

Факултет инжењерских наука Универзитета у Крагујевцу



Назив студијског програма: Машинско инжењерство

Ниво студија: Основне академске студије

Модул: Индустијски инжењеринг

Предмет: Производни системи

Број индекса: 2004/2014

Петар М. Илић

**ПРИМЕНА INTERNET OF THINGS
АПЛИКАЦИЈА У САВРЕМЕНИМ
ПРОИЗВОДНИМ СИСТЕМИМА
ЗАВРШНИ РАД**

Комисија за преглед и одбрану:

1. др. Александар Ђорђевић, доцент- ментор

2. _____

3. _____

Датум одбране: _____

Оцена: _____

ПРИЛОГ 3: Образац пријаве завршног рада

	Универзитет у Крагујевцу Факултет инжењерских наука	 
--	--	---

Основне студије: **Основне академске студије**

Студијско подручје (усмерење): **Индустријски инжењеринг**

Име и презиме: **Петар Илић**

Број индекса: **2004/2014**

ПРИЈАВА ЗАВРШНОГ РАДА

Тема рада: Примена Internet of things у савременим производним системима

Задатак: Приликом пријаве завршног рада ментор задаје тему по правилу преузету са листе тема коју је усвојила одговарајућа Катедра Факултета. Циљ Завршног рада је да студент докаже способност примене стечених знања и вештина при решавању задатака који су у складу са усвојеним исходима знања. Препорука је да завршни рад буде пројекат мањег обима, експериментално-лабораторијско испитивање, примена инструменталне методе, прегледни рад, теоријска разрада, компјутерска симулација једноставнијег реалног проблема и сл. Након одобравања теме, ментор је дужан да студента упуту у начин обраде теме, упуту га на додатну литературу, одреди обим завршног рада и током консултација усмерава и контролише рад кандидата. **Образац Пријава завршног рада попуњава се у електронском облику и штампа у три примерка од којих по један примерак задржавају: студент, ментор и Студентска служба.**

Затамњени делови су промењиви, а приликом испуњавања затамњење је потребно избрисати.

Ментор:

Др. Александар Ђорђевић, доцент

Крагујевац, 2020.

ABSTRACT:

The subject of this paper is to present IoT systems from a functional aspect, explain their application in factories, present them as the foundation of future infrastructures in new generation manufacturing plants and through the paper point out the benefits of using these applications in future business ventures. The introductory part of this paper refers to a brief introduction to IoT applications and their application, in the first part of the paper I made an introductory idea about how smart IoT components entered the industry, what are the smart components, what technologies are used and with which operating systems we meet when we talk about this type of component in the industry. The central part is dedicated to the application of IoT components and IoT applications in factories, ie smart factories, explains the basic principles and methods of implementation of the entire system in factories as well as a clear link between IoT and IT systems in production and business systems. The third part of the paper refers to the security conditions that this type of platform and business gives us.

Keywords: IoT applications, production business system, IoT components, smart factory, combination of IoT and IT systems, IoT system security.

РЕЗИМЕ:

Предмет овог рада је да презентује IoT системе са функционалног аспекта, образложи њихову примену у фабрикама, представи их као темељ будућих инфраструктура у производним фабрикама новије генерације и кроз рад укаже на бенефите који су условљени применом ових апликација у бућим пословним подухватима. Уводни део овог рада односи се на кратак увод у IoT апликације и њихову примену, у првом делу рада направио сам уводну представу о томе како су паметне IoT компоненте ступиле у индустрију, које су то паметне компоненте, које се технологије користе и са којим оперативним системима се сусрећемо када говоримо о овој врсти компоненти у индустрији. Средишњи део посвећен је примени IoT компоненти и IoT апликација у фабрикама, дакле паметним фабрикама, објашњени су основни принципи рада и методе имплементације читавог система у фабрикама као и јасна спрега између IoT и IT система у производно-пословним системима. Трећи део рада се односи на безбедносне услове које нам овакав вид платформе и пословања пужа.

Кључне речи: IoT апликације, производно пословни систем, IoT компоненте, паметна фабрика, спрега IoT и IT система, безбедност IoT система

САДРЖАЈ

1. УВОД.....	8
2. <i>Internet Of Things</i>	10
2.1. Кратак опис паметних компоненти.....	11
2.2. Компоненте и платформе за израду паметних уређаја.....	14
2.3. Кључне технологије укључене у IoT-.....	18
3. ПРИМЕНА IoT АПЛИКАЦИЈА У САВРЕМЕНОЈ ПРОИЗВОДЊИ.....	19
3.1. Концепт примене и функционисања IoT апликација у фабрикама.....	24
3.2. <i>Emerson DeltaV</i> пример.....	28
4. ПРЕДНОСТИ И НЕДОСТАЦИ IoT-a.....	31
5. БЕЗБЕДНОСТ IoT СИСТЕМА У ИНДУСТРИЈИ.....	32
6. ПРИМЕНА IoT АПЛИКАЦИЈА У УПРАВЉАЊУ ОДРЖАВАЊЕМ У ПРОИЗВОДЊИ.....	38
7. КРАТАК ОСВРТ НА БЕНЕФИТЕ IoT АПЛИКАЦИЈА У САВРЕМЕНИМ ПРОИЗВОДНИМ ПРОЦЕСИМА У ВРЕМЕ ПАНДЕМИЈЕ <i>Covid-19</i>	40
ЗАКЉУЧАК.....	43
ЛИТЕРАТУРА	

1. УВОД

Управљање уређајима преко интернета може се применити у свим областима живота савременог човека. Апликације су већ достигле такав ниво развоја да се свакодневно срећемо са њима, у нашим домаћинствима, у здравству, индустрији, образовању и многим другим областима. (engl. *Internet of Things, IoT*) је потпуно нова област, која је пронашла примену у различитим областима живота и пословања, а у савременом свету у њен развој се улажу значајна средства. Технологија интернета и паметних уређаја омогућавају повезивање већег броја корисника. Уређаји који су директно повезани са другим уређајима, међусобно размењују податке, захваљујући примени нове технологије. Суштина је да је примена информационих технологија у савременом свету заузела примат на целокупном светском тржишту. Информационе технологије саме по себи осавремениле су све гране индустрије, начине образовања, сасвим измениле дијагностику и лечење пацијената и још је много области које су потпуно покривене коришћењем и применом информационих технологија. Интернет је сасвим нови начин презентовања, али и комуникације, тако да ако га посматрамо у сфери индустрије, тачније производње сасвим је евидентно да су промене пословања и производње драстично промењене у последњих 20 година.¹

IoT је сасвим нова сфера у дигитализацији производног сектора. Оно што доноси овај нови аспект пословања у производњи, је смањење трошкова и дигитално унапређење производа и услуга и увођење нових пословних модела.

Прва идеја о аутоматизацији производње се јавила са концептом о смањењу трошкова и повећања производње. Сходно томе наступа савим нова етапа дигитализације, увођењем *IoT*-а постиже се бољи квалитет производа и трошкови су смањени, а са друге стране примењују се различита мерења, уведена је имплементација интелигентног управљања и обезбеђена је комуникација машина. Још једна велика погодност ових паметних система је управо комуникација, купаца, и погона путем интернет сервиса.

Управо циљ овог рада и јесте да представе *IoT* системе, њихове основне принципе рада и егзистирања. Након тога и да се представи концепт нових техника и технологија у савременом процесу производње, као основног средства комуникације, прво између руководиоца и људи, затим комуникације између људи, затим могућност комуникације машине са машином и слично. Следећи концепт представљања *IoT* система је у процесу управљања, како људима, тако и машинама и производним процесима.

Примена *IoT* решења у индустрији ће у будућности по већини предвиђања бити најмасовнија. То подразумева да ће се велики део послова захваљујући новим технологијама бити аутоматизовани. Тај читав процес увођења програмибилних компоненти ће утицати на повећање ефикасности и продуктивности.

General Electric је у сарадњи са *Intel* креирао *IoT* систем за индустријска постројења *Predix*, којим планирају да што већи број индустрија ”опамете” и повежу. Један део овог система чине сензори уграђени у машине који лако лоцирају квар, а друга врста сензора који су уграђени имају превентивну улогу, односно да дају системску грешку на тај начин да

¹ Извор: <https://elab.fon.bg.ac.rs/udzbenik-internet-inteligentnih-uredaja/uvod-u-internet-inteligentnih-uredaja/>

укажу на потенцијални квар, чиме се остварују значајне уштеде на пољу поправке и одржавања машина.²

Аутомобилска индустрија представља огледало стања индустрије једне земље. Присуство групације ФЦА у Србији има огромни значај. „Индустрија 4.0 све брже постаје реалност. У нашој фабрици у Крагујевцу, почели смо да приступамо дигиталној производњи кроз развој напредних решења за виртуелну симулацију наспрам физичког окружења, укључујући решења базирана на анализи података, адитивној производњи, предиктивном одржавању и хоризонталној и вертикалној интеграцији“, изјавио је Алесио Леонарди, директор фабрике ФЦА Србија.

„Конкуренција и технолошки напредак захтевају капацитет да се управља велики процесима производње на ефикасан и поуздан начин, тражећи бржа решења и одговоре, стално учећи са константном отвореношћу за иновације да би све ове потребе биле одрживе и ефикасне“, нагласио је Леонарди.³

² Извор: <https://startit.rs/iot-101/>

³ Извор: <https://www.securitysee.com/2018/06/industrija-4-0-dolazak-na-srpsko-trziste/>

2. *Internet Of Things* (IoT)

Током последњих неколико година, у области бежичних комуникација и умрежавања, нова парадигма названа “Интернет ствари (IoT)” коју је први представио Кевин Ештон 1998, године почела је да добија све више пажње у академској заједници и индустрији. Главна снага IoT визије је њен велики утицај који ће имати на неколико аспеката свакодневног живота и понашања потенцијалних корисника. Са становишта приватног корисника, најочигледнији ефекти IoT-а биће видљиви и на радном и на домаћем пољу. У овом контексту, олакшано живљење, паметни домови и канцеларије, е-здравље, побољшано учење су само неки примери могућих сценарија у којима ће нова парадигма играти водећу улогу у блиској будућности. Слично томе, из перспективе за пословне кориснике, најочигледније последице биће подједнако видљиве на пољима као што су аутоматизација и индустријска производња, логистика, пословни процес управљања, интелигентан превоз људи и робе.⁴

Убрзани развој и раст у области информационих технологија омогућио је пројектовање, производњу, постављање и умрежавање великог броја уређаја који поседују сензоре и актуаторе. Нано технологија (научна дисциплина која укључује физику, хемију, биологију, инжењерство и још много научних дисциплина, које ће своју примену пронаћи у свим областима људског живота), IPv6 (IPv6 мрежне адресе имају дужину од 128bita, тако да адресни простор има $3.4 \cdot 10^{38}$ јединствених адреса) умрежавање су генерално главни кривци за приступање и управљање путем интернета, свим паметним уређајима. Пошто уређаји повезани на интернет могу да размењују информације једни са другима и на тај начин остварују комуникацију, такав вид комуникације зове се M2M комуникација⁵(омогућава комуникацију између два уређаја).

Најједноставније речено структура интернета интелигентних уређаја се може поделити на три слоја, што је и приказано на слици 2. :

- Хардвер,
- Инфраструктура и
- Апликације и сервиси.

