# Sadržaj

# 1. Uvod

*Industrijski upravljački sustavi* (engl. *Industrial control systems*, skr. ICS) je naziv za skupinu sustava koji se koriste za nadzor i upravljanje industrijskim procesima [1]. ICS-ovi su široko rasprostranjeni sustavi koji se podjednako koriste za upravljanje malih i velikih industrijskih sustava od kojih neki čine sustave kritične infrastrukture. *Kritična infrastruktura* je definirana kao skup sustava od iznimne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu, okoliš, sigurnost i ekonomsku stabilnost [2]. Zbog karakteristika sustava koji se nalaze pod njihovom kontrolom, sigurnost u radu ICS-ova je od vrlo visoke važnosti.

U povijesti su se ICS-ovi razlikovali od tradicionalnih IT sustava svojom izoliranošću od vanjskih mreža te korištenjem specijaliziranog hardvera, softvera i vlastitih protokola, no modernizacijom ICS-ova uvodi se nova tehnologija kojom se omogućuje veća povezivost unutar samih sustava kao i povezivost sustava sa vanjskim mrežama. Veća povezivost donosi poboljšanja u funkcionalnosti industrijskih sustava, odnosno donosi veću učinkovitost u njihovom radu, no izlaže ih potencijalnim napadačima koji zbog izoliranosti tih sustava prije modernizacije nisu bili u mogućnosti iskoristiti njihove ranjivosti. Kako bi se osigurala sigurnost ICS sustava potrebno je otkloniti možebitne ranjivosti, ali zbog potrebe industrijskih sustava za konstantnim radom tradicionalne metode otkrivanja ranjivosti nisu adekvatne. Kao rješenje ovog problema se predstavljaju okviri za simuliranje industrijskih kontrolnih sustava koji će služiti kao vjerna replika stvarnih sustava nad kojom će biti moguće provoditi sigurnosna istraživanja.

Cilj ovog rada je predstaviti arhitekturu ICS sustava i simulacijskih okvira, objasniti razliku između fizičkih, virtualnih i hibridnih okvira te dati pregled nekolicine fizičkih i hibridnih simulacijskih okvira koje se nalaze u upotrebi. Drugo poglavlje rada opisuje arhitekturu industrijskih kontrolnih sustava pomoću Purdue referentnog modela i sigurnosne probleme tih sustava. U trećem poglavlju opisana je arhitektura simulacijskih okvira i njihove karakteristike dok četvrto poglavlje sadrži ukratko opisane pojedinačne simulacijske okvire i tablicu okvira sa sažetim informacijama. U petom poglavlju se nalazi zaključak nakon kojeg slijedi popis korištene literature, sažetak rada i skraćenice korištene u radu.

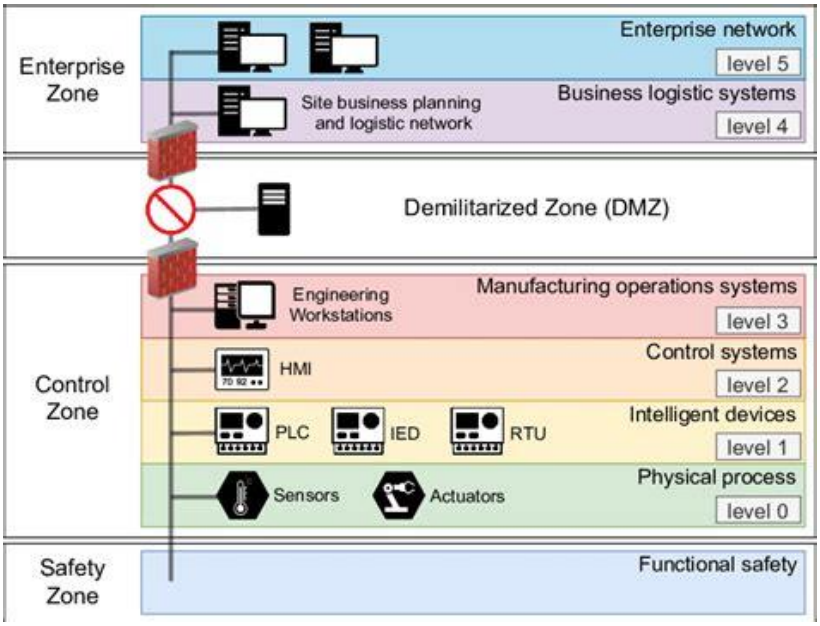
# 2. Industrijski upravljački sustavi

Ovo poglavlje prvo uvodi arhitekturni model industrijskih upravljačkih sustava nakon čega se opisuje kako su upravljački sustavi razvijani kroz povijest. Na kraju poglavlja objašnjeno je zašto modernizacija upravljačkih sustava može biti problematična za sigurnost tih sustava.

## 2.1. Arhitekturni model industrijskih upravljačkih sustava

Industrijski upravljački sustavi su sustavi koji upravljaju velikim dijelom svjetske kritične infrastrukture te obuhvaćaju nekolicinu različitih vrsta upravljačkih sustava kao što su SCADA (engl. *Supervisory Control and Data Acquisition*) i DCS (engl. *Distributed Control Systems*) [1][3]. Industrijski upravljački sustavi se sastoje od kombinacija različitih računalnih, električkih i mehaničkih komponenti čiji je zajednički cilj upravljanje fizičkim procesima.

Kompleksnost takvih sustava može biti na vrlo visokoj razini, stoga je za pojednostavljeni prikaz arhitekture ICS sustava često koristi Purdue referentni model prikazan slikom (Sl. 1.1) koji dijeli ICS sustave na četiri zone, poslovnu, demilitariziranu, kontrolnu i sigurnosnu zonu. Arhitekturni model dodatno radi i podjelu na šest razina [2][4]:




Sl. 1.1 Purdue referentni model [4]

### 2.1.1. Poslovna zona

*Poslovna zona* je zona u kojoj se obavljaju primarne poslovne funkcije. Sadrži četvrtu i petu razinu modela te se sastoji od tradicionalnih sustava informacijske tehnologije (IT) koji primaju podatke iz proizvodnog dijela sustava te na temelju tih podataka donose poslovne odluke koje utječu na ostatak sustava. Sadrži ERP (engl. *Enterprise Resource Planning*) sustav koji predstavlja integrirane alate za upravljanje resursima, logistikom, planiranjem i financijama. Poslovna zona je dio ICS-a koji je direktno spojen na Internet.

### 2.1.2. Demilitarizirana zona

*Demilitarizirana zona* (DMZ) služi kao pristupna točka između poslovne IT mreže i mreže operacijske tehnologije (OT) koja se nalazi na nižim razinama modela. Sastoji se od vatrozida i drugih uređaja čiji je cilj zaštititi sustav tako da ostvari sigurnu podjelu između poslovne zone i OT mreže. Sva komunikacija poslovne zone sa nižim razinama modela se odvija kroz demilitariziranu zonu koja filtracijom sprječava dolazak neželjenih poruka do OT mreže. Demilitarizirana zona se nije nalazila u originalnom Purdue modelu, nego je naknadno dodana te u mnogim ICS sustavima vatrozidi nisu ispravno konfigurirani ili nisu uopće implementirani [5].

### 2.1.3 Upravljačka zona

*Upravljačka ili OT zona* se sastoji od sustava i opreme za nadziranje, upravljanje i kontrolu industrijskog procesa koja može biti ostvarena centralizirano ili decentralizirano, ovisno o primjeni. Upravljački sustavi mogu biti raspodijeljeni po velikoj geografskoj površini i nalaziti se na teško dostupnim područjima[6]. Upravljačka zona je dodatno podijeljena na četiri razine:

a. Treća razina sadrži proizvodne operativne sustave čija je zadaća upravljanje operacijama postrojenja radi dobivanja željenog rezultata industrijskog procesa. Na ovoj razini se ovisno o postrojenju mogu nalaziti radne stanice, povijesne baze koje spremaju podatke prikupljene tokom rada industrijskog postrojenja za kasniju analizu, sustavi za udaljeni pristup, sustavi za održavanje postrojenja te DNS serveri i drugi IT sustavi. Komunikacija sa četvrtom i petom razinom se odvija kroz DMZ dok se sa nižim razinama komunikacija odvija direktno.

b. Druga razina se sastoji od upravljačkih sustava kao što su SCADA sustavi čija je zadaća nadzor, nadgledanje i kontrola fizičkih procesa. Ti upravljački sustavi sadrže alarme, kontrolne radne stanice i HMI-ove (engl. *Human Machine Interface*) koji operatorima omogućuju ručno upravljanje procesima te vizualiziraju podatke kako bi prikazali stanje procesa.

c. Prva razina sadržava inteligentne uređaje koji primaju podatke fizičkih procesa te ih obrađuju nakon čega donose daljnje odluke. Primjeri inteligentnih uređaja su PLC-ovi (engl. *Programmable Logic Controller*), RTU-ovi (engl. *Remote Terminal Unit*) i IED-ovi (engl. *Intelligent Electronic Device*). PLC-ovi, RTU-ovi i IED-ovi su elektronički uređaji dizajnirani za rad u teškim uvjetima koji imaju mogućnost čitanja podataka sa senzora, izvođenja programiranih instrukcija te komunikacije sa drugim upravljačkim sustavima.

d. Nulta razina sadrži senzore, aktuatore, ventile i druge slične uređaje koji su u direktnim kontaktom sa samim fizičkim procesom. Ovim uređajima upravljaju uređaji sa prve razine.

