

ИЗПОЛЗВАНЕ НА ЦИФРОВИ ДВОЙНИЦИ И ВИРТУАЛИЗИРАНИ ЛАБОРАТОРНИ СРЕДИ ЗА ИЗСЛЕДВАНЕ НА КИБЕРАТАКИ СРЕЩУ ЕЛЕКТРОЕНЕРГИЙНИ СИСТЕМИ

гл. ас. д-р Димитър Иванов Николов

Висше военноморско училище „Н. Й. Вапцаров“ – Варна

E-mail: d.nikolov@naval-acad.bg

Резюме: *Настоящата статия разглежда възможностите за използване на цифрови двойници и виртуализирани лабораторни среди при изследване на киберзаплахи срещу електропроизводствени, електропреносни и електроразпределителни системи. Анализирани са ограниченията на традиционните подходи за тестване на индустриални системи за управление и необходимостта от експериментални платформи, които съчетават модели на физически процеси, комуникационни протоколи, средства за управление и защитно наблюдение. Предложена е методологична архитектура за безопасно и възпроизводимо провеждане на киберфизически експерименти, основана на функционално разделяне между симулирания електрически процес, виртуализираните контролери, SCADA компонентите и системите за събиране на доказателства. Разгледани са особеностите на протоколите IEC 60870-5-104, DNP3, Modbus TCP и PROFINET, както и възможностите за използване на процесно ориентирана телеметрия при откриване на аномалии. Формулирани са критерии за оценяване на достоверността, наблюдаемостта, повторяемостта и безопасността на лабораторните изследвания. Представеният подход има методологичен характер и е предназначен за последващо експериментално валидиране.*

Ключови думи: *цифров двойник, електроенергийни системи, индустриални системи за управление, SCADA, виртуализация, киберфизическа сигурност, IEC 60870-5-104, DNP3, киберустойчивост.*

DIGITAL TWINS AND VIRTUALIZED TESTBEDS FOR INVESTIGATING CYBERATTACKS AGAINST ELECTRIC POWER SYSTEMS

chief assist. professor **Dimitar I. Nikolov, PhD**

Nikola Vaptsarov Naval Academy – Varna

E-mail: d.nikolov@naval-acad.bg

Abstract: *This article examines the application of digital twins and virtualized testbeds to cybersecurity research involving power generation, transmission, and distribution systems. It analyzes the limitations of conventional industrial control system security testing and the need for experimental platforms combining physical process models, industrial communication protocols, supervisory control components, and defensive monitoring. A methodological architecture is proposed for safe and reproducible cyber-physical experiments, separating the simulated electrical process from virtualized controllers, SCADA components, and evidence collection systems. The study discusses IEC 60870-5-104, DNP3, Modbus TCP, and PROFINET, together with the role of process-aware telemetry in anomaly detection. Evaluation criteria are introduced for experimental fidelity, observability, reproducibility, and operational safety. The proposed approach is methodological and requires subsequent empirical validation.*

Keywords: *digital twin, electric power systems, industrial control systems, SCADA, virtualization, cyber-physical security, IEC 60870-5-104, DNP3, cyber resilience.*

1. ВЪВЕДЕНИЕ

Съвременните електроенергийни системи представляват сложни киберфизически инфраструктури, в които информационните и комуникационните технологии участват непосредствено в управлението на производството, преноса и разпределението на електрическа енергия. Диспечерските центрове, системите за автоматизация на подстанции, програмируемите контролери и отдалечените терминални устройства осигуряват непрекъснат обмен на измервания, команди и технологични състояния. Разширяването на цифровата свързаност създава условия за по-ефективно управление, но едновременно с това увеличава зависимостта на физическите процеси от надеждността и сигурността на комуникационната инфраструктура. Специфичните изисквания към оперативните технологии, включително тяхната наличност, надеждност и безопасност, са разгледани подробно в NIST SP 800-82 Rev. 3 (STOUFFER et al., 2023).