⁴ Извор: Debasis Bandyopadhyay, Jaydip Sen, page 2

⁵ Извор: <https://elab.fon.bg.ac.rs/udzbenik-internet-inteligentnih-uredaja/komunikacija-inteligentnih-uredaja-machine-to-machine-m2m>



Слика1. Слојеви интернета интелигентних уређаја⁶

Први и најосновнији слој представља хардвер. То подразумева да само уређаји који су хардверски модификовани да могу да комуницирају путем интернета улазе у читав пројекат. То у неким случајевима, када се ради о машинама подразумева и модификацију машина на тај начин што се уграђују недостајуће компоненте или се уређаји на било који начин умрежавају, било да се ради о кабловској мрежи или да користе *WI-fi* мрежу. Уређаји који улазе у хардверски део су почевши од најпримитивнијих машина, са дограђеним деловима за мрежну комуникацију, актуатори, сензори, свичеви, рутери, сервери, контролни панели, мобилни телефони и многи други уређаји, у крајњој линији и лаптопови који помажу при интервенцији и отклањању критичних тачака. Управо други слој IoT система је то умрежавање и успостављање комуникационих канала. Трећи ниво IoT система је управо највиши ниво и односи се на апликације и сервисе које је неопходно развити и поставити да читав систем оптимално функционише. Овај слој подразумева константно усавршавање и надоградњу, учење и имплементацију. Јер на овом нивоу добијају се улазни подаци, обрађују се и излазе информације.

2.1.Кратак опис паметних компоненти

Често се уређаји који могу да комуницирају називају паметним уређајима, основни принцип ових уређаја је да поседују пре свега комуникациони интерфејс (апликацију која ће контролисати вид комуникације уређаја било да се ради о бежичној или кабловској мрежи), затим имају своју интерну меморију и самостално напајање и процесор, тако да можемо слободно рећи да су назив, паметне компоненте с правом и добиле. Ова врста уређаја најчешће се напаја путем електричне мреже, али свакако начини напајања могу бити разнолики, па ту спадају: соларни панели или различите врсте батерија... Меморија коју поседује ова врста уређаја служи за чување прикупљених података из окружења, али и операције за које су уређаји програмирани се одвијају управо у меморији паметног уређаја. По самој логици ствари намеће се да један паметни уређај поседује улазно/излазне сензоре и актуаторе, затим интерфејс за интернет повезивање, интерфејс за складиштење и

⁶ Извор: <https://elab.fon.bg.ac.rs/udzbenik-internet-inteligentnih-uredaja/uvod-u-internet-inteligentnih-uredaja/>

меморисање и приказ стања меморије, зати мпостоји урађен и интерфејс за звучне и видео информације. У ову врсту уређаја спадају⁷:

- **Сензори** за праћење стања и обавештавање о насталим променама у окружењу,
- **Актуатори** који детектују промене у окружењу и на основу информација о променама у окружењу, добијају управљачке акције, заправо извршавају низ физичких активности,
- Затим **модули** који омогућавају пријем команди у одређеном окружењу.
- **Микроконтролери**, обично су базирани на микропроцесорима, имају уграђену меморију, часовник, хардвер за повезивање на друге уређаје за бежични пренос података и
- **Микрорачунари** односно лаички речено малени рачунари који на једном чипу имају микропроцесор, меморију и улазно/излазне уређаје.

Основне карактеристике *IoT* уређаја су⁸:

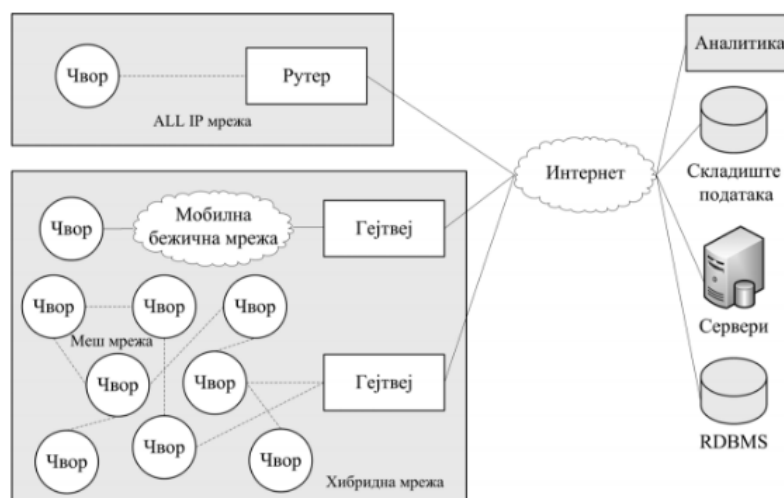
- Управо могућност да се динамички адаптирају окружењу и реагују на промене из окружења, ова карактеристика назива се још **динамичка самоадаптивност**,
- **Конфигурација се одвија скоро аутоматски**, дакле учешће корисника сведено је на минимум,
- Ови уређаји своју **комуникацију** остварују путем **интероперабилних комуникационих протокола**,
- Ови уређаји имају јединствени симболички или нумерички идентификатор, обично IP адреса, али може примера ради да буде и идентификатор ресурса(eng. Uniform Resource Identifier, URI). Без обзира који је јединствени идентификатор у питању, поента је да преко њега корисници приступају уређају, контролишу уређај, конфигуришу га и прате у каквом је стању и
- Следећа карактеристика је свакако **повезаност у мрежу**, то је веома битно јер на тај начин сам уређај је видљив у локалној и глобалној мрежи, а уједно, може и да види друге уређаје у тој мрежи и да комуницира са њима.

⁷ Извор: <https://elab.fon.bg.ac.rs/udzbenik-internet-inteligentnih-uredaja/komunikacija-inteligentnih-uredaja-machine-to-machine-m2m/>

⁸ Извор: : <https://elab.fon.bg.ac.rs/udzbenik-internet-inteligentnih-uredaja/komunikacija-inteligentnih-uredaja-machine-to-machine-m2m/>

Генерално све ово делује изузетно примамљујуће јер може да се извуче закључак да су створени роботи новије генерације, који су од велике помоћи човеку у раду, па и у животу уопште. У *IoT* уређаје убрајамо, примера ради:

- Кућне апарате,
- Паметне телефоне,
- Штампаче,
- Аутомобиле,
- Индустијске машине,
- Уређаји у енергетским системима,
- Уређаји у здравственим системима....



Слика 2. Пример повезивања паметних уређаја⁹

У предходном излагању већ је поменута комуникацију паметних уређаја. Поменута М2М комуникација свакако да захтева стандардизацију и развој протокола који би чинили јединствен систем. Протоколи М2М комуникације су следећи:

1. **Протокол који обезбеђује оперативни систем** и платформу за М2М апликације,
2. **Затим протокол XML за М2М**, који се заснива на синтакси, семантици и формалним дефиницијама за уређаје и гејтвеје.
3. **Следеће је Oracle софтверска платформа**, за израду апликација за филтрирање и обраду догађаја у реалном времену,

⁹ <https://elab.fon.bg.ac.rs/udzbenik-internet-inteligentnih-uredaja/uvod-u-internet-inteligentnih-uredaja/>

4. Један веома важан протокол, **XML за M2M апликације**, за комуникацију са имплементацијом отвореног кода, који је кодиран у Java програмском језику, али и C програмски језици су значајно укључени у израду ових софтверских решења. Отворени код програмерима омогућава да изврше различите модификације и софтвер прилагоде потребама које им се намећу.
5. Дакле прешли смо на протоколе, свакако да значајно место заузима протокол за комуникацију паметних уређаја MQTT (eng. *Message Queue Telemetry Transport*). Ови уређаји захтевају минимални проток информација и малу потрошњу енергије.
6. Затим протокол сличан HTTP-у, **CoAP (eng. Constrained Application Protocol)**, то је протокол који се заснива на раду типа клијент сервер и за њега нису неопходни додатни рачунарски ресурси.
7. Платформа за повезивање уређаја, процеса и апликација **Cloud оријентисана**, омогућава поуздан рад на Cloud-у кроз остваривање редундантности, контроле, базе података се аутоматски креирају, као и њихов бекап.

2.2. Компоненте и платформе за израду паметних уређаја

У основне компоненте за развој интрнета интелигентних уређаја, убрајамо: хардверске и софтверске компоненте.

У хардверске компоненте спадају:

- Сензори(различите врсте сензора спадају у ову групу, као што су сензори за мерење температуре, притиска, влажности ваздуха...)
- Актуатори (то су уређаји за контролу осветљења или климатизације),
- Микрорачунари,
- Микроконтролери (као што је, примера ради Arduino),
- Мрежна инфраструктура (рутери, свичеви и каблови...).

У софтверске компоненте спадају:

- Развојна окружења као што су *Eclipse*, затим *Arduino IDE*,
- Оперативни системи прилагођени за уређаје као што је *Raspbian*,
- Софтвер за специфично паметно окружење.

Што се IoT платформе тиче, можемо је посматрати као софтверско и хардверско окружење за развој и рад IoT паметних система. Процеси који су обухваћени IoT платформама су:

- откривање ресурса,

- праћење ресурса и
- реконфигурација софтверских платформи за развој паметних софтверских система.

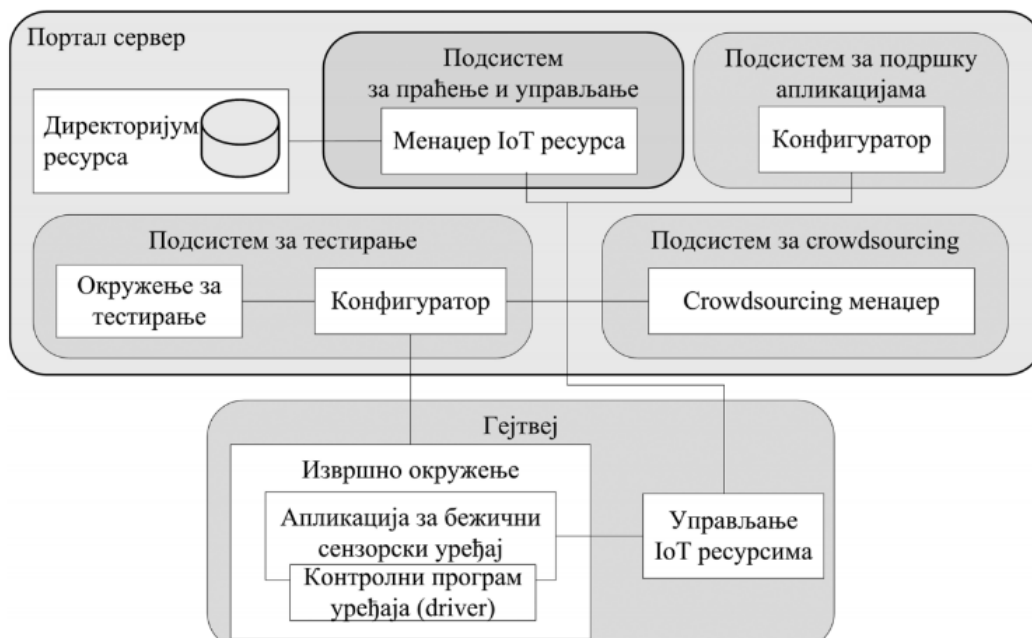
На серверу се налазе и функционишу, компоненте које су одговорне за пружање функционалности су: директоријум ресурса, менаџер IoT ресурса, конфигуратор за подешавање системске подршке апликацијама, конфигуратора за подешавање посистема за тестирање.

Постоји више врста IoT чворова:

- инфраструктурни чворови,
- експериментални чворови,
- чворови за пружање сервиса,
- партиципативни чворови(ручни уређаји).