### 2.1.4. Sigurnosna zona

*Sigurnosna zona* uključuje sustave i uređaje čija je zadaća održavanje sigurnog stanja industrijskog procesa koju obavljaju praćenjem stanja procesa, obavještavanjem operatora o anomalijama te oporavkom procesa iz neželjenog stanja.

## 2.2. Razvoj upravljačkih sustava

U industrijskoj povijesti postoje četiri tranzicijska perioda koja su označena kao industrijske revolucije [7]. Prve dvije revolucije su periodi u kojima je industrija modernizirana prvotno parnim strojevima, a potom i strojevima pogonjenima električnom strujom i naftnim derivatima.

Treća industrijska revolucija koja je započela sredinom 20. stoljeća uvodi računalnu tehnologiju, naprednu telekomunikaciju i sustave za obradu podataka u proizvodne procese. Industrijska postrojenja se počinju digitalizirati korištenjem PLC-ova i sličnih uređaja radi automatiziranja određenih procesa te prikupljanjem i dijeljenjem podataka. Postrojenja su bila građena izolirano od vanjskih mreža i nije postojala direktna komunikacija između ta dva entiteta. Upravljački sustavi tih postrojenja su koristili specijalizirani hardver, softver i protokole u svom radu.

Četvrtu industrijsku revoluciju, ili takozvanu *Industriju 4.0,* karakterizira povećavanje automatizacije industrijskih postrojenja i njihova modernizacija novim pametnim uređajima, odnosno takozvana IT/OT konvergencija u kojoj se IT sustavi integriraju sa OT sustavima čime se ostvaruje povećana povezivost unutar samog industrijskog postrojenja, ali i sa vanjskim mrežama. Modernizacija postrojenja uz korištenje pametnih uređaja je provedena i uvođenjem internetskih protokola, omogućavanjem bežične komunikacije i spajanje upravljačkih sustava na Internet. Glavni motivi za modernizaciju su olakšavanje upravljanja proizvodnim procesima, manji operativni troškovi i veća efikasnost rada sustava [8].

## 2.3 Sigurnost upravljačkih sustava

Prije nego su u industrijska postrojenja uvedeni modernizirani sustavi jedina prijetnja su bili napadači koji su imali fizički pristup postrojenju. Zbog izoliranosti industrijskih postrojenja njihovi upravljački sustavi nisu implementirali sigurnosne mehanizme [9]. Također, komunikacijski protokoli korišteni u tim sustavima, kao što su Modbus, PROFINET i S7, nisu ni na koji način brinuli o sigurnosti komunikacije.

Iako je modernizacija industrijskih upravljačkih sustava i njihovo povezivanje sa vanjskim mrežama povećalo učinkovitost proizvodnih procesa, uvelo je i sigurnosne probleme. Uz ranjivosti komunikacijskih protokola, napadačima postaju dostupne i ranjivosti tehnologija korištenih u upravljačkim sustavima [10]. Neke od komponenata korištenih u radu upravljačkih sustava mogu imati vijek trajanja od nekoliko desetljeća te njihova otpornost na kibernetičke napade nije poznata. Dodatne ranjivosti se u upravljačke sustave unose korištenjem zastarjelog softvera, operacijskih sustava kojima je istekla podrška i neprimjenjivanje softverskih zakrpa [11].
U statističkom izvješću tvrtke Kaspersky 2016. godine objavljeno je kako je broj ranjivosti ICS sustava porastao sa 19 poznatih ranjivosti 2010. godine na 189 ranjivosti 2015. godine [12]. Dodatno, prema kriteriju CVSS v2 i v3 (engl. *Common Vulnerability Scoring System*) 49% ranjivosti otkrivenih 2015. godine su označene kritičnima, dok je 42% njih označeno ranjivostima srednjeg rizika. Također, primjeri napada kao što su Stuxnet i napad na ukrajinsku elektroenergetsku mrežu otkrivaju s kakvim se rizikom suočavaju sustavi kritične infrastrukture [13][14].

Ovi podatci ukazuju na potrebu za sigurnosnim istraživanjima koja bi unaprijedila sigurnost industrijskih upravljačkih sustava. Kako bi se sigurnost upravljačkih sustava testirala penetracijskim testovima i drugim tradicionalnim metodama industrijska postrojenja moraju biti djelomično ili u potpunosti stavljena van pogona. Tokom provođenja takvih testiranjima postoji rizik od nastanka fizičke štete na sustavu što, uz period u kojem je postrojenje izvan funkcije, može dovesti do velikih financijskih gubitaka za vlasnika industrijskog postrojenja kao i obustave krucijalnih usluga kritičnih infrastrukturnih sustava. Zbog toga se u sigurnosnim istraživanjima industrijskih upravljačkih sustava koriste simulacijski okviri.

# 3. Simulacijski okviri

*Simulacijski okviri* su alati koji vjerno repliciraju stvarne industrijske upravljačke sustave kako bi pružili okolinu u kojoj je moguće ispitivati ranjivosti upravljačkih sustava, ispitivati sigurnosna rješenja, educirati stručno osoblje te provoditi druga sigurnosna istraživanja korištenjem punog spektra dostupnih metoda bez nastanka štete na industrijskom postrojenju [1].

Kako bi simulacijski okvir efektivno izvršavao svoju zadaću on mora ispunjavati četiri zahtjeva [15][16]:

- Vjernost
- Ponovljivost
- Preciznost mjerenja
- Sigurno izvođenje procesa

Vjernim simuliranjem stvarnih sustava osigurava se da će sve akcije poduzete u simulacijskom okviru na jednak način preslikati na stvarni sustav. Ponovljivost dozvoljava uspoređivanje rezultata dobivenih korištenjem različitih simulacijskih okvira ili usporedbom različitih obrambenih mehanizama od istog napada, dok preciznost mjerenja osigurava točnost i pouzdanost izmjerenih podataka. Sigurno izvođenje procesa osigurava da neće biti ugroženo zdravlje i sigurnost korisnika simulacijskog okvira, čak i ako se simuliraju sustavi kod kojih napadi mogu stvoriti opasne uvjete. Sva četiri zahtjeva je relativno teško ispuniti u potpunosti, stoga kod izgradnje svakog okvira određenim zahtjevima je dan prioritet nad drugima, ovisno o cilju simulacijskog okvira.

Simulacijski okviri imaju mnoga područja primjene [17][18]. Mogu se koristiti u istraživanjima ranjivosti industrijskih uređaja, protokola i konfiguracija sustava te u analizi fizičkih posljedica kibernetičkih napada. Nadalje, okviri se mogu koristiti u testiranju obrambenih mehanizama, forenzičkoj analizi, generiranju skupova podataka za daljnja istraživanja i za edukaciju industrijskog osoblja, ali i na obrazovnim institucijama.

Simulacijski okviri se mogu podijeliti u tri kategorije, *fizičke*, *virtualne* i *hibridne*. Fizički simulacijski okviri koriste stvarne industrijske uređaje pri izgradnji fizičkog procesa i mrežnog dijela ICS-a. Prednost fizičkih okvira je vrlo vjerna reprezentacija stvarnog ICS-a i mogućnost provođenja istraživanja nad specifičnim uređajima, ali su zbog korištenja stvarnih uređaja iznimno

skupi za izgradnju, održavanje i daljnju nadogradnju te ne mogu simulirati određene fizičke procese zbog potencijalne opasnosti.

