EasyChair Preprint

№ 9327

The Importance of the Impact Determination Workflow in the Cyber Security Assessment of Industrial Plants and Objects

Sándor Semperger and István Dénes

November 16, 2022

Impact detemination munkafolyamat jelentősége az ipari üzemek és objektumok kiberbiztonsági felmérésénél

DR. Semperger Sándor

Óbudai Egyetem, **Bécsi** út 94-96, H1034 Budapest, Hungary, semperger.sandor@kvk.uni-obuda.hu

Dénes István

Accenture ISS Kft, Hauszmann Alajos utca 2, H1116 Budapest Hungary, i.denes2accenture.com

Az előadás azt taglalja, hogy miért fontos egy komolyabb ipari üzem vagy egyéb ipari objektum irányító rendszere (OT, Operational Technology) kiberbiztonsági vizsgálatánál részletesen felmérni és számszerűsíteni egy jövőben bekövetkező támadás lehetséges következményeit.

Az OT akár több ezer számítástechnikai eszközből állhat. Ezek kiberbiztonsági védelme elsősorban a létesítmény rendelkezésre állásának fenntartását célozza.

Az ipari objektum OT-ján belül az összes ilyen eszközt reálisan nem lehet minden elképzelhető támadástól megvédeni. A reális cél csak annak elérése lehet, hogy a támadás ráfordításai (beleértve a támadó mérnöki óradíjának becsült piaci értékét) lényegesen magasabbak legyenek, mint a támadás által okozott lehetséges kár és a támadó ezzel arányos várható jutalma.

Ennek fényében az OT kiberbiztonsági felmérésének első lépése egy leginkább valószínűsíthető támadás következményeinek felbecsülése (Impact Determination) kell hogy legyen a legrosszabb eset figyelembe vételével. Ezt három lépésben lehet megtenni:

- Első lépésben körben le kell szűkíteni a komolyabb vizsgálat alá vont eszközök vagy eszköz típusok számát (Risk Framing)

- Második lépésben a risk framing során kiválasztott eszközökre vagy eszköz típusokra egyenként számszerűsíteni kell egy lehetséges támadás elképzelhető legrosszabb következményeit (Impact Determination).

- Harmadik lépésben a risk framing során kiválasztott eszközökre meg kell állapítani a védelem azon legalacsonyabb szintjét (Target Security Level, SL-T), ahol egy támadás ráfordításai már lényegesen meghaladják a következmények által okozott kárt vagy a támadó várható jutalmát.

Az előadás a fent ismertetett munkafolyamat kivitelezését vázolja röviden.

Kulcsszavak: ipari kiberbiztonság, lehetséges hatás, következmény, Impact Determination

Bevezetés

Az ipari és infrastrukturális objektumok kiberbiztonságával foglalkozó ANSI/ISA 62443-2-1 (99.02.01)-2009 szabvány "4.2.2 Element: Business rationale"[5] fejezete szerint "Az üzleti indoklás elengedhetetlen ahhoz, hogy a szervezet vezetése megfelelő szinten támogassa a befektetéseket az ipari automatizálási rendszerek kiberbiztonsági programjába".

Más szóval, mielőtt kiberbiztonságra kérnénk pénzt, meg kell tudnunk mondani, hogy mekkora kárt hárítunk el vele.

A jelenlegi gyakorlat viszont általában rögtön az eszközök és hálózatok kitettségének oldaláról közelíti meg az ipari objektumok kiberbiztonságát, ami téves következtetésekhez vezethet.
Ez emberileg érthető, hiszen az ipari objektumok kiberbiztonságával többnyire informatikusok foglalkoznak, akik inkább a számítógépek és hálózatok világában mozognak otthonosan, a valós ipari folyamatokhoz, beleértve a PLC-ket, nem értenek.