Са друге стране основни функционални елементи који треба да буду разјашњени приликом израде ове врсте платформи су:

1. Уређаји који служе за прикупљање података и извршавање већ унапред дефинисаних акције, али служе и за надгледање контроле.
2. Комуникационе компоненте које заправо служе за повезивање ове врсте уређаја.
3. Сервиси у оквиру ове врсте платформи који служе за надгледање уређаја, за управљање уређајима, за извештавање о прикупљеним подацима и за откривање уређаја на мрежи.
4. Управљање функционалностима IoT платформе, у смислу конфигурисања, праћења платформе....
5. Сигурносна компонента се свакако односи на реализацију функционалности, затим аутентификације, ауторизације, заштите интегритета и приватности података.
6. Апликациона компонента, њена основна улога је пружање могућности да корисници надгледају и користе функционалности платформе за паметне уређаје, а и сто тако корисници имају могућност да том софтверском платформом и управљају.



Слика 3. Компоненте система за управљање IoT платформом¹⁰

За будућност индустрије, производње и живота уопште веома значајну улогу имају паметни уређаји, карактеристике ових уређаја су следеће:

Сензор мери физичке величине из окружења. Подаци које прикупља су: вибрације, температура, притисак....Када прими улазне податке сензор их претвара у резултат који је читљив кориснику или инструменту. Према врсти физичке величине коју мере сензори се деле на:

- Топлотне,
- Механичке,
- Хемијске,
- Оптичке,
- Сензоре јонског зрачења, акустичке и друге.

Актуатори су врсте мотора који могу да померају и контролишу механизаме или системе компоненти. Користе се у комбинацији са сензорима или другим актуаторима. Основна подела је на :

- механичке,

¹⁰ <https://elab.fon.bg.ac.rs/udzbenik-internet-intelligentnih-uredaja/uvod-u-internet-intelligentnih-uredaja/>

- електронске и
- софтверске актуаторе.

У бежичној сензорско-актуаторској мрежи, *Wireless Sensor Actuator Network*, WSA_N, актуатори могу имати следећа стања: неактиван, прикупљање података, координатор, покретач и вршилац активности.

Микрорачунари и микроконтролери су врсте рачунара, који поседују микропроцесор, интерну меморију, али имају и професионално одрађен улазно и излазни интерфејс. Улазни подаци су у бинарном облику, подаци се обрађују и кроз излазни интерфејс излазе. Микроконтролер је микропроцесор са уграђеном меморијом, генератором такта, часовником и хардвером за повезивање са спољњим уређајима као што су сензори, актуатори и преносиоци података. Микроконтролери имају следеће типове меморије:

- ROM (eng. *Read-Only Memory*),
- RAM (eng. *Random Access Memory*) и
- неовалентну меморију за чување програма.

Што се оперативних система за паметне уређаје тиче, најпознатији међу њима су :

- **Contiki** ово је оперативни систем који је кодиран и имплементиран у C програмском језику и потпуно је обезбеђено повезивање IPv4 и IPv6, преко протокол стека uIP и uIPv6. То је први оперативни систем који је омогућио IP комуникацију, коришћењем TCP/IP стека,
- **TinyOS** ово је оперативни систем отвореног кода, за сензорске мреже и паметне уређаје. Захваљујући овом оперативном систему омогућена је имплементација и рутирање великог броја мрежа. Новије верзије овог оперативног система имају основну IPv6 подршку. Овај оперативни систем програмиран у #C програмском језику,
- **FreeRTOS** –ово је такође оперативни систем отвореног кода који је прављен за отворене системе. За разлику од предходних оперативних система, принцип рада овог оперативног система заснива се на покретању апликације у тренутку када одређени догађај треба да се деси. Иначе пружа TCP/IP подршку.

Wearable су уређаји, електронске компоненте, које се најчешће уграђују у одевне предмете или се постављени уз тело. Поред значајне примене у медицини, у сврху праћења пацијената са одређеним обољенима, користе се и у војној индустрији, примера ради за препознавање лица, затим камера за *finger tracking*. Основне карактеристике ових уређаја јесу: мобилност, комуникативност, аутоматизација и мултитаскинг.

2.3 Кључне технологије укључене у IoT-у

IoT се може остварити само корисном применом више технологија које покрива у домену хардвера, софтвера и изузетно робусних апликација око сваког домена индустрије и оперативног сектора. Неки од кључних технолошких подручја која ће омогућити IoT су: технологија идентификације, технологија архитектуре, комуникациона технологија, мрежна технологија, технологија откривања мреже, софтвери и алгоритми, хардверска технологија, технологија обраде података и сигнала, технологија откривања и претраживања, управљање мрежом односа технологија, технологија напајања и складиштења енергије, технологије безбедности и приватности и стандардизација. Неке од ових кључних технолошких могућности ћу укратко разматрази у следећим подељцима.¹¹

2.3.1 Технологија идентификације

Функција идентификације је мапирање јединственог идентификатора или UID-а (глобално јединствен или јединствен у одређеном опсегу), ентитету како би га направио без двосмислености препознатљив и дохватљив. У визији IoT ствари имају дигитални идентитет (описано јединственим идентификаторима), идентификују се са дигиталним именом и односима, између осталог могу се навести у дигиталном домену.¹²

2.3.2 Мрежна технологија

IoT постављање захтева развој одговарајуће мрежне технологије за спровођење визије IoT -а да се дође до предмета у физичком свету и да се уведу на Интернет. Технологије попут RFID-а, бежичне везе кратког домета, комуникационе и сензорске мреже су средство за постизање мрежне повезаности, док верзија Интернет протокола 6 (IPv6), са проширеном адресом простора, омогућава адресирање, повезивање и праћење ствари. У IoT парадигми, сигурност, скалабилност и компатибилност више платформи између различитих мрежних система биће основни захтеви. У овом контексту, мрежне технологије морају да понуде решења која могу да понуде одрживост повезујући готово све на мрежу по смањеној цени. Свеприсутност мрежног приступа такође ће променити начин обраде информација. Данас, IP обезбеђује целокупну комуникацију између уређаја без икаквог захтева за прелазом за превођење средњег протокола.¹³

2.3.3 Технологије управљања мрежом односа

IoT ће захтевати управљање мрежама које садрже милијарде хетерогених ствари и тамо где постоји широк спектар софтвера, међуопреме и хардверских уређаја. Технологије за управљање мрежом мораће да обрате пажњу на неколико важна питања, укључујући сигурност, перформансе и поузданост. Управљање мрежом укључује управљање дистрибуираним базама података, складиштима, аутоматским испитивањем мрежних

¹¹ Debasis Bandyopadhyay, Jaydip Sen, page 6

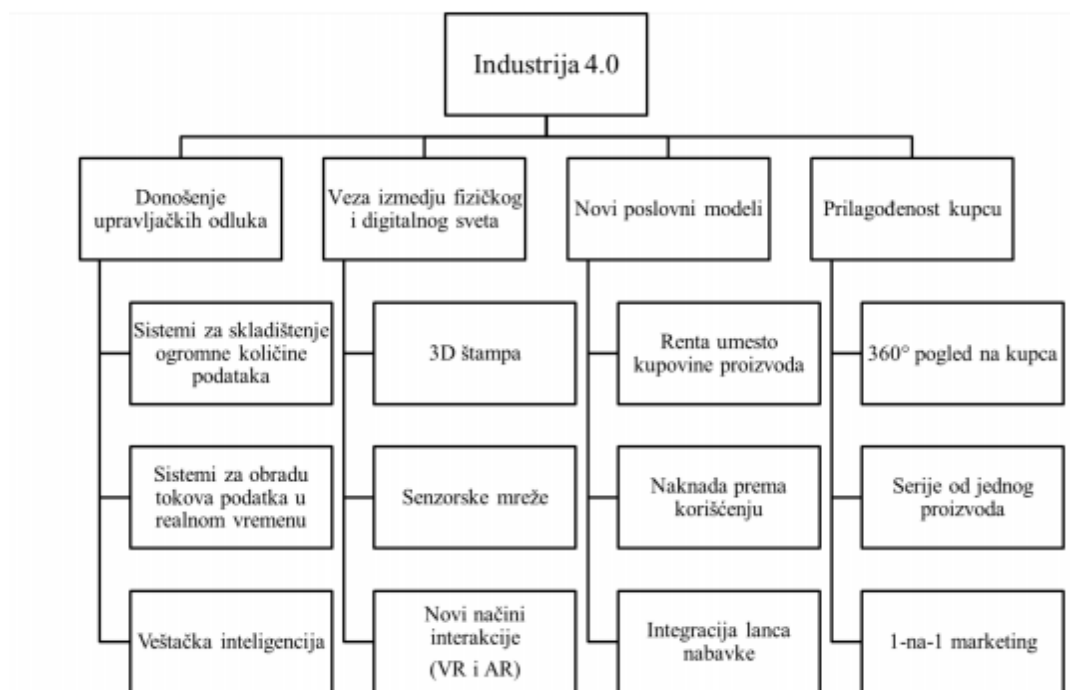
¹² Debasis Bandyopadhyay, Jaydip Sen, page 6

¹³ Debasis Bandyopadhyay, Jaydip Sen, page 7

уређаја и графичким приказима мреже у реалном времену промене топологије и саобраћај. Услуга управљања мрежом користи низ алата, апликација и уређаја који помажу у праћењу и одржавању мреже укључене у ИоТ апликације. Слично услугама друштвених мрежа које данас цветају на Интернету, постојале би потребе за стварима у мрежи како би створили међусобне односе. Ови односи могу бити формални, попут чланства у федерацији, или би могли бити лабави засноване савезе изазване инцидентом или догађајем.¹⁴

3. ПРИМЕНА ИОТ АПЛИКАЦИЈА У САВРЕМЕНОЈ ПРОИЗВОДЊИ

Дигиталне технологије као што су: IoT, robotics, cloud computer syber, су физички системи који су кључни у примени појма Индустрија 4.0. Будући да све ово заједно представља сасвим нови начин функционисања индустрије и производње, слободно можемо рећи да је ово четврта индустријска револуција. У принципу сви производни процеси су потпуно дигитализовани и све ове дигиталне технологије имају удела у реализацији неке идеје о производу, о инжењерингу производа, затим о организацији производње, реализацији производње, контроли процеса и пружања индустријских услуга.



Слика 4. Индустрија 4.0¹⁵

¹⁴ Debasis Bandyopadhyay, Jaydip Sen, page 11

¹⁵ Извор: PRIMENA INTERNET OF THINGS (IoT) REŠENJA U UPRAVLJANJU ODRŽAVANJEM U PROIZVODNJI, Dejan DAMNJANOVIĆ, 2019

Индустрија 4.0 је фаза дигитализације производног процеса која доноси суштинске промене у виду дигитално унапређених производа и услуга. Последица тога је да ће многе области у једној производној фирми у наредним годинама бити драстично измењене, као и технолошки поступци.

Доношење одлука се све више дигитализује, захваљујући великом броју података управо у дигиталној форми. Са друге стране да би се од тих података у дигиталној форми добиле чињенице које могу унапредити управљање, односно, манипулацију, примењују се напредне аналитичке методе. Постоји метода машинског учења, која подразумева креирање аутономних управљачких система, који су способни да се самостално усавршавају.

У савременом свету егзистирају технологије које значајно унапређују **интеракције између физичког и дигиталног света**.

Што се **нових пословних модела тиче**, карактерише их понуда целовитих услуга уместо продаје производа. Надокнада за пружене услуге се обрачунава углавном према употреби, а такав пословни модел пружалац услуга је стално повезан са објектом који се налази код корисника услуга и даљински може да прати и управља рад поменутог објекта.

