplikacij, ki bi lahko ogrožale varnost informacij in imele posledice za širšo javnost. Dodatne določbe zadevajo priporočila informacij in preglednost uporabe tehnologije RFID, natančneje aplikacij RFID, ki se uporabljajo v trgovini na drobno, ukrepe ozaveščanja, raziskave in razvoj kot tudi nadaljnje ukrepe [96].

V svojem posebnem sporočilu Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o internetu stvari (Akcijski načrt za Evropo) [77], je Evropska komisija ponovno opozorila na pomen varnosti in zasebnosti na področju interneta stvari. Zlasti ukrepi št. 2 vključujejo stalno spremljanje vprašanj zasebnosti in varstva osebnih podatkov; kot tudi del ukrepov št. 3 Evropska komisija načrtuje začetek razprave o tehničnih in pravnih vidikih *molčečih čipov* ter izražajo idejo, da se posamezniki lahko odklopijo iz svojega omrežnega okolja v vsakem trenutku [96].

7.4 Ukrepi povezani s tehnologijo RFID v ZDA

V Združenih državah Amerike je zakonodaja odvisna od posamezne zvezne države. Do leta 2010 je 14 zveznih držav vpeljalo zakonske ukrepe v zvezi s tehnologijo RFID. Največ ukrepov sta uvedli zvezni državi Washington in Kalifornija. V grobem se ukrepi delijo na pet kategorij: prepoved potrebe po implantaciji čipov RFID, prepoved neavtoriziranega branja, uporaba sistemov RFID v vozniških dovoljenjih, komisija za preučevanje tehnologije RFID in nazadnje kategorija drugo. Kot primer iz kategorije drugo navajamo ukrep iz Kalifornije, ki se nanaša na branje na daljavo osebne izkaznice posameznika brez njegovega vedenja in dovoljenja. V ZDA so se začeli s to problematiko ukvarjati že leta 2004 [115].

7.5 Akcijska vodila in smernice

Obravnava zakonodajnih vidikov interneta stvari razkriva, da nekatere vidike interneta stvari slovenska zakonodaja že pokriva. Pri dodajanju novih elementov pa strokovnjaki opozarjajo na previdnost. Predlagamo, da se:

- sprejmejo morebitni manjkajoči akti, ki zagotavljajo varovanje zasebnosti uporabnikov v internetu stvari, pri čemer velja biti izredno previden in ne sprejemati preveč na tehnologijo vezane zakonodaje;
- sledi normativnim dejavnostim na ravni Evropske unije na področju interneta stvari;
- osvešča javnost o pravicah in načinih varovanja zasebnosti.

8 Zaključna razprava

V tem poročilu smo prikazali tehnologije, ki sestavljajo internet stvari. V nadaljevanju smo predstavili veliko scenarijev uporabe na različnih področjih; od infrastrukture, gospodarstva in okolja. Predstavili smo (potencialne) vplive na družbo ter osvetlili zakonodajne vidike. Vse to skozi prizmo zagotavljanja varnosti ter varovanja zasebnosti posameznika v internetu stvari.

8.1 Scenariji razvoja interneta stvari

Nekatere tehnologije in scenariji uporabe so že realizirani in se uporabljajo, nekateri še bodo, nekateri mogoče nikoli. Razlogi za zavračanje scenarijev uporabe (in posledično interneta stvari) so različni; scenarij je lahko tehnično neizvedljiv, lahko je tehnično izvedljiv, a ni stroškovno upravičen, lahko pa ga družba zavrne kot neprimernega ali neželenega. Zato bomo v tem razdelku skušali podati smernice, vzdolž katerih se lahko internet stvari v prihodnosti razvije. Takšno napovedovanje je seveda nehvaležno, saj na nek način spominja na vedeževanje. Uporabili bomo prognozo, ki jo je izdelal Nacionalni obveščevalni svet ZDA (angl. United States National Intelligence Council, NIC) [2], in velja za obdobje med letoma 2008 in 2025.

Pri določanju smernic razvoja interneta stvari sta ključnega pomena naslednji spremenljivki:

- hitrost razvoja dogodkov (počasi ali hitro);
- prodornost tehnologije (nišno ali vseprisotno).

Klasični internet in mobilna telefonija sta primera izjemno hitrega razvoja dogodkov. Podobna zgodba je možna tudi za internet stvari, a le če bodo za to ustrezni pogoji: naklonjena politika, zadosten tehnološki napredek in ustrezno sodelovanje gospodarskih akterjev. V nasprotnem primeru se bodo stvari odvijale počasneje.

In podobno kot sta klasični internet in mobilna telefonija prodrla v praktično vse pore družbe razvitih držav, lahko internet stvari postane naslednja od vseprisotnih tehnologij. Vendar zopet le v primeru, da naleti na javnost, ki ga sprejema z navdušenjem in izvaja zadostno povpraševanje po

tehnologijah interneta stvari. Če pa, nasprotno, javnost dojema, da stroški, pomanjkljivosti in tveganja interneta stvari nadvladajo koristi, bo internet stvari ostal omejen na nišno uporabo v industriji, trgovini in državnih ustanovah.

Če omenjeni spremenljivki obravnavamo binomsko (hitrost razvoja dogodkov je bodisi *hitra* bodisi *počasna*, prodornost tehnologije pa bodisi *nišna* bodisi *vseprisotna*), lahko izpeljemo štiri različne scenarije razvoja interneta stvari do leta 2025 [2]. Ti scenariji so *hitro izgorevanje* (angl. fast burn), *povezane niše* (angl. connected niches), *počasi, a gotovo* (angl. slowly but surely) in *ambientalna interakcija* (angl. ambiental interaction).

Tabela 4. Scenariji razvoja interneta stvari v prihodnosti

		Prodornost tehnologije	
		Nišno	Vseprisotno
Hitrost razvoja dogodkov	Hitro	Hitro izgorevanje	Ambientalna interakcija
	Počasi	Povezane niše	Počasi, a gotovo

Naj bo hitro in vseprisotno ali počasno in nišno, razvoj internet stvari bo izbral določeno smernico in imel definitivne vplive na družbo. V nadaljevanju bomo podrobneje predstavili obe ekstremni smernici, tj. ambientalno interakcijo in povezane niše, ter na kratko obdelali tudi vmesni različici.

8.1.1 Hitro izgorevanje

V scenariju *hitro izgorevanje* (angl. fast burn) se internet stvari razvija pospešeno, a v omejenem obsegu in tako ne zadrži začetnega zagona. Čeprav ima konkreten vpliv na določenih področjih (industrijska avtomatika, zdravstvo, varnostne storitve), internet stvari ne postane vseprisoten. Posledično ima manjši vpliv na vsakodnevno življenje, poslovanje v splošnem in vladanje. Tehnologija vseprisotnega pozicioniranja (angl. ubiquitous positioning technology) ni razvita, saj ob primanjkljaju drugih storitev interneta stvari predstavlja preveliko tveganje za teroristične napade in ostale grožnje. V tem scenariju tehnologije interneta stvari izkazujejo podobna tveganja in koristi kot tista, opisana v scenariju povezanih niš.

8.1.2 Počasi, a gotovo

V scenariju *počasi, a gotovo* (angl. slowly but surely) internet stvari postane vseprisoten, a ne pred letom 2035[59]. Končni rezultati so primerljivi s tistimi iz scenarija *ambientalna interakcija*, vendar obstajajo tudi pomembne razlike. Relativno počasen razvoj dogodkov omogoči gospodarstvu in državam, da se na internet stvari dobro pripravijo in ublažijo ključna tveganja. Nekatera tveganja seveda ostanejo, a tudi že sama tehnologija bo v prihodnosti manj dovzetna za napade. Določena tveganja iz scenarija *ambientalna interakcija* ostajajo, obenem pa koristi iz omenjenega scenarija niso tako dramatične.