Провеждането на киберексперименти върху действащи електроенергийни съоръжения е ограничено от потенциалните последствия за технологичната непрекъснатост и физическата безопасност. Определени тестови действия могат да засегнат комуникацията с контролерите, достоверността на измерванията или изпълнението на управляващите алгоритми. Дори когато проверката е насочена към информационен компонент, нейното въздействие може да се прояви в реалния процес чрез забавена реакция, неправилно състояние на оборудването или загуба на наблюдаемост. Тези обстоятелства налагат разработването на експериментални среди, в които киберсъбитията могат да бъдат изследвани без пренасяне на риска към производствената инфраструктура.

Виртуализираните лабораторни платформи и цифровите двойници предоставят възможност за контролирано възпроизвеждане на определени характеристики на индустриалните системи. Чрез тях могат да бъдат моделирани комуникационни зависимости, логика на управление, технологични състояния и защитни механизми. Изследването на Conti, Donadel и Turrin (2021) систематизира особеностите на експерименталните ICS среди и използваните набори от данни, като показва значението на тяхната архитектура и предназначение за достоверността на научните резултати. Разработката ICSSIM допълва тази проблематика чрез рамка за изграждане на индустриални тестови среди с виртуализирани и симулирани компоненти (DEHLAGHI-GHADIM et al., 2023).

Целта на настоящата статия е да се предложи методологична рамка за използване на цифрови двойници и виртуализирани лабораторни среди при изследване на кибератаки срещу електроенергийни системи. Обект на изследването са експерименталните киберфизически среди, а предмет — възможностите за съвместно моделиране на електрически процеси, индустриална комуникация и защитно наблюдение. Използваният подход включва сравнителен анализ на научни публикации, функционално моделиране на лабораторна архитектура и формулиране на критерии за експериментална проверка. Предложеният модел не представлява описание на напълно валидирана физическа инсталация, а основа за последващи възпроизводими изследвания.

2. ЦИФРОВИ ДВОЙНИЦИ И ЕКСПЕРИМЕНТАЛНИ СРЕДИ В КИБЕРФИЗИЧЕСКАТА СИГУРНОСТ

Понятието „цифров двойник“ обозначава цифрово представяне на физически обект или процес, което позволява анализ на неговото състояние и поведение чрез модели и данни. В контекста на електроенергийната сигурност е необходимо това понятие да бъде използвано прецизно. Самостоятелен симулационен модел, който не обменя информация с реален физически обект, не следва автоматично да се определя като пълнофункционален цифров двойник. За лабораторни изследвания е по-точно да се разграничават симулиран процес, виртуализирана управляваща система и цифров двойник с установена връзка към представяния физически обект. Това разграничение има значение за оценяването на достоверността на получените резултати и за възможността те да бъдат пренесени към действителна инфраструктура.

Научните публикации за индустриални тестови среди показват, че съществуват различни подходи към представянето на технологичната инфраструктура. Физическите лаборатории използват реални контролери, сензори и изпълнителни механизми, докато виртуалните среди възпроизвеждат част от функционалността чрез софтуерни компоненти. Хибридните архитектури комбинират двата подхода, като предоставят възможност за изследване на взаимодействието между реални устройства и моделирани процеси. Известната изследователска среда SWaT демонстрира приложението на физически индустриален тестов стенд за изследване и обучение по киберсигурност (MATHUR; TIPPENHAUER, 2016). Нейното значение за електроенергийния сектор е методологично, тъй като технологичният процес на пречистване на вода се различава съществено от динамиката на електрическите мрежи.

Виртуализацията предоставя предимства по отношение на възстановяването на първоначалното състояние, управлението на конфигурациите и възможността за паралелно изпълнение на различни експерименти. Тя позволява отделяне на комуникационните роли, контролерите, операторските интерфейси и защитните системи в самостоятелни логически компоненти. От друга страна, софтуерната емуляция невинаги възпроизвежда времевите характеристики, хардуерните ограничения и механизмите за безопасност на действителните индустриални устройства. Поради това достоверността на виртуалната платформа трябва да се оценява по отношение на конкретната изследователска задача, а не чрез общото

твърдение, че средата имитира определена промишлена инсталация (CONTI; DONADEL; TURRIN, 2021).