Висок степен **персонализације** производа и услуга и наступа према купцу представља четврту битну карактеристику Индустрије 4.0. Пластична представа би била прављење обуће према карактеристикама стопала, или маркетиншка порука која је намењена само једном потрошачу. Генерално то је заживело у такси возилима у Крагујевцу, где постоје софтвери који циљано јављају где се позвано такси возило налази и за колико стиже на адресу, са друге стране, рекламни панел у такси возилима прилагођава се окружењу, дакле циља се на муштерију тог таксија, баш у том тренутку. Па уколико такси пролази поред Трнавe, на панелу у возилу налазиће се реклама за Трnavу или поред Темпа, рекламе ће презентовати Темпо.

Дигитализација фабрика. У ужем смислу речи дигитализација фабрика представља фабрику у којој су реализована интелигентана сарадња процеса производње и повезује се физички, дигитални и виртуелни свет. За једну дигитализовану фабрику није довољно да има само дигитализоване машине, неопходан је и софтвер који обухвата производне процесе, комуникациону инфраструктуру, дигитализоване индустријске сервисе и наравно безбедоносни систем.

Постоје фабрике које имају информатичке центре у којима се развијају оваква софтверска решења, али у последње време све је више фабрика које овакву врсту софтвера купују од специјализованих продаваца. Свакако да треба поменути да су и у прошлом веку, средином осамдесетих година, постојали покушаји да се производни процес дигитализује, али то није успешно спроведено на читав систем једне фабрике. Системи који су представљали почетак, тачније покушај дигитализације били су CIM, CAM i CAD.

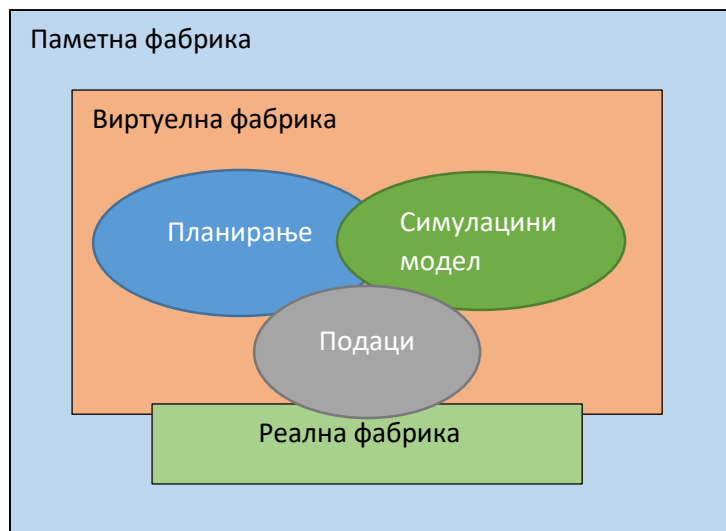
У оквиру спровођења стратегије јединственог дигитаног тржишта, европска комисија је у априлу 2016. представила планове и мере за подршку дигитализације европске индустрије. Један од приоритета јесте свакако развој Индустрије 4.0, па су сходно томе формиран бројни фондови, предложени су нови прописи и усвојени су нови стандарди. У Европској унији до 2030. године планирају се и инвестиције од 1.350 милијади евра за Индустрију 4.0.

Што се тиче индустрије у Србији последњих двадесет пет година није баш у завидном стању и положају. Али наду пружа управо то што у појединим фабрикама у Србији постоје стручњаци који одлично познају дигиталне технологије, могу да развију део индустријског софтвера и имају искуства да помогну развој Индустрије 4.0.

Паметну фабрику у савременом свету можемо да дефинишемо као, интернет, физичке системе који комуницирају преко индустријског IoT-а. Ако бисмо лаички описивали паметну фабрику, онда слободно може да се каже да је паметна фабрика скуп, реалне и виртуелне фабрике. У овом случају под **појмом реалне фабрике** посматраћемо као скуп свих података о производу, кроз интеграцију хетерогених *CAD*, *CAPP*, *CAM*, *CAE* система и свакако управљање различитим модулима информација као што су управљање документацијом, спецификацијама, радним налозима. **Виртуелна фабрика** у овом случају подразумева да се на принципу реалних података моделирају производи, моделирају процеси и ресурси и интезивно се тестирају и унапређују коришћењем виртуелних модела.

Интеграција капацитета у фабрици где је имплементиран систем Индустрија 4.0 има као основни циљ да се успоставе глобалне мреже које ће да обухвате све ресурсе фабрике. Под свим ресурсима фабрике подразумевају се машине, производни објекти и складишта, у форми виртуелног физичког система. Постоје два типа интеграције: хоризонтална и вертикална интеграција.

- **Хоризонтална интеграција** подразумева – различите IT у различитим фазама планирања и производње и интегришу се унутар фабрике (то су функције попут набавке, логистике, маркетинга), а та интеграција може бити остварена и између различитих предузећа.
- **Вертикална интеграција** – овде је принцип end to end решења, који се заснива на хијерархији. Примери у нама познатим фабричким окружењима за то су: актуатори и сензори, планирање производње, производња...



Слика 5. Интеграција виртуелне и реалне фабрике¹⁶

Да би се IoT систем имплементирао и интегрисао у једној фабрици неопходно је да постоје следећи предуслови:

- Да буде испоштована способност прикупљања неопходних података са свих система у окружењу,
- Да интернет има непрекидну комуникацију са сензорима и
- Да постоји адекватна инфраструктура за транспорт података кроз све нивое производног процеса.

У фабрикама постоје два кључна тренда која су вођена применом IoT-а, а то су дистрибуирано рачунарство и ширење сензора. Дистрибуирана контрола подразумева примену PLC контролера, који се постављају ближе машинама које контролишу, на тај начин се убрзава производња, елиминишу се евентуална уска грла и уноси се велики степен флексибилности. Ширење сензора или Pervasive sensing ¹⁷, подразумева да произвођачи уносе све више сензора и прате више промењљивих и типова података. У савременом свету цена сензора је драстично пала, па је то и главни разлог што су сензори широко доступни произвођачима.

¹⁶ Извор: <http://docplayer.rs/187258792-Dizajn-industrijskih-iot-sistema.html>

¹⁷Извор: termin lansirao Emerson



Слика 6. Од IT до IOT решења кроз подељене нивое контролеPurdue референтни модел (PRM – ISA-99) ¹⁸

Притом треба подвући чињеницу да је улога система за управљање подршка различитим стандардима комуникације уз помоћ мерно регулационе опреме која је различитим I/O картицама повезана на заједнички контролер. У фабрици системи управљања би се могли поделити на:

- Централизоване системе управљања,
- Надзорно-управљачке системе (eng. *Supervisory Control and DataAcquisition – SCADA*) и
- Дистрибуиране системе управљања.

Притом веома је важно навести да се за процесе надзора и контроле индустријских процеса и опреме користе : системи са *PLC* и *SCADA* комбинацијом. Притом *SCADA* системи имају задатак да визуализују податке из процеса којим управљају *PLC*-ови, друга врста система су *DCS (FCS)* системи, који се заснивају на дистрибуираним елементима. Елементи су у овом случају дистрибуирани преко радних станица, локалних контролера све до паметних уређаја. Овакав концепт даје флексибилност остварења оптимизације.

Ако читав овај систем посматрамо са аспекта сигурности, објашњењ би изгледало овако: само једна грешка у *PLC*-у онемогућила би управљање делом процеса, тачније делом којим та *PLC* компонента управља. Са друге стране посматрано у *DCS* систему, када дође до грешке, та грешка утиче на само једну управљачку петљу.

¹⁸Извор: <http://docplayer.rs/187258792-Dizajn-industrijskih-iot-sistema.html>

Са аспекта финансија цена игра пресудну улогу, тако да због ниже цене код мањих индустријских целина примењују се комбинације *SCADA* и *PLC* система, а код већих и комплекснијих пословних система као и географски удаљених фабрика, односно система примењују се *DCS* системи.

DCS системи могу комуницирати са **HMI**-em (то су *Touchpaneli* за управљање), са фреквентним претварачима, инструментима, сензорима, али и са *SCADA*-ом. Основни елементи *DCS* система су:

- Чворови (*Nodes*) то су контролер или радна станица, који се подешавају како да реагују, али и коју информацију да прихвате и упамте из једног производног процеса.
- Ознака уређаја (*Device Tag-DT*) једнозначно одређује уређај о ком се ради.
- Ознака сигнала(*Device Signal Tag-DST*) , што подразумева да едан уређај може имати више различитих *DST*, односно врста сигнала.
- База података која садржи информације о читавој конфигурацији система и може се *offline* мењати без обзира на остале елементе система, односно без утицаја на остале делове процеса.
- *On-line* праћење надзорно управљачких алгоритама и њихова реалтима модификација.

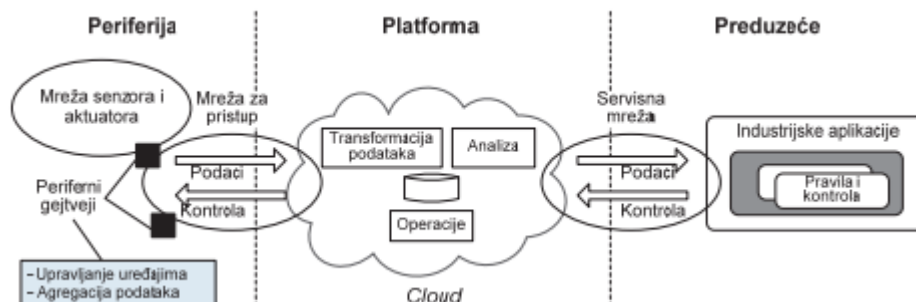
Логичка целина *DCS*-а се конфигурише повезивањем модула. Модули су као што је поменуто у предходном излагању најмање логичке целине. Сваки модул садржи алгоритме, који су логички кораци који одређују понашање модула, услове, аларме, дисплеје, информације о историји догађаја на пример на тачно одређеној машини, као и све остале параметре који дефинишу производну целину.

3.1.Концепт примене и функционисања *IoT* апликација у фабрикама

Када се говори о *IoT* системима у фабрикама, прва мисао која прође кроз главу јесте управо пословање у облаку или популарно речено *Clouding*. То је концепт примене паметних уређаја и програма у фабричким постројењима, а комуникација и прикупљање података врши се путем интернета. Отуда и појам пословања у облаку, јер обично се базе података којима управљају сервери и обрађују их, налазе на интернету.

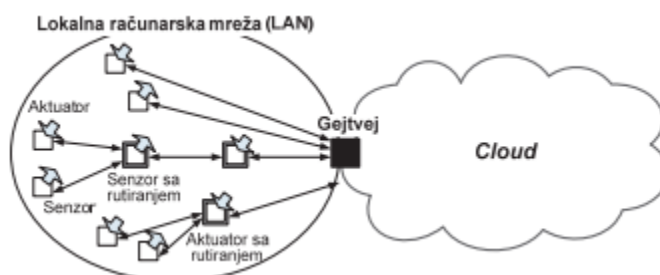
На првом месту треба поменути **трислојни модел**. Овај модел обухвата слојеве: периферних (*edge*) уређаја и слој платформе. Периферни слој добија информације из мреже сензора и актуатора, који су постављени у производно пословном систему, а све се одвија преко периферних гејтвеј уређаја. Оно што карактерише слој уређаја су: локација самог уређаја, опсег управљања уређајима, природа мреже сензора и актуатора, а да притом све ове карактеристике зависе од специфичних индустријских примена. Слој платформе, односно слој урађеног интерфејса за унос команди, добија и прихвата контролне команде од људи који су добили предходне инструкције, затим слој платформе обрађује информације их и прослеђује слоју периферије. Овај слој обједињује процесе, анализира токове података и управља уређајима и осталом опремом, најтипичнији начин реализације

овог слоја је преко информатике у облаку. Овај слој су интерфејси за крајње кориснике, имплементира индустријске апликације и читаве системе за подршку у одлучивању.