A kutatásunk éppen ezért az ipar elleni kibertámadások várható következményeinek hatékony és pontos felmérésére ad egy olyan módszertant, amellyel az informatikus az ipari folyamat ismeretének hiányát egy kvalitatív elemzéssel tudja pótolni.

A fent vázolt törekvésünket támasztja alá Daniele Del Sale "Operational Technology Services to Support Business Activities" [9] című írása, amely szintén az ipari folyamat elemzésének oldaláról közeliti meg az ipari kiberbiztonságot. "Egy viszonylag új szempont, hogy az IT nem csak adatfeldolgozást végezhet, de gyakran berendezések monitorozására és ellenőrzésére használják, beleértve OT berendezéseket is, ezáltal kézzelfoghatóan kihatnak a fizikai folyamatokra"
Ez, szembemenve a korábbi szigorú IT (informatika) és OT (automatizálás) elkülönítéssel, minden számítástechnikai eszközt, akár OT, akár IT, vizsgál az ipari kiberbiztonság szemszögéből.
Ennek fényében még egy SAP rendszer is érdekes lehet az ipari kiberbiztonság oldaláról, amennyiben az ipari folyamat működésének feltétele például a Process Order megléte.

A módszertan kialakulása. Az ANSI/ISA 62443-2-1 szabvány nem tartalmaz útmutatást arra, hogy mily módon becsüljük meg egy kibertámadás lehetséges következményét. Ennek ellensúlyozására a szerzők hosszú évek során alakították ki azt a gyakorlatot, hogy célzott beszélgetéseket folytattak az ipari objektumok dolgozóival a várható következmények megértése céljából. A kutatás által vázolt módszertan ebből a gyakorlatból kristályosodott ki.

Alapfogalmak. A kutatás az alábbi, szabványok által meghatározott fogalmak magyar fordítását használja:

IACS	Ipari Automatizálási rendszer (ISA ANSI 63443-1-1, 3.3 Abbrevations[17])
Kiberbiztonság	Egy rendszer kiberbiztonsági védelmére tett intézkedések (ISA/ANSI 642443-1-1, 3.2.98 / 1 [17])
Kiberbiztonsági incidens	Olyan kiberbiztonsági esemény, melynek hatása választ és kárenyhítést igényel,(NIST Cybersecurity Framework, V1.1[6])
Lehetséges hatás	Egy kiberbiztonsági incidens közvetlen következménye. Lehet pl. control funkció elvesztése, kijelzett érték manipulálása SCADA-n, adatvesztés
Következmény	Egy adott kiberbiztonsági esemény eredménye (ISA/IEC 642443-2-1, 3.1.11)
Impact Determination	Egy IACS eszközön esetlegesen a jövőben bekövetkező kiberbiztonsági incidens várható legsúlyosabb következményének meghatározása az ISA/ANSI 642443-3-2 [1] szabvány szerint
Biztonság kockázatától,	mentesség a fizikai sérülés elfogadhatatlan MSZ EN/IEC61508 2010:CMV [2]

Jelen kutatás az első részében felvázolja a Impact Determination jelenlegi értelmezését és helyét az IACS kiberbiztonságban.

Második részében ismerteti a javasolt módszertant egy nagy egészségügyi mosoda példáján levezetve.

Irodalmi áttekintés

Az ISA 62443-3-2 [1] szabvány szerint
”minden, az 5.1 és 5.2 fejezetben azonosított fenyegetésre és kitettségetre meg kell határozni a lehetséges hatásokat és következményeket a fenyegetés bekövetkeztének esetére. A következményeket az alábbi területekre kell dokumentálni: emberéletben keletkezett kár, pénzügyi veszteség, kiesett termelés és környezeti kár ” (ISA 62443-3-2 [1] 5.3 Determine Consequence and Impact). Mi a következmények körét kissé kiszélesítettük, mint alább látni fogjuk.

