SEMINAR HO CIRED-a

HRVATSKOG OGRANKA MEĐUNARODNE ELEKTRODISTRIBUCIJSKE KONFERENCIJE
Zagreb, 14. ožujka 2024.

OTPORNOST NA KIBERNETIČKE PRIJETNJE U EES-u

Tema 6:

GOVERNANCE FUNKCIJA U KIBERNETSKOJ SIGURNOSTI IZMEĐU EKOSUSTAVA DIGITALNIH PLATFORMI I DIGITALNIH BLIZANACA

Razvoj digitalne platforme za izgradnju sustava zaštite kritičnih infrastruktura u pametnim industrijama – CIP4SI

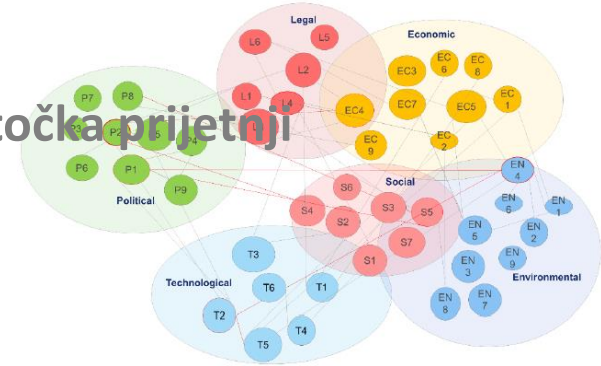
Prof. dr. Hrvoje Pandžić, FER; Prof. dr. Slavko Vidović, ILBA Institut; dr.sc. Stjepan Sučić, Končar Digital; mr.sc. Domen Verdnik

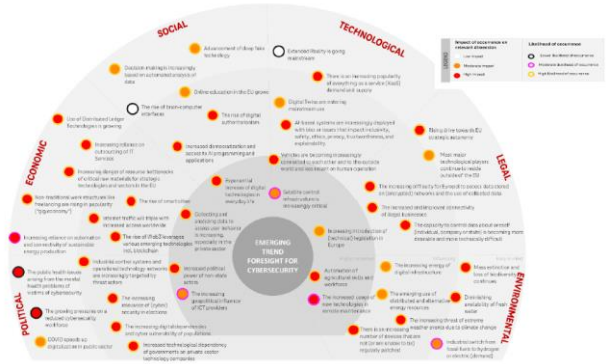
Sadržaj

1. Top 10 prijetnji kibernetičkoj sigurnosti
2. EU i izazovi
3. Propisi vs Smjernice
4. NIST CSF 2.0
5. Razumijevanje rizika i incidenata
6. Procesna arhitektura po BPF
7. Model upravljanja
8. CIP4SI - arhitektura
9. Poslovni subjekt u odnosu na rizike i prijetnje
10. CIP4SI
    - SCADA,
    - Samoprocjena i povećanje spremnosti
    - portal
    - Digital Twin
    - Blockchain (DLT)

TOP 10 prijetnji kibernetičkoj sigurnosti

1. Ugrožavanje lanca opskrbe softverskih komponenata
2. Napredne kampanje dezinformiranja
3. Porast autoritarnosti digitalnog nadzora/gubitak privatnosti
4. Ljudska pogreška i korištenje naslijeđenih sustava unutar kiber-fizičkih ekosustava
5. Ciljani napadi poboljšani podacima iz pametnih uređaja
6. Nedostatak analize i kontrole svemirske infrastrukture i objekata
7. Porast naprednih hibridnih prijetnji
8. Nedostatak vještina
9. Prekogranični pružatelji ICT usluga kao jedinstvena točka prijetnji
10. Zlouporaba umjetne inteligencije





EU i izazovi u području kibersigurnosti

Ključni sektori visoke rizičnosti kao što su:

- Energetika,
- promet,
- zdravstvo i
- financije
- .... kao i
- pružatelji javnih elektroničkih komunikacijskih mreža ili usluga
- digitalne usluge kao što su usluge društvenih mreža

ovise o digitalnim tehnologijama za obavljanje svojih osnovnih djelatnosti.

Vaš život na internetu: što EU čini kako bi bio jednostavniji i sigurniji?

EU aktivno radi na poboljšanju digitalnog okružja u korist svih Europljana i Europljanki. Naš digitalni život treba biti siguran, jednostavan i u skladu s temeljnim slobodama.

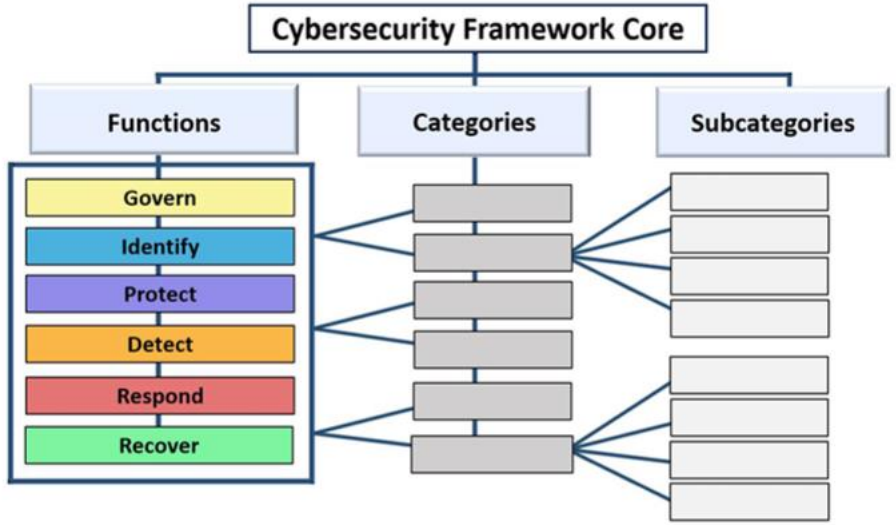
Pročitajte našu priču i saznajte kako EU štiti korisnike na internetu, osigurava kibersigurnost i olakšava razmjenu informacija među sustavima e-pravosuđa država članica EU-a.

Digitalizacija pruža goleme mogućnosti i rješenja za brojne izazove koji su pred Europom, kao hibridne prijetnje, krize uzrokovane bolešću COVID-19, elementarne nepogode, situacijom u Ukrajini a i **također izlaže gospodarstvo i društvo kiberprijetnjama.**

PROPISI VS. SMJERNICE - EU-SAD

- **Poboljšanje kibernetičke pripravnosti**
  - EU i SAD razvili su zakone ili mjere za rješavanje problema.
    - EU je proveo Direktivu o sigurnosti mrežnih i informacijskih sustava - **Direktiva NIS 2**
    - SAD je stvorio **NIST Framework**, skup dobrovoljnih standarda i najboljih praksi u industriji koji pomažu organizacijama, identificiraju, određuju prioritete i upravljaju kibernetičkim rizicima.
- **Iskoristiti najbolje dostupne mjere kibersigurnosti**
  - Direktivu NIS 2 i okvir NIST-a pozivaju državne subjekte i organizacije privatne industrije da iskoriste najbolje dostupne mjere kibersigurnosti za povećanje ukupne otpornosti sustava. Direktiva NIS 2 te mjere naziva "najsuvremenijim" sigurnosnim pristupima, dok ih okvir NIST-a smatra "najboljim praksama industrije".
- **Nema univerzalnog rješenja**
  - Direktiva NIS 2 i okvir NIST-a zahtijevaju od svojih jurisdikcija da provedu mjere kibersigurnosti koje imaju smisla - **ono što je prikladno za jednu organizaciju možda nije najbolje rješenje za drugu**.
- **Posebna agencija za kibersigurnost usmjerena na zaštitu ključnih infrastruktura**
  - Obje regije uspostavile su agencije za kibersigurnost usmjerene na zaštitu ključnih infrastruktura.
    - EU je 2018. poduzeo mjere u svojem Aktu o kibersigurnosti, kojim je obnovljen mandat **Agencije EU-a za mrežnu i informacijsku sigurnost – ENISA**.
    - SAD je iste godine djelovao sa Zakonom o CISA-i iz 2018., zakonom kojim se osniva Agencija za kibernetičku sigurnost i infrastrukturu (CISA)

NIST Cybersecurity Framework (CSF) 2.0



CIP4SI: Imamo li isto razumijevanje rizika

Što je **rizik**:

- ✓ Moramo imati ranjivost;
- ✓ Mora postojati prijetnja toj ranjivosti;
- ✓ Netko ili nešto mora biti spremno iskoristiti tu ranjivost.

Da bi se **rizik ostvario**, potrebno je **sve troje** – ne radi se samo o ranjivosti, već i o tome može li je prijetnja iskoristiti i hoće li je iskoristiti - Organizacije moraju sagledati vlastiti profil rizika.