8.1.3 Povezane niše

V scenariju *povezane niše* (angl. connected niches) se internet stvari razvije okoli aplikacijskih rešitev, ki obetajo hitro povračilo investicij in ki so realizirane kljub prevladujočemu odporu in malodušnosti nad tehnologijo. Povpraševanje po njej je primerljivo s tehnologijami, ki evolucijsko, ne pa revolucionarno, nižajo stroške in splošen vtis je, da gre le še za eno izmed tehnologij, ki ima še veliko nerešenih vprašanj. Industrija je zadržana, politika pa v najboljšem primeru internet stvari benigno zanemarja in ne vidi vseh potencialnih koristi. V najslabšem primeru pa ga diskriminira na račun starejših in ustaljenih tehnologij. V letu 2025 je tehnologija pozicioniranja še vedno omejena na uporabo v zunanjih prostorih in večina predmetov ni opremljena z značkami RFID. Kljub temu poznamo povezane predmete in senzorska omrežja v varovanju, logistiki, zdravstvu, dokumentnih sistemih, upravljanju z inventarjem, flotami (avtov, tovornjakov, ladij, itd.), industrijski avtomatiki in robotiki. Povezane naprave so pogoste na delovnem okolju in v vojaških operacijah, ne pa tudi v gospodinjstvih. Podobno najdemo senzorična omrežja večinoma le v delovnih okoljih in na javnih površinah. Povezani predmeti in senzorska omrežja imajo dodano vrednost v ekonomiji in v vojaških organizacijah, a hkrati prinašajo tveganja. S časom, ko se niše širijo, lahko pride do združevanja, ki ima nepredvidljive učinke – lahko so sinergijski, lahko pa kontraproduktivni.

Potencialne priložnosti. Kratkotrajne ekonomske prednosti izhajajo predvsem iz uporabe tehnologij interneta stvari na področju logistike in industrijske avtomatike. Tu se kaže učinek interneta stvari predvsem kot način nižanja stroškov. Letališča in druga žarišča javnega prevoza postanejo prizorišča velikih senzoričnih omrežji za namene varovanja. Ta tehnolo-

[59] Ta in druge letnice v tem razdelku so podane kot (grobe) ocene, ki jih seveda moramo jemati s pridržkom.

gija pomaga pri iskanju sumljivih posameznikov vendar ni avtonomna in še vedno potrebuje pomoč ljudi in tako ne zmanjšuje števila potrebnih nadzornikov in analitikov. Podobno internet stvari zavrača kraje in pomaga pri iskanju izgubljenih predmetov, a le v posebnih, za to prirejenih prostorih, ki so relativno redki. Bolnišnice in podobni domovi stalne oskrbe postanejo visokotehnološki pristani z izboljšano kvaliteto oskrbe. Niši upravljanja s flotami in dokumentnimi sistemi sta primera, kjer so prednosti interneta stvari najbolj očitne v primerjavi s tradicionalnimi pristopi. Serviserji in ostali ponudniki vozil koristijo storitve oddaljenega diagnosticiranja pokvarjenih vozil, ki jim omogočajo, da opravljajo vzdrževalna dela po potrebi, kar omogoča precejšnje prihranke in hkratno povečanje zanesljivosti. S padanjem cen (bo predvidoma do leta 2020) večina papirnatih dokumentov in publikacij kot tudi njihovih elektronskih ekvivalentov (e-knjige, pametne kartice in druge naprave) vsebovala značke RFID, kar bo omogočalo avtomatizacijo mnogih, danes dolgotrajnih in utrujajočih, procesov.

Potencialna tveganja. Ekonomske prednosti interneta stvari v posameznih državah se deloma zmanjšajo na račun asimetričnega trgovanja, saj je večina (pametnih) predmetov proizvedenih v državah daljnega vzhoda. Geolokacijske sposobnosti začetnih rešitev so relativno slabe. Na področju fizičnega varovanja pogosto prihaja do napačnih ugotovitev (bodisi napak prve vrste ali napak druge vrste). Smo v situaciji, kjer je z vidika stroškov tehnologija komajda upravičljiva. Podobna je situacija v zdravstvu, kjer internet stvari v splošnem deluje blagodejno, vendar nekatere bolnišnice in domovi stalne oskrbe zmanjšujejo stroške na način, kjer zamenjujejo nego za nadzor. Internet stvari je definitivno koristen na področju servisiranja vozil in dokumentnih sistemov, vendar tudi tu prihaja do resnih varnostnih tveganj.

8.1.4 Ambientalna interakcija

V scenariju *ambientalna interakcija* (angl. ambient interaction) tehnološki napredek, pogosta uporaba v gospodarstvu in naklonjena politika omogočijo, da se internet stvari razvije hitro in postane vseprisoten. Velik del gospodarstva izraža veliko povpraševanje po tehnologijah interneta stvari, saj inovativne rešitve motivirajo ljudi, da uporabljajo aplikacije, ki zmanjšujejo naporna in utrujajoča dela in brišejo meje med delom, zabavo in trgovanjem. Povezani vsakodnevni predmeti in senzorska omrežja so pogosti tako na delovnih mestih, javnih površinah kot v gospodinjstvih. V letu 2017 so brezblagajniške trgovine standard v maloprodaji in nekatere države že imajo razvito tehnologijo vseprisotnega pozicioniranja tako na prostem kot v zaprtih prostorih. Kljub temu pa takšen razvoj dogodkov spremljajo neredka

tveganja. Tako kot je klasični internet povečal nevarnosti kibervojskovanja, neželene pošte, kraje identitete in napadov z zavrnitvijo storitve, bo internet stvari postal tarča za zlonamerno programsko opremo, ki vsakodnevne naprave bodisi onemogoči ali jih spremeni v sredstva za vohunjenje in sledenje. Senzorska omrežja lahko postanejo medij za nepooblaščen nadzor s strani napadalcev.

Potencialne koristi. Z uporabo označevanja posameznih izdelkov z značkami RFID in lokacijskimi storitvami, ki delujejo tudi v zaprtih prostorih, je mogoče doseči dolgotrajne pozitivne gospodarske učinke, ki se kažejo zlasti na področju logistike. Hkrati se zaradi pritrjenih naprav poveča tudi vrednost predmetom samim. Potencial interneta stvari ni zgolj v tem, da okrepi logistične procese, temveč, da jih revolucionarno spremeni. V letu 2025 so lahko oskrbovalne verige v veliki meri robotizirane, kar povečuje varnosti in zanesljivost, saj so taki sistemi manj dovzetni za vmešavanje ljudi kot obstoječi. V pristaniščih poteka razlaganje z ladij in nalaganje na tovornjake samodejno, saj zabojniki sami sporočajo njihovo vsebino in cilje dostave. Podobna avtomatizacija je izvedena na mestih razpečave, kjer na podoben način palete komunicirajo z viličarji, tako da neredki predmeti pridejo na police trgovin, ne da bi se jih ljudje sploh dotaknili. Pametni telefoni so opremljeni s čitalniki RFID, preko katerih lahko potrošniki v trgovinah preverjajo stanje hrane in drugih izdelkov. S pametim kombiniranjem podajanja nasvetov in marketinškimi prijemi je mogoče združiti ideji zabave in oglaševanja (angl. advertainment). Tako lahko pametni telefoni postanejo zasloni za večjezična navodila za uporabo izdelkov, navodila za recikliranje in podobno. Ljudje z navdušenjem sprejemajo idejo vseprisotnega pozicioniranja, s čimer se drastično zmanjša število založenih, izgubljenih ter ukradenih predmetov.