Virtualni simulacijski okviri koriste računalne simulacije pri izgradnji i fizičkog procesa i mrežnog dijela ICS-a. Računalne simulacije omogućavaju simuliranje upravljačkih sustava vrlo velikih dimenzija te mogu biti simulirani opasni fizički procesi poput nuklearne fisije. Računalne simulacije omogućuju vrlo lako mijenjanje konfiguracije sustava i ponavljanje eksperimenata. Virtualni okviri se mogu izgraditi po relativno niskoj cijeni, ali zbog isključivog korištenja računalnih simulacija vjernost simuliranog sustava nije na visokoj razini te je verificiranje rezultata dobivenih korištenjem ovakvih okvira otežano [19].

Kao kompromis između fizičkih i virtualnih okvira se nude hibridni okvir koji kombiniraju korištenje stvarnih uređaja i računalnih simulacija. Ugradnjom stvarnih komponenti u okvir se dobiva vjerna replika dijela sustava koji je bitan za provođenje željenog istraživanja, dok se ostatak sustava ostvari računalnom simulacijom čime se smanjuje cijena izgradnje okvira.

# 4. Primjeri simulacijskih okvira

Ovo poglavlje sadrži ukratko opisane primjere fizičkih i hibridnih simulacijskih okvira kao i tablicu u kojoj su sažete informacije o tim okvirima. Pretragom izvora pronađeno je oko četrdeset radova koji opisuju simulacijske okvire te još veći broj radova koji su tematski vezani uz sigurnost ICS sustava. Pretraga je obavljena pomoću internetskih tražilica gdje su kao ključne riječi korišteni izrazi ics testbed, ics security, scada testbed i cyber-physical testbed. Dodatno, izvor za radove je bila literatura radova pronađenih internetskom pretragom.

## 4.1 Fizički simulacijski okviri

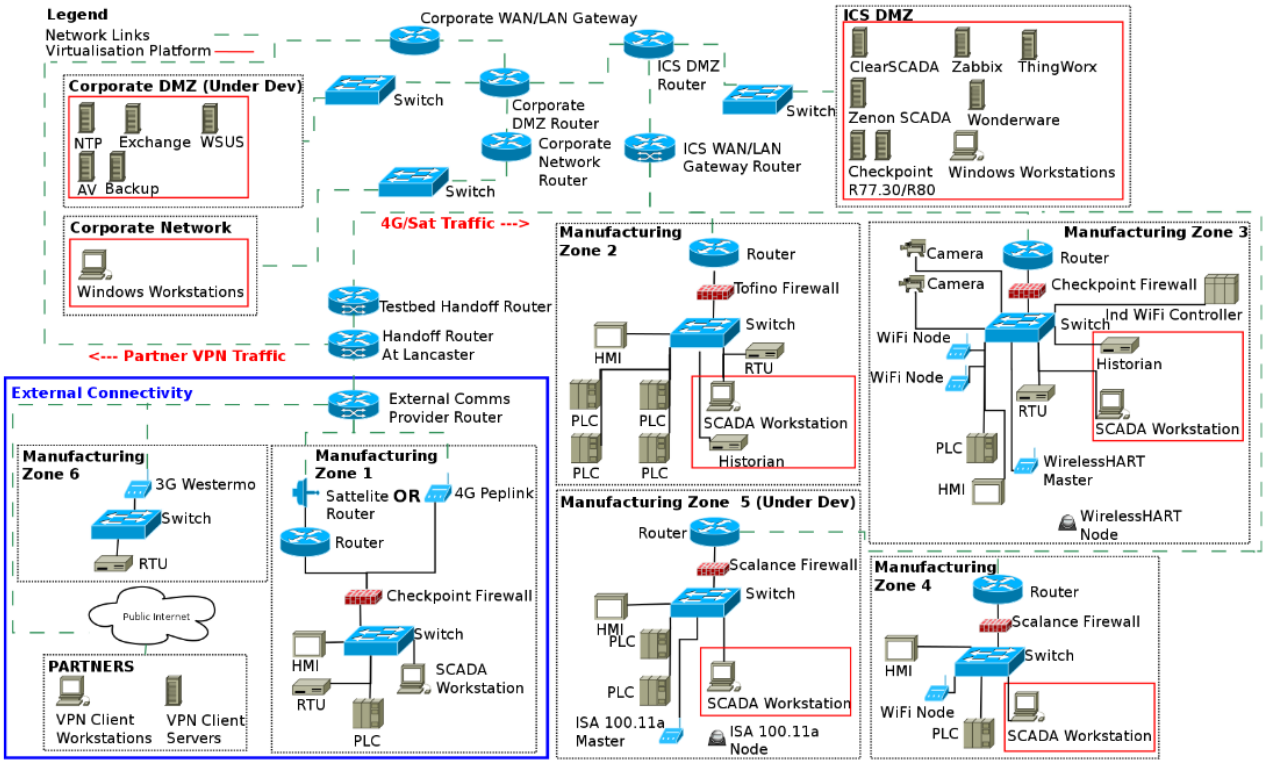
U ovom potpoglavlju se nalaze opisi sedam fizičkih simulacijskih okvira koji su ostvareni tako da su opisani simulirani procesi, arhitekture okvira te područja njihove primjene.

SWaT i WADI su dva međusobno integrirana fizička simulacijska okvira razvijena na Sveučilištu tehnologije i dizajna u Singapuru [20][21]. SWaT je napravljen kao umanjena verzija postrojenja za pročišćavanje vode u suradnji sa singapurskim vodoopskrbnikom kako bi okvir vjerno prikazao stvarni sustav. Okvir simulira puni ciklus obrade vode sa kapacitetom od oko 22 litre po minuti te se prostire na približno 90 kvadratnih metara. Sustav se sastoji od 6 ogranaka procesa, svaki sa zasebnim parovima PLC-ova za decentralizirano upravljanje. Ljudski operator može upravljati procesom putem HMI-a. Komunikacija komponenata sustava se može odvijat žičano ili bežično protokolima Ethernet/IP i CIS. Arhitektura upravljačke zone prati referentni model u svim segmentima osim u implementaciji povijesne baze podataka koja se nalazi u zasebnoj mreži. Okvir SWaT prikazan je slikom (Sl. 3.1).

Sl. 3.1 SWaT simulacijski okvir [20]

WADI je okvir koji simulira skaliranu verziju vodoopskrbnog sustava. Okvir se sastoji od primarnih i sekundarnih spremnika vode, senzora i povratnog dijela koji omogućuju opskrbu 45 litara vode po minuti. Fizički proces je podijeljen na tri dijela, svaki od kojih sadrži vlastite PLC-ove koji su spojeni u centralni upravljački čvor. U centralnom čvoru se nalazi SCADA radna stanica sa HMI sučeljem te je čvor od poslovne zone odvojen vatrozidom. WADI i SWaT su korišteni za provođenje kibernetičkih napada kojima su otkrivene postojeće ranjivosti na industrijskim uređajima. Glavna zadaća ova dva okvira je provođenje istraživanja vezanih uz posljedice kibernetičkih napada na vodoopskrbne sustave i evaluacija mehanizama otkrivanja potencijalnih napada Također, integracijom WADI-ja i SWaT simulacijskog okvira omogućena je analiza kaskadiranja efekata napada sa jednog sustava na drugi. Zbog korištenja industrijskog hardvera i softvera te suradnje sa industrijskim stručnjacima SWaT i WADI vrlo vjerno prikazuju stvarni vodoopskrbni sustav, ali posljedica toga je vrlo visoka cijena izgradnje i održavanja okvira što je njihov glavni nedostatak.

Lancaster University simulacijski okvir je okvir koji uz poslovnu i demilitariziranu zonu simulira šest različitih industrijskih procesa [22][23]. Mrežna topologija okvira prikazana je Slika 3.2 Mrežna topologija Lancaster simulacijskog okvira [22]. Svaki fizički proces podijeljen je u svoju proizvodnu zonu te svaka od proizvodnih zona sadrži vlastitu konfiguraciju upravljačkih sustava i fizičkih procesa što omogućava provođenje vrlo raznolikih istraživanja. Okvir također sadrži poslovnu zonu i demilitariziranu zonu. Sami fizički proces nisu ostvareni potpuno realistično radi olakšanja konfiguracije i operacija nad tim procesima. Proizvodne zone okvira mogu sadržavati industrijske komponente istog proizvođača, komponente različitih proizvođača te kombinaciju zastarjelih i ažurnih komponenti. Komunikacija u okviru se može odvijati žičano, ali i bežično putem 3G, 4G i satelitske veze. Okvir je u trenutno stanju došao inkrementalnim nadogradnjama. Nakon izgradnje prvotnog okvira, istraživači su ušli u suradnju sa relevantnim industrijskim organizacijama kako bi poboljšali okvir i unijeli raznolikost što je rezultiralo implementacijom više industrijskih procesa podijeljenih u zone te potpora za mnoge različite industrijske protokole i uređaje. Okvir je poslužio za provođenje mnogih sigurnosnih istraživanja, od kojih se može izdvojiti izgradnja SENAMI-ja, alata za detektiranje upada u ICS sustave. Okvir je dostupan za kolaboraciju zainteresiranim suradnicima.