Използването на цифрови модели създава допълнителни възможности за защитно наблюдение. Когато поведението на физическия процес е представено чрез независим математически модел, получените от SCADA измервания могат да бъдат съпоставяни с очакваните стойности. Разработките в областта на цифровите двойници за откриване на прониквания в индустриални системи разглеждат подобно съпоставяне като възможен източник на допълнителни индикатори за аномално поведение (VARGHESE et al., б. г.). Независимо от това несъответствието между модел и наблюдение не представлява само по себе си доказателство за кибератака, тъй като може да произтича от неточни параметри, непредвиден преходен режим или техническа неизправност.

3. АРХИТЕКТУРА НА ВИРТУАЛИЗИРАНА ЛАБОРАТОРНА СРЕДА ЗА ЕЛЕКТРОЕНЕРГИЙНИ СИСТЕМИ

Предложената архитектура се основава на функционално разделяне между симулирания електрически процес, индустриалните управляващи компоненти, комуникационната инфраструктура и системите за защитно наблюдение. В технологичния слой се разполагат модели на електропроизводствени и електроразпределителни процеси, които предоставят измервания и приемат предварително разрешени управляващи въздействия. Контролният слой включва виртуализирани PLC и RTU компоненти, които обменят данни с операторските станции и SCADA системата. Отделен защитен сегмент осигурява събиране на мрежова телеметрия, системни събития и технологични времеви редове. Подобна организация позволява изследването на различни аспекти на киберфизическата сигурност, без наблюдаващите компоненти да получават неограничен достъп до управлението на процеса.

Мрежовата сегментация трябва да отразява функционалните зависимости между корпоративните и индустриалните системи. Виртуалната инфраструктура може да бъде организирана в административен сегмент, тестова корпоративна мрежа, междинна защитена зона, SCADA мрежа, мрежа на контролерите и самостоятелен сегмент за събиране на доказателства. Разпределението може да използва принципите на йерархичните индустриални архитектури, но не следва да се представя като пълно съответствие със стандартите за индустриална сегментация без отделна проверка на

зоните, комуникационните зависимости и правилата за достъп. Практическата реализация изисква контролирано маршрутизиране, ограничени комуникационни услуги и забрана за непредвиден обмен с производствени мрежи (STOUFFER et al., 2023).

Съществена част от архитектурата представлява моделирането на електрическия процес. За електропроизводствен обект могат да бъдат представени измененията на активната мощност, напрежението, честотата и състоянието на основни управляващи елементи. При електроразпределителните системи моделът може да включва натоварвания, комутационни състояния, измервания в разпределителни възли и допустими работни диапазони. Изборът на параметри трябва да съответства на конкретния клас изследвани съоръжения, като не се допуска механично пренасяне на опростени модели между различни технологични обекти. Специализираната литература по управление на технически обекти и сигурност на електроенергийните системи предоставя основа за разграничаване на управляващата логика от динамиката на физическия процес (ДЖАГАРОВ, 2018; ДЖАГАРОВ, 2026).

За осигуряване на независима оценка е необходимо моделът на физическия процес да функционира отделно от източника на измервания, който подлежи на проверка. Ако защитната система използва единствено стойностите, предоставяни от потенциално компрометиран SCADA компонент, тя може да не разполага с достатъчна информация за установяване на тяхната недостоверност. Самостоятелният процесен модел предоставя референтни данни за сравнение, при условие че неговите параметри са предварително определени и не се изменят неконтролирано по време на експеримента. Подобен принцип е приложим и при изследване на алгоритми за откриване на аномалии, при които независимостта на еталонните данни има пряко значение за достоверността на оценката (KRAVCHIK; SHABTAI, 2018).

Виртуализираната среда може да използва отделни софтуерни компоненти за PLC логика, RTU комуникация, SCADA функции, операторска визуализация и събиране на данни. Изборът на конкретна платформа трябва да бъде съобразен с реално поддържаните протоколи, ограниченията на лицензите и възможността за фиксиране на софтуерните версии. Особено важно е да се разграничава функционалното изпълнение на протоколна операция от пълната емуляция на конкретно индустриално устройство. Например библиотека, която поддържа определени S7 съобщения, не възпроизвежда непременно всички защитни механизми и инженерни процедури на физически

контролер. Изследването Rogue7 показва значението на специфичните особености на инженерните станции и реалните PLC реализации за анализа на индустриалните заплахи (BINAM et al., 2019).