Potencialna tveganja. Tveganja, opisana v scenariju povezanih niš, se v tem primeru povečajo za nekaj velikostnih stopenj. Ko se države in gospodarski subjekti zanašajo na tehnologije interneta stvari, se motnje pri dobavi tehnologije manifestirajo v motenem delovanju držav in gospodarskih subjektov. Podjetja iz azijskih držav so praktično edini proizvajalec omenjenih tehnologij ter tako predstavljajo kritično točko odpovedi interneta stvari. Napadalci lahko izkoristijo senzorska omrežja, ki imajo varnostne mehanizme, ki jih je mogoče napasti s prenosnimi računalniki, ki so v letu 2025 precej bolj zmogljivi kot računske naprave v teh omrežjih. Podobno podcenjevanje in nerazumevanje varnostnih vprašanj, ki so v klasičnem internetu pripeljale do virusov, ki se širijo z uporabo elektronske pošte, in računalnikov, ki jih oddaljeno nadzorujejo nepridipravi, lahko v internetu

stvari omogoči kiberkriminalcem, da izrabijo povezane vsakodnevne predmete za raznovrstne napade.

8.1.5 Kazalniki razvoja interneta stvari

Navajanje več različnih scenarijev je posledica negotovosti, ki jo prinaša prihodnost. Ugotavljanje, kateri izmed scenarijev najbolje odraža realno sliko v nekem trenutku, je odvisno predvsem od ocen dejanskega stanja, našega poznavanja problematike ter spremljanja različnih kazalnikov, ki nakazujejo smer in korak razvoja interneta stvari. Nekatere ključne spremenljivke, ki, v kolikor zavzamejo pozitivne vrednosti, nakazujejo internetu stvari naklonjena okolja, so:

- Velikost in namen povpraševanja po pospešeni logistiki v trgovanju in v vojaških organizacijah.
- Učinkovitost začetnih poskusov z internetom stvari kot načinom zmanjševanja stroškov, s čimer se ustvarjajo pogoji za razširjenost v vertikalna aplikacijska področja vštevši uporabo v policiji, zdravstvu, dokumentnih sistemih in v vladnih ustanovah.
- Zmožnost naprav, da sprejemajo geolokacijske signale v zaprtih prostorih (po možnosti z uporabo obstoječe infrastrukture).
- Tehnološki napredek na področji miniaturizacije naprav, energijsko učinkovite elektronike (mikroračunalniki z nizko porabo energije in učinkovitimi komunikacijskimi mehanizmi, učinkovitimi transformatorji za zajemanje energije (angl. energy-harvesting transducers), ter izboljšanimi baterijami).
- Napredki v razvoju programske opreme, ki delujejo v imenu uporabnikov in ki znajo učinkovito uporabiti senzorične informacije iz več različnih virov.

Literatura

[1] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 2010.

[2] National Intelligence Council. Disruptive civil technologies – six technologies with potential impacts on us interests out to 2025. Conference Report CR 2008-07, 2008. Pridobljeno 28. 7. 2011 iz `http://www.dni.gov/nic/confreports_disruptive_tech.html`.

[3] European Commission Information Society and Media. Internet of things in 2020, roadmap for the future. INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems in co-operation with the Working group RFID on the ETP EPoSS, 2008. Pridobljeno 18. 8. 2011 iz `http://www.smart-systems-integration.org/public/internet-of-things`.

[4] EPCglobal. The epcglobal architecture framework, epcglobal final version 1.4, 2010. Pridobljeno 8. 8. 2011 iz `http://www.epcglobalinc.org`.

[5] Mirko Presser and Alexander Gluhak. The internet of things connecting the real world with the digital world. *EURESCOM mess@ge – The Magazine for Telecom Insiders*, 2009.

[6] Bruce Sterling. *Shaping things – Mediawork Pamphlets*. The MIT Press, 2005.

[7] International Telecommunications Union. *ITU Internet Reports, The internet of things*. International Telecommunication Union (ITU), Geneva, 2005.

[8] CASAGRAS. Rfid and the inclusive model for the internet of things. CASAGRAS an EU Framework 7 Project, Final report, 2007. Pridobljeno 21. 8. 2011 iz `http://www.rfidglobal.eu`.

[9] IEEE. *IEEE Std 802.15.4-2006: Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*. IEEE, 2006.

[10] Jonathan Hui, David Culler, and Samita Chakrabarti. 6lowpan: Incorporating ieee 802.15.4 into the ip architecture. White paper #3, Internet Protocol for Smart Objects (IPSO) Alliance, 2009.

[11] Neil Gershenfeld, Raffi Krikorian, and Danny Cohen. The internet of things. *Scientific American*, 2004.

[12] Artem Katasonov, Olena Kaykova, Oleksiy Khriyenko, Sergiy Nikitin, and Vagan Y. Terziyan. Smart semantic middleware for the internet of things. In *Proceedings of the Fifth International Conference on Informatics in Control, Automation and Robotics, Intelligent Control Systems and Optimization*, 2008.

[13] Ioan Toma and Elena Simperl. A joint roadmap for semantic technologies and the internet of things. In *Proceedings of the Third STI*, 2009.

[14] Lara Srivastava. Pervasive, ambient, ubiquitous: the magic of radio. In *European Commission Conference 'From RFID to the Internet of Things'*, 2006.

[15] Banks, David Hanny, Manuel A. Pachano, and Les G. Thompson. *RFID applied.* John Wiley & Sons, Inc, 2007.

[16] Ian F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 2002.

[17] Daniel Giusto, Antonio Iera, Giacomo Morabito, Luigi Atzori, Gaetano Marrocco, Cecilia Occhiuzzi, and Francesco Amato. Sensor-oriented passive rfid. In *The Internet of Things*, 2010.

[18] Michael Buettner, Ben Greenstein, Alanson Sample, and Joshua R. Smith. Revisiting smart dust with rfid sensor networks. In *Proceedings of the 7th ACM Workshop on Hot Topics in Networks (HotNets-VII)*, 2008.

[19] Innovision. Near field communication in the real world, turning the nfc promise into profitable, everyday applications. White paper, Innovision Research & Technology plc, 2001. Pridobljeno 2. 9. 2011 iz `http://www.nfc-forum.org/resources/white_papers/Innovision_whitePaper1.pdf`.

[20] Scott de Deugd, Randy Carroll, Kevin E. Kelly, Bill Millett, and Jeffrey Ricker. Soda: Service oriented device architecture. *Pervasive Computing, IEEE*, 2006.

[21] Patrik Spiess, Stamatis Karnouskos, Dominique Guinard, Domnic Savio, Oliver Baecker, Luciana Moreira Sa de Souza, and Vlad Trifa. Soa-based integration of the internet of things in enterprise services. In *Web Services, 2009. ICWS 2009. IEEE International Conference on*, pages 968–975, 2009.

[22] Markus Eisenhauer, Peter Rosengren, and Pablo Antolin. A development platform for integrating wireless devices and sensors into ambient intelligence systems. In *Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009. SECON Workshops '09. 6th Annual IEEE Communications Society Conference on*, 2009.

[23] Simon Duquennoy, Gilles Grimaud, and Jean-Jacques Vandewalle. The web of things: Interconnecting devices with high usability and performance. In *Embedded Software and Systems, 2009. ICESS '09. International Conference on*, 2009.

[24] Christian Buckl, Stephan Sommer, Andreas Scholz, Alois Knoll, Alfons Kemper, Jorg Heuer, and Anton Schmitt. Services to the field: An approach for resource constrained sensor/actor networks. In *Proceedings of the 2009 International Conference on Advanced Information Networking and Applications Workshops*, 2009.