Uvijek pokušati vratiti stvari na jednostavne. Jedine dvije stvari koje zapravo pokušavate i morate shvatiti su:

1. **O čemu se zapravo trebam-o brinuti?**
2. **Kako da riješim-o te brige?**

Ako se može odgovoriti na ta pitanja u šest ili sedam procjena rizika - briljantno.
(ne treba raditi 200 kompliciranih stvari jer to neće pokazati ono što trebate znati)

Organizacija mora biti u mogućnosti pokazati na nešto i reći:

To je ono na što se moram usredotočiti. Tu leži moj pravi rizik, s kojim stvarno moram nešto poduzeti.

(Sve ostalo je samo buka!)

Što je značajan incident prema NIS 2

Direktiva NIS 2 navodi samo obveze izvješćivanja iz članka 23.

Incident je

događaj koji ugrožava dostupnost, autentičnost, integritet ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje nude mrežni i informacijski sustavi ili koji su dostupni putem mrežnih i informacijskih sustava.

NIS 2 zahtijeva prijavljivanje samo značajnih incidenata.

Značajan incident definira kao

"svaki incident koji ima značajan utjecaj na pružanje "usluga koje pružaju ključni i važni subjekti, ako:

(a) prouzročila je ili može uzrokovati ozbiljne operativne poremećaje usluga ili financijske gubitke za dotični subjekt;

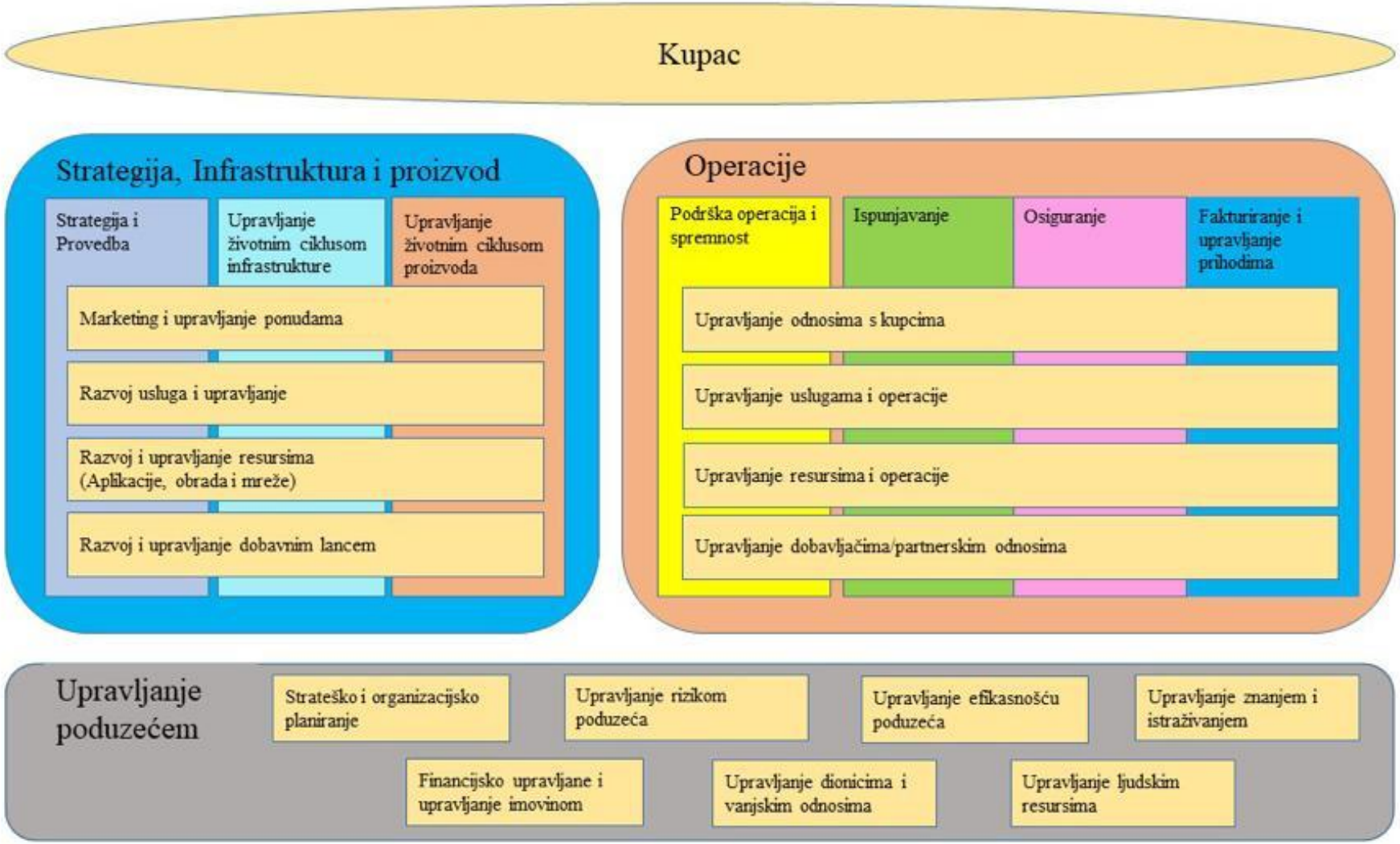
(b) utjecala je ili može utjecati na druge fizičke ili pravne osobe uzrokujući znatnu materijalnu ili nematerijalnu štetu."

U uvodnoj izjavi 101. u preambuli NIS 2 navodi se:

"Pokazatelji kao što su opseg u kojem je funkcioniranje usluge pogođeno, trajanje incidenta ili broj pogođenih primatelja usluga mogli bi imati važnu ulogu u utvrđivanju je li operativni poremećaj usluge ozbiljan."

Ključni i važni subjekti moraju prijaviti značajne incidente, dok ne postoje zahtjevi za prijavljivanje drugih vrsta incidenata.

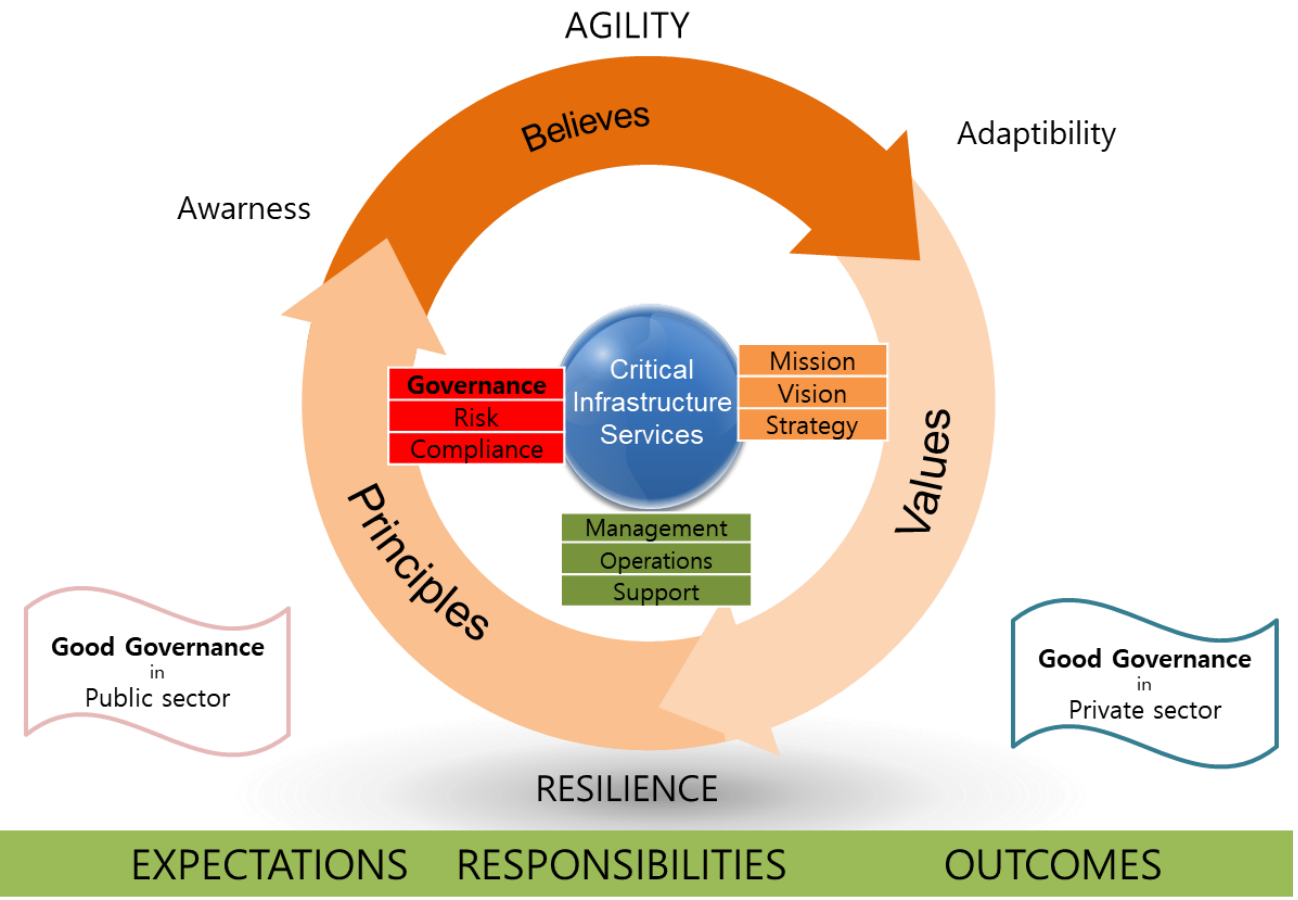
CIP4SI - Procesna arhitektura po BPF okviru od TMF