4. ИНДУСТРИАЛНИ ПРОТОКОЛИ И КИБЕРФИЗИЧЕСКИ СЦЕНАРИИ

Индустриалните комуникационни протоколи представляват основен компонент на лабораторната архитектура, тъй като осигуряват обмена между управляващите устройства, операторските системи и симулирания технологичен процес. При електроенергийните инфраструктури особено значение имат IEC 60870-5-104 и DNP3, които се използват в системи за телеметрия и дистанционно управление. Modbus TCP може да бъде приложен при определени устройства и лабораторни контролери, докато PROFINET има отношение към индустриалната автоматизация и комуникацията с полеви устройства. Използването на тези протоколи в една експериментална среда позволява сравняване на различни комуникационни модели, но не означава, че всеки от тях има еднаква приложимост към всички електроенергийни обекти.

За IEC 60870-5-104 изследователският интерес може да бъде насочен към типовете информационни обекти, последователността на съобщенията, адресирането, времевите характеристики и състоянието на комуникационните сесии. При DNP3 могат да бъдат наблюдавани ролята на управляваща и подчинена станция, функционалните кодове, типовете данни и механизмите за обмен на измервания. Важно методологично изискване е да бъде доказано, че лабораторната реализация действително обменя технологично свързани данни, а не само установява мрежова връзка. Успешното отваряне на комуникационен порт или регистрирането на протоколен пакет не представлява достатъчно доказателство за коректно функциониране на киберфизическия модел.

При PROFINET ограниченията на виртуализацията са особено съществени поради специфичните времеви изисквания и зависимостта от реалната комуникационна инфраструктура. Възпроизвеждането на предварително записан трафик позволява анализ на определени протоколни характеристики, но не доказва функциониране на цикличен обмен в реално време. Съответно резултатите от пасивен анализ, софтуерна емуляция и реален обмен между контролер и полево устройство трябва да бъдат разграничавани. Изследването на Meshram et al. (2023), посветено на моделирането на поведението при PROFINET операции, показва значението на комуникационните закономерности за индустриалното наблюдение. То обаче не премахва необходимостта

от отделна проверка на функционалността и времевите характеристики на конкретната лабораторна реализация.

Сценариите за изследване на киберзаплахи следва да бъдат ориентирани към предварително определени защитни въпроси. В електропроизводствена среда могат да бъдат разглеждани нарушения в достоверността на измерванията, отклонения в последователността на разрешени управляващи действия и промени в комуникационната видимост. При електроразпределителните системи интерес представляват нехарактерни заявки към отдалечени устройства, несъответствия между отчетени и моделирани състояния и прекъсвания на наблюдението. Всички тестови въздействия трябва да бъдат ограничени до безопасни лабораторни стойности, а тяхната последователност — предварително документирана. По този начин се създава възможност за анализ на защитното поведение, без да се възпроизвеждат опасни въздействия върху реални съоръжения.

Изследователската стойност на подобни сценарии зависи от способността да бъдат разграничени нормалните технологични преходи от целенасочените отклонения. При промяна на електрически товар например могат да възникнат изменения в токовете и напреженията, които не представляват признак за злонамерено действие. Обратно, определена комуникационна операция може да изглежда допустима на протоколно ниво, но да противоречи на текущите ограничения на процеса. Следователно лабораторният модел трябва да включва не само очакваните признаци на кибервъздействие, но и достатъчно разнообразни нормални режими, за да се избегне изкуствено завишаване на ефективността на защитните алгоритми (INOUE et al., 2017).

5. ЗАЩИТНО НАБЛЮДЕНИЕ, ДОКАЗАТЕЛСТВА И ОЦЕНЯВАНЕ НА ЕКСПЕРИМЕНТАЛНАТА СРЕДА

Защитното наблюдение в киберфизическа лаборатория трябва да обединява мрежова, системна и технологична информация. Мрежовите сензори предоставят сведения за комуникационните участници, използваните протоколи и характеристиките на обмена, докато системните журнали документират събития от операторските станции, сървърите и управляващите приложения. Процесната телеметрия допълва тези данни с информация за електрическите величини и състоянието на симулираните съоръжения. Комбинираният анализ позволява да бъдат изследвани случаи, при които определено действие е видимо на мрежово ниво, но неговото технологично значение може да бъде установено единствено чрез съпоставяне с физическия модел.