A szabvány olyan források használatát javasolja a következmények felmérésére, amelyek eredetileg nem kiberbiztonsági célra készültek. Ezek egyrészt a funkcionális biztonság területéről származó források, másrészt az üzemek eszköztárában (remélhetőleg) fellelhető kritikalitás információ.

Funkcionális biztonság területéről származó források használhatósága

Minden komolyabb üzem rendelkezik Process Hazard Analysis-el (PHA). A PHA az „ipari folyamat egészének potenciális veszélyeire vonatkozó szisztematikus és célirányos vizsgálatainak gyűjteménye” (PHA Process Hazard Analysis: ISA 62443-3-2 (99.03.02), 3.1.14 [1]). A ISA 62443-3-2 szabvány ezt javasolja a következmények meghatározása egyik forrásának.

A funkcionális biztonság területéről származó felmérések kiberbiztonsági alkalmazására vannak egyéb kezdeményezések is. Andrew J Clarck vezetésével készült “Cyber Process Hazard Analysis and Risk Management” [7] c. tanulmány leírja a Hazard and Consequence analysis for Digital Systems (HAZCADS) módszert: “(HAZCADS) kombinálja a Systems Theoretic Process Analysis (STPA) a Fault Tree Analysis (FTA)-val” azaz HAZCADS e két, funkcionális biztonság területen alkalmazott módszer ötvözésével hoz létre kiberbiztonsági incidensek következményeinek elemzésére alkalmas eljárást.

Mind a PHA, mind a HAZCADS alkalmazásának az a korlátja, hogy csak emberéletben keletkező és környezeti kárral foglalkozik, nem érinti például a kiberbiztonság szempontjából fontos termelés kiesés kockázatát.

Emellett a „Process hazard analysis... [8]” írás más oldalról is kétségbe vonja a funkcionális biztonságra kidolgozott metodológiák használhatóságát: eszerint ezek

”Alapvetően az emberi képzelőerőre támaszkodnak a káresemények kialakulásának irányáról, a következmények mélységének és kiterjedtségének felbecslésekor” Mivel azonban egy kiberbiztonsági incidens következményeire nem áll rendelkezésre sok precedens, ezért a felméréseknél a képzelőerő helyett csak a folyamat közelében levő emberek tudására támaszkodhatunk.

A kritikalitás használhatósága

A másik forrás, amit a szabvány említ, az eszközleltárakban fellelhető Criticality információ (ISA 62443-3-2 (99.03.02), Partition the System under Consideration). Ennek a forrásnak a mi szempontunkból az a korlátja , hogy, mint a “Data taxonomy to manage information and data in Maintenance Management” írásában A. Polenghi, I. Roda, M. Macchi és A. Pozzetti [12] kifejti, „a kritikalitás megállapítására végzett adatelemzés célja a karbantartás management támogatása az eszközleltár irányából” Vagyis egy incidens során várható kiszámíthatatlan viselkedés következményeire ez aligha ad támpontot.

A fentiek mellet az ipari kiberbiztonsági felmérések során gyakran alkalmazzák az alapvetően kormányzati rendszerek biztonságára készített NIST 800 framework Risk Criteria módszertanát, amely a kockázatok elviselhetőségét számszerűsíti (NIST Special Publication 800-30 rev.1, Guide for Conducting Risk Assessments [6]). Ez egy hasznos eszköz a már ismert következmények számszerűsítésére, az elemzésükre azonban nem ad segitséget.

Impact Determination az ipari folyamat felöl megközelítve

Kevés szakirodalom foglalkozik az ipari folyamat ismeretének fontosságával a IACS kiberbiztonsági Impact Determination készitése során.

Ennek egyik oka, mint a bevezetőben írtuk, hogy a Impact Determination-al nagyobbrészt informatikusi végzettséggel rendelkező szakemberek foglalkoznak, akik gyakran idegenkednek a számukra kevésbé ismert IACS komponensektől, az egyes komponensek elleni támadások lehetséges következményeit pedig végképp nem képesek jól felmérni.