Слика 7. Шема имплементације IoT трослојног модела у индустрији¹⁹

Други модел подразумева примену концепта повезивања рачунарске мреже IoT система са *Cloud* окружењем преко гејтвеја-медијатора. Гејтвеј има принцип функционисања такав да представља као крајњу тачку облака, а са друге стране је граница између локалне мреже и других периферних чворова. Ова архитектура јасно дефинише скалабилност IoT система на тај начин што локализује операције и контролу над операцијама и уређајима, а на тај начин се побољшава функционисање читавог система.



Слика 8. Повезивање локалне мреже предузећа на интернет преко gateway-a²⁰

Трећи модел се заснива на слојевито организованим магистралама података (databus). Комуникација између крајњих тачака, одвија се преко магистрале. Магистрала података је логички простор, у коме је имплементиран скуп модела података, протокола и

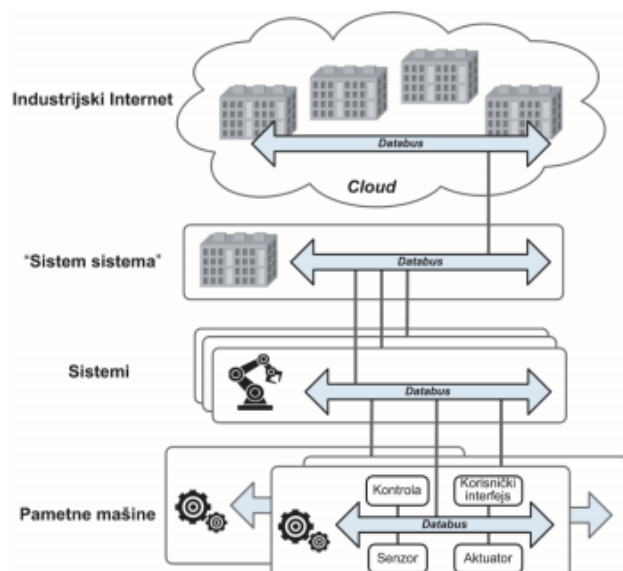
¹⁹ Извор:

<http://postel.sf.bg.ac.rs/simpozijumi/POSTEL2019/RADOVI%20PDF/Telekomunikacioni%20saobracaj,%20mreze%20i%20servisi/8-Stojanovic-Bostjancic-Rakas-Markovic-Petrovic.pdf>

²⁰ Извор:

<http://postel.sf.bg.ac.rs/simpozijumi/POSTEL2019/RADOVI%20PDF/Telekomunikacioni%20saobracaj,%20mreze%20i%20servisi/8-Stojanovic-Bostjancic-Rakas-Markovic-Petrovic.pdf>

безбедносних решења. Паметне машине на најнижем слоју користе магистралу података за преузимање информација о локалној контроли, аутоматизацији и целокупној анализи система у реалном времену. На другом нивоу су системи који користе други ниво или другу магистралу која садржи податке за надзор система и управљање процесима и машинама. Удруживање удруживање више нивоа система или више магистрала води ка креирању комплексних апликација за надзор, управљање и анализу. Највиши слој овог модела, индустријски IoT, заснован је на принципу пословања у облаку.



Слика9. Трећи модел- слојевите магистрале података²¹

Сам процес управљање IoT платформом је веома комплексан. Састоји се од следећих процеса:

- откривање ресурса,
- праћење ресурса и
- реконфигурација платформе.

На серверској платформи, компоненте које су одговорне за пружање функционалности за управљања платформом су:

- Директоријум ресурса,
- Менаџер IoT ресурса,
- Конфигуратор за подешавање подсистема за подршку апликацијама,

²¹ Извор:

<http://postel.sf.bg.ac.rs/simpozijumi/POSTEL2019/RADOVI%20PDF/Telekomunikacioni%20saobracaj,%20mreze%20i%20servisi/8-Stojanovic-Bostjancic-Rakas-Markovic-Petrovic.pdf>

- Конфигуратор за подешавање подсистема за тестирање и
- Crowdsourcing менаџер.

У предходном излагању било је речи о хардверским компонентама које омогућавају имплементацију паметних система у савременим процесима производње. Са друге стране постоје и софтверске компоненте, у њих спадају:

- развојна окружења (Eclipse, Arduino IDE, DeltaV),
- оперативни системи прилагођени за уређаје (нпр. Raspbian) и
- софтвер за специфично паметно окружење.

За развој IoT система се користе следеће технологије:

- мрежне технологије и протоколи,
- сензорске мреже,
- мобилне технологије,
- Cloud computing и
- Big data.

Интелигентни уређаји се повезују у PAN, LAN, MAN, WAN и сензорским мрежама. Иначе развоју паметних фабрика су значајно допринеле мобилне мреже. **Мобилне технологије** које су допринеле развоју и примени IoT-а су мреже мобилне телефоније и мобилни интернет, Bluetooth, RFID, WiMAX, глобални систем позиционирања (GPS), комуникација у блиском пољу (NFC), ZigBee и друге.

Интеграција IoT-а са Cloudom-ом подразумева да је потребно задовољити следеће захтеве:

- Cloud сервиси треба да олакшају лакше функционисање хардвера у складу са софтверским командама у IoT систему,
- Неопходна је подршка за Cloud протоколе, као што су најпознатији REST и WebsocketREST и још много других,
- Неопходно је обезбедити адекватну подршку за сигурно даљинско ажурирање софтвера на уређајима,
- WEB и мобилне апликације треба да омогуће приказ података, обраду података и управљање удаљеним уређајима.

Квалитетна IoT инфраструктура, поред *Cloud computing* система, може да има принцип Big data инфраструктуре.

Lora

У савременом свету већина савремених IoT мрежа широм света заснива се на Lora (*Long Range*) модулацији и LORA технологији. То је бежична технологија великог домета и мале снаге. Ово решење је широкопојасно мрежно покривање које обећава велике домете уз ниску потрошњу енергије и савршено одговара IoT апликацијама. LORA је основа за паметне IoT апликације које решавају неке од највећих изазова са којима се суочава наша планета, а то су: управљање енергијом, смањење природних ресурса, контрола загађења, ефикасност инфраструктуре, спречавање еколошких катастрофа итд.

Са преко 50 милиона уређаја повезаних у мрежама у 95 земаља, са тенденцијом ширења, за LORA технологију кажу да је DNK IoT-а, која ствара паметнију планету.

LoRaWAN мрежна архитектура има топологију звезде у којој gateway преносе поруке између крајњих уређаја и централног мрежног сервера. Gateway су повезани на мрежни сервер преко стандардних IP веза и делују као транспарентни мост, једноставно претварајући RF пакете у IP пакете и обрнуто. Бежична комуникација користи предности Long Range карактеристика физичког слоја LoRan, омогућавајући повезивање са једним хором између крајњег уређаја и једне или више гејтвеја. Сви режими су способни за двосмерну комуникацију и ефикасну употребу спектра.

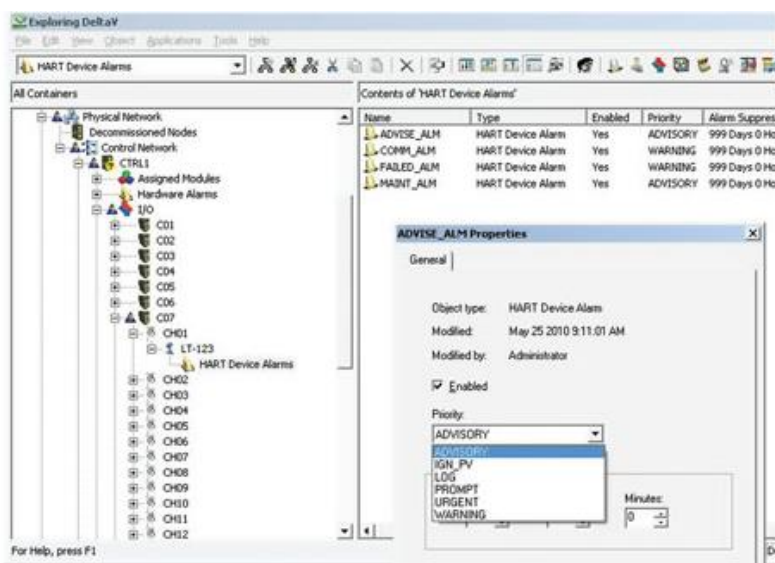
Detaqna дефиниција параметра физичког слоја уређаја и инфраструктуре обезбеђује беспрекорну интероперабилност између произвођача. Протокол који се користи је мрежни протокол LPWA (*Low Power, Wide Area*) који је дизајниран да бежично повезује "ствари" са батеријама на Интернет у регионалним, националним или глобалним мрежама и циља на кључне захтеве IoT као што су двосмерна комуникација, безбедност, *end-to-end* мобилност итд.

LORA Alliance је најбрже растући технолошки савез. То је непрофитно удружење више од 500 компанија чланица. Ово удружење посвећено је великом размештању мрежа широких подручја и мале снаге кроз(LPWAN) развој и промоцију отвореног стандарда. Фирме које су чланице имају користи од живог екосистема активних доприноса који нуде решења, производе и услуге, који стварају нове и одрживе пословне могућности.

3.2. Emerson DeltaV пример

Као пример може се навести *DeltaV* дистрибуирани систем управљања, који корисницима пружа могућност лаког покретања и коришћење система, коришћењем *plug-and-play*, технологије за конфигурисање и пуштање у рад хардверских компоненти и свакако за доступну библиотеку готових контролних модула. Познате технике коришћења овог система пружају могућност да се убрза и модификује конфигурација система, а графички интерфејс је прилагођен *Microsoft Windows* графичком окружењу. Примену је пронашао у хемијској индустрији, петрохемији, хемијској индустрији, производним погонима широм света. Примарни DeltaV систем има два основна елемента, а то су контролер и радна станица, ови елементи могу бити повеани на два начина, директно, што подразумева да су повезани путем кабла и други начин је помоћу свича. Систем је конфигуриран путем повезивања модула, а модули се једноставно искључују или доводе у стање мировања без утицаја на целину, тако да је креирање, download, целокупан рад, анализа грешки и њихово отклањање је доста поједностављено овим принципом рада. Треба напоменути да алгоритам у надређеном модулу одређује рад подређених модула које садржи. Тако да су сви модули

управљања опремом и процесима придружени тачно одређеној процесној јединици. Управљање процесима се врши помоћу функционалних блокова. Функционални блокови обухватају креирање континуалних и дискретних алгоритама у модулу, који омогућавају управљање и надзор над процесом. Постоје библиотеке већ креираних модула у одређеном производном процесу, када корисник жели да креира нови модул, може се послужити већ креираним модулом из библиотеке или може свој потпуно новокреирани модул да уврсти у библиотеку модула. Сваки функционални блок садржи параметре за конкретну примену. А алгоритми поред тога што могу бити веома једноставни улазни алгоритми иду и до веома



сложених стратегија.