Slika 3.2 Mrežna topologija Lancaster simulacijskog okvira [22]

Sveučilište New Orleans je napravilo svoj fizički simulacijski okvir koji simulira tri različita industrijska procesa [24]. Korištenjem stvarnih industrijskih uređaja u okviru su implementirani plinovodski i elektroenergetski sustav te sustav za pročišćavanje vode. Svaki od ovih procesa je odvojen u zaseban dio koji koristi jedan od standardnih komunikacijskih protokola, Ethernet/IP, Modbus ili PROFINET. Fizički procesi su kontrolirani od strane PLC-ova te se mogu nadzirati korištenjem HMI sučelja. Upravljački centar koji sadrži HMI i povijesnu bazu podataka je u arhitekturnom modelu također odvojen od industrijskih procesa koje kontrolira dok se komunikacija među upravljačkim centrom i procesima odvija preko izolirane komunikacijske mreže. Ovaj okvir je instaliran na pokretnim kolicima te se koristi u nastavi na sveučilištu gdje studenti uče programiranje PLC-ova, računalnoj forenzici i sigurnosti SCADA sustava. Korištenje tri različita proizvođača PLC uređaja studentima nudi raznovrsnost u učenju i razumijevanju stvarnih sustava. Nedostatci okvira su izolirana mreža koja ne nudi mogućnost spajanja na oblak te otežano dodavanje novih senzora i ostalih uređaja. Autori u svome radu nisu provodili

eksperimente, ali ističu potencijal korištenja okvira u analizi ranjivosti na napade, obrambenih mehanizama i digitalnoj forenzici.

Istraživači sa Mississippi State sveučilišta su razvili fizički simulacijski okvir koji sadrži sedam različitih primjera kritične infrastrukture [25]. Okvirom su modelirani petrokemijski, elektroenergetski, vodoopskrbni i proizvodni industrijski procesi koji su simulirani korištenjem komercijalno dostupnog industrijskog hardvera i softvera. Fizički procesi su ostvareni korištenjem RTU-ova, PLC-ova, senzora, aktuatora, spremnika i ostalih uređaja potrebnih za rad industrijskih sustava. Upravljački centar je udaljen od instalacija fizičkih procesa i nudi udaljenu kontrolu procesima. Upravljački centar također sadrži sustav za bilježenje mrežnog prometa i ugrađeni sustav detekcije napada. HMI sučelje može biti smješteno direktno unutar fizičkih procesa, ali i na udaljenoj lokaciji. Industrijski procesi simulirani u okviru su podijeljeni u 2 kategorije, ovisno o vrsti komunikacije koja može biti ostvarena Serial port konekcijom ili Ethernet konekcijom. Ovakva raznovrsnost u samom okviru je omogućila provođenje opsežnog istraživanja ranjivosti infrastrukturnih sustava kojim su otkrivene ranjivosti industrijskih uređaja. Okvir je uspješno integriran u nastavni program kolegija na sveučilištu te je osnovan samostalni kolegij koji se bavi sigurnošću infrastrukturnih sustava, zahvaljujući znanju dobivenim korištenjem ovog okvira. Također, planirano je osnivanje tečaja za radnike na elektroenergetskim infrastrukturnim postrojenjima.

LICSTER je simulacijski okvir koje je zamišljen kao jeftina alternativa za ljude i institucije koje su zainteresirane za istraživanje i edukaciju sigurnosti ICS sustava [26]. On nudi mogućnost implementiranja industrijskih komponenata i stvarnog fizičkog procesa po relativno vrlo jeftinoj cijeni. Okvir simulira proces proizvodnje na pokretnoj traci. Okvir se sastoji od PLC-a, HMI-a, senzora, SCADA servera i ostalih komponenti koje omogućuju rad pokretne trake. Zbog korištenja industrijski prihvaćenih protokola te realistično simuliranih industrijskih uređaja okvir nudi mogućnost testiranja raznovrsnih kibernetičkih napada primjenjivih u stvarnosti. U istraživanju provedenom korištenjem ovog okvira pokazano je da i ovakav jeftini okvir nudi mnoge mogućnosti testiranja napada i implementacije obrambenih mehanizama. Okvir se dodatno može proširiti korištenjem virtualnih ICS komponenata što pridonosi skalabilnosti okvira.

CENTER je simulacijski okvir konstruiran na Sveučilištu Sakarya u Turskoj koji simulira postrojenje za upravljanjem otpadnih i postrojenje za upravljanjem pročišćene vode za piće [16].

Fizički dio sustava je izveden korištenjem izvora vode, pročišćivača i spremnika za vodu. Proces upravljanja otpadnih voda i proces upravljanja pročišćenom vodom se mogu izvoditi u više različitih konfiguracija. Moguće je oba procesa izvoditi istodobno, ali i pojedinačno, dok je u svakom od dva dijela sustava moguće izvršavati postupak primanja vode u sustav, postupak pročišćavanja i postupak distribucije vode. Arhitektura simulacijskog okvira u potpunosti preslikava Purdue arhitekturni model. U fizičkom procesu su korišteni PLC-ovi i RTU-ovi koji kontroliraju senzore, ventile i druge uređaje na najnižoj razini. Operatori pristup upravljačkom dijelu sustava imaju kroz HMI-ove, dok njime upravljaju SCADA serveri. U upravljačkom dijelu okvira postoji baza podataka u kojoj se bilježe podatci prikupljeni tokom procesa. U osiguravanju komunikacijske mreže upotrjebljeni su vatrozidi, dok komunikacijske protokole podržane u radu sustava sačinjavaju Modbus TCP, DNP3, EtherCAT i TCP/IP. Okvir je izgrađen korištenjem uređaja različitih proizvođača kako bi svojim korisnicima pružio raznovrsnost. U okvir su također ugrađeni sustav za otkrivanje neovlaštenog pristupa, sustav za otkrivanje napada, sustav za bilježenje događaja i sustav za upravljanjem ranjivostima. CENTER je dostupan stranama zainteresiranim za istraživanje i kolaboraciju na sigurnosnim projektima. Glavni cilj pri uporabi ovog okvira je pružiti okolinu u kojoj je moguće provoditi istraživanja vezana uz ICS sigurnost te podići svijest o bitnosti sigurnih ICS sustava.

## 4.2 Hibridni simulacijski okviri

Ovo potpoglavlje sadrži kratak opis četrnaest hibridnih simulacijskih okvira. Opisi su po sadržaju slični opisima fizičkih okvira, ali dodatno su opisani dijelovi upravljačkih sustava koji su simulirani, odnosno koji alati su korišteni za ostvarivanje računalnih simulacija.

Sveučilište u Belfastu je razvilo okvir koji simulira rad nuklearne elektrane te koji pruža realističnu okolinu za istraživanje efekata i prikupljanje podataka o kibernetičkim napadima na fizičke procese kako bi se olakšalo stvaranje mehanizama detekcije i obrane od napada [27]. Fizički proces u reaktoru je podijeljen na četiri dijela kojima upravljaju PLC-ovi te su svi dijelovi međusobno povezani tako da promjena u jednom uzrokuje promjenu u svim ostalim dijelovima. Zbog karakteristika simuliranog fizičkog procesa ponovljivost pokusa na okviru je otežana. Pri izgradnji mrežnog dijela okvira referenciran je Purdue arhitekturni model. Mrežna arhitektura je ostvarena kombinacijom fizičkih i virtualnih usmjernika, preklopnika i vatrozida. Vatrozidi onemogućuju

neovlašteno kretanje unutar mreže te su učestalije implementirani u nižim razinama arhitekturnog modela. U okviru je dodatno implementiran OT centar operacijske sigurnosti u kojem se nalaze sigurnosni alati za nadgledanje rada sustava i upravljanje resursima. Glavna svrha ovog okvira je prikupljanje informacija o interakciji među procesima, ICS komponentama i fizičkim svojstvima sustava kako bi se okvir mogao nadograditi sustavom za detekciju anomalija nastalih kibernetičkim napadom. Okvir koristi alate i protokole otvorenog koda što omogućava replikaciju osnovne arhitekture okvira, ali sami kod okvira nije dostupan.