[25] Christian Floerkemeier, Christof Roduner, and Matthias Lampe. Rfid application development with the accada middleware platform. *IEEE Systems Journal*, 2007.

[26] Evan Welbourne, Leilani Battle, Garret Cole, Kayla Gould, Kyle Rector, Samuel Raymer, Magdalena Balazinska, and Gaetano Borriello. Building the internet of things using rfid: The rfid ecosystem experience. *IEEE Internet Computing*, 2009.

[27] Yi-Wei Ma, Chin-Feng Lai, Yueh-Min Huang, and Jiann-Liang Chen. Mobile rfid with ipv6 for phone services. In *Consumer Electronics, 2009. ISCE '09. IEEE 13th International Symposium on*, 2009.

[28] Dong Geun Yoon, Dong Hyeon Lee, Chang Ho Seo, and Seong Gon Choi. Rfid networking mechanism using address management agent. In *International Conference on Networked Computing and Advanced Information Management*, 2008.

[29] Ian F. Akyildiz, Jiang Xie, and Shantidev Mohanty. A survey of mobility management in next-generation all-ip-based wireless systems. *IEEE Wireless Communications*, 2004.

[30] Charles E. Perkins. Mobility support in ipv6. RFC 6275 (Proposed Standard), 2011. `http://www.ietf.org/rfc/rfc6275.txt`.

[31] Vladimir Krylov, Dmitry V. Ponomarev, and Dmitry Ponomarev. Epc object code mapping service software architecture: web approach. In *MERA Networks Publications*, 2009.

[32] T. V. Lakshman and Upamanyu Madhow. The performance of tcp/ip for networks with high bandwidth-delay products and random loss. *IEEE/ACM Trans. Netw.*, 1997.

[33] Demirkol Demirkol, Fatih Alagoz, Hakan Delic, and Cem Ersoy. Wireless sensor networks for intrusion detection: packet traffic modeling. *IEEE Communications Letters*, 2006.

[34] Dazhi Chen and Pramod K. Varshney. QoS Support in Wireless Sensor Networks: A Survey. In *Proceedings of the 2004 International Conference on Wireless Networks (ICWN 2004), Las Vegas, Nevada, USA*, 2004.

[35] August Nilssen. Security and privacy standardisation in internet of things. In *eMatch '09 — Future InternetWorkshop*, 2009.

[36] Zach Shelby. Etsi m2m standardization, 2009. Pridobljeno 13. 9. 2011 iz `http://zachshelby.org/2009/03/16/etsi-m2m-standardization`.

[37] K. Pister, P. Thubert, S. Dwars, and T. Phinney. Industrial routing requirements in low-power and lossy networks. RFC 5673 (Informational), 2011. `http://www.ietf.org/rfc/rfc5673.txt`.

[38] Gerald Santucci. Internet of the future and internet of things: What is at stake and how are we getting prepared for them? In *eMatch '09 — Future InternetWorkshop*, 2009.

[39] ISO. *ISO/IEC 27005:2008: Informacijska tehnologija – Varnostne tehnike – Obvladovanje tveganja pri varovanju informacij*. International Organization for Standardization, Ženeva, Švica, 2008.

[40] Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02, pages 41–47, New York, NY, USA, 2002. ACM.

[41] Ari Juels. Rfid security and privacy: a research survey. *IEEE Journal on Selected Areas in Communications*, 2006.

[42] Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips. Guidelines for securing radio frequency identification (rfid) systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication, 2007.

[43] Ram Kumar, Eddie Kohler, and Mani Srivastava. Harbor: software-based memory protection for sensor nodes. In *Proceedings of the 6th international conference on Information processing in sensor networks*, 2007.

[44] H. Krawczyk, M. Bellare, and R. Canetti. Hmac: Keyed-hashing for message authentication. RFC 2104 (Informational), 1997. `http://www.ietf.org/rfc/rfc2104.txt`.

[45] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong authentication for rfid systems using the aes algorithm. In *Cryptographic Hardware and Embedded Systems - CHES 2004*, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2004.

[46] Benoît Calmels, Sébastien Canard, Marc Girault, and Hervé Sibert. Low-cost cryptography for privacy in rfid systems. In *Smart Card Research and Advanced Applications*, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2006.

[47] Denis Trček and Pekka Jäppinen. Rfid security. In Yan Zhang, Laurence T. Yang, and Jiming Chen, editors, *RFID and Sensor Networks: Architectures, Protocols, Security, and Integrations*. CRC Press, 2009.

[48] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., 2001.

[49] Jehan Wickramasuriya, Mahesh Datt, Sharad Mehrotra, and Nalini Venkatasubramanian. Privacy protecting data collection in media spaces. In *Proceedings of the 12th annual ACM international conference on Multimedia*, 2004.

[50] Haowen Chan and Adrian Perrig. Security and privacy in sensor networks. *Computer*, 2003.

[51] Daniel Giusto, Antonio Iera, Giacomo Morabito, Luigi Atzori, Olivier Savry, and François Vacherand. Security and privacy protection of contactless devices. In *The Internet of Things*. Springer New York, 2010.

[52] Georgios V. Lioudakis, Eleftherios A. Koutsoloukas, Nikolaos Dellas andSofia Kapellaki, George N. Prezerakos, Dimitra I. Kaklamani, and Iakovos S. Venieris. A proxy for privacy: the discreet box. In *EUROCON, 2007. The International Conference on Computer as a Tool*, 2007.

[53] Viktor Mayer-Schönberger. *Delete: The virtue of forgetting in the digital age*. Princeton University Press, 2009.

[54] David Jelenc and Denis Trček. Internet stvari: priložnosti in problemi zasebnosti. In *Zbornik devetnajste mednarodne Elektrotehniške in računalniške konference ERK 2010*, 2010.

[55] Aikaterini Mitrokotsa, Melanie R. Rieback, and Andrew S. Tanenbaum. Classification of rfid attacks. In *Proceedings of the 2nd International Workshop on RFID Technology – Concepts, Applications, Challenges, IWRT 2008*, 2008.

[56] Wassim Znaidi, Marine Minier, and Jean-Philippe Babau. An ontology for attacks in wireless sensor networks. Technical report, Unité de recherche INRIA Rhône-Alpes, 2008.

[57] Iztok Starc. Zagotavljanje varnosti za okolja omrežnih sistemov radiofrekvenčne identifikacije. Magistrsko delo. Fakulteta za računalništvo in informatiko, Univerza v Ljubljani, 2011.

[58] Online Compact Oxford English Dictionary. Infrastructure, 2011. Pridobljeno 29. 9. 2011 iz http://oxforddictionaries.com/definition/infrastructure.

[59] Jeffrey Fulmer. What in the world is infrastructure? *PEI Infrastructure Investor*, 2009. Pridobljeno 29. 9. 2011 iz http://www.tortoiseadvisors.com/documents/Infrastructure_Investor.pdf.

[60] Joint Chiefs of Staff, The Pentagon, and Washington DC. Department of defense dictionary of military and associated terms, 2001. Pridobljeno 29. 9. 2011 iz http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA439918&Location=U2&doc=GetTRDoc.pdf.

[61] CIP ICT Management Committee. Competitiveness and innovation framework programme (cip), 2009. Pridobljeno 5. 2. 2011 iz http://ec.europa.eu/information_society/activities/ict_psp/documents/ict_psp_wp2010_agreed_at_committee_191109.pdf.

[62] Ljubljana, pametno mesto, 2011. Pridobljeno 5. 2. 2011 iz http://www.ljubljanapametnomesto.si.

[63] Robert A. Dolin. Deploying the internet of things. In *International Symposium on Applications and the Internet (SAINT)*, 2006.