Публикациите за откриване на атаки чрез машинно обучение показват потенциала на времевите редове, но същевременно поставят въпроси относно представителността на използваните данни (KRAVCHIK; SHABTAI, 2018).

Надеждното събиране на доказателства изисква предварително определена структура на експерименталните записи. За всяко изпълнение трябва да бъдат документиран идентификаторът на сценария, конфигурацията на средата, версиите на компонентите, началното технологично състояние и времевите характеристики на действията. Суровите мрежови записи, системните събития и технологичните измервания следва да бъдат съхранявани независимо от последващите аналитични обобщения. Използването на времева синхронизация и механизми за проверка на целостта позволява да се реконструира последователността на наблюдаваните събития и да се установи дали защитният сигнал съответства на конкретно тестово действие. Подобна организация създава основа за проверимост на научните резултати и за повторно анализиране на експерименталните данни.

Оценяването на лабораторната платформа може да се основава на четири взаимосвързани критерия: функционална достоверност, наблюдаемост, повторяемост и безопасност. Функционалната достоверност характеризира степента, в която моделираните устройства, комуникационни операции и електрически процеси изпълняват предварително определените изисквания. Наблюдаемостта отразява възможността действията и техните последствия да бъдат установявани чрез независими източници на данни. Повторяемостта се определя от способността за възстановяване на началните условия и получаване на съпоставими резултати. Безопасността оценява дали експерименталните въздействия остават в допустимите граници и дали съществуват надеждни механизми за прекратяване. Тези критерии представляват предложена методологична система, а не експериментално валидирана универсална оценъчна скала.

При сравняване на различни конфигурации или алгоритми за откриване е необходимо да се използват еднозначни измервателни правила. Подходящи показатели могат да бъдат делът на правилно откритите тестови събития, честотата на погрешните предупреждения, времето за откриване и качеството на установените технологични зависимости. Отделно следва да се измерват ресурсното натоварване, забавянето на комуникацията и стабилността на симулирания процес, тъй като те могат да влияят върху наблюдаваните резултати. Статистическата интерпретация изисква достатъчен

брой повторения, контрол върху променливите и подходящ избор на метод за сравнение. Demšar (2006) разглежда ограниченията при статистическо сравняване на класификатори върху множество набори от данни; неговите изводи подчертават необходимостта от внимателен подбор на сравнителната процедура, без автоматично да предоставят готов статистически модел за всеки киберфизически експеримент.

Особено важно е разграничаването между вътрешна и външна валидност. Успешното откриване на аномалия в определена виртуална среда доказва единствено, че използваният механизъм е функционирал при конкретните условия на теста. От това не следва непосредствено, че същият резултат ще бъде постигнат при различни производители на оборудване, мрежови натоварвания, топологии или технологични режими. Изследванията върху индустриалните системи подчертават многообразието на архитектурите и необходимостта от отчитане на специфичните ограничения на всяка инсталация (BHAMARE et al., б. г.). Следователно лабораторните резултати трябва да бъдат представяни заедно с описанието на използваните модели, ограниченията на емуляцията и условията, при които е допустимо тяхното обобщаване.

6. ЗАКЛЮЧЕНИЕ

Предложената методологична рамка показва възможностите за съчетаване на виртуализация, моделиране на електрически процеси и защитно наблюдение в единна експериментална среда. Нейното основно предимство е функционалното разделяне между технологичната симулация, комуникационната инфраструктура и източниците на доказателства. Подобна организация позволява определени киберсъбития да бъдат анализирани едновременно по отношение на мрежовото им проявление и потенциалното им въздействие върху управлението процес. Съществено ограничение остава степента на съответствие между виртуализираните компоненти и действителното индустриално оборудване, особено при времечувствителни протоколи, специфични инженерни функции и механизми за физическа безопасност. Поради това методологията трябва да бъде прилагана чрез последователна верификация на отделните компоненти, а не чрез предварително допускане за пълна еквивалентност между лабораторната и производствената среда.