SCADASim je simulacijski okvir čiji je cilj omogućiti efikasnu izgradnju fleksibilnih SCADA sustavskih simulacija [28]. To je okvir koji omogućuje integraciju stvarnih i simuliranih uređaja te komunikaciju u stvarnom vremenu sa vanjskim uređajima koristeći SCADA protokole. SCADASim simulaciju industrijskih uređaja i komunikacijskih mreža ostvaruje korištenjem alata OMNET++ koji nudi *plug-n-play* opciju za jednostavno spajanje stvarnih uređaja na simulaciju. SCADASim također sadrži ugrađene RTU, PLC i MTU module i podršku za 150 različitih industrijskih protokola, ali ima i mogućnost dodavanja vlastitih implementacija. Uz to što je SCADASim alat za izgradnju simulacija SCADA sustava, on nudi i mogućnost kreacije malicioznih napada na te sustave. Okvir ima i vlastitu biblioteku kibernetičkih napada koja olakšava korištenje okvira. Radi demonstracije funkcionalnosti okvira provedeni su *DoS* (engl. *Denial of Service*) i *Spoofing* napadi na simulirane sustave čiji su rezultati prikazali da okvir realistično prikazuje ponašanje stvarnih SCADA uređaja. Kod SCADASim okvira je javno dostupan.

*Virtual power system testbed* (VPST) je okvir koji je dizajniran za integraciju sa drugim simulacijskim okvirima radi istraživanja performansi i sigurnost SCADA sustava [29]. Primjeri primjene VPST-a su obučavanje stručnog osoblja, analiza integracije nove tehnologije u ICS sustave i analiza otpornosti ICS-a na napade. VPST je sposoban simulirati više od milijun uređaja, što značajno pridonosi skalabilnosti okvira. Okvir je podijeljen na tri dijela, VPST-E se uz pomoć alata PowerWorld brine o simulacijama elektroenergetske mreže, VPST-C se uz pomoć alata RINSE brine o simulacijama komunikacijske mreže, a VPST-R-local predstavlja sve stvarne uređaje. Dodatni dio okvira je sustav za spajanje sa drugim okvirima koji se brine o kontroli komunikacije, upravljanju resursima i ispravljanju grešaka u zajedničkom radu više okvira.

Istraživači iz Sandia National Laboratoriesa su razvili hibridni simulacijski okvir koji su iskoristili za istraživanje ranjivosti SCADA sustava na kibernetičke napade [30]. Arhitektura okvira se dijeli na poslovni i upravljački dio čija je međusobna konekcija zaštićena vatrozidom. Komunikacijska mreža je simulirana korištenjem alata OPNET Modeler koji omogućava simulaciju mreža sa velikim brojem čvorova te sadrži sučelje za komunikaciju stvarnih uređaja sa simuliranima. Virtualizacija i emulacija se koriste kod izgradnje usmjernika, dok se fizički uređaji ugrađuju u onaj dio okvira koji ovisno o području primjene okvira zahtijeva visoku vjernost, što smanjuje cijenu izgradnje okvira. Fizički uređaji koji se ne nalaze u primarnom dijelu sustava su ostvareni simulacijom uz pomoć alata VCSE (engl. *Virtual Control System Environment*). Komunikacija unutar okvira se odvija korištenjem protokola Modbus TCP, DNP3 i IEC 60870. Napadima na poslovnu i upravljačku zonu pružen je primjer kako se ovaj okvir može koristiti u analizi sigurnosti ICS sustava. Uz sigurnosne eksperimente provedeni su i eksperimenti u kojima su računalno modelirane komponente zamijenjene stvarnima radi ispitivanja vjernosti modela. Okvir osim za analizu ranjivosti sustava može služiti i kao okolina za učenje i usavršavanje sigurnosnih stručnjaka.

Simulacijski okvir HYDRA je okvir otvorenog koda razvijen na sveučilištu Roma Tre koji simulira sustav gradske vodoopskrbe [31][32][33]. Zamišljen je kao jeftino rješenje koje će adekvatno prikazati vodoopskrbnu infrastrukturu radi provođenja istraživanja i edukacije o sigurnosti infrastrukturnih sustava. Arhitektura okvira je podijeljena u četiri modula, upravljački sustav, sustav za otkrivanje grešaka (engl. *Fault Detection System, FDS*), stanicu mrežne sigurnosti i HMI sučelje. Sva četiri modula su spojena na lokalnu mrežu. Fizički proces je simuliran korištenjem spremnika za vodu, cijevi, senzora, aktuatora i ventila, dok su RTU-ovi i PLC-ovi koji se nalaze u upravljačkom dijelu emulirani. Sustav za otkrivanje grešaka ima zadaću održavanja sustava u mehanički sigurnom stanju, dok se o kibernetičkoj sigurnosti sustava brine stanica mrežne sigurnosti koja se sastoji od analizatora mrežnih protokola i sustava za otkrivanje upada (engl. *Intrusion Detection System, IDS*). Rad koji predstavlja simulacijski okvir HYDRA demonstrira napad u kojem napadač koji ima pristup mreži sustava ubacuje lažne podatke. Sustav je uspješno razlikovao pokušaje napada od običnih grešaka u radu fizičkog procesa te je se pokazao kao efektivan alat u dijagnosticiranju grešaka u radu sustava, istraživanju sigurnosnih strategija i testiranju kontrolnih algoritama. Planirana je nadogradnja sustava industrijskim PLC-ovima.

RESLab predstavlja okvir koja simulira elektroenergetski industrijski sustav korištenjem stvarnih uređaja te računalne emulacije i simulacije [34][35]. Arhitektura okvira preslikava Purdue arhitekturni model ICS sustava. Mrežni dio je ostvaren korištenjem alata CORE koji emulira usmjernike, vatrozide, osobna računala i servere te posjeduje sučelja za spajanje na vanjske mreže. Elektroenergetski dio okvira je simuliran korištenjem alata PowerWorld DS, a upravljački dio je ostvaren vlastitim alatom CYPRES koji obavlja nadgledanje, upravljanje i vizualizaciju sustava. Dodatno, CYPRES upravlja i sustavom za otkrivanje upada. Komunikacija u okviru se odvija korištenjem DNP3 protokola. Zbog korištenja alata za simulaciju RESLab ima mogućnost simuliranja vrlo velikih elektroenergetskih mreža. Pomoću okvira provedeno je ekstenzivno istraživanje u kojim su provedeni DoS i MITM napadi. Ciljevi istraživanja su bili istražiti efektivnost napada na sustav, razumjeti dinamiku napada, te validirati obrambena rješenja.

MSICST simulacijski okvir je okvir sa arhitekturom koja sadrži upravljačku zonu, poslovnu zonu i demilitariziranu zonu i u kojem upravljačka zona sadrži četiri različita modela industrijskih postrojenja, termoelektranu, željezničku liniju, pametnu elektroenergetsku mrežu i pametni proizvodni proces [36][37]. Fizički procesi su ostvareni kombiniranjem industrijskog hardvera i softvera sa računalnim simulacijama. Svaki fizički proces implementiran u okviru ima vlastitu privatnu mrežu kojoj je pristup ograničen vatrozidom i HMI sučelja za interakciju sa sustavom. Upravljački dio je ostvaren standardnim SCADA sustavom, dok proces pametne proizvodnje dodatno implementira DNC (engl. *Distributed Numerical Control*) sustav za kontrolu CNC (engl. *Computer Numerical Control*) uređaja. Protokoli korišteni u radu okvira su Modbus/TCP, S7 i S7+. Demilitarizirana zona ostvaruje separaciju kontrolne i poslovne zone te sadrži bazu podataka u kojoj se zapisuju podatci o radu svih sustava. Poslovna zona simulira uredsku mrežu koja se sastoji od web servera, mail servera i uredskih radnih stanica, no zbog ograničenog budžeta nije implementiran ERP sustav. Tvorci okvira su korištenjem vlastitog modela napadača proveli scenarije napada pomoću kojih su otkrili ranjivosti na uređajima i ispitali sigurnosna rješenja. Plan za budućnost okvira je dodavanje dodatnih industrijskih procesa i provođenje naprednijih sigurnosnih istraživanja.