Слика10. Изглед графичког интерфејса DeltaV управљачког решења²²

DeltaV систем покрива свеобухватан систем алармног обавештавања. Упозорења се у овом систему зову *PlantWeb* упозорења. Та упозорења могу стићи са уређаја који међусобно комуницирају. *PlantWeb* упозорења са уређаја у паметној фабрици су веома значајна из разлога што се добијају информације са производних трака директно и могу да укажу на евентуалне проблеме, што дефинитивно помаже да се ти проблеми предупреду и више не догоде. Класични управљачки системи имају развијен систем упозерења само у случају да су одступања значајно већа од предвиђених или ако у производном процесу дође до неочекиваних промена.

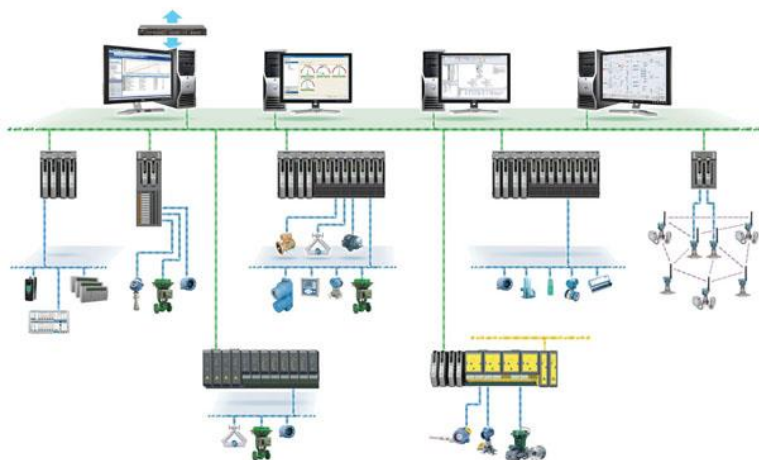
Треба напоменути да већина управљачких система користи један механизам за обавештавање о алармима везаним за процес, а други за обавештавањима о исправности хардвера. Са друге стране *PlantWeb* упозорења имају проширени обим праћења исправности система и покрива све уређаје у пољу. То подразумева да су хардверска упозорења и упозорења са уређаја конзистентна и да се прикупљају упозорења из читавог система.

²² Извор: <http://www.ivdamprocess.com/novosti/uvod-u-distribuirane-sisteme-upravljanja-kroz-emerson-deltav-dcs/>

PlantWeb упозорења су тако урађена да се користе за приказивање стања уређаја. Извештаји су у прегледној, форми која кориснику система да реагује на најоптималнији начин у датом тренутку. Генерално упозорења која се добијају са уређаја, се организују у три врсте упозорења. И четврто комуникационо упозорење је од самог DeltaV система.

- Пример упозорења: ГРЕШКА (*FAILED_ALM*), у том случају се подразумева да уређај није у стању да функционише,
- ОДРЖАВАЊЕ (*MAINT_ALM*), ово упозорење указује да је уређај ван функције и да то значајно може утицати на одвијање процеса,
- САВТОДАВНИ (*ADVISE_ALM*), значи да је уређају неопходан превентивни сервис или има подтке који чекају на упис и
- КОМУНИКАЦИОНИ (*COMM_ALM*), овај вид грешке указује да уређај не комуницира више преко H1 сегмента или преко *HART* канала.

PlantWeb упозорења поседују приоритете у циљу бољје организације производње. Рецимо, упозорења везана за стање уређаја могу бити једнака за све врсте уређаја тог типа, али са друге стране утицај одређеног уређаја на производњу и квалитет производа је сасвим другачији, наравно, у зависности од тога на који начин се тај уређај користи. У том случају, приоритет, одређује ниво важности упозорења. *DeltaV* систем обезбеђује за напредне кориснике могућност да подешавају параметре аларма у зависности од практичних потреба. Напредни корисници могу применити неке од стратегија управљања и то веома лако.



Слика 11. Изглед једног производно-пословног система где је примењен *DeltaV* модел²³

Савремени системи овог типа, обезбеђују и упозорења која се односе на окружење уређаја. Са повећањем броја упозорења, неопходно је да се добро познаје улога сваког појединачног

²³ <http://www.ivdamprocess.com/novosti/uvod-u-distribuirane-sisteme-upravljanja-kroz-emerson-deltav-dcs/>

уређаја у производном систему, али и да дефиниција о упозорењима буде прецизно урађена, у смислу које упозорење је одговарајуће за одређену врсту проблема. Вођењем евиденције о упозорењима, која се јављају у вези сваког уређаја постиже се да када се касније јави потреба за конфигурисањем уређаја или потенцијални проблем, постоје сачуване информације за ефикасно подешавање.

4. ПРЕДНОСТИ И НЕДОСТАЦИ IoT-а

Изузетно је важно у сваком систему нагласити добре старне функционисања система, али и потенцијалне опасности које овај концепт носи са собом. Примена IoT компоненти је изузетно широк спектар области, а могућности су неограничене. Генерално у широком спектру области у ком се IoT компоненте могу користити, на основу литературе и искустава, може се издвојити осам области примене:

1. Паметне куће, у савременом свету нису реткост и све више људи прибегава овом концепту. Програмибилне компоненте се користе у сврху заштите домаћинства, али и у најбаналније сврхе, попут укључивања светла.

2. Здравство, има можда и највеће бенефите од увођења програмибилних компоненти, јер многи тешки захвати су сада постали могући захваљујући програмибилним компонентама. Тако да се и ниво здравствене заштите на овај начин подигао на виши ниво.

3. Саобраћај, велики број саобраћајних незгода смањен је захваљујући употребом програмибилних компоненти,

4. Енергетика, веома је значајно увођење програмибилних компоненти, из разноразних углова или разлога, степен искоришћења енергије.

5. Јавна сигурност,

6. Индустријска производња;

7. Пољопривреда;

8. Екологија.

Предности употребе IoT-а се свакодневно намећу за крајње кориснике, али и за компаније:

- Побољшава се ангажованост клијената,
- Долази до оптимизације технологије,
- Побољшава се управљање ресурсима,
- Побољшава се прикупљање података.²⁴

²⁴ Извор: <http://www.emc-review.com/sites/default/files/2017-2/EMC%20-%20godina%20VII%20broj%202-Sanel%20Jakupovic.pdf>

Недостаци употребе IoT-а у индустрији су:

- Сигурност, јер је IoT-а систем који се заснива на умреженим уређајима, то подразумева да је могућност различитих напада велика, а самим тим је и безбедност доведена у питање,
- Приватност, IoT садржи врло детаљне и личне податке без активног учествовања особе,
- Комплексност и флексибилност се односи на дизајн, одржавање великог сета нових технологија,
- Постоји усклађеност са одговарајућим регулаторним прописима,
- Непредвидивост понашања,
- Немогућност унапређења уређаја, наиме многи IoT уређаји, као и мобилни телефони нису фабрички намењени унапређењу,
- Корисници не надгледају уређаје и нису упознати уколико нешто не иде по протоколу.

5. БЕЗБЕДНОСТ IoT СИСТЕМА У ИНДУСТРИЈИ

Основни циљ IoT система у савременим производним системима је да оптимизује потрошњу, да омогући контролу трошкова, оствари ефикасност и континуитет операција индустријског процеса. Ово је систем који примарно усредсређен на надзор производње и параметара животне средине који су повезани са индустријским процесом. Архитектура овог система је пројектована тако да испуни строге захтеве индустријских апликација који се односе на рад у реалном времену, са врло високом расположивошћу и поузданошћу. IoT опрема мора да функционише и у екстремним радним условима, као што су велике варијације температуре, варијације притиска и запремине гаса, електромагнетске сметње и још много других фактора.

У читавом производном процесу наравно да постоје ризици различитих врста. Ако узимемо у обзир слојевиту IoT структуру, у једној паметној фабрици безбедносни ризици би изгледали овако:

1. Локалне рачунарске мреже прикупљају и обрађују податке од објеката индустријског система на најнижем слоју. Главни безбедносни ризик је одсуство аутентификације, идентификације и других безбедносних механизма у сензорској опреми.
2. Подаци се преносе до облака посредством гејтвеја. Основни ризици су последица одсуства безбедносних механизма у комуникационим протоколима и гејтвејима.
3. Подаци се складиште и обрађују у облаку, при чему се користе одговарајуће платформе и специфични алгоритми, као што је алгоритам за анализу велике количине података (*Big data*). Главни проблем су небезбедни подаци.

4. Интерфејси између платформи и крајњих корисника могу проузроковати проблеме због небезбедних комуникационих протокола.

Са аспекта IoT система, постоје следећи безбедоносни аспекти који се могу посматрати као ризични: небезбедни WEB, небезбедни мобилни и *Cloud* интерфејси, потпуни недостатак енкрипције на транспортном слоју, угрожена приватности, лош небезбедан софтвер, небезбедне мрежне конекције. Један успешан напад на IoT систем има последице које се манифестују низом проблема као што су:

- угрожавање личне безбедности,
- оштећење опреме,
- оперативни проблеми и
- регулаторни
- проблеми .

Проблеми који настају могу бити оперативни и регулаторни. **Оперативни проблеми** проузрокују опадање квалитета производа и индустријских услуга, а у екстремним случајевима чак и ускраћивање индустријске услуге крајњим корисницима. **Регулаторни проблеми** настају када су напади преко интернета покренути из друге државе или са другог континента, и односе се на надлежности за истрагу и правно санкционисање интернет криминала.

Безбедност IoT система је област која обухвата низ решења:

- Са системског нивоа решења су следећа: архитектура заштите, управљање ризиком и имплементација политике заштите,
- Са аспекта специфичних безбедносних механизма то су системи за детекцију и превенцију напада, шифрирање и механизми за аутентификацију, развој специјалних окружења за тестирање могућих решења и дефинисања процедура које се примењују у процесу експлоатације система.

Као и сви савремени производни системи и процеси у производњи , тако су и безбедоносне процедуре стандардизоване. Стандарди који обухватају безбедоносне процедуре су следећи:

- (1) стандарди и препоруке за безбедност. Односе се на безбедност информационих система и безбедност комуникационих система опште намене,
- (2) општи стандарди и смернице за безбедност IoT система и
- (3) специфичне смернице које се односе на решења заштите система и података у појединачним индустријским секторима.

Глобална непрофитабилна заједница индустрије, владиних организација и академских институција је основана 2014. године и управо представља **Индустријски Интернет конзорцијум (ИКС)**. Основни циљ овог конзорцијума је управо помоћ индустријским предузећима да имплементација IoT-а буде ефикасна. Ефикасност имплементације спроводи се путем идентификације, прикупљања, тестирања и промоције тзв. најбоље праксе. Следеће што треба поменути је ИКС радна група, ово је радна група за безбедност и управо ова радна група је креирала доношење општег оквира за безбедност IoT-а. Оквир за безбедност IoT-а обухвата:

- заштиту података,
- модел и политику безбедности,
- заштиту комуникација и повезивања,
- заштиту крајњих тачака (односи се на периферне делове система, облак),
- надзор и анализу,
- као и конфигурацију и
- управљање заштитом.

Рад на безбедности IoT започет је 2016. године, а пројекат се одвијао у оквиру америчког државног института за стандарде и технологију (*National Institute of Standards and Technology, NIST*). Овај пројекат о безбедности обухвата дефинисање оквира за интернет безбедност, инжењеринг безбедносних система, безбедност рачунарства у облаку, профиле за индустрију и производњу, и још много тога. Не треба да се изгуби из вида да је рачунарство у облаку централни и најважнији део IoT-, сви аспекти безбедности који се примењују на cloud окружење, по аутоматизму су примењени и на IoT.