Ez tetten érhető ”A review of cyber security risk assessment methods for SCADA systems” ,[13} című, egyébként igényes publikációban, amely a SCADA rendszer kiberbiztonságát szinte minden irányból vizsgálja, a PLC, RTU és a hozzájuk tartozó protokolok felől érkező támadásokkal viszont nem foglalkozik.

Ezzel szemben az utóbbi időben egyre több forrás hiányolja a PLC kódok védelmére tett erőfeszítéseket. ” Most of the research related to PLC threats or attacks focuses on the hardware portion of ICS or SCADA systems such as: industrial components, peripheral devices, or networks. It does not adequately

discuss PLC code-level vulnerabilities and attacks" (PLC Code-Level Vulnerabilities [14]).

A hagyományos PLC-k sebezhetőségén is túlmutat, hogy egyre több Windows alapú PLC jelenik meg. Ezeket a "soft PLC"-ket ráadásul előszeretettel használják az OT security támadások szempontjából vonzó célpontot képező villamos hálózatokban: "..the control system is becoming more and more complex, the requirement of PLC is also becoming more and more high, multi-core PLC came into being" (PLC Controller in Electric Control System,[11]).

A fent vázolt felismerésektől vezérelve alakítottunk ki egy olyan módszertant, amely az ipari folyamat felől közelítve meg a kiberbiztonságot, minden lehetséges számítástechnikát tartalmazó eszköz hatását vizsgálja a műszerezéstől a termelés irányitó szintig.

3. A módszertan ismertetése

A módszernek az a célja, hogy minél jobban megismerjük az ipari folyamatot és olyan következményekről is információt szerezzünk, amelyek az eddig ismert módszerekkel nem felderíthetőek. Ehhez olyan emberek bevonására vállalkoztunk, akikkel általában a kiberbiztonsági szakemberek nem nagyon foglalkoznak.

A hatásvizsgálathoz fókuszcsoportot hoztunk létre a kiválasztott szakemberekből és szerepjátékkal, narratívák felvázolásával irányítottuk a beszélgetést.

A fókuszcsoport összetétele

Egy Impact Determination fókuszcsoportban legfeljebb 3 ember vett részt:

az egyik olyan volt, aki magát az adott ipari folyamatot a legjobban ismerte. A kiválasztásánál kerültük a magas beosztású embereket. Leginkább egy legalább 5 éve a cégnél dolgozó műszakvezető volt a jelöltünk, aki már sok üzemzavar elhárításán dolgozott, mérnöki jogosultsággal kezeli a SCADA, DCS rendszereket.

Mindig bevontuk a csoportba az IACS karbantartás helyi vezetőjét is. Ő az, aki az összes PLC, RTU-t ismeri, becsukott szemmel megtalálja a műszerezés kritikus elemeit, ismeri a kommunikációs protokolokat, a kábelek, szekrények fizikai hozzáférhetőségét, kitettségét.

Gyakran bevontunk a csoportba egy környezetvédelmi szakembert is.

A fókuszcsoportban alkalmazott alapelvek

Fontosnak tartottuk, hogy a rendelkezésre álló korlátozott időben a következményekre koncentráljunk, ezért, hogy kizárjuk a támadás valószínűsége körüli vitát, a csoportot mindig kész helyzet elé állítottuk, mintha a nem kívánt esemény már bekövetkezett volna.

A kérdéseket egymástól izolálva beszéltük meg. Minden egyes rendszer következményénél feltételeztük, hogy a többi jól működik- például egy vészhelyzeti leállító rendszernél feltételeztük, hogy az alá tartozó DCS működik.

Mindíg worst case-t feltételeztünk a bekövetkező eseményeknél

Egy fókuszcsoport foglalkozást legfeljebb 45 percesre terveztünk, mivel azok az emberek, akik valóban értékes információval rendelkeznek, nem reális, hogy érdemben tovább rendelkezésre tudjanak állni.