Istraživači sa instituta NIST su razvili okvir koji simulira tri različita fizička procesa te čiji je cilj mjeriti performanse ICS sustava kada su u taj sustav ugrađene sigurnosne mjere zahtijevane od strane određenih industrijskih standarda, poput ISA/IEC-62443 i NIST Special Publication 800-82

[38][39]. Prvi fizički proces simuliran u okviru je Tennessee Eastman (TE) proces koji modelira kemijski proizvodni proces. TE proces je proces koji je vrlo često korišten u istraživanju industrijskih kontrolnih sustava. Glavni razlog za korištenje TE procesa je njegova nestabilnost, odnosno svojstvo procesa da prelazi u nestabilno i nesigurno stanje ukoliko nije pod adekvatnom kontrolom, čime je predstavljen primjer iz stvarnog svijeta u kojem kibernetički napad predstavlja veliku opasnost za sustav. Arhitektura procesa je podijeljena na upravljačku, operativnu i demilitariziranu zonu te zonu za mjerenje. Sami fizički proces je ostvaren računalnom simulacijom, dok kontroli dio dodatno čine stvarni PLC-ovi, OPC (engl. *Open Platform Communications*) server i lokalna povijesna baza. U operativnoj zoni se nalazi HMI sučelje za nadzor, vizualizaciju podataka i upravljanje procesom. DMZ odvaja poslovnu i upravljačku zonu i sadrži povijesnu bazu podataka. Drugi proces je proces pametne proizvodnje korištenjem robota koji ima sličnu arhitekturu kao i TE proces. Treći proces modelira inteligentni transportni sustav, ali u vrijeme objave rada taj proces nije bio implementiran u okviru. Mrežni dio okvira čine lokalne mreže, preklopnici, integrirani usmjernici i vatrozidi. Za provođenje sigurnosnih istraživanja na okviru koriste se zasebna računala i alati za napade.

Istraživači sa Sveučilišta Rowan su razvili simulacijski okvir koji prikazuje rashladni sustav nuklearne elektrane i željeznički sustav sa stanicom i pružnim prijelazom [40][41]. Nuklearni sustav se sastoji od senzora i rashladnih elemenata, dok se željeznički sustav sastoji od modela lokomotive, senzora za automatizaciju pružnog prijelaza i senzora za automatsko upravljanje lokomotivom. Model fizičkog procesa predstavljenog ovim okvirom je prikazan Slika 3.**3** Model fizičkog procesa simulacijskog okvira Sveučilišta Rowan [40]Cijelim fizičkim sustavom upravlja PLC upravljački sklop koji se sastoji od PLC-a i ulazno-izlaznih elemenata. HMI sučelje je na kontrolni sklop spojeno putem Wi-Fi mreže te nudi mogućnost udaljenog nadziranja i upravljanja upravljačkim sustavom. Na upravljački dio okvira putem Wi-Fi mreže je omogućeno spajanje i drugim uređajima, poput osobnog računala kojim se u okviri putem alata Wireshark bilježi mrežni promet okvira. Korištenjem okvira i iskorištavanjem ranjivosti Modbus/TCP protokola korištenog u okviru izvršeni su napadi manipulacijom podataka i DoS napadi kojima je ukazano na ranjivosti ovakve implementacije industrijskih sustava. Ovaj okvir su uz pomoć mentora konstruirala dva studenta u periodu od šest mjeseci i on služi kao primjer drugim zainteresiranim stranama kako relativno jeftino konstruirati vlastiti istraživački i edukacijski simulacijski okvir.

Slika 3.3 Model fizičkog procesa simulacijskog okvira Sveučilišta Rowan [40]

Katarsko sveučilište uz potporu NATO saveza je razvilo simulacijski okvir koji simulira Tennessee Eastman proces u stvarnom vremenu [42]. Okvir je konstruiran kako bi se pomoću njega proveli kibernetički napadi na upravljački sustav te se pomoću podataka prikupljenima tokom napada evaluirali različiti algoritmi za otkrivanje napada. Fizički proces je ostvaren računalnom simulacijom koji su preko sučelja spojeni na stvarne ulazno-izlazne module. Cijeli upravljački dio je izgrađen korištenjem Siemens PLC-ova, dok se komunikacija u sustavu odvija PROFINET i S7 protokolima. Kibernetički napadi provedeni korištenjem okvira su iskorištavali ranjivosti PROFINET protokola kako bi ubacili lažne podatke u upravljački dio sustava te je proučavan njihov utjecaj na rad sustava. Kako bi se takvi napadi uočili u okviru su implementirani algoritmi strojnog učenja za otkrivanje napada koji su napade uspjeli detektirati uz relativno visoku uspješnost.

PowerCyber je simulacijski okvir razvijen na Iowa State sveučilištu koji koristi stvarne, emulirane i simulirane komponente kako bi stvorio realistični prikaz pametne elektroenergetske mreže

[43][44]. Upravljački dio okvira se sastoji od upravljačkog centra čija je zadaća upravljanje pojedinačnim upravljačkim stanicama. Upravljački centar je konfiguriran da podržava generalne SCADA funkcije poput prikupljanja podataka sa uređaja fizičkog procesa, prosljeđivanje naredbi tim uređajima te bilježenje i upravljanje povijesnim podatcima o radu industrijskog postrojenja. Upravljački sustav je izgrađen korištenjem SCADA servera, HMI-ova i povijesnih baza podataka koje odgovaraju industrijskim standardima. Upravljačke operacije upravljačkog centra stavljaju fokus na pristupe koje koriste ljudskog operatora koji donosi odluke o radu sustava. SCADA server šalje upite upravljačkim stanicama o statusu fizičkog procesa te dobivene podatke prikazuje operatoru na HMI sučelju. Upravljačke stanice se sastoje od RTU-ova i IED-ova koje su u okviru modeliranje korištenjem stvarnog industrijskog hardvera ili virtualizacijom. Komunikacija upravljačkog centra i upravljačkih stanica se odvija korištenjem DNP3 protokola. Svaka upravljačka stanica u okviru ima vlastitu virtualnu privatnu mrežu. WAN (engl. *Wide Area Network*) mreža u okviru je ostvarena integracijom ISEAGE simulacijskog okvira koji omogućava emuliranje mreža velikih dimenzija. U komunikaciji unutar upravljačkih stanica se koristi IEC 61850 protokol. PowerCyber koristi dva alata za simuliranje energetskih sustava. RTDS (engl. *Real Time Digital Simulator*) je platforma koja pruža sposobnost simuliranja energetskih sustava u stvarnom vremenu i omogućava integraciju fizičkih i virtualiziranih komponenata. PowerFactory je alat koji ne nudi simulaciju u stvarnom vremenu i nema mogućnost integracije fizičkih komponenata, ali nudi sposobnost simuliranja vrlo velikih energetskih sustava te sadrži napredne analitičke sustave. Pomoću PowerCyber okvira provedeni pojedinačni i koordinirani napadi na kontrolni sustav kojima su demonstrirane sposobnosti okvira u istraživanju sigurnosti ICS sustava. Dodatno, napadima su otkrivene ranjivosti pojedinih industrijskih uređaja koje su prijavljene proizvođačima.

Sveučilište South Dakota je po uzoru na PowerCyber razvilo okvir koji simulira pametnu elektroenergetsku mrežu koji će moći realistično simulirati sustav u stvarnom vremenu. Energetski sustav okvira je simuliran korištenjem alata RT-LAB [45]. To je alat opremljen digitalnim i analognim ulazno-izlaznim sučeljima koja omogućuju simulaciju u stvarnom vremenu i integraciju fizičkih uređaja. Za prikupljanje podataka fizičkog procesa i kontrolu na niskoj razini koriste se IED-ovi, RTU-ovi i HMI-ovi. Upravljački sustav je podijeljen na upravljački centar i upravljačke stanice koje u međusobnoj komunikaciji koriste protokol DNP3. Mrežni dio okvira je preslika mrežne arhitekture PowerCyber okvira. Nad okvirom su provedeni scenarij napada u kojima

napadač uzrokuje prestanke rada dijela elektroenergetske mreže kako bi se ispitale posljedice sličnih napada na stvarne sustave te su ispitani mehanizmi ublaživanja posljedica kako bi se sustav vratio u željeno stanje.