IoT апликације користе у већини случајева већ постојећу опрему, сасвим је логично да на тај начин наслеђују безбедносне пропусте и недостатак безбедносних механизма који постојећа опрема са собом носи. Управо то је разлог што већина таквих уређаја не користи стандардизоване протоколе и гејтвеје, већ протоколе који су се користили у неким предходним периодима. Веома је битно за ефикасну заштиту IoT система да се сви његови делови изнова пројектују, имплементирају и атестирају у циљу заштите у својих компоненти и подсистема, пре интеграције у IoT и пуштања у имплементацију. Препорука је да се кориште универзални индустријски протоколи. У универзалне протоколе примера ради спада OPC UA (*Open Platform Communications Unified Architecture*). Принципи заштите OPC UA, протоколом подразумева поверљивост, интегритет и расположивост података, као и контролу приступа, да би ниво безбедности био на нивосу савремених стандарда и протокола.

Сегрегација је оодела мреже на логичке сегменте. Сегрегација је принцип поделе велике мреже на неколико логичких мрежа. Затим сегрегација обухвата спровођење политике за контролу комуникација између специфичних хостова и сервера у оквиру информационог система. Коришћење безбедносних механизма у свакој логичкој мрежи, омогућава да се ефикасно изолује свака логичка мрежа и да се лакше надгледају активности у тој мрежи.

Пример за примену овог метода је имплементациони модел који се заснива на слојевито организованим магистралама података.

За ефикасну заштиту једног пословног система значајну улогу има непрекидан надзор и анализа активности у мрежи, а све се одвија у циљу детекције и идентификације аномалија и сумњивих догађаја. Након тога лог фајлови представљају записе о свим обављеним акцијама, трансакцијама, процесима и омашинама. **Анализом лог фајлова** веома лако је лоцирање и отклањање отказа уређаја, сензора, актуатора, чак и машина, затим детекција аномалија је значајно олакшано и прегледно, а и утврђивање мрежне форензике је могуће на доста прецизнији начин него у предходним системима. Након лог фајлова врши се **анализа дампа** фајлова, ова анализа омогућава детекцију познатих и непознатих малициозних активности присутних у RAM меморији система. Поред анализе лог фајлова веома је значајна и анализа **мрежног саобраћаја**. Ова анализа обавља се да би се детектовале неправилности у саобраћају података. Ова врста анализе обухвата анализу понашања и анализу узорака саобраћаја. Анализа се обавља по принципу пакета или по принципу саобраћајних токова.

Метод атрибуције напада, је откривање идентитета и локације нападача. Овај метод изузетно је битан када су напади извршени из друге државе, због регулаторних питања дипломатских послова.

Дошли смо до алати за **детекцију малициозних активности и прокси решења**, односно до заштитних “заштитне зидове” (*firewall*). Обичним рачунарским корисницима познат је појам заштитног зида. У пословним системима то су системи за детекцију и превенцију напада, антивирусни програми. Што се прокси решења тиче у њих спадају **филтрирање пакета и контрола приступа**. Прокси решења се користе да формирају заштитни слој око слабије обезбеђених или технолошки старијих компонената. Под појмом одржавање система, сматрамо редовно тестирање незаштићености система и неопходно га је примењивати због детектовања нових и непознатих претњи. Притом **Update** је веома битна ставка, због ажурних верзија софтвера и софтверских додатака, веома је важно редовно обављати надоградњу система, јер је то једна од основних предиспозиција за откривање најновијих вируса и малициозних напада.

Постоје четири градивна блока функционалне архитектуре заштите IoT система:

- заштита крајњих тачака,
- заштита комуникација и повезаности,
- надзор и
- анализа механизма заштите и безбедности и управљање механизмима безбедности.

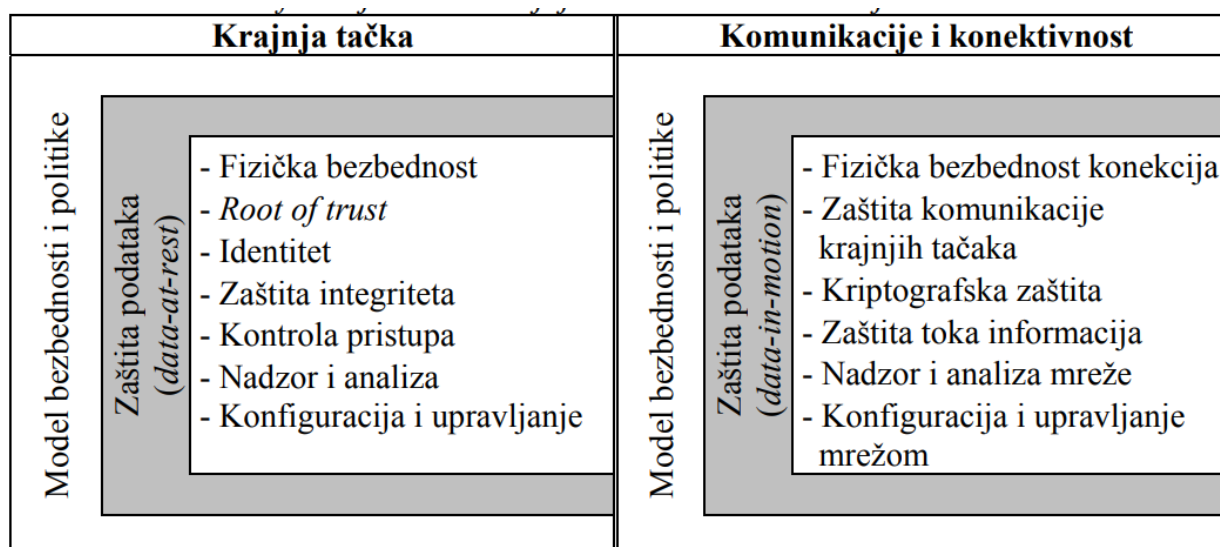
Блок за заштиту крајњих тачака односи се на заштитне механизме у уређајима на периферији мреже и у облаку. У основне функције овог блока спадају: физичка безбедност уређаја, интернет безбедност уређаја и управљање идентитетом.

Блок за заштиту комуникација и повезаности ради по принципу управљања идентитетом. Користи се за имплементацију аутентификације и ауторизације саобраћаја. У случају када су крајње тачке заштићене и комуникације обезбеђене, стање система

обезбеђује се током оперативног циклуса. Тако да надзором и анализом механизма безбедности и контролом конфигурације заштите свих компоненти система, постиже се одређени ниво заштите система.

Функција заштите података пружа подршку за сва четири претходно описана градивна блока. Функција заштите се примењује на све врсте података. Почевши од неактивних података, који се чувају у крајњим тачкама, односно на удаљеним серверима или у облаку, до података који се обрађују и преносе у комуникационом слоју система. Функција заштите такође обухвата податке конфигурационе и управљачке природе, али и податке прикупљене у процесима надзора и анализе.

Модел безбедности подразумева управљање свим функционалним елементима система. Направљен је тако да одређује начин имплементације заштите и политике заштите система. Политика заштите и начин имплементације заштите гарантују за: поверљивост, интегритет и расположивост ИИоТ система током оперативног циклуса. То су веома битне ставке за оптимално управљање системом.



Слика 12. Структура фаункција заштите крајњих тачака и комуникације²⁵

Заштита крајње тачке обухвата:

- дефинисање компоненте која ће бити компонентаод апсолутног поверења у криптографском систему, полазна криптографска компонента (*root of proof*),
- дефинисање јединственог идентитета крајње тачке,

²⁵ Извор:

<http://postel.sf.bg.ac.rs/simpozijumi/POSTEL2019/RADOVI%20PDF/Telekomunikacioni%20saobracaj,%20mreze%20i%20servisi/8-Stojanovic-Bostjancic-Rakas-Markovic-Petrovic.pdf>

- заштиту интегритета,
- контролу приступа,
- надзор и анализу,
- као и конфигурацију заштите и
- редовно ажурирање заштитних полиса.

Заштита комуникација и повезивања подразумева:

- физичко обезбеђивање конекција,
- заштиту комуникација између крајњих тачака,
- криптографске заштитне механизме,
- Заштиту токова информација, надзор и анализу напада, у то спадају контрола приступа мрежи, анализа логова и још много тога,
- као и конфигурацију заштите и управљање мрежом.

6. ПРИМЕНА IoT АПЛИКАЦИЈА У УПРАВЉАЊУ ОДРЖАВАЊЕМ У ПРОИЗВОДЊИ

Основни циљеви које треба остварити приликом организације и планирања решења су:

- да је предложено решење примењљиво за производне погоне без IT инфраструктуре,
- да решење које приступа реализацији максимално искористи постојеће ресурсе,
- да је решење дугорочно одрживо захваљујући коришћењу сензорских мрежа и IoT платформе водећих произвођача који гарантују његов даљи развој, одржавање и подршку,
- да је почетна инвестиција за решење које се реализује минимална и да купац плаћа само за оно што користи.

У пракси најчешће се примењује следећа архитектура решења на четири нивоа:

- Аквизиција података,
- Пренос податка,
- IoT платформа,
- Напредна аналитика и машинско учење.

Аквизиција података подразумева да се прикупљају подаци са постојећих уређаја и подаци са постојећих сензора (4-20mA), као и са додатних сензора. Додатне сензоре је неопходно поставити тако да би се лакше прикупили недостајући подаци за управљање одржавањем система.



Слика 13. Сензорски чвор за прикупљање информација са производних машина²⁶

²⁶ Извор: Dejan DAMNJANOVIĆ, PRIMENA INTERNET OF THINGS (IOT) REŠENJA U UPRAVLJANJU ODRŽAVANJEM U PROIZVODNJI, Atoms and Bits, 2017.

Код **преноса података** могуће су различите конфигурације. Ако се користи већи број сензорских чворова економски је оправдано да се користи уређај, који се инсталира локално у фабрици и који пружа могућност да се повеже велики број сензорских чворова путем радио везе мале снаге. Овај начин повезивања сензорских чворова, решава и проблеме непостојања приступа електричној и рачунарској мрежи, на тачно одређеним локацијама где се постављају сензорски чворови, . Поред тога овај уређај, који повезивање врши путем радио таласа, може поседовати и локалну меморију података, на тај начин се обезбеђује самосталност система када дође до отказа везе или отказа преноса података са централним системом. Иначе комуникација се може обавати и путем мреже мобилних оператера као и Wi-fi путем комуникације.

IoT платформа направљена је тако да има улогу да управља са неколико врсти компоненти, кључне компоненте којима управља су:

- **IoT HUB** компонента служи за комуникацију са сензорским чворовима. Та комуникација треба да пружи поузданост и сигурност. *IoT HUB* може да прихвати велики број, порука у кратком временском интервалу, а то је особина која се назива скалабилност. Како би се постигао висок ниво безбедности *IoT HUB* проверава идентитет сваког уређаја који му шаље податке.
- **Процесори токова података** податке добијају преко *IoT HUB*-а. Иначе то су софтверске компоненте које имају могућност да прихватају и обрађују податке у реалном времену. на основу унапред дефинисаних правила формирају се упозорења, у случају да вредност одређеног параметра достигне граничне вредности. Сви приспели подаци смештају у јединствено складиште ради дугорочног чувања. Зато што није довољно пратити само појединачне вредности, да би се правовремено креирало упозорење, ова компонента омогућава и анализу комплексних догађаја који настају кроз интеракцију токова података са већег броја сензора и поређење ових добијених вредности са ранијим вредностима. Аларми који су уграђени у систем се углавном приказују на порталу или прослеђују пословним апликацијама које покрећу одговарајуће радне процедуре.