[64] Stephan Haller, Stamatis Karnouskos, and Christoph Schroth. The internet of things in an enterprise context. In *First Future Internet Symposium – FIS*, 2008.

[65] Ovidiu Vermesan, Mark Harrison, Harald Vogt, Kostas Kalaboukas, Maurizio Tomasella, Karel Wouters, and Stephan Haller. Internet of things -– strategic research roadmap. European Commission – Information Society and Media DG, 2009.

[66] Gregor Broll, Enrico Rukzio, Massimo Paolucci, MMatthias Wagner, Albrecht Schmidt, and Heinrich Hußmann. Perci: Pervasive service interaction with the internet of things. *Internet Computing, IEEE*, 2009.

[67] Patrik Fuhrer and Dominique Guinard. Building a smart hospital using rfid technologies. In *Proceedings of the ECEH '06*, 2006.

[68] H. Daud, N. Yahya, M. Sakri, and M. Syazwan. Tagging System for New-born Babies using RFID System (BabyTraXX). In *Conference on Engineering and Technology Education*, 2010.

[69] Walter H. Dzik. Emily cooley lecture 2002: transfusion safety in the hospital. *Transfusion*, 2003.

[70] K. Sazama. Reports of 355 transfusion-associated deaths: 1976 through 1985. *Transfusion*, 1990.

[71] Atul A. Gawande, David M. Studdert, E. John Orav, Troyen A. Brennan, and Michael J. Zinner. Risk factors for retained instruments and sponges after surgery. *New England Journal of Medicine*, 2003.

[72] Steve Ranger. Rfid to cure nhs hardware thefts, 2006. Pridobljeno 24. 9. 2011 iz http://www.silicon.com/management/public-sector/2006/02/28/rfid-to-cure-nhs-hardware-thefts-39156833/.

[73] Patrick Schmitt and Florian Michahelles. Economic impact of rfid report. Technical report, ETH Zurich, European research project BRIDGE, 2008. Pridobljeno 30. 9. 2011 iz http://www.bridge-project.eu/data/File/BRIDGE_WP13_Economic_impact_RFID.pdf.

[74] Komisija evropskih skupnosti: Generalni direktorat za informacijsko družbo in medije. 2nd transatlantic symposium on the societal benefits of rfid – symposium report, 2009. Pridobljeno 27. 1. 2011 iz http://www.gs1.org/docs/epcglobal/euus_symposiumreport.pdf.

[75] Gerald Santucci. From internet of data to internet of things. In *International Conference on Future Trends of the Internet*, 2009.

[76] Paul A. Moskowitz, Andris Lauris, and Stephen S. Morris. A privacy-enhancing radio frequency identification tag: Implementation of the clipped tag. In *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on*, pages 348 –351, march 2007.

[77] Komisija evropskih skupnosti. Internet stvari -- akcijski načrt za evropo, com(2009) 278 konč. Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, 2009.

[78] Stephan Haller. The things in the internet of things. Poster at the Internet of Things Conference, Tokyo (IoT 2010), 2010.

[79] Matthias Lampe and Christian Flörkemeier. The smart box application model. In *Advances in pervasive computing*, 2004.

[80] Dadong Wan. Magic wardrobe: Situated shopping from your own bedroom. *Personal Ubiquitous Computing*, 2000.

[81] Gro Harlem Brundtland. Our common future. Report of the World Commission on Environment and Development, 1987. Pridobljeno 26. 1. 2011 iz http://www.un-documents.net/wced-ocf.htm.

[82] Helmut Hlavacs, Karin A. Hummel, Roman Weidlich, Amine M. Houyou, and Hermann de Meer. Modeling energy efficiency in distributed home environments. Technical Report MIP-0713, Department of Informatics and Mathematics, University of Passau, Germany, 2007.

[83] Friedemann Mattern, Thorsten Staake, and Markus Weiss. Ict for green: how computers can help us to conserve energy. In *Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking*, 2010.

[84] John A. Laitner and Karen Ehrhardt-Martinez. Information and communication technologies: The power of productivity (part i). *Environmental Quality Management*, 2008.

[85] Claudia R. Binder, Raffaele Quirici, Svetlana Domnitcheva, and Beat Stäubli. Smart labels for waste and resource management. *Journal of Industrial Ecology*, 2008.

[86] Harald Sundmaeker, Patrick Guillemin, Peter Friess, and Sylvie Woelfflé. Vision and challenges for realising the internet of things. Cluster of European Research Projects on the Internet of Things, European Commision – Information Society and Media DG, 2010.

[87] Thomas E. Graedel and Braden R. Allenby. *Industrial Ecology*. Prentice Hall, 2002.

[88] Steven Saar and Valerie Thomas. Toward trash that thinks: Product tags for environmental management. *Journal of Industrial Ecology*, 2002.

[89] Sarah Darby. Smart metering: what potential for householder engagement? *Building Research & Information*, 2010.

[90] Axiros Axess. Smart home, 2010. Pridobljeno 23. 9. 2011 iz `http://axiros.com/solutions/by-solution/smart-home.html`.

[91] Energetski zakon. Uradni list Republike Slovenije, 27/2007.

[92] Pravilnik o načinu delitve in obračunu stroškov za toploto v stanovanjskih in drugih stavbah z več posameznimi deli. Uradni list Republike Slovenije, 7/2010.

[93] U. Greveler, B. Justus, and D. Löhr. Hintergrund und experimentelle ergebnisse zum thema 'smart meter und datenschutz'. Technical Report ENTWURF, v0.6, Fachhochschule Münster, 2011. Pridobljeno 30. 9. 2011 iz `http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf`.

[94] Kai Daniel, Bjoern Dusza, Andreas Lewandowski, and Christian Wietfeld. Airshield: A system-of-systems muav remote sensing architecture for disaster response. In *3rd Annual IEEE Systems Conference*, 2009.

[95] Fadi Hamad, Leonid Smalov, and Anne James. Energy-aware security in m-commerce and the internet of things. *IETE Technical Review*, 2009.

[96] Rolf H. Weber. Internet of things — new security and privacy challenges. *Computer Law & Security Review*, 2010.

[97] Nicole A. Ozer. Rights 'chipped' away: Rfid and identification documents. *Stanford Technology Law Review*, 2008.

[98] Katherine Albrecht. Rfid tag – you're it. *Scientific American*, 2008.

[99] Katherine N. Hayles. Rfid: Human agency and meaning in information-intensive environments. *Theory, Culture & Society*, 2009.

[100] Komisija evropskih skupnosti. Priporočilo komisije z dne 12. maja 2009 o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah, podprtih z radiofrekvenčno identifikacijo (notificirano pod dokumentarno številko c(2009) 3200) (2009/387/es). Uradni list Evropske unije, 2009.

[101] Christian Floerkemeier, Matthias Lampe, and Thomas Schoch. The smart box concept for ubiquitous computing environments. In *Proceedings of Smart Objects Conference*, 2003.

[102] Derek Reilly, Michael Welsman-Dinelle, Colin Bate, and Kori Inkpen. Just point and click?: using handhelds to interact with paper maps. In *Proceedings of the 7th international conference on Human computer interaction with mobile devices &*

services, 2005.

[103] Coordinating european efforts for promoting the european rfid value chain, 2008. Pridobljeno 27. 1. 2011 iz http://www.rfid-in-action.eu.

[104] Zakon o varstvu osebnih podatkov. Uradni list Republike Slovenije, 86/2004.

[105] Andreas Kruse, Camino Mortera-Martinez, and Véronique Corduant. The regulatory framework for rfid. Final report Work package 5, 2008. Pridobljeno 27. 1. 2011 iz http://www.rfid-in-action.eu/public/results/legal-aspects/framework.pdf.

