# 6. KOKKUVÕTE

Uurimistöö, mis on tehtud antud diplomitöö raames tõi välja tehnilised, juriidilised ning turvalisuse aspektid IoT-st spetsiifilisest integratsioonist tööstusesse. IoT printsiibid mängivad tähtsat rolli läbi kogu väitekirja. Antud põhjal, iga käesoleva uurimistöö kiht oli spetsifitseeritud.

Asjakohane IoT arhitektuur oli esmalt arutatud, andes lugejale põhjaliku ülevaate sellest kuidas IoT peaks töötama, tutvustades riistvara, tarkvara, kommunikatsiooni ning pilve alused, mille arhitektuuri kihtide seosega: seadmed, andmete kogumise tööriistad, portaalid, eeltöötlus, analüütilised ning pilvede tööriistad.

Vastavalt, võtme kommunikatsiooni tehnoloogiad, mis on rakendatavad IoT paradigmale, on olnud uuritud ning lühikirjeldus koos sobivuse testiga ühest või teisest sideprotokollist oli kirjeldatud. Lisaks, võrgu klassid olid lugejale esitatud, andes laiema visandi kommunikatsiooni rakendustest.

Analüüs protokollide kihtidest oli järgnevalt. Autor on uurinud erinevate kommunikatsiooni protokollide tähtsust ning pakkus välja lühikest ülevaadet kihtidest, mis on ehitatud erinevate protokollidega. Kommunikatsioonide protokollide integreerimise tähtsus oli ka nimetatud antud osas.

Järgnevalt, autor on tutvustanud kasvava trendi erinevate IoT platvormide loomises ja säilitamises, mis lubavad lihtsamal moel integreerida IoT lahendusi ettevõtetes ja tagada kontrolli nende üle. Erinevate platvormide uurimine oli tehtud siin. Seega, autor on uurinud ning valinud mitmeid neist platvormidest, mis on kõige sobilikumad IoT tehnoloogiate integreerimiseks tööstuse keskkonda Järgnevas osas on selgitatud juriidilised aspektid, viidates IoT-le ning takistustele selle tee peal. Esiteks, murekohad on esile toodud. Andmekaitse küsimused olid üle vaadatud, kuna need on suurimad murekohad nii isiklikult kui ka tööstuse poolt. EU juriidilised dokumendid oli uuritud ning autor, siinkohal andis oma arvamuse ning nägemuse antud murest.

Vastutuse teema olid arutatud järgmisena, kui esmane mure teel IoT globaliseerumisele. Reegel "by design and by default" oli tutvustatud antud osas – see on kõige tähtsam ametlik seadus, viidates vastutusega seonduvatele probleemidele.

Siduvad dokumendid, nagu juriidiliste aspektide osa, oli arutatud hiljem. Autor on avaldanud oma arvamust ning eeldas, et mitmete osanikute vastutus, kaasaarvatud ka siduvad dokumendid ning mõlemad tsiviil- ja kriminaalõigus varsti asendavad praeguseid seadusi.

Järgmine osa keerleb ümber turvalisuse aspekti. Peamised väljakutsed on arutatud, ning autori vaade turvalisuste kihtide peale on tutvustatud. Lisaks, IoT paradigma riistvara on analüüsitud ning võimalikud lahendused välja pakutud kasutades reegli „by design and by default" ning TPM on tutvustatud.

Side turvalisus viidetega erinevate kihtide peale, mis määratlevad erinevaid protokolle kasutamiseks andmete jagamiseks seadmete, kontrollerite, arvutite, portaalide, pilvede ja rakenduste vahel, oli põhjalikult arutatud antud osas. Mõned huvitavad lahendused olid leitud ning selgitatud autoril.

Järgmiselt, pilve ning elutsükli haldamise turvalisus oli üle vaadatud. Autor on analüüsinud erinevaid ressursse ning pannud kokku nõuandeid nende teemade kohta.

Lõpuks, uurimistöö praktiline osa oli tutvustatud lugejale. Selgitus sellest, mis on FMS ning IoT tähtsamad andmed olid selgitatud. Järgmiselt, autor on pakkunud välja optimaalse lahenduse IoT integreerimist FMS süsteemi, kasutades vabavara ning tasuta tööriistu.