Што се процесора тиче догађаји генерисани са процесорске стране могу бити прослеђени на ниво **напредне аналитике и машинског учења**. У процесу напредне аналитике, врши се уочавање законитости анализом великих скупова података. Тај процес је сам по себи сувише веома сложено за људе и препушта се техникама вештачке интелигенције, односно техникама софтверске обраде. У процесу машинског учења примењују се статистичке технике над великом количином података у потрази са обрасцем који најбоље описује одређени проблем. На тај начин креира се модел. Модел се претвара у програмски код.

7. КРАТАК ОСВРТ НА БЕНЕФИТЕ IoT АПЛИКАЦИЈА У САВРЕМЕНИМ ПРОИЗВОДНИМ ПРОЦЕСИМА У ВРЕМЕ ПАНДЕМИЈЕ Covid-19

Сведоци смо дешавања да је читав свет погођен пандемијом широких размера, услед вируса коме се још увек прецизно није стало на пут, смртност је изузетно велика, и скоро све земље света су у неком тренутку биле приморане да уведу ванредне мере услед доласка смртоносног вируса. Осим промене начина живота промениле су се и околности у пословном окружењу. Многе фабрике биле су принуђене да раднике пошаљу на принудне одморе или су тражиле друге моделе да пошуљу људе кућама, само да би се спасили људски животи.

У Србији IoT апликације у производним процесима нису заживеле у великом проценту. Без обзира што је примарни циљ да се смање трошкови и успостави бржа и ефикаснија комуникација са крајњим корисником, недостатак IoT система довео је до колапса. Из вида не треба изгубити податак да су главни произвођачи аутомобила у Европи, за време короне затворили компаније. Резултат свега тога је да је дошло до прекида целих ланаца вредности. Са друге стране у компанијама где су настављени процеси рада, повећане су одговорности запослених и особља.

Тамо где је довољно развијен и имплементиран Индустријски IoT у овом тренутку може помоћи компанијама док наставе са процесом пословања. Генерално то је систем који је током предходних година пронашао своју примену у многим производним системима, али наравно, као и увек постоје скептици, према свему, па и према овом систему. Веома мали број компанија ће се одлучити за IoT да би наставио процес рада, у временима кризе или пандемије, а нарочито ако то већ није био део њихове делатности, то представља додатни ризик пословања.

Једног дана када дође до стабилизације пандемије и када се буду успостављали нормални токови пословања и производње, приоритет ће на првом месту увек да буде да се смање трошкова. Наравно смањење трошкова у што краћем року временском року, је приоритет Индустријски произвођачи могу имати користи од краткорочног смањења трошкова, а неколико алата који подржавају IoT могу помоћи у том погледу и то су:

- **Дигитално управљање перформансама.** Подразумева се да софтверска решења заснована на IoT апликацијама могу пружити realtime контролну таблу где су приказани кључни показатељи перформанси за подршку прегледа перформанси на продајним местима, повећавајући транспарентност. У раду је већ изложена и још једна особина ове врсте алата који омогућавају праћење акција побољшања и шаљу упозорења оператерима преко мобилних уређаја.
- **Даљинска помоћ,** свакако је од великог значаја у новонасталим, условима. Поред побољшања безбедности запослених, искуство показује да алати за помоћ на даљину и одржавање могу довести до 10 до 20 посто смањења трошкова теренских услуга, посебно путовања, смањујући потребу за личним посетама. Уштеда је нарочито висока код произвођача машина са великом инсталираном базом.
- **Повезивање и cyber безбедност** утичу на безбедност у ланцу снабдевања, омогућавајући индустријама брже реаговање на поремећаје. Време потребно за

побољшање повезаности и кибернетичке сигурности варираће, у зависности од оперативног подешавања компаније, укључујући и број машина и софтверских решења.

- **Транспарентност набавке** у реалном времену. Овде акценат треба ставити на realtime информације јер су оне од од кључног значаја из разлога што сам алат IoT на тај начин помаже компанијама у оптимизацији набавки, а све се базира на информацијама у реалном времену. На тај начин манипулише се са реалним подацима.
- **Извођење повезивања великог обима**, често се дешава да компаније буду у позицији да запосленима омогуће даљински приступ на машине, да би неки посао био обављен. Будући да многе машине сада имају дуже од уобичајеног застоја, компаније ће свакако бити у прилици да инсталирају интерфејс на њих. Препорука је да би се убрзало извођење, да радници би могли инсталирати кутију за повезивање сваки пут када обављају услуге рутинског одржавања. Свака машина која је повезана на интернет. То је од велике помоћи произвођачима из разлога што то постаје машина доступна за даљинско надгледање, прикупљање информација и друге услуге.

Чињеница је да ће се много тога променити у пословном свету и у животу уопште, дистанца која је постала основна животна форма промениће много тога, од система школовања, преко трговине, производње и тржишта уопште, здравство не треба ни помињати. Са аспекта паметних фабрика у будућим временима сви процеси ће се темељити на:

1. Развоју уникатних производа,
2. *PLM* – *Saas* системи ће бити примењивани да би се развијали уникатни производи, на овај начин омогућиће се развој поступака израде, монтаже и контроле у стандардизованом облику за постпроцесирање на производним облацима, подаци ће се преко облака сакупљати током целог животног века производа,
3. Основна производна јединица је радни-услужни-контролни-монтажни облак, а неке машине ће бити на точићима и сами ће директно обликовати производна облака с обзиром на технолошки поступак појединог производа,
4. Производни системи ће бити децентрализовани, високо флексибилни,
5. Аутоматизација и роботика ће се променити уз сарадњу човека и машина. Због аутоматизације уводи се сасвим нови концепт поделе послова. Радно место се дели на тежи физички рад, и тај посао обавља робот и лакши односно стваралачки који обавља човек,
6. Полупроизводи, алати и производи комуницирају међусобно, са машинама, програмима и особама,
7. Логистика након производње изводиће се помоћу транспортних средстава (виљушкар, аутоматских колица, ...) на темељу ажурних података о производима,
8. Планирање логистике производа након производње биће децентрализовано,

9. У производњи конкретно паметна производња подразумева да се производи производе за тачно одређена на која производна острва и све је софтверски дефинисано, чак и софтверу за које обраде ће се транспортовати уз помоћ аутоматских колица,
10. Одржавање ће бити предиктивно, предвидиво из разлога што ће се захвати одржавања која се темље на трендовима, већ измерених параметара процеса и машине,
11. Квалитет ће се темељити на контроли процеса производње и монтаже током процеса,
12. Технолошки поступци, односно програмски модули који се односе на израду, монтажу и контролу, биће развијени са САх алатима,
13. Базе података биће на удаљеним серверима код провајдера са којима је компанија склопила уговор, односно биће у облаку,
14. Комуникације ће бити бежичне са агилним-мобилним (делимично и стационарним) терминалима,
15. Унос података биће аутоматизован, а изузетно добро биће развијен говорни интерфејс, затим биће уведени екрани осетљивимна додир и камерама,
16. Израда података о производним процесима биће аутоматизована са аналогним сензорима и мерачима, мерачима пута, брзине, прекидачима и процесним системима. А правовремено ће бити укључено аутоматско дијагностификовање и визуелизација процеса и њихових одступања или грешака,
17. Производни облаци састављени од обрадних, услужних, монтажних и контролних машина, биће конструисане за индивидуалне производе, који ће са собом носити технолошке, услужне и контролне поступке, којима ће се исте прилагођавати у ходу,
18. Свака машина у коадној производњи имаће управљање које комуницира с другим машинама, производима, особама и програмима у мрежи,
19. Едукација ће се одвијати прво у школи, а затим сваки дан на радном месту у производњи преко мултимедијске едукације до одласка у пензију.

Паметна фабрика је еколошки оптимална, стога јој предвиђају локацију усред насеља. Са друге стране материјална егзистенција људи биће задовољена, осигурана радна места и на овај начин омогућен рад запосленима чак и у време пандемије као што је ова, у случају неких других нежељених околности. Зато ово и јесте индустријска револуција 4. Самим тим мења се читав светски поредак. Поједини научници предвиђају да са увођењем 5G мреже све добија на квалитету и брзини, интернет великих брзина управљање IoT апликацијама значајно убрзава, што се додатно огледа у смањењу трошкова и олакшаног рада на даљину.

IoT компоненте и апликације пронашле су примене у свим сферама живота, тако да у свету већ постоје паметне кеће, паметне радње, паметни бутици, паметне лекарске ординације. Било како било у будућности свет ће изгледати потпуно другачије.

ЗАКЉУЧАК

Док се није појавила пандемија и окренула живот и рад људи у читавом свету предвиђања стручњака су била да се до 2020. године број "ствари" које су повезане интернетом превазиђе људску популацију чак до три пута. Од играчака за децу преко кућних апарата и машина до робота и аутомобила, ове ствари ће отпремити и преузети богате токове података.

На жалост то се у индустрији није остварило у проценту у ком су то стручњаци предвиђали. Али свакако не треба губити наду, можда је баш спас међународне индустрије и читавог светског пословања и економије баш у IoT системима. Прва ствар IoT апликације ће корисницима, омогућити да имају и даљински увид и приступ производњи, да фабрике могу нормално да функционишу и са смањеним бројем људи, једноставно да се креира једна нова потпуно непозната будућност, која ће кроз егзистенцију радних места и производних процеса омогућити да светска економија живи.

Време не може да стане.

ЛИТЕРАТУРА

1. Dejan Damjanović, *PRIMENA INTERNET OF THINGS (IoT) REŠENJA U UPRAVLJANJU ODRŽAVANJEM U PROIZVODNJI*, Atoms and Bits, 2017.
2. Преузето са Интернет странице (10.09.2020) <http://www.ivdamprocess.com/novosti/uvod-u-distribuirane-sisteme-upravljanja-kroz-emerson-deltav-dcs/>
3. Преузето са Интернет странице (10.09.2020) https://nastava.sf.bg.ac.rs/pluginfile.php/34208/mod_resource/content/1/OTS_9.pdf
4. Преузето са Интернет странице (10.09.2020) , <http://erpsusreti.rs/2017/prezentacije/p4.pdf>
5. Mirjana D. Stojanović, Slavica V. Boštjančič Rakas, Jasna D. Marković-Petrović, *BEZBEDNOST INDUSTRIJSKIH IoT SISTEMA*, Београд, 2019.
6. Доц.Др. Живко Бојовић, Увод у индустријски ЈоТ, Нови Сад, 2019.
7. Преузето са Интернет странице (11.09.2020) <https://elab.fon.bg.ac.rs/udzbenik-internet-inteligentnih-uredaja/uvod-u-internet-inteligentnih-uredaja/>
8. Преузето са Интернет странице (11.09.2020), <http://docplayer.rs/187258792-Dizajn-industrijskih-iot-sistema.html>
9. Преузето са Интернет странице (11.09.2020), <http://docplayer.rs/187258792-Dizajn-industrijskih-iot-sistema.html>
10. Преузето са Интернет странице (14.09.2020), <http://www.ivdamprocess.com/novosti/uvod-u-distribuirane-sisteme-upravljanja-kroz-emerson-deltav-dcs>
11. Преузето са Интернет странице (11.09.2020), <https://startit.rs/iot-101/>
12. Преузето са Интернет странице (11.09.2020), <https://www.securitysee.com/2018/06/industrija-4-0-dolazak-na-srpsko-trziste/>
13. Debasis Bandyopadhyay, Jaydip Sen