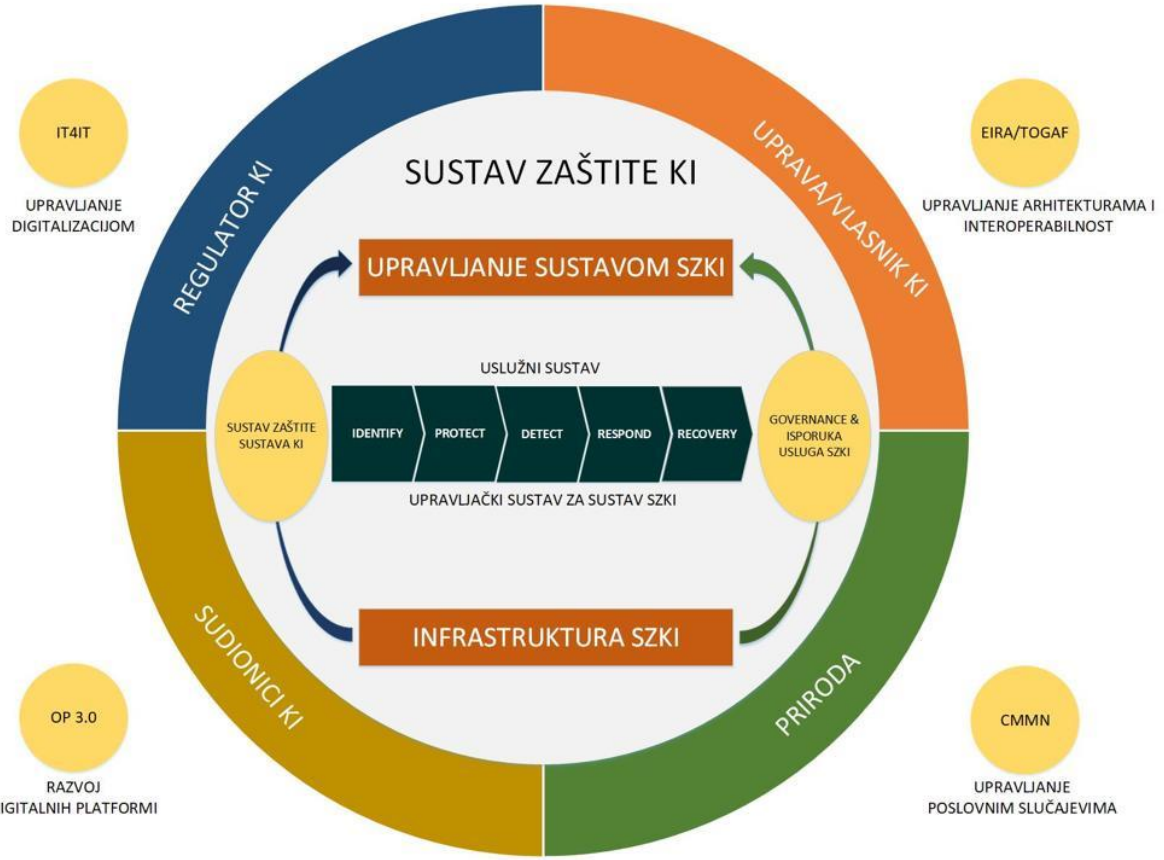


Model upravljanja kibernetičkom sigurnošću

1. Pravna regulativa
2. Dobro upravljanje
3. Upravljanje rizicima
4. Sigurnosna kultura
5. Upravljanje tehnologijama
6. Upravljanje incidentima

CIP4SI - GOOD GOVERNANCE





CIP 4 SI

Naziv projekta		Razvoj digitalne platforme za izgradnju sustava zaštite kritičnih infrastruktura u pametnim industrijama – CIP 4 SI
Trajanje:		**29 + 3 mjeseci** (od datuma definiranog u Ugovoru) – **17.03.2021. – 18.11.2023.** - Faza 1: Industrijsko istraživanje od početka do 16.07.2022. - Faza 2: Eksperimentalni razvoj od 17.07.2022. do 18.11.2023.
Prijavitelj: Partneri:		InfoDom d.o.o. Zagreb 1. KONČAR - INŽENJERING ZA ENERGETIKU I TRANSPORT d.d. 2. BEYONDI d.o.o. za marketing, dizajn i usluge 3. SVEUČILIŠTE U ZAGREBU FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

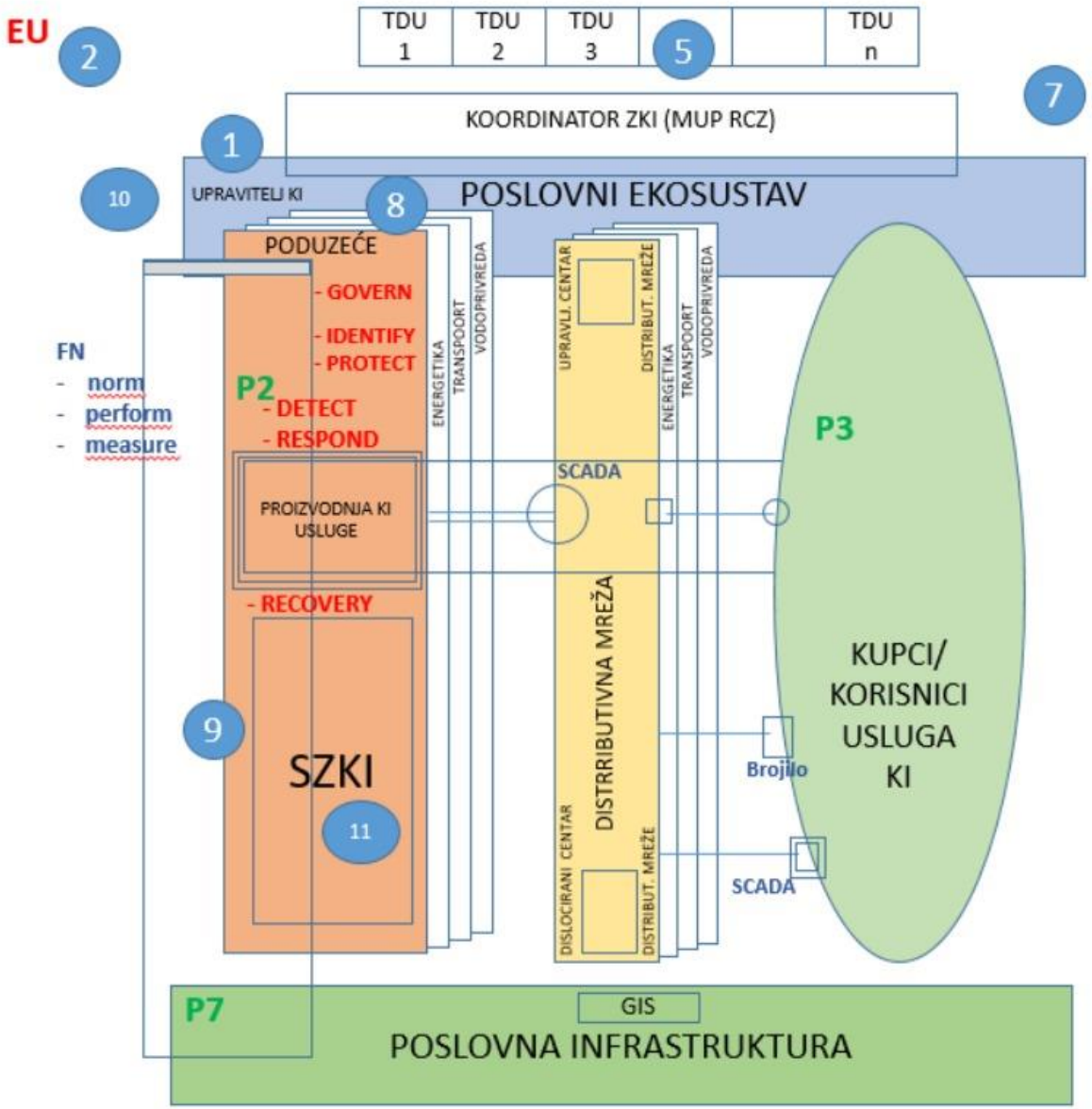
U fokusu projekta je razvoj proizvoda i usluga vezanih primarno za alineju 3 Tematskog područja 4 važeće Strategije pametne specijalizacije RH – Sigurnost:

- PTTP1- Kibernetička sigurnost): zaštitu kritičnih infrastruktura (određenih ZKI zakonom, a posebno povezanim na pametne industrije);
- TPP 2 Strategije (Energija i održivi okoliš);
- PTPP 1. Energetske tehnologije, sustavi i oprema; posebno u dijelu doprinosa razvoju pametnih energetskih sustava.