A fókuszcsoport tematikája

A fókuszcsoportban négy témát beszéltünk végig:

1. A következmény típusok kiválasztása
2. Vizsgálatba vonni kívánt rendszerek (System under Consideration, SuC) kiválasztása
3. A közvetlen hatás meghatározása rendszerenként
4. Következmények szöveges meghatározása rendszerenként

A következmény típusok kiválasztása

Az interjú első része arra irányult, hogy az adott ipari objektumon milyen típusú következmények fordulhatnak elő egyáltalán. Mi az alábbiakat ajánlottuk fel:

1. Táblázat. Felkínált következmény tipusok Forrás: szerző összeállítása a fókuszcsoport eredménye alapján

Termelés kiesés	A termeléskiesésből adódó kárt minden ipari objektumnál vizsgálatuk-nem csak a közvetlen, hanem a közvetett kárt, például a berendezés károsodását is. ISA/ ANSI-62443-3-2-2020 3.1.7 [1]
Emberéletben keletkezett kár	Szinte minden ipari üzemben vizsgáltuk az emberéletben keletkező lehetséges kárt ISA/ ANSI-62443-3-2-2020 3.1.7 [1]
Környezeti kár	A környezeti károkat leginkább olajipari, vegyipari, élelmiszeripari üzemekben vizsgáltuk. A kármentőkben felfogott anyag illetve a fáklyán elégetett anyagot nem tekintettük környezeti kárnak ISA/ ANSI-62443-3-2-2020 3.1.7 [1]
Megfelelőség	Az egyetlen hely, ahol a megfelelőség-et külön vizsgáltuk, az egy egészségügyi mosoda volt, ahol a RAL megfelelőség kritikus volt
Financial	Ezt a kategóriát akkor ajánlottuk fel, ha volt olyan jelentős pénzügyi következmény, amely nem mozog együtt a termelés kieséssel. Nem volt ilyen vizsgálat.

A példaként kiválasztott nagymosoda a termelés kiesést, az emberéletben keletkezett kárt és a megfelelőséget választotta. A környezeti kárral nem kívánt foglalkozni, mivel a mosodában mindenütt van kármentő. A megfelelőség viszont nagyon érdekelte, mert ha az incidens pont egy szúrópróbaszerű ellenőrzéskor történik, akkor a mosoda elveszítheti értékes RAL minősítését.

A következmény típus kiválasztása után számszerűsítési táblázatot készítettünk 1-8 értékig.

A példaként használt nagymosoda esetében ez így nézett ki:

2.Táblázat. A következménytípusok és azok számszerűsítése. (Forrás: szerző összeállítása a fókuszcsoport eredménye alapján)

	Termelés kiesés	Emberéletben keletkezett kár	Megfelelőség
1	Nincs termelés kiesés	Nincs sérülés	Nincs megfelelőségi következmény
2	<1 nap termelés kiesés, nincs kiesés szerződéses kötelezettségben .	1-10 korházi ellátást nem igénylő sérülés	Belső szabályok kisebb sérülése hatósági következmény nélkül
3	1-7 nap termelés kiesés, nincs kiesés szerződéses kötelezettségben .	>10 korházi ellátást nem igénylő sérülés. 1-10 nem maradandó sérülés(>24 óra korházi ellátás)	Belső szabályok súlyosabb sérülése hatósági következmény nélkül
4			
5	Termeléskiesés kisebb késedelmet okoz szerződéses terjedelem teljesítésében		Súlyos megfelelőségi következmény, RAL minősítés elvesztése 1 telephelyen
6			
7		1-10 maradandó sérülés. 1 haláleset	
8	Kulcsfontosságú ügyfelek elvesztése	11-100 maradandó sérülés. Több haláleset	Súlyos bírságok, RAL minősítés elvesztése több telephelyen

Az 1 és 8 közötti számokhoz azért ragaszkodtunk, mert a fókuszcsoportból nyert értékeket később egy olyan, jelen kutatás tárgyát nem képező szoftverrel dolgoztuk fel, amely 1 és 8 közötti bemenő paramétereket kezel.