[106] Zakon o elektronskih komunikacijah. Uradni list Republike Slovenije, 43/2004.

[107] Zakon o telekomunikacijah. Uradni list Republike Slovenije, 30/2001.

[108] Zakon o industrijski lastnini. Uradni list Republike Slovenije, 45/2001.

[109] Zakon o varstvu okolja. Uradni list Republike Slovenije, 41/2004.

[110] Zakon o varstvu pred ionizirajočimi sevanji in jedrski varnosti. Uradni list Republike Slovenije, 67/2002.

[111] Evropski parlament and Evropski svet. Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (dpd), 95/46/ec, 1995. Pridobljeno 27. 1. 2011 iz http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[112] Evropski parlament and Evropski svet. Direktiva o odpadni električni in elektronski opremi (weee), 2002/96/es, 2002. Pridobljeno 27. 1. 2011 iz http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0096:SL:HTML.

[113] Evropski parlament and Evropski svet. Direktiva o omejevanju uporabe nekaterih nevarnih snovi v električni in elektronski opremi (rohs), 2002/95/es, 2002. Pridobljeno 27. 1. 2011 iz http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0095:SL:HTML.

[114] Evropski parlament and Evropski svet. Direktiva o zasebnosti in elektronskih komunikacijah, 2002/58/ec, 2002. Pridobljeno 27. 1. 2011 iz http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:SL:HTML.

[115] National conference of state legislatures, 2004. Pridobljeno 27. 1. 2011 iz http://www.ncsl.org/default.aspx?tabid=13442.

[116] Gerald Santucci. The governance of the internet of things, 2010. Pridobljeno 22. 6. 2011 iz http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-europe2010.pdf.

[117] David Bartlett. Want to be a smarter bussiness? listen to your 'things', 2011. Pridobljeno 22. 6. 2011 iz http://asmarterplanet.com/blog/2011/02/david-bartlett-the-pulse-of-iot.html.

[118] Internation Business Macines (IBM). Ibm helps organizations secure mobile and instrumented devices – smartphones, meters and beyond, 2011. Pridobljeno 22.

6. 2011 iz http://www-03.ibm.com/press/us/en/pressrelease/33598.wss.

[119] Ministry of Economic Affairs of the Netherlands. Ict 2020: 4 scenario stories – hidden assumptions and future challenges, 2010. Pridobljeno 22. 6. 2011 iz http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2010/05/25/ict-2020-4-scenario-stories-hidden-assumptions-and-future-challenges/281042-toekomstscenarios-web.pdf.

[120] Cisco. The internet of things – how the next evolution of the internet is changing everything, 2011. Pridobljeno 22. 6. 2011 iz http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[121] IDTechEx. Rfid forecasts, players and opportunities 2011-2021, 2010. Pridobljeno 22. 6. 2011 iz http://www.idtechex.com/research/reports/rfid_forecasts_players_and_opportunities_2011_2021_000250.asp.

[122] CE RFID. A roadmap for rfid applications and technologies, 2008. Pridobljeno 22. 6. 2011 iz http://www.rfid-in-action.eu/public/results/roadmap/a-roadmap-for-rfid-applications-and-technologies.

[123] IDTechEx. Active rfid and sensor networks 2011-2021, 2010. Pridobljeno 22. 6. 2011 iz http://www.idtechex.com/research/reports/active-rfid-and-sensor-networks-2011-2021-000255.asp.

[124] IDTechEx. Printed and chipless rfid forecasts, technologies & players 2011-2021, 2010. Pridobljeno 22. 6. 2011 iz http://www.idtechex.com/research/reports/printed-and-chipless-rfid-forecasts-technologies-and-players-2011-2021-000254.asp.

[125] IDTechEx. Apparel rfid 2011-2021, 2010. Pridobljeno 22. 6. 2011 iz http://www.idtechex.com/research/reports/apparel-rfid-2011-2021-000256.asp.

[126] Geoff Mulligan. A new revolution part 1: Ip enabled smart objects, 2008. Pridobljeno 22. 6. 2011 iz http://www.sensorsmag.com/sensors-mag/a-new-revolution-part-1-ip-enabled-smart-objects-7451.

[127] Internation Business Macines (IBM). Ibm delivers new software to advance industry transformation, 2011. Pridobljeno 22. 6. 2011 iz http://www-03.ibm.com/press/us/en/pressrelease/33836.wss.

[128] Kurt Stammberger, Monique Semp, M. B. Anand, and David Culler. Introduction to security for smart object networks. White paper #4, Internet Protocol for Smart Objects (IPSO) Alliance, 2010.

[129] Mocana. Mobile & smart device security survey 2011: Device malware takes off, 2011. Pridobljeno 22. 6. 2011 iz http://mocana.com/spring2011/mocanaspring2011dsr.pdf.

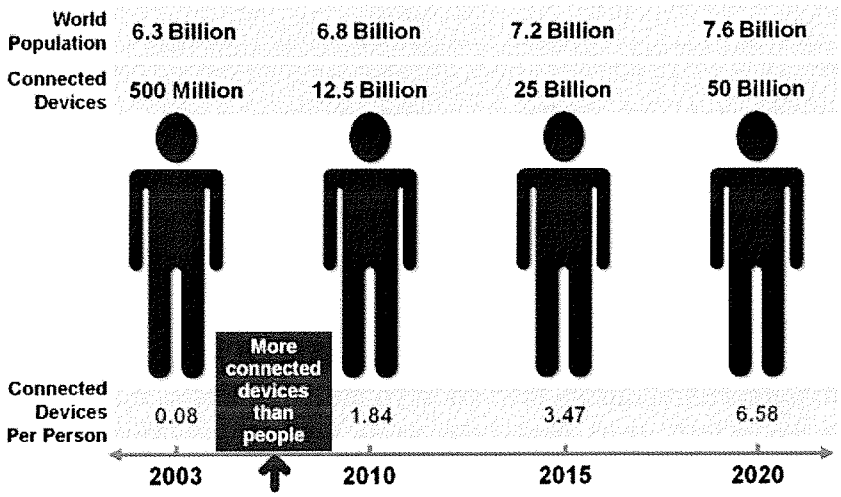
[130] IDTechEx. Nfc-enabled phones and contactless smart cards 2010-2020, 2010. Pridobljeno 22. 6. 2011 iz http://www.idtechex.com/research/reports/nfc_enabled_phones_and_contactless_smart_cards_2010_2020_000249.asp.

Dodatek A: Statistične raziskave

V letu 2010 je bilo po ocenah 1,5 milijarde osebnih računalnikov in 1 milijarda mobilnih telefonov povezanih v omrežje. Ta *internet osebnih računalnikov* bo zrasel v internet stvari, kjer bo do leta 2020 v internetno omrežje povezanih med 50 in 100 milijardami naprav [86]. Komunikacija stroj-s-strojem potencialno zadeva med 50 in 70 milijard strojev, toliko jih namreč obstaja danes [116, 100], izmed teh pa jih je bilo v omrežje leta 2009 povezanih le 1% [77]. Že do konca leta 2011 naj bi bilo na svetu v omrežje povezanih 30 milijard naprav [117]. Po oceni IBM, enega izmed inovatorjev na področju interneta stvari, bo do leta 2015 v omrežje povezanih bilijon naprav [118]. Ob upoštevanju možnosti internetne komunikacije – ne samo med stroji, temveč še komunikacije *vseh vrst stvari* – bi bilo lahko v prihodnosti na omrežje povezanih 100 bilijonov stvari [86]. Vizionarji interneta stvari tako vidijo vsakega posameznika povezanega s 3.000 do 5.000 vsakdanjimi objekti, kar bo med drugim omogočil protokol IPv6, ki bi lahko povezoval nekaj 100 bilijonov objektov simultano [116]. Trenutni protokol IPv4 namreč omogoča približno 4,3 milijarde naslovov, IPv6 pa približno $3,4 \times 10^{38}$, kar je po pogosto uporabljeni analogiji dovolj za vsako zrno peska na Zemlji. Leta 2020 naj bi bilo tako v uporabi več bilijonov v omrežje povezanih senzorjev: v stvareh in v naših okoljih, in ki se bodo nahajali v naših napravah, sistemih, telesih. Ti senzorji, ki bodo zmožni zbiranja podatkov iz okolja in predvideti naše namere, so ključna tehnologija, ki bo spremenila našo interakcijo s stvarmi [119].