Četiri **proizvoda / usluge**, te ih ponuditi postojećim i potencijalnim korisnicima (vlasnicima KI i tvrtkama koje upravljaju zaštitom KI), primarno na tržištu EU, a zatim i na svjetskom tržištu, koristeći postojeće mreže partnera i klijenata:

1. **Digitalna platforma za uspostavu i potporu sustava zaštite kritične infrastrukture te za sigurnost upravljačkih sustava poduzeća u pametnim industrijama (sa pripadnim fleksibilnim komponentama).**
2. **Usluge razvoja digitalnih ekosustava za potporu sustavima zaštite kritičnih infrastruktura te razvoj sigurnosti upravljačkih sustava poduzeća u pametnim industrijama.**
3. **Smart-SCADA platforma (Končar – proširenje na SZKI, sa postojećih SUS)**
4. **SZKI GRC- Compliance**

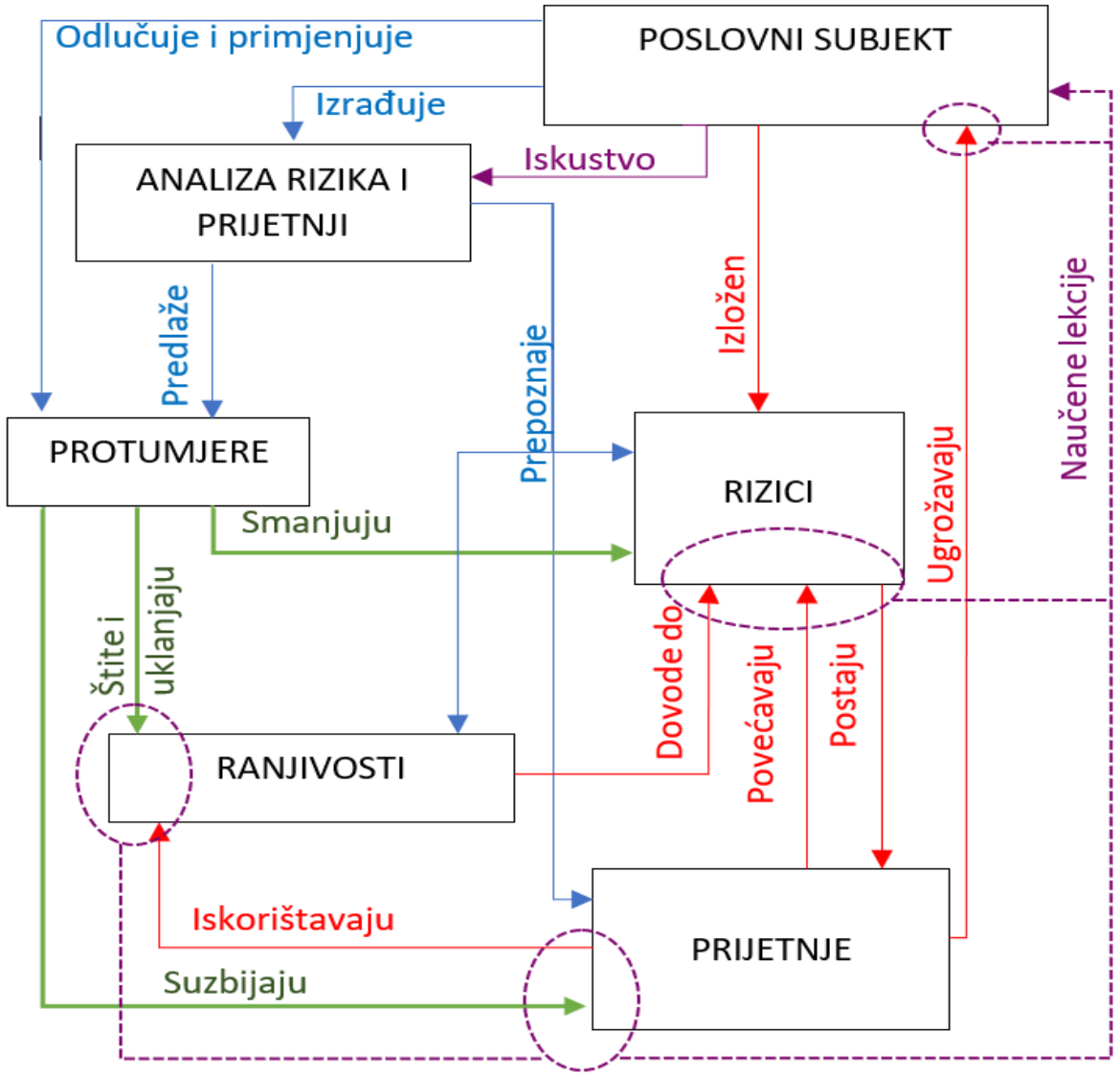
CIP4SI EKOSUSTAV - GOOD GOVERNANCE



N **Pojmovi iz Zakona o kritičnim infrastrukturama**

1. *Analiza rizika*
2. *Europska kritična infrastruktura*
3. *Međusektorska mjerila*
4. *Osjetljivi podaci*
5. *Kontaktna točka*
6. *Sektorska mjerila*
7. *Sigurnosni koordinator za kritičnu infrastrukturu*
8. *Sigurnosni plan vlasnika/upravitelja*
9. *Upravljanje kritičnom infrastrukturom*
10. *Vlasnici/upravitelji*
11. *Zaštita kritične infrastrukture*

Poslovni subjekt u odnosu na rizike i prijetnje



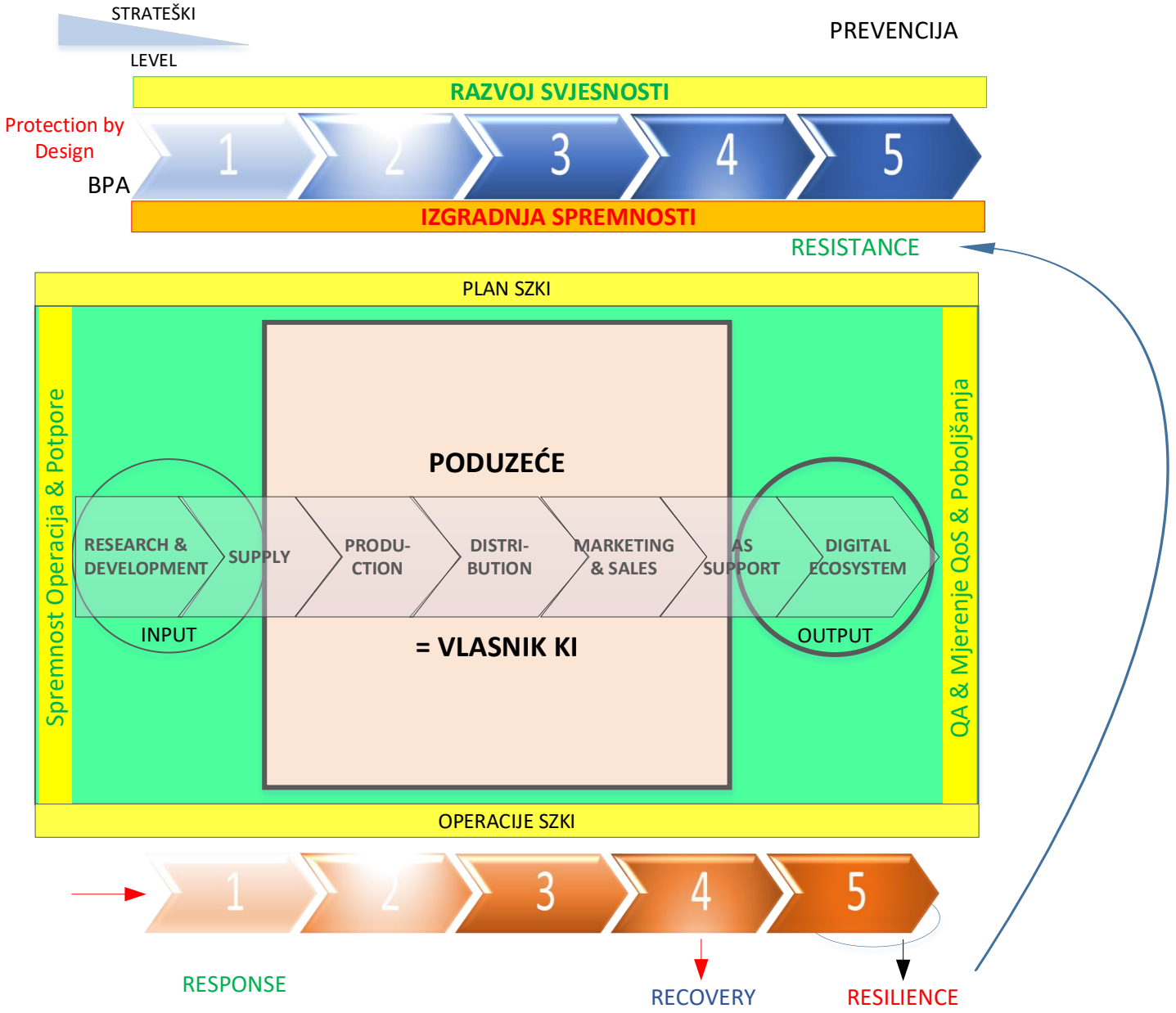
Plavom bojom prikazan je odnos i povezanost preventivnih djelovanja poslovnog subjekta u procesima prepoznavanja vlastitih slabosti, rizika s kojima se može suočiti te vlastitih sposobnosti koje može iskoristiti kako bi se suočio s pojavom prijetnji.