Istraživači sa sveučilišta Sam Houston su razvili SCADA simulacijski okvir čiji je cilj reproducirati dizajn ICS arhitekture koja se koristi u stvarnim industrijskim postrojenjima [46]. Primarni cilj ovog okvira koji simulira kemijski proizvodni proces je ponuditi studentima sveučilišta istraživačku okolinu u kojoj će moći primijeniti teorijsko znanje. Okvir je izgrađen korištenjem stvarnih i simuliranih PLC-ova, simulacijom SCADA hardvera i HMI sučeljem. Uređaji okvira koriste različite operativne sustave, kao što su Windows 7, Windows XP i Windows 2000, radi vjernijeg prikaza stvarnih sustava. Okvir sadrži dvije baze podataka, jedna koja služi kao primarna baza podataka kontrolnog sustava, a jedna koja služi kao povijesna baza podataka. Okvir posjeduje i poslovnu zonu sa aplikacijama koje simuliraju mrežni promet poslovne zone i koja je od upravljačke zone odvojena vatrozidima u demilitariziranoj zoni. Komunikacijski protokoli korišteni u okviru su Modbus, DNP3, KOYO, OPC DA/UA, CodeSYS i TCP/IP. Kako bi što vjernije prikazali sigurnosne probleme stvarnih sustava, autori okvira su uz zastarjele operacijske sustave koristili slabe lozinke, sustave koji nisu ažurirani, lozinke zapisane na papirima i slabe vatrozide. Funkcionalnost okvira je testirana provođenjem penetracijskih testova, testiranjem lozinki i drugih sličnih eksperimenata. Simulacija industrijskog hardvera uvelike pomaže u skalabilnosti okvira, dok se fizička oprema po potrebi može uklanjati ili dodavati. Glavne zadaće okvira su provođenje obrambenih i napadačkih pokusa, forenzička istraživanja te upravljanje incidentima, ranjivostima i rizikom.

## 4.3 Tablica radova

Tablica 3.1 sadrži popis svih simulacijskih okvira opisanih u poglavljima 3.1 i 3.2. Stupci tablice redom sadrže ime simulacijskog okvira, odnosno ime autora okvira ako okvir nema ime, i referencu na rad koji opisuje okvir, instituciju koja je vlasnik simulacijskog okvira, fizički proces koji je simuliran u okviru, licencu okvira i njegovu relativnu cijenu u odnosu na druge okvire. Tablica radova je podijeljena na dio sa fizičkim i dio sa hibridnim okvirima.

| Ime okvira/Autori | Institucija | Simulirani proces | Licenca | Cijena |
|---|---|---|---|---|
| **Fizički okviri** | | | | |
| SWaT [20] | SUTD | Pročišćivač vode | Edukacijska | Visoka |
| WADI [21] | SUTD | Vodoopskrbni sustav | Edukacijska | Visoka |
| Green et al. [22] | Lancaster University | Generički procesi | Kolaboracijska | Visoka |
| Ahmed et al. [24] | New Orleans | 3 različita procesa | Nedostupan kod | Visoka |
| Morris et al. [25] | Mississippi | 7 različitih procesa | Edukacijska | Srednja |
| LICSTER [26] | Hochschule Augsburg | Proizvodna traka | Otvorenog koda | Niska |
| CENTER [16] | Sakarya University | Pročišćivač vode | Edukacijska | Srednja |
| **Hibridni okviri** | | | | |
| Hui et al. [27] | Queen's University Belfast | Nuklearni reaktor | Nedostupan kod | Srednja |
| SCADASim [28] | RMIT University | Generički proces | Otvorenog koda | Niska |
| VPST [29] | University of Illinois | Elektroenergetska mreža | Nedostupan kod | Niska |
| Urias et al. [30] | Sandia National Laboratories | Generički proces | Nedostupan kod | Niska |
| HYDRA [31] | Universit`a degli Studi Roma Tre | Vodoopskrbni sustav | Otvorenog koda | Niska |
| RESLab [34] | Texas A&M University | Elektroenergetska mreža | Nedostupan kod | Visoka |
| MSICST [36] | - | 4 različita procesa | Nedostupan kod | Visoka |
| NIST simulacijski okvir [38] | NIST | 3 različita procesa | Nedostupan kod | Srednja |
| Stranahan et al. [40] | Rowan University | 2 različita procesa | Nedostupan kod | Niska |
| Noorizadeh et al. [42] | Qatar | Kemijski proizvodni proces | Nedostupan kod | Niska |
| PowerCyber [43] | Iowa State University | Elektroenergetska mreža | Nedostupan kod | Niska |
| Poudel et al. [45] | South Dakota State University | Elektroenergetska mreža | Nedostupan kod | Niska |
| Krishnan et al. [46] | Sam Houston State University | Kemijski proizvodni proces | Nedostupan kod | Niska |

Tablica 3.1 Usporedba hibridnih i fizičkih simulacijski okviri opisanih u radu

# 5. Zaključak

U ovom radu predstavljena je arhitektura industrijskih upravljačkih sustava, sigurnosni problemi koji su nastali modernizacijom upravljačkih sustava te kako simulacijski okviri pomažu u sigurnosnim istraživanjima upravljačkih sustava. Opisani su zahtjevi koje okviri moraju ispuniti kako bi se mogli koristiti u sigurnosnim istraživanjima te su navedena područja primjene u kojima se okviri koriste. Simulacijski okviri su dodatno podijeljeni u kategorije fizičkih, virtualnih i hibridnih te su opisane prednosti i nedostatci pojedine kategorije. Nakon toga predstavljeno opisane su karakteristike sedam fizičkih i četrnaest hibridnih simulacijskih okvira i tablica sa sažetim informacijama svakog okvira.

Simulacijski okviri koji simuliraju industrijske upravljačke sustave su koristan alat u sigurnosnim istraživanjima koja bi bila teško provedena na stvarnim sustavima. Ovaj rad može poslužiti kao uvod u područje sigurnosti industrijskih upravljačkih sustava ili kao dodatni materijal koji će poslužiti u daljnjem istraživanju istih sustava tako da da pregled u postojeće simulacijske okvire koji se koriste u sličnim istraživanjima.

# 6. Literatura


[1] K. Stouffer, S. Lightman, V. Pillitterri, M. Abrams i A. Hahn, »Guide to Industrial Control Systems (ICS) Security,« NIST, 2015.

[2] N. 56/13, *Zakon o kritičnim infrastrukturama,* 2013.

[3] L. Obregon, »Secure Architecture for Industrial Control Systems,« SANS Institute, 2021.

[4] T. Williams, »The Purdue Enterprise Reference Architecture,« IFAC 12th Triennial World Congress, Sydney, 1993.

[5] I. N. Laboratory, »Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program,« Idaho Falls, Idaho, 2008.

[6] S. Groš i M. Vašak, *Sigurnost upravljačkih sustava,* 2016..

[7] »What is Indurstry 4.0?,« IBM, [Mrežno]. Available: https://www.ibm.com/topics/industry-4-0. [Pokušaj pristupa 3 lipanj 2022.].

[8] C. Alcaraz, *Secure Interconnection of IT-OT networks in Industry 4.0,* Malaga: University of Malaga, Spain, 2019..

[9] G. Yadav i K. Paul, *Architecture and Security of SCADA Systems: A review,* School of Information Technology IIW Delhi, India.

[10] A. N. Bessani, P. Sousa, M. Correa, N. F. Neves i P. Verissimo, »The Crutial Way of Critical Infrastructure Protection,« *IEEE Security & Privacy*, pp. 44-51, studeni-prosinac 2008.

[11] M. Cheminod, L. Durante i A. Valezano, »Review of Security Issues in Industrial Networks,« *IEEE Transactions on Industrial Informatics, vol. 9, no. 1,* pp. 277-293, Feb. 2013..

[12] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potuseluevskaya, S. I. Sidrov i A. A. Timorin, »Industrial Control Systems Vulnerabilities Statistics,« Kaspersky Lab, 2016..

[13] D. Albright, P. Brannan i C. Walrond, »Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?,« Institute for Science and International Security, 2010.

[14] R. M. Lee, M. J. Assante i T. Conway, »Analysis of the Cyber Attack on the Ukrainian Power Grid,« E-ISAC, 2016..

[15] M. Conti, D. Donadel i F. Turrin, »A Survey on Industrial Control System Testbeds and Datasets for Security Research,« u *IEEE Communications Surveys & Tutorials, vol. 23, no. 4*, IEEE, 2021, pp. 2248-2294.