Ocene podjetja Cisco se nekoliko razlikujejo (Slika A1). Leta 2003 je bilo povezanih 500 milijonov naprav pri 6,3 milijardah ljudi, kar nanese 0,08 naprave na človeka. Po njihovi definiciji se je internet stvari *rodil*, ko je število naprav preseglo število prebivalcev, kar se je zgodilo med letoma 2008 in 2009 [120]. Leta 2010 je bilo na prebivalca sveta 1,84 povezane naprave, leta 2015 naj bi številka narasla na 3,47 in leta 2020 na 6,58. Če bi bilo v izračun vzeto samo prebivalstvo, kjer je internetni dostop na voljo (2 milijardi), bi bilo že leta 2010 6,25 z internetom povezanih naprav na prebivalca. Ob teh številkah v podjetju poudarjajo, da v izračune ni vštet hiter napredek v tehnologijah interneta in naprav, temveč so upoštevali zdajšnje stanje.

Značke RFID so ena glavnih značilnosti interneta stvari in po oceni IDTechEx je bilo v letu 2009 prodanih 1,98 milijarde RFID značk, v letu 2010 pa

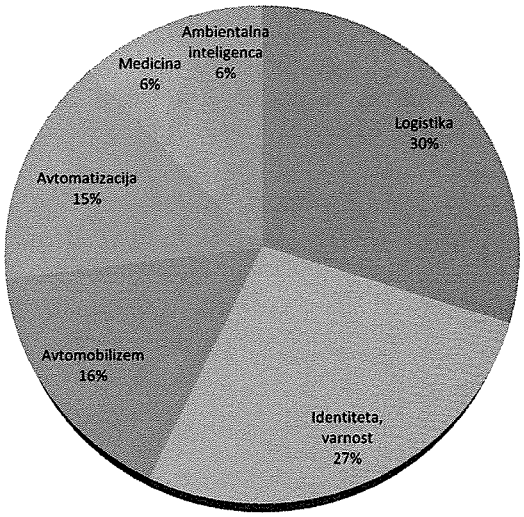


Slika A1. Število naprav povezanih z internetom, vir Cisco

naj bi številka narasla na 2,31 milijarde [121]. Podatki iz leta 2008 (Slika A2) kažejo, da je bil največji uporabnik značk *logistika* s 30% deležem, podobno visok delež pa je s 27% imela kategorija *identiteta, varnost*, delež 16% je predstavljal *avtomobilizem* in 15% *avtomatizacija*.

Takrat (2008) je bilo po ocenah v uporabi 60% pasivnih, 35% aktivnih in 5% semi-pasivnih značk RFID [122]. Ko gre za aktivne značke, so ti v začetku leta 2010 z 772 milijoni čipov predstavljali 13% trga, večina, približno 90%, jih je bila uporabljenih v napravah za daljinsko odklepanje avtomobilov. Do leta 2020 naj bi se delež aktivnih značk povišal na 25%, do leta 2020 se jim namreč napoveduje desetkratna rast v številu [123]. V letu 2010 je za *avtomobilsko industrijo* drugi največji porabnik aktivnih značk *vojska*, ki je uporabljala 14 milijonov enot [123]. Do leta 2020 naj bi bil največji delež aktivnih značk s 37% v kategoriji *živali, kmetovanje, raziskovanje, knjižnice, arhiviranje, prosti čas, proizvodnja, finance in drugo* (Slika A3), kar pa je precej obsežna kategorija. Napovedi IDTechEx [123] kažejo, da bo *vojska* z 9% deležem prehitela *avtomobilsko industrijo skupaj s potniškim transportom* (7% delež), z 9% aktivnih značk bo pomemben porabnik še *logistika*, z 8% *prevzgojne ustanove in službe za pogojne izpuste*, prav tako 8% delež napovedujejo skupini *potrošno blago in maloprodaja*, enak delež še *letalski industriji*. V kategoriji natisnjenih značk RFID in ostalih značk brez čipov, se pričakuje še večji porast uporabe tehnologije; od 12 milijonov značk v letu 2011 do 209 milijard v letu 2021 [124].

Na področju maloprodaje hitro narašča uporaba označevanja s tehnologijo RFID, že samo na področju označevanja oblačil, kjer v kategoriji maloprodaje uporaba narašča najhitreje (dvakrat hitrejša rast v primerjavi s celo-



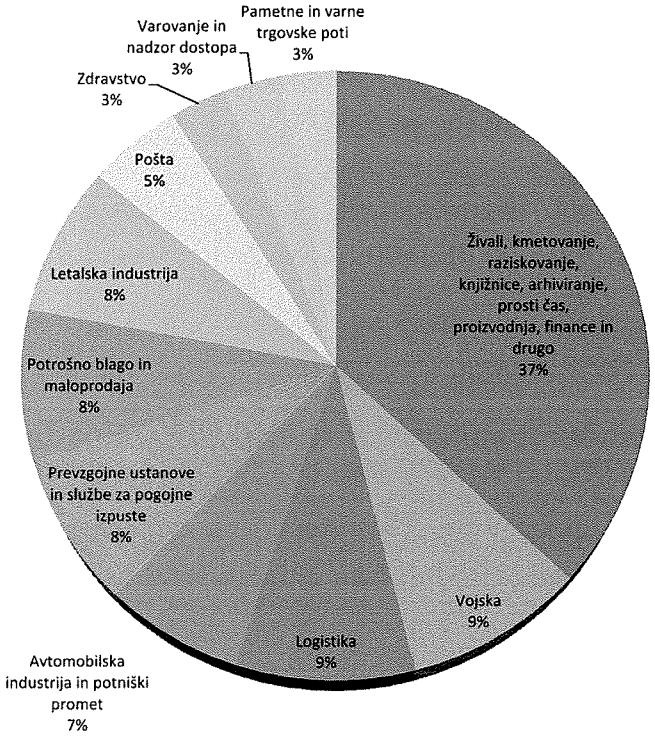
Slika A2. Delež RFID ponudnikov po aplikacijah, vir CE RFID

tnim trgom v naslednjih 10 letih), se ocenjuje zahteva po 300 milijonih značk v letu 2010 [125, 121]. V istem letu se ocenjuje potreba po 178 milijonov značkah za označevanje živali (npr. prašičev in psov), ki se ga po zakonu zahteva v določenih državah, 380 milijonov značk pa je ocena za uporabo pri vozovnicah v tranzitu v letu 2010 [121]. Že leta 2008 se je za vozovnice v potniškem transportu uporabljalo nekaj 10 milijonov pasivnih značk mesečno [122].

IDTechEx leta 2016 pričakuje (Slika A4), da bo največji del trga na področju vzhodne Azije (37,1%), sledila bo Severna Amerika (34,2%), Evropa pa bo z 26,1% še nekoliko manj pomembna, ves preostali svet pa naj bi predstavljal le 2,5% delež trga [121]. To pomeni najhitrejšo rast tehnologije med kontinenti v Aziji, ta je namreč glede na ponudnike značk leta 2008 imela le 7% delež (med državami 2% delež Japonske), med tem ko je imela 50% Amerika (48% delež ZDA med državami), Evropa z 41% drugi največji delež (Nemčija 20% in Združeno Kraljestvo 6% delež med državami), Afrika in Oceanija pa vsaka po 1% delež [122].