За електроенергийните системи особено значение има разработването на представителни модели за електропроизводство и електроразпределение, които

позволяват анализ на измервания, комутационни състояния и допустими оперативни режими. Интегрирането на индустриални протоколи, независима процесна телеметрия и централизирано събиране на доказателства създава предпоставки за възпроизводими изследвания на киберфизическата сигурност. Бъдещото експериментално валидиране следва да включва проверка на реалния протоколен обмен, съответствието между управляващите действия и симулираните електрически величини, надеждността на защитното наблюдение и възможността за възстановяване на началното състояние. При изпълнение на тези условия виртуализираните лабораторни среди могат да подпомогнат разработването и сравнителното оценяване на защитни механизми, без да създават неоправдан риск за действащата критична инфраструктура.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. BHAMARE, Deval; ZOLANVARI, Maede; ERBAD, Aiman; JAIN, Raj; KHAN, Khaled; MESKIN, Nader. Cybersecurity for Industrial Control Systems: A Survey. *Computers & Security*, 2020, Vol. 89, Article 101677. DOI: <https://doi.org/10.1016/j.cose.2019.101677>.
2. BIHAM, Eli; BITAN, Sara; CARMEL, Aviv; DANKNER, Alon; MISHRA, Uriel; O'FLYNN, Colin. Rogue7: Rogue Engineering-Station Attacks on S7 Simatic PLCs. In: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020. [Публикация, свързана с изследването Rogue7.]
3. CONTI, Mauro; DONADEL, Denis; TURRIN, Federico. A Survey on Industrial Control System Testbeds and Datasets for Security Research. *IEEE Communications Surveys & Tutorials*, 2021.
4. DEHLAGHI-GHADIM, Amir et al. ICSSIM – A Framework for Building Industrial Control Systems Security Testbeds. *Computers in Industry*, 2023. DOI: <https://doi.org/10.1016/j.compind.2023.103906>.
5. DEMŠAR, Janez. Statistical Comparisons of Classifiers over Multiple Data Sets. *Journal of Machine Learning Research*, 2006, Vol. 7, pp. 1–30. Достъпно на: <https://jmlr.org/papers/v7/demsar06a.html>.
6. INOUE, Jun et al. Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning. 2017.
7. KRAVCHIK, Moshe; SHABTAI, Asaf. Detecting Cyberattacks in Industrial Control Systems Using Convolutional Neural Networks. 2018.
8. MATHUR, Aditya P.; TIPPENHAUER, Nils Ole. SWaT: A Water Treatment Testbed for Research and Training on ICS Security. In: *International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*. IEEE, 2016.

9. MESHRAM, Aniket et al. POET: A Self-learning Framework for PROFINET Industrial Operations Behaviour. 2023. DOI: https://doi.org/10.1007/978-3-031-33458-0_1.
10. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Protecting Information and System Integrity in Industrial Control System Environments. NIST Special Publication 1800-10. Gaithersburg: NIST. Достъпно на: <https://www.nccoe.nist.gov/projects/protecting-information-and-system-integrity-industrial-control-system-environments>.
11. STOUFFER, Keith et al. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82, Revision 3. Gaithersburg: National Institute of Standards and Technology, 2023. DOI: <https://doi.org/10.6028/NIST.SP.800-82r3>.
12. VARGHESE, S. A. et al. Digital Twin-based Intrusion Detection for Industrial Control Systems. [Научна публикация от библиотеката DSc_sources; пълните издателски данни подлежат на уточняване.]
13. ДЖАГАРОВ, Н. Управление на технически обекти чрез програмируеми логически контролери. Варна, 2018.
14. ДЖАГАРОВ, Н. Сигурност на електроенергийните системи. Варна, 2026.
15. MILLER, Douglas et al. Automated Adversary Emulation: A Case for Planning and Acting with Unknowns. MITRE, 2018. Достъпно на: <https://www.mitre.org/news-insights/publication/automated-adversary-emulation-case-planning-and-acting-unknowns>.
16. SCARFONE, Karen; SOUPPAYA, Murugiah; CODY, Amanda; OREBAUGH, Angela. Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115. Gaithersburg: National Institute of Standards and Technology, 2008. DOI: <https://doi.org/10.6028/NIST.SP.800-115>.