Vizsgálatba vonni kívánt rendszerek körülhatárolása

Talán a legnehezebb feladat az volt, hogy kijelöljük és meghúzzuk a határait azoknak a rendszereknek, amelyeket vizsgálatát el kívántuk végezni.

A szabvány pontos leírást ad a vizsgálatba vont rendszerek határainak meghatározására (ISA/ ANSI-62443-3-2-2020 [1] 4.1 Identification of System under Consideration). Nem ad azonban útmutatást arra, hogy hogy válasszuk ki azokat a rendszereket, amelyeket részletes vizsgálat alá kell vetni.

Mi a kiválasztásnál az alábbi módszert alkalmaztuk:

1.A DCS, SCADA, ESD, VMS rendszereket első körben mindíg vizsgálat tárgyává tettük. Az alájuk tartozó PLC-ket, RTU-kat és hálózati eszközöket a rendszer részének tekintettük. Amennyiben több, azonos feladatot ellátó rendszert találtunk (például több vasúti töltőrendszer), akkor egybevonva vizsgáltuk őket és worst case-t feltételeztünk.

2. Minden egyéb rendszer esetében narratívaként felvezettünk olyan elképzelt eseteket, amikor egy egyedülálló PLC, vagy éppen MES, ERP rendszeren történik kiberbiztonsági incidens. Ha nem volt bizonyítható, hogy a rendszeren egy incidensnek nem lehet komoly következménye, akkor a rendszert bevontuk a vizsgálatba. Például, elengedtük a vizsgálat alól annak a légkompresszornak a vezérlő PLC-jét, amely kompresszornak volt 4 párhuzamos alternatívája és az elmondás szerint az üzem két kompresszor kiesése után sem kényszerült leállásra.

A közvetlen hatás meghatározása rendszerenként

Talán a leginkább kvalitatív része a gyakorlatnak: a fókuszcsoportnak meg kell egyeznie abban, hogy milyen közvetlen hatástól félnek a leginkább minden egyes rendszernél. Itt szerepjátékot játszottunk: képzeletben minden eszközre, egyenként idéztünk elő a közvetlen hatásokat és megkérdeztük a résztvevőket, hogy melyiktől mennyire félnek.

A lehetséges közvetlen hatások az alábbi táblázatban láthatóak:

3.Táblázat. A közvetlen hatások (Forrás: szerző összeállítása a fókuszcsoport eredménye alapján)

Megnevezés	Hatás leírása	Példa
Irányítás elvesztése	Az irányítás tartós ellehetetlenülése, a kezelők nem képesek beavatkozni egy katasztrófahelyzet esetén	A támadás eredményeként a megjelenítés lefagy, kezelők nem tudnak beavatkozni
A megjelenitès manipulálása	Az operátorok hibás döntéseket hoznak hibás információk alapján, amit a megjelenítés szándékos befolyásolása okoz	A vezérlőrendszer által jelentett értékek nem tükrözik a folyamat valóságát

Folyamat hibás működése	A folyamat nem a várt módon működik. Ezt a rendszer meghibásodása vagy a paraméterek jogosulatlan módosítása okozza	A támadó módosította a PLC kódját, és a folyamat hibásan működik
Információ biztonság sérülése	A rendszer által használt vagy generált adatokat ellopják és megosztják; vagy engedély nélkül módosítják	A támadó megszerzett egy mérnöki jogosultságot biztosító nevet és jelszót

A következmények meghatározása rendszerenként

Ez volt a fókusz csoport utolsó része, mely során először kvalitatív válaszokat vártunk, amiket aztán számszerűsítettünk: leírást kértünk a bekövetkező eseményekről, majd egy táblázat alapján megkíséreltük számszerűsíteni őket 1 és 8 között.