Do leta 2015 se pričakuje več kot 100 milijonov pametnih merilcev, ki bi potencialno lahko znatno pripomogli k zmanjševanju onesnaževanja zraka in nižanju stroškov za proizvodnjo energije [126]. Po napovedih podjetja IBM pa naj bi se v naslednjih nekaj letih vpeljalo že 300 milijonov pametnih merilcev [127]. Smart Gird[60] je projekt ZDA s ciljem vzpostavitve mreže, ki IKT koristi za učinkovito, zanesljivo in varno distribucijo električne energije

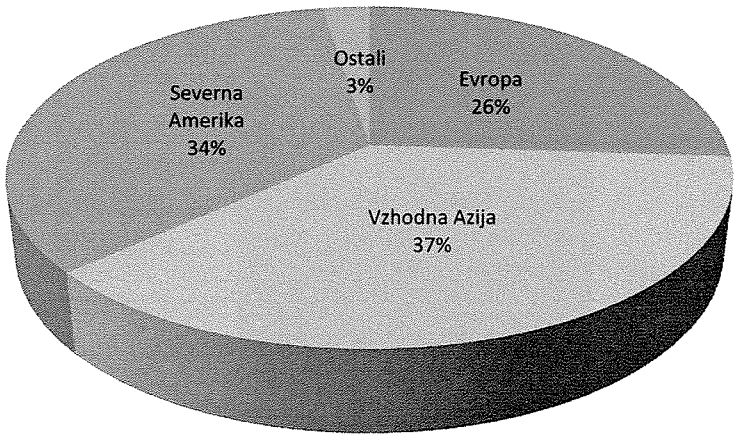
[60] http://www.nist.gov/smartgrid



Slika A3. Deleži aktivnih RFID čipov do 2020, vir IDTechEx

po državi. V okviru tega projekta se bo prek protokola IP v Smart Grid – omrežje omrežij – povezalo med 300 in 500 milijonov naprav, kot so električni števci na domovih, poleg tega pa tudi naprave izven domov, kot so generatorji in transformatorji [126]. Že danes pa je razmerje naprav povezanih na internet, ki niso osebni računalniki proti povezanim osebnim računalnikom 10:1, do leta 2020 pa se ocenjuje, da se bo razmerje povečalo na 100:1 [128].

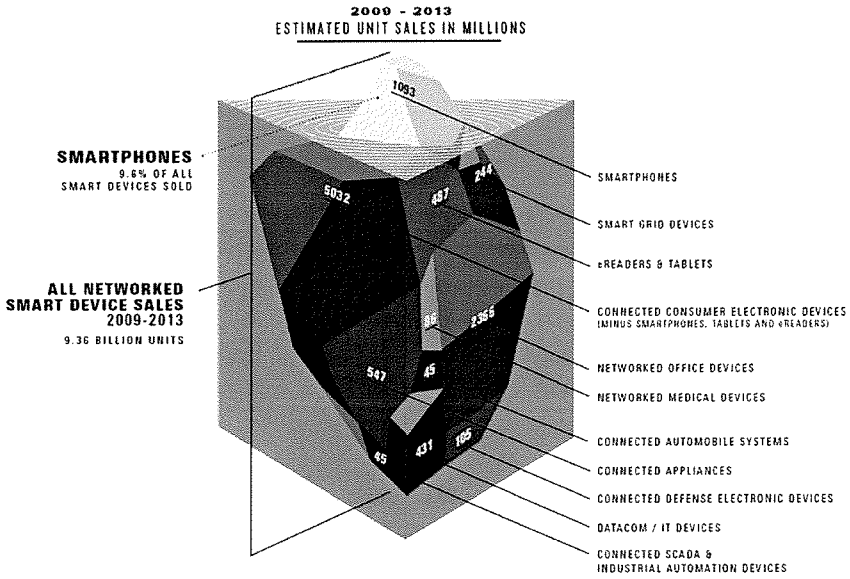
Ekosistem naprav povezanih v omrežje (brez osebnih računalnikov in strežnikov) je zelo raznolik in pametni telefoni, ki so morda prva stvar na katero pomislimo, so dejansko le vrh ledene gore (Slika A5). Ocene za obdobje 2009-2013 namreč kažejo na 9.36 milijarde prodanih naprav, ki se povežejo v internetno omrežje, izmed njih je le 1,09 milijarde pametnih telefonov, kar pomeni 9,6%. Največji delež predstavlja kategorija *potrošna elektronika (brez pametnih telefonov, tablic in eBralnikov)*, ki pomeni več kot polovico (približno 53%) prodanih naprav, približno četrtina pa je *pisarniških naprav*, ki jim po velikosti deleža sledi kategorija *pametnih telefonov* [129]. IDTechEx sicer v naslednjih nekaj letih pričakuje rast prodaje mobilnih telefonov iz ene na dve milijardi letno, prodaja mobilnih telefonov z



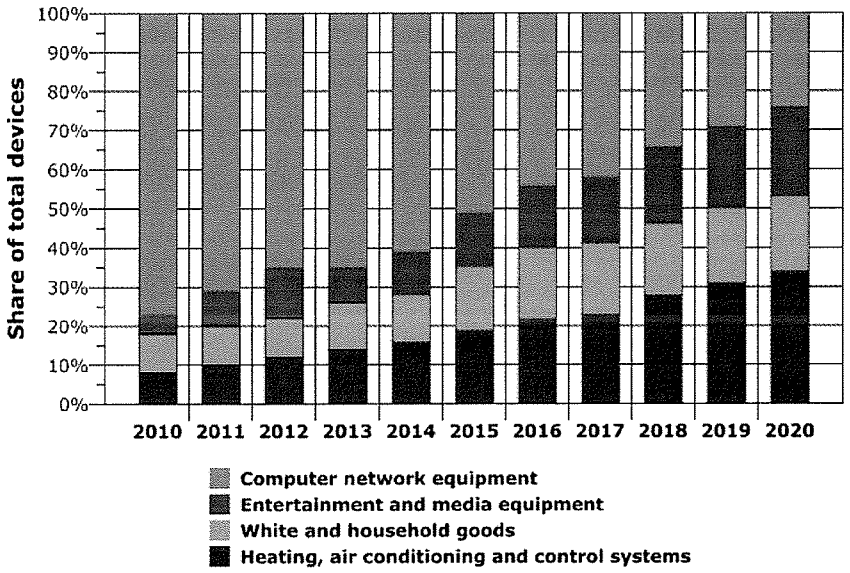
Slika A4. Napoved RIFD trga po teritorijih za leto 2016, vir IDTechEx

RFID pa bo narasla iz 50 milijonov v letu 2010 na 945 milijonov leta 2020 [130].

V letu 2010 naj bi več kot 75% delež z internetom povezanih naprav v domači uporabi predstavljala računalniška mrežna oprema, do leta 2020 pa bi ta delež padel na manj kot 25% (Slika A6). V tem času naj bi največji delež predstavljala kategorija *ogrevanje, hlajenje in nadzorni sistemi*, močno pa se bo povečal odstotek preostalih dveh kategorij, *zabavne elektronike* in nekoliko manj *beli tehniki* [65].



Slika A5. Ocena prodaje omreženih naprav (brez osebnih računalnikov in strežnikov) v milijonih 2009-2013, vir Mocana



Slika A6. Delež z internetom povezljivih naprav v gospodinjstvih 2010-2020, vir Vermesan