Crvenom bojom označen je odnos ranjivost-rizik-prijetnja u poslovnom procesu, moguća pojava prijetnji, kao i njihovo maliciozno djelovanje.

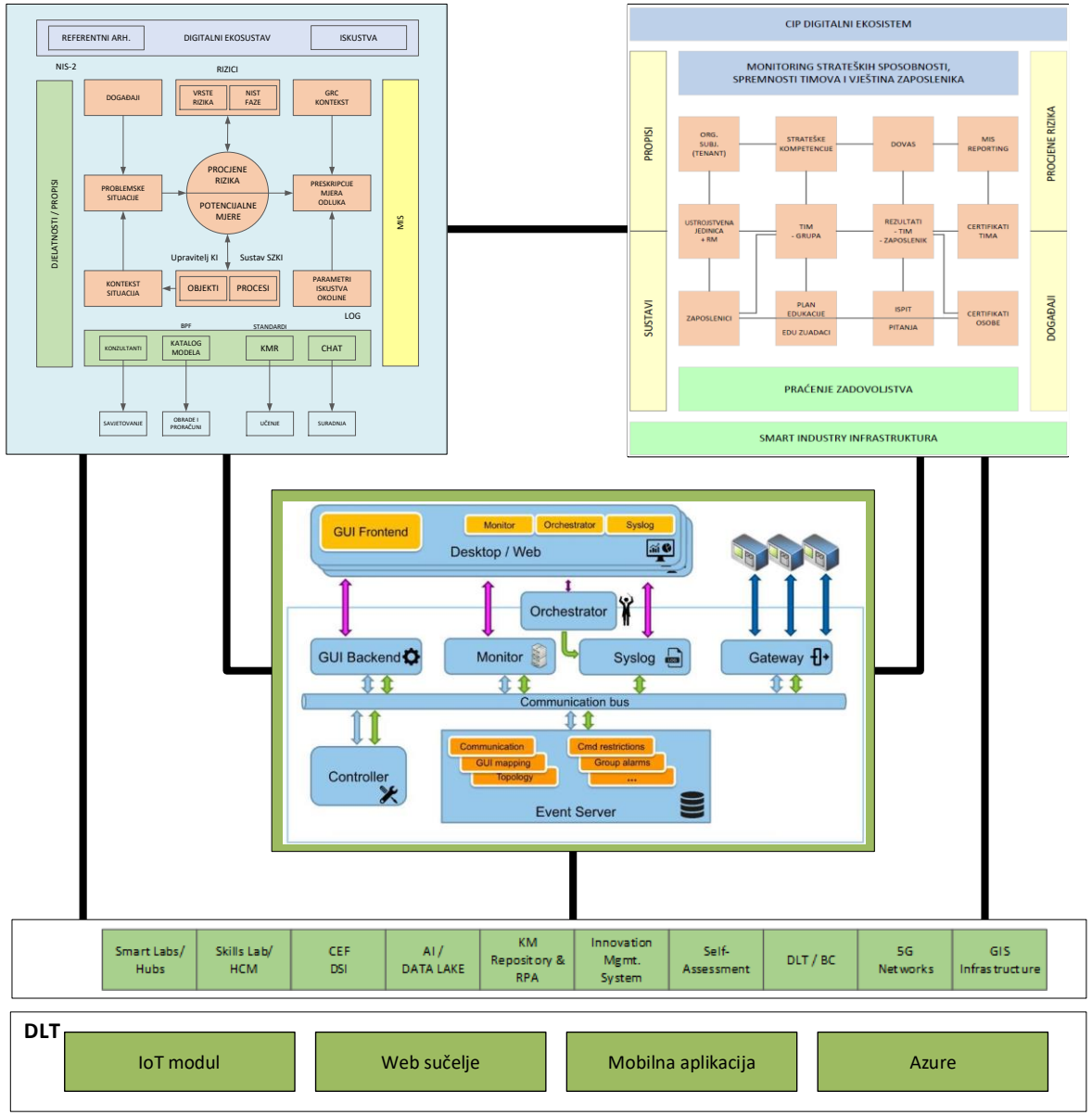
Zelenom bojom prikazani su procesi i aktivnosti obrambenih (preventivnih i reakcijskih) djelovanja koje je neophodno pokrenuti prije kao i tijekom pojave prijetnji.

Bordo bojom označen je proces učenja sustava o posljedicama njegove (ne)izloženosti određenom riziku i transformaciji rizika u prijetnju.

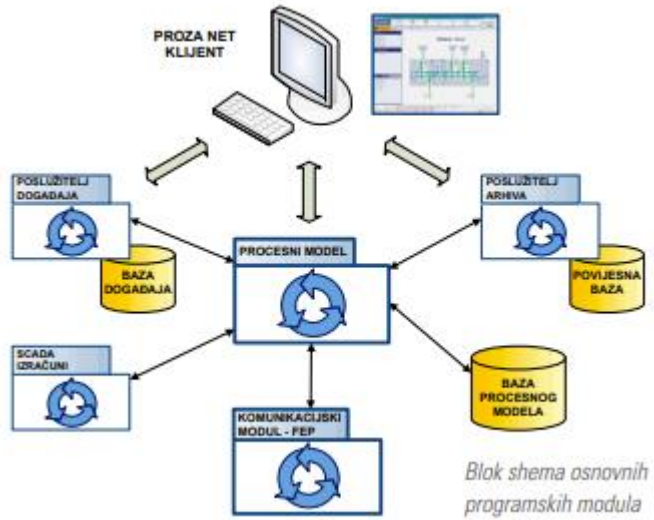
Sustav ZKI


STRATEŠKI
LEVEL
PREVENCIJA
RAZVOJ SVJESNOSTI
Protection by Design
BPA
1
2
3
4
5
IZGRADNJA SPREMNOSTI
RESISTANCE
PLAN SZKI
Spremnost Operacija & Potpore
PODUZEĆE
RESEARCH & DEVELOPMENT
SUPPLY
PRODU-CTION
DISTRI-BUTION
MARKETING & SALES
AS SUPPORT
DIGITAL ECOSYSTEM
INPUT
OUTPUT
= VLASNIK KI
QA & Mjerenje QoS & Poboljšanja
OPERACIJE SZKI
1
2
3
4
5
RESPONSE
RECOVERY
RESILIENCE