[16] İ. Özçelİk, M. İskefiyeli, M. Balta, K. O. Akpinar i F. S. Toker, »CENTER Water: A Secure Testbed Infrastructure Proposal For Waste And Potable Water Management,« Sakarya University, Sakarya, Turkey, 2021..

[17] S. Krishnan i M. Wei, »SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics,« Sam Houston State Univesity, Huntsville, Texas.

[18] A. Hahn, A. Ashok, S. Sridhar i M. Govindarasu, »Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid,« u *IEEE Transaction on Smart Grid, vol. 4, no. 2*, IEEE, 2013, pp. 847-855.

[19] Y. Geng, Y. Wang, W. Liu, Q. Wei, K. Liu i H. Wu, »A survey of industrial control system testbeds,« u *IOP conference series*, 2019.

[20] A. P. Mathur i N. O. Tippenhauer, »SWaT: A Water Treatment Testbed for Research and Training on ICS Security,« *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater),* pp. 31-36, 2016.

[21] C. M. Ahmed, V. R. Palleti i A. P. Mathur, »WADI: A Water Distribution Testbed for Research in the Design of Secure Cyber Physical Systems,« *Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks,* 2017.

[22] B. Green, A. Le, R. Antrobus, U. Roedig, D. Hutchinson i A. Rashid, »Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research«.

[23] W. Jardine, S. Frey i B. Green, »SENAMI: Selective Non-Invasive Active Monitoring for ICS Intrusion Detection,« Assiciation for Computing Machinery, New York, 2016..

[24] I. Ahmed, V. Roussev, W. Johnson, S. Senthivel i S. Sudhakaran, »A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy,« u *the 2nd Annual Industrial Control System Security Workshop*, 2016..

[25] T. Morris, A. K. Srivastava, B. Reaves, W. Gao, K. Pavurapu i R. Reddi, »A control system testbed to validate critical infrastructure protection concepts,« *International Journal of Critical Infrastructure Protection 4.* , pp. 88-103.

[26] F. Sauer, M. Niedermaier, S. Kiessling i D. Merli, »LICSTER -- A Low-cost ICS Security Testbed for Education and Research,« 2019..

[27] H. Hui, P. Maynard i K. McLaughlin, »ICS Interaction Testbed: A Platform for Cyber-Physical Security Research«.

[28] C. Queiroz, A. Mahmood i Z. Tari, »SCADASim - A Framework for Building SCADA Simulations,« u *IEEE Transactions on Smart Grid, vol. 2, no. 4*, doi: 10.1109/TSG.2011.2162432., 2011., pp. 589-597.

[29] D. C. Bergman, D. Jin, D. M. Nicol i T. Yardley, »The Virtual Power System Testbed and Inter-Testbed Integration,« CSET, 2009..

[30] V. Urias, B. Van Leeuwen i B. Richardson, »Suprevisory Command and Data Acquisition (SCADA) system Cyber Security Analysis Using a Live, Virtual and Constructive (LVC) Testbed,« u *IEEE Military Communications Conference*, 2012..

[31] L. Faramondi, F. Flammini, S. Guarino i R. Setola, »A Hardware-in-the-Loop Water Distriburion Testbed Dataset for Cyber-Physical Security Testing,« *IEEE Access, vol. 9*, pp. 122385-122396, 2021..

[32] G. Bernieri, F. Del Moro, L. Faramondi i F. Pascucci, »A Testbed for Integrated Fault Diagnosis and Cyber Security Investigation,« u *2016 International Conference on Control, Decision and Information Technologies (CoDIT)*, 2016..

[33] F. Battisti, G. Bernieri, M. Carli, M. Lopardo i F. Pascucci, »Detecting integrity attacks in IoT-based Cyber Physical Systems: a case study on Hydra testbed,« u *2018 Global Internet of Things Summit (GIoTS)*, 2018..

[34] A. Sahu, P. Wlazlo, Z. Mao, H. Huang, A. Goulart, K. Davis i Z. Zonouz, »Design and Evaluation of A Cyber-Physical Resilient Power System Testbed,« *IET Cyber-Physical Systems: Theory & Applications*, 2021..

[35] P. Wlazo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis i S. Zonouz, »Man-in-The-Middle Attacks and Defense in a Power System Cyber-Physical Testbed,« *IET Cyber-Physical Systems: Theory & Applications* , 2021..

[36] W. Xu, Y. Tao i H. Chen, »MSICST: Multiple-Scenario Industrial Control System Testbed for Security Research,« *Computers, Materials and Continua 58(2*, pp. 691-705, 2019..

[37] Y. Tao, W. Xu, L. Hongbin i S. Ji, »Experience and Lessons in Building an ICS Security Testbed,« u *2019 1st International Conference on Industrial Artificial Intelligence (IAI)*, 2019..

[38] R. Candell, T. Zimmerman i K. Stouffer, »An Industrial Control System Cybersecurity Performance Testbed,« NIST, 2015..

[39] R. Candell, K. Stouffer i D. Anand, »A Cybersecurity Testbed for Industrial Control Systems,« u *2014 Process Control and Safety Symposium, International Society of Automation*, Houston, Texas, 2014..

[40] J. Stanahan, T. Soni i V. Heydan, »Supervisory Control and Data Acquisition Testbed for Research and Education,« u *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019..

[41] J. Stranahan, T. Soni i V. Heydari, »Supervisory Control and Data Acquisition Testbed Vulnerabilities and Attacks,« u *2019 SoutheastCon*, 2019..

[42] .. Noorizadeh, M. Shakerpour, N. Meskin, D. Unal i K. Khorasani, »A Cyber-Security Methodology for a Cyber-Physical Industrial Control System Testbed,« *IEEE Access, vol. 9*, pp. 16239-16253, 2021..

[43] A. Ashok, S. Krishnaswamy i M. Govindarasu, »PowerCyber: A remotely accessible testbed for Cyber Physical security of the Smart Grid,« u *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2016..

[44] A. Hahn, A. Ashok, S. Sridhar i M. Govindarasu, »Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid,« *IEEE Transactions on Smart Grid*, pp. 847-855, 2013..

[45] S. Poudel, Z. Ni i N. Malla, »Real-time cyber physical system testbed for power system security,« 2017..

[46] S. Krishnan i M. Wei, »SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics,« u *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 2019..

**Pregled fizičkih i hibridnih simulacijskih okvira za simulaciju kibernetičkih napada koji imaju posljedice u fizičkom svijetu**


## Sažetak

Modernizacija industrijskih upravljačkih sustava i njihovo spajanje na Internet potencijalnim napadačima izlaže ranjivosti tih sustava koje prije nisu bile dostupne. Kako bi se uklonile ranjivosti upravljačkih sustava i provela sigurnosna istraživanja u upotrebi se nalaze simulacijski okviri koji simuliraju upravljačke sustave. U ovom radu opisana je arhitektura upravljačkih sustava, opisane su karakteristike simulacijskih okvira i predstavljena područja njihove primjene, a potom je dan pregled fizičkih i hibridnih simulacijskih okvira u kojem je opisano dvadeset različitih okvira.



**Ključne riječi**: industrijski upravljački sustavi, simulacijski okviri, kibernetička sigurnost


**Overview of physical and hybrid testbeds for simulation of cybernetic attacks that have an consequences in the physical world**


## Summary

Modernizing industrial control systems and connecting them to the Internet exposes potential attackers to vulnerabilities in these systems that were not previously available. In order to eliminate vulnerabilities in control systems and conduct security research, testbeds that simulate control systems are in use. This paper describes the architecture of control systems, describes the characteristics of testbeds and presents the areas of their application, and then gives an overview of physical and hybrid testbeds in which twenty different testbeds are described.



**Keywords**: industrial control systems, testbeds, cybersecurity

# Skraćenice

| | | |
|---|---|---|
| ICS | *Industrial Control Systems* | Industrijski upravljački sustavi |
| PLC | *Programmable Logic Controller* | Programirljivi logički kontroler |
| RTU | *Remote Terminal Unit* | Udaljena terminalna jedinica |
| IED | *Intelligent Electronic Device* | Inteligentni elektronički uređaj |
| HMI | *Human-Machine Interface* | Sučelje čovjek-stroj |
| SCADA | *Supervisory Control and Data Acquisition* | |
| DCS | *Distributed Control Systems* | Distribuirani kontrolni sustavi |
| ERP | *Enterprise Resource Planning* | Poslovni informacijski sustav |
| DMZ | *Demilitarized zone* | Demilitarizirana zona |
| IDS | *Intrusion Detection Sistem* | Sustav za detekciju upada |