A például vett mosoda Impact Determination végeredménye:

4.Táblázat. A következmények (Forrás: szerző összeállítása a fókuszcsoport eredménye alapján)

Vizsgálatba bevont rendszerek	A választott, legrosszabb Impact	Termelés kiesés		Emberéletben keletkezett kár		Megfelelőség	
		következmény	értékek	következmény	értékek	következmény	értékek
Vízkezelő rendszer	**Folyamat hibás működése**	Vízkezelő rendszer meghibásodása nem vezethet leálláshoz, legfeljebb enyhén növeli a költségeket	**1**	Korházi ellátást igénylő nem maradandó sérülés, legfeljebb 2 fő	**3**	Vízkezelő rendszer hibája nem vezethet RAL minősítés elvesztéséhez	**1**
Csőmosógép SCADA	**A megjelenítés manipulálása.** Ha nem látom a helyes értékeket a SCADAn az nagyobb baj mintha nem működik, ez utóbbi esetben áttérhetek más gépekre	Egy kibertámadás esetén a csőmosógép egy hétre is leállhat, ez esetben más gépekkel magasabb költségen tudják kiszolgálni az ügyfeleket.	**1**	A prés és a hozzátartozó szállító kiszámíthatatlan működés esetén akár egy dolgozó halálát okozhatja	**7**	Amennyiben a reporting kiesése nem teszi lehetővé a megfelelő kísérőbizonylatok kiadását, ez megfelelőség problémákhoz vezethet	**3**
Cool Chemistry berendezés	**Folyamat hibás működése** amennyiben a vegyszereket nem az előírt sorrendben adagolják, robbanás történhet	A cool chemistry kiesését könnyű pótolni magasabb hőmérsékleten történő mosással más vegyszerekkel. Ez némi költségnövekedést okoz de a termelés nem áll le	**1**	A berendezés biztonsági műszerezéssel van ellátva, ami kizárja, hogy ténylegesen kár keletkezzen emberéletben	**1**	A Cool Chemistry berendezés leállása látható és azonnal kiváltható. Ha ez RAL ellenőrzés alatt történik, az sem okoz megfelelőség nehézséget	**1**

Vegyszer adagoló rendszer	**Folyamat hibás működése** A vegyszeradagoló kiszámíthatatlan működése miatt nagy nyomás keletkezhet vegyszert szállító csövekben	A vegyszeradagoló meghibásodását a mosóberendezés azonnal észleli a Proof of Delivery elmaradásakor. Ilyenkor kézi adagolásra lehet átállni	**1**	A nagynyomású cső sérülése korházi ellátást igénylő sérüléshez vezethet legfeljebb 2 fő esetében	**3**	Az adagoló berendezés leállása látható és azonnal kiváltható. Ha ez RAL ellenörzés alatt történik, az sem okoz megfelelőség nehézséget	**1**

A táblázatból következik, hogy a Cool Chemistry berendezés, noha elméletileg borzalmas következményekkel járhat a megtámadása, az egész folyamat ismeretében a legkevésbé kockázatos. Ugyanakkor a csőmoső berendezés SCADA-ja elleni támadás járna a legsúlyosabb következményekkel.

Eredmények, a módszertan igazolása

A módszerrel az elmúlt 4 évben számtalan vegyi üzem következményét mértük fel. Számos esetben derítettünk fel olyan súlyos következményeket, amelyet hagyományos módszerrel nem ismertünk volna fel. Álljon itt három példa.