CIP4SI – Ukupna arhitektura digitalne platforme

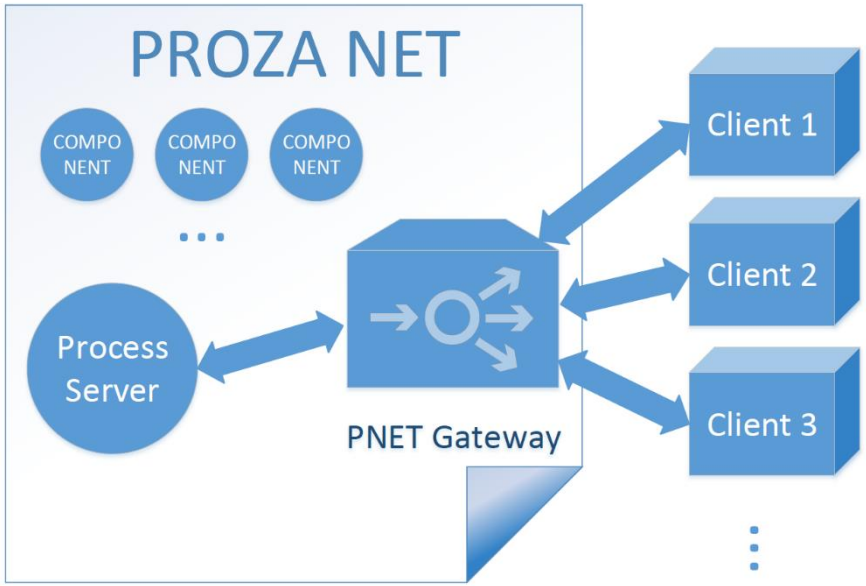


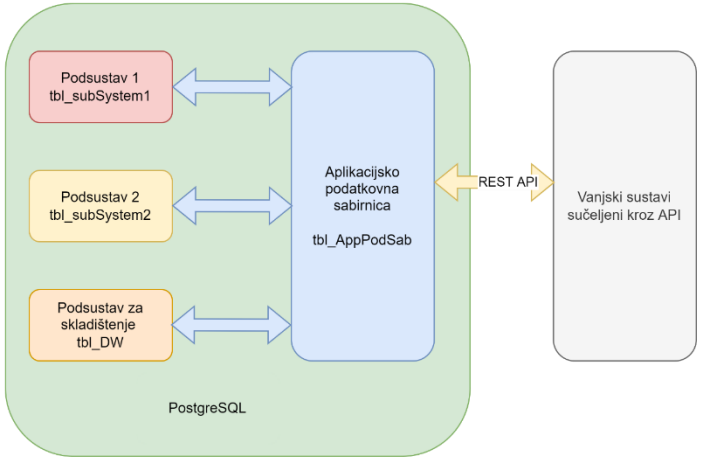
CIP4SI – SCADA



Blok shema osnovnih programskih modula

Sofverska arhitektura

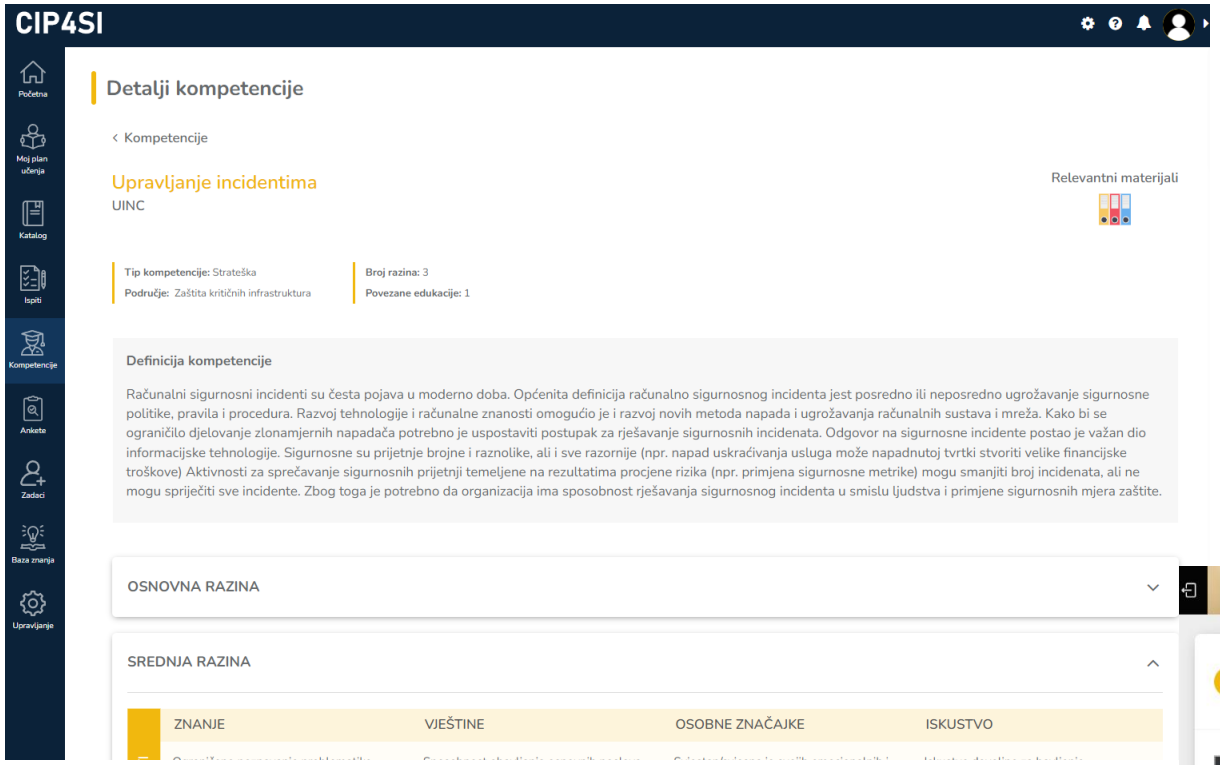


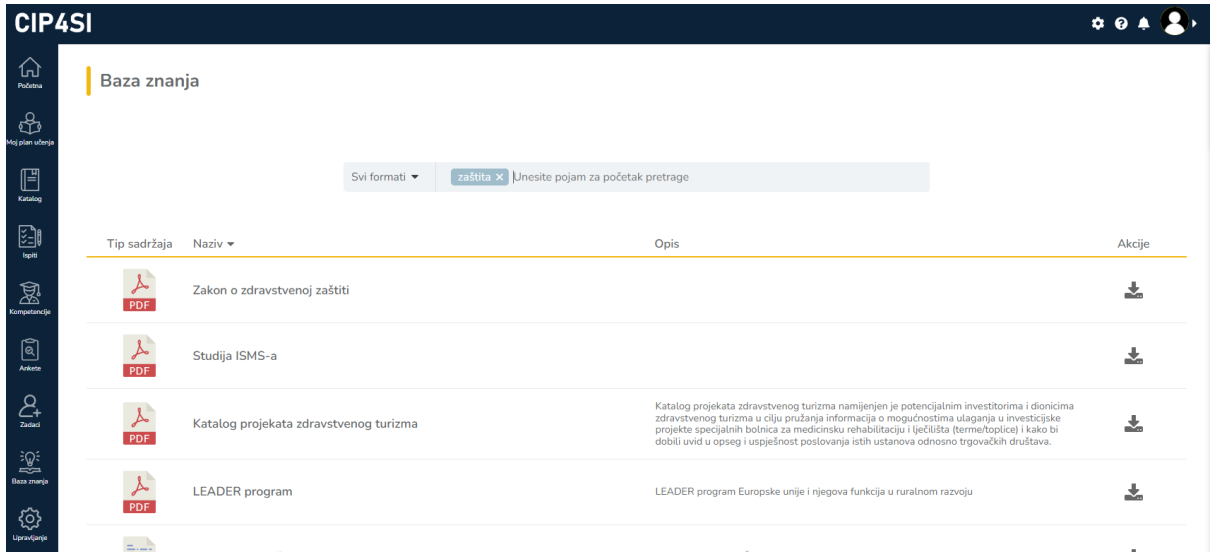


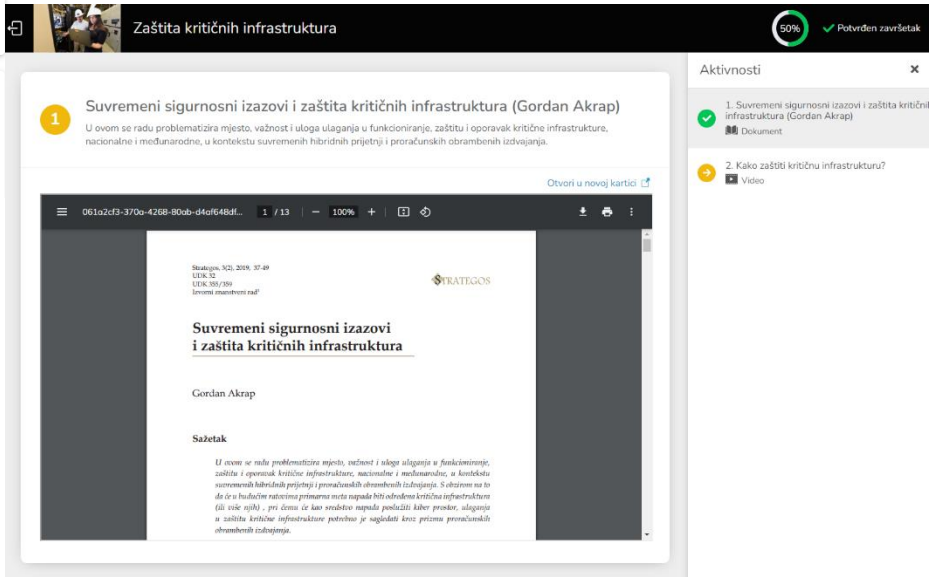
Implementacija podatkovne sabirnice

Tijek slanja procesnih podataka na platformu

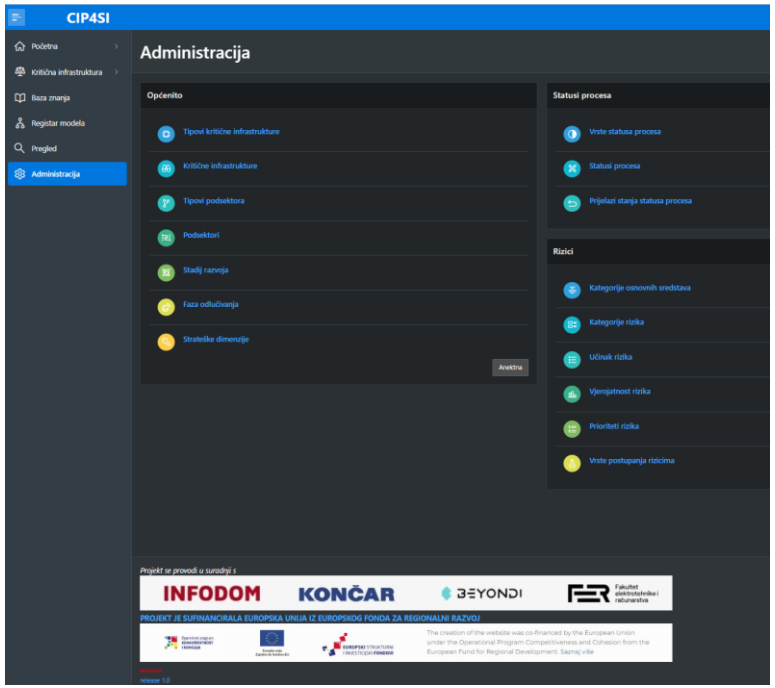
CIP4SI – Samoprocjena i povećanje spremnosti

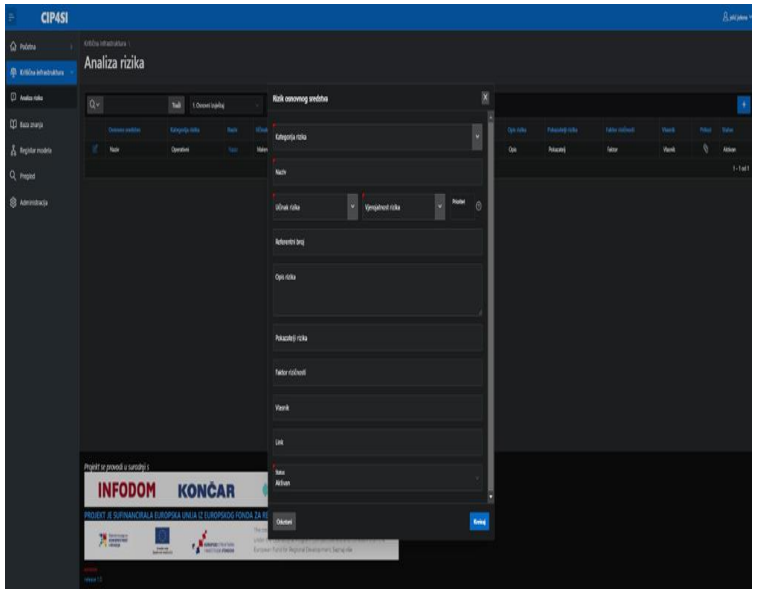


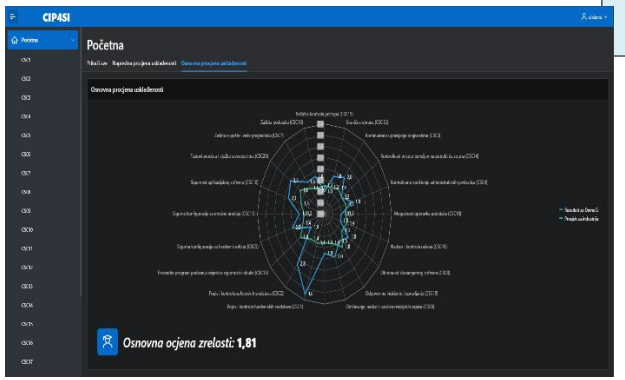


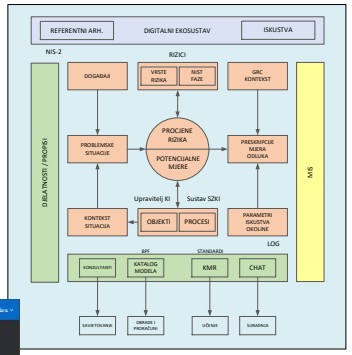


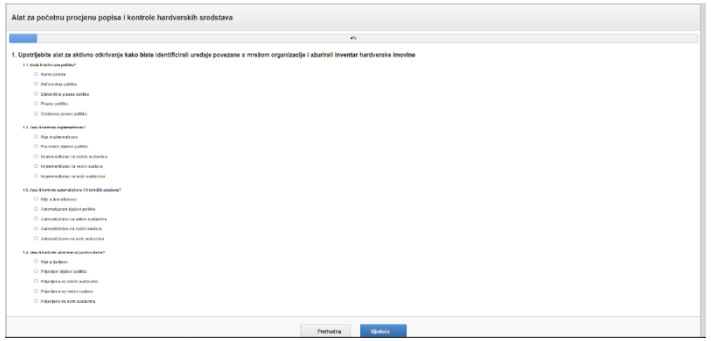
CIP4SI – portalski dio

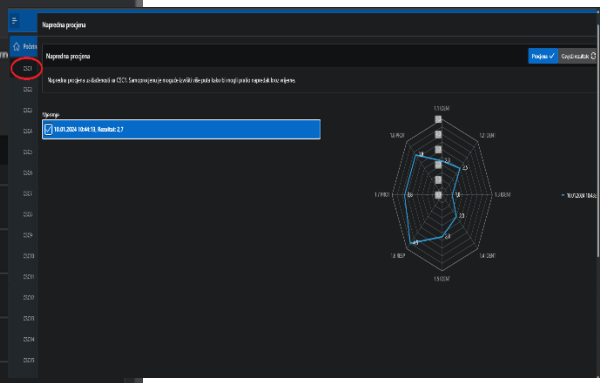








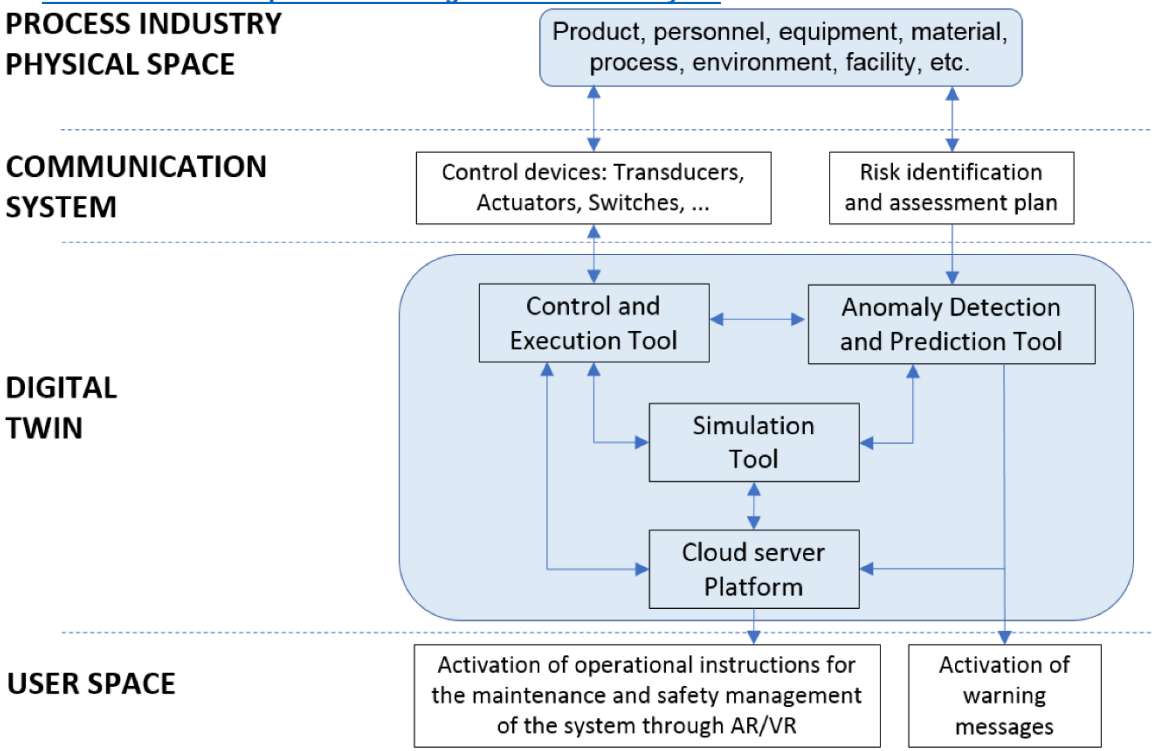




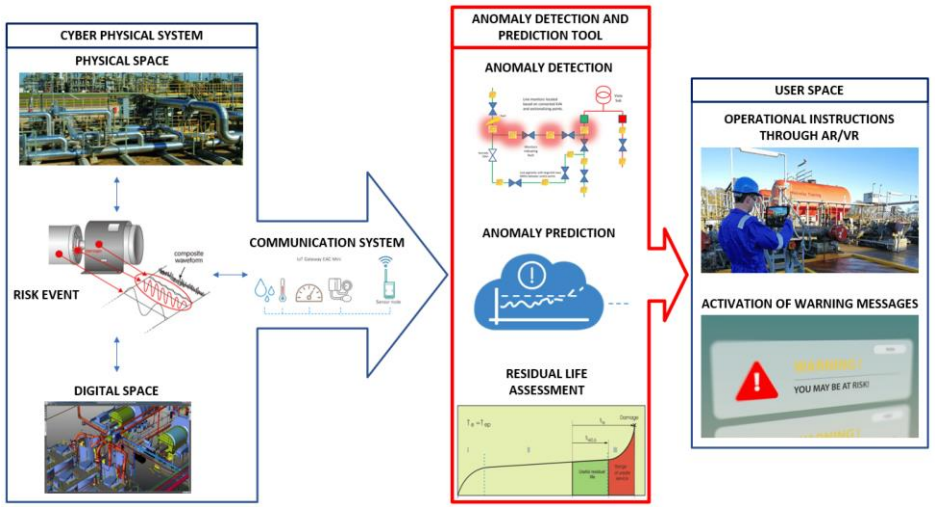
CIP4SI: Digital Twin - DT

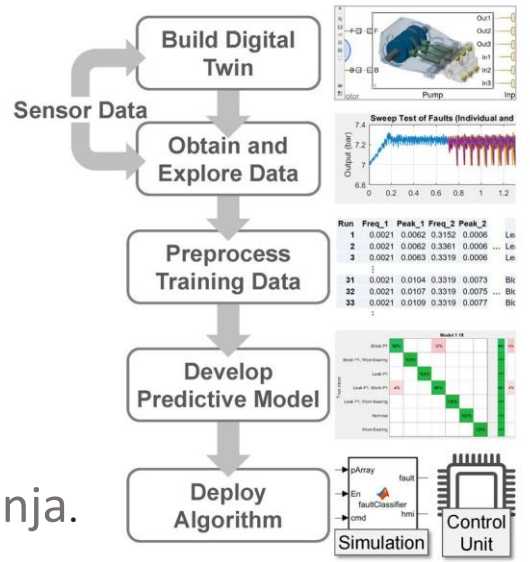
Referentni model Digital Twin:

Smart Production Operations Management and Industry 4.0



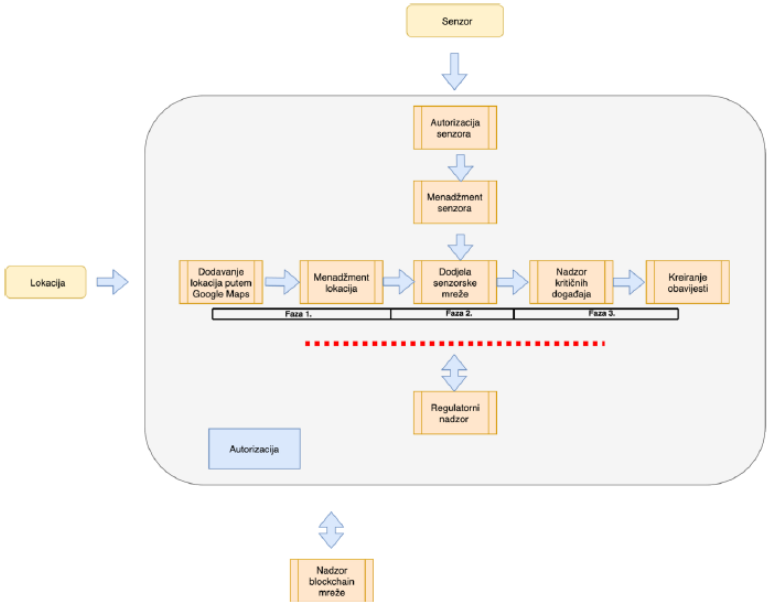
Procijena rizika povezanih s fizičkim sustavima

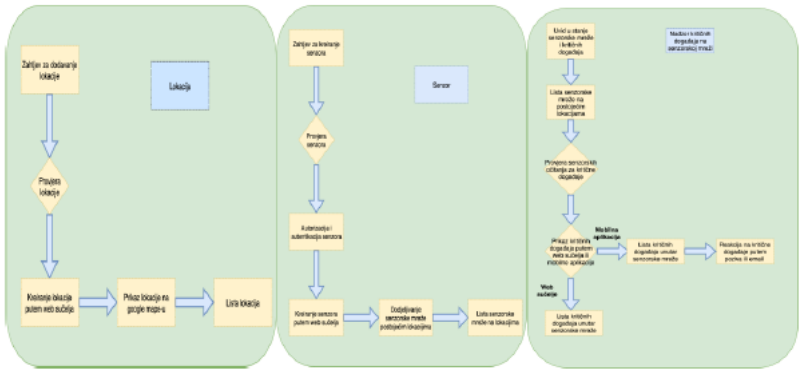


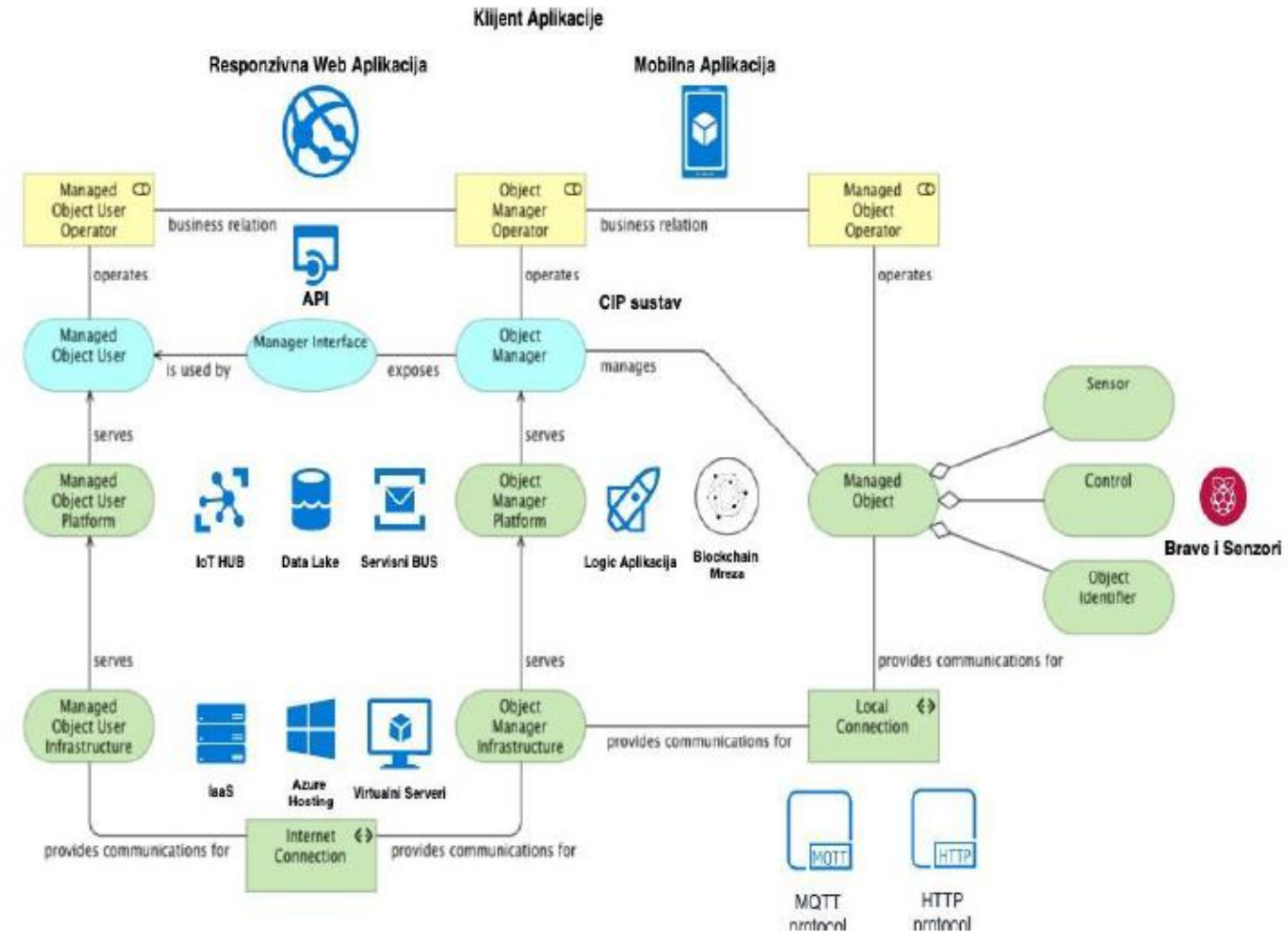


Tijek rada prediktivnog održavanja.

CIP4SI: BlockChain (DLT): Zaštita podataka upravljačkih funkcija







CIP4SI: koraci za Governance funkcije

1.	**Podrška rukovodstva**			
2.	Postavljanje upravljanjem projektom-ima		9.	Uspostava sigurnosti lanca opskrbe
3.	Početno osvješćivanje i obuka		10.	Procjena učinkovitosti kibersigurnosti
4.	Politika sigurnosti informacijskog sustava		11.	Izvješćivanje o incidentima
5.	Metodologija upravljanja rizicima		12.	Kontinuirano osposobljavanje
6.	Procjena rizika i obrada		13.	Periodična unutarnja revizija
7.	Odobreni plan obrade rizika		14.	Periodični pregledi
8.	Provedba mjera kibersigurnosti		15.	Korektivne radnje