1. Csővezetéki SCADA rendszer, Közel Kelet, olajipar.

   A SCADA rendszer nem lát el vezérlő funkciókat, nem avatkozik be a csővezeték működésébe. Hagyományos szemlélet mellett ezt a rendszert alacsony következményű rendszerré kellett volna nyilvánítani. A kvalitatív elemzés során viszont megtudtuk, hogy a SCADA képernyőjéről leolvasott nyomás és hőmérséklet értékek alapján adják ki a karbantartóknak a hegesztési engedélyeket. Innentől kezdve a rendszer magas következményű rendszernek lett tekintve, mert ha egy támadás miatt nem valós nyomásértékeket mutat a SCADA, és emiatt kiadnak egy hegesztési engedélyt egy nagynyomású szakaszra, az emberéletben is súlyos kárt okozhat

2. Csőszivárgást jelző rendszerek, Közel Kelet, olajipar

   Két országos csőszivárgást jelző rendszert vizsgáltunk. A rendszerek rendeltetése, hogy meghatározzák egy szivárgás helyét pár m pontossággal a csővezetéken. Eleinte megállapítottuk, hogy a rendszereknek alacsony a következménye, mert egy szivárgás helyét pár óra alatt egy járőr is megtalálja. De a kvalitatív elemzés alatt kiderült, hogy a két rendszer közül az egyik egy olyan csőhálózaton volt, amelynek egy része föld alatt van. Itt megemeltük a következményt.

3. Vegyipari üzem, Magyarország

Egy üzem gázkromatográf állomását eleinte alacsony következményűnek gondoltuk, mert a rendszer nem játszik semmilyen szerepet a gyártásban, nem jelent veszély a hibás működése. De a kvalitativ elemzés kimutatta, hogy nem lehet árút elszállítani az üzemből gázkromatgráfiás elemzés és az az alapján kiadott üzemi tanúsítvány nélkül. Itt is megemeltük a következményt.

Hivatkozott irodalom:

[1] ISA/ ANSI-62443-3-2-2020, Security for industrial automation and control systems, Edition 1.0 2020-06 Part 3-2: Security risk assessment for system design

[2] MSZ EN/IEC61508 2010:CMV

[3] WSH council Singapore, 2017: Workplace Safety and Health Guidelines Process Hazard Analysis [3]

[4] Hal Thomas Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies,

[5]ANSI/ISA 62443-2-1 (99.02.01)

[6] NIST Special Publication 800-30 rev.1, Guide for Conducting Risk Assessments

[7]Cyber Process Hazard Analysis and Risk Management. National Cyber-Infor med Engineering Strategy June 29, 2021, Andrew J. Clark,

[8]Ian Cameron, Sam Mannan, Erzsébet Németh, Sunhwa Park, Hans Pasman, William Rogers, Benjamin Seligman , 2017 Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better? Process Safety and Environmental Protection

[9]Daniele Del Sale, 2020 Operational Technology Services to Support Business Activities

[10]Sandeep Gogineni Ravindrababu, Jim Alves-Foss 2020 Analysis of Vulnerability Trends and Attacks in OT Systems

[11]Ying Yao, 2022 PLC Controller in Electric Control System. Ying Yao, Journal of Electrotechnology, Electrical Engineering and Management) Clausius Scientific Press, Canada

[12]A. Polenghi, I. Roda, M. Macchi, A. Pozzetti Data taxonomy to manage information and data in Maintenance Management. Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Piazza Leonardo da Vinci 32, Milan 20133, Italy

[13]Yulia Cherdantseva, Pete Burnap, Andrew Blyth,Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart 2021 A review of cyber security risk assessment methods for SCADA systems ,

[14] Abraham Serhane, Mohammad Raad, Raad Raad, Willy Susilo PLC Code-Level Vulnerabilities

[15] J. Beringer, J. Kurz Hospital laundries and their role in medical textiles,

[16] Daria A. Gaskova , Aleksei G. Massel Modeling scenarios of extreme situations in the energy sector caused by cyber threats,

[17] ISA ANSI 63443-1-1, 99.01.01.2007 Security for industrial automation and control systems Part 1.1 terminology, Concepts and models

-