# Hírlevél az ipari irányító rendszerek biztonságáról

A Black Cell elkötelezett az ipari irányító rendszerek (Industrial Control Systems – ICS), és/vagy kritikus infrastruktúrák biztonságának megteremtésében, ezért havonta hírlevelet bocsát ki a témában. A hírlevélben az érintett szervezetek, illetve kritikus infrastruktúra üzemeltetők tájékozódhatnak, valamint információkat nyerhetnek az ipari irányító rendszerek sérülékenységeiről; jó gyakorlatokról; a témát érintő képzésekről, oktatásokról, és konferenciákról; az ipari irányító rendszerek üzemeltetőit ért incidensekről. A Black Cell javaslatokat, megoldásokat kínál az ipari irányító rendszerekhez kapcsolódó tevékenységek hatékony elvégzéséhez, és ezáltal a biztonság minél magasabb szintű megteremtéséhez.

## Tartalom:

## ICS sérülékenységek

2019. szeptemberben az alábbi ipari irányító rendszereket érintő sérülékenységeket publikálta a National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs), vagyis az ICS-CERT:

ICSA-19-262-01: **Tridium Niagara**
Magas szintű sérülékenységek: információ feltárás, nem megfelelő hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-262-01

ICSA-19-260-01: **Advantech WebAccess**
Kritikus szintű sérülékenységek: kód és parancs befecskendezés, puffer túlcsordulás, nem megfelelő hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-260-01

ICSA-19-260-02: **Siemens SINEMA Remote Connect Server**
Magas szintű sérülékenységek: a magas számú hitelesítési kísérletek nem megfelelő korlátozása, információ feltárás, XXS, CSRF, jelszó hash probléma.
https://www.us-cert.gov/ics/advisories/icsa-19-260-02

ICSA-19-260-03: **Honeywell Performance IP Cameras and Performance NVRs**
Közepes szintű sérülékenység: információ feltárás.
https://www.us-cert.gov/ics/advisories/icsa-19-260-03

ICSMA-19-255-01: **Philips IntelliVue WLAN**
Közepes szintű sérülékenységek: beégetett jelszó használata, sértetlenség vizsgálat nélküli kód letöltés.
https://www.us-cert.gov/ics/advisories/icsma-19-255-01

ICSA-19-255-01: **3S-Smart Software Solutions GmbH CODESYS V3 Web Server**
Kritikus szintű sérülékenységek: útvonal bejárás, puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-19-255-01

ICSA-19-255-02: **3S-Smart Software Solutions GmbH CODESYS V3 Library Manager**
Magas szintű sérülékenység: XSS.
https://www.us-cert.gov/ics/advisories/icsa-19-255-02

ICSA-19-255-03: **3S-Smart Software Solutions GmbH CODESYS Control V3 Online User Management**
Magas szintű sérülékenység: kritikus erőforrások nem megfelelő engedélyezése.
https://www.us-cert.gov/ics/advisories/icsa-19-255-03

ICSA-19-255-04: **3S-Smart Software Solutions GmbH CODESYS Control V3 OPC UA Server**
Közepes szintű sérülékenység: Null Pointer dereferencia.
https://www.us-cert.gov/ics/advisories/icsa-19-255-04

ICSA-19-255-05: **3S-Smart Software Solutions GmbH CODESYS V3 Products Containing a CODESYS Communication Server**

Magas szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-255-05

ICSA-19-253-01: Delta Electronics TPEditor
Magas szintű sérülékenységek: puffer túlcsordulás, pufferen kívüli adatok írásának lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-19-253-01

ICSA-19-253-02: Siemens SINETPLAN
Magas szintű sérülékenység: nem megfelelő hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-253-02

ICSA-19-253-03: Siemens Industrial Products
Magas szintű sérülékenységek: szoftver kalkulációs probléma erőforrás kezelésnél, ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-253-03

ICSA-19-253-04: Siemens IE-WSN-PA Link WirelessHART Gateway
Magas szintű sérülékenység: XSS.
https://www.us-cert.gov/ics/advisories/icsa-19-253-04

ICSA-19-253-05: Siemens SIMATIC TDC CP51M1
Magas szintű sérülékenység: nem megfelelő bemeneti itelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-253-05

ICSA-19-253-06: OSIsoft PI SQL Client
Magas szintű sérülékenység: szoftver kalkulációs probléma erőforrás kezelésnél.
https://www.us-cert.gov/ics/advisories/icsa-19-253-06

ICSA-19-192-02: Siemens SIMATIC WinCC and PCS7 (Update B)
Magas szintű sérülékenység: veszélyes típusú fájlok korlátozatlan feltöltési lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-19-192-02

ICSA-19-134-08: Siemens SIMATIC PCS7, WinCC, TIA Portal (Update C)
Kritikus szintű sérülékenységek: SQL befecskendezés, funkció kivétel probléma, veszélyes módszer és funkció nem megfelelő korlátozása.
https://www.us-cert.gov/ics/advisories/ICSA-19-134-08

ICSMA-19-248-01: BD Pyxis
Magas szintű sérülékenység: session rögzítésből eredő hiba.
https://www.us-cert.gov/ics/advisories/icsma-19-248-01

ICSA-19-248-01: Red Lion Controls Crimson
Magas szintű sérülékenységek: memória felszabadítási hiba, memória pufferen belüli műveletek nem megfelelő korlátozása, pointer probléma, beégetett kriptográfiai kulcs használat.
https://www.us-cert.gov/ics/advisories/icsa-19-248-01

ICSA-19-246-01: EZAutomation EZ Touch Editor

Magas szintű sérülékenység: puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-19-246-01

ICSA-19-246-02: EZAutomation EZ PLC Editor
Magas szintű sérülékenység: memória pufferen belüli műveletek nem megfelelő korlátozása.
https://www.us-cert.gov/ics/advisories/icsa-19-246-02

A sérülékenységek részletezve a kapcsolódó linkeken, illetve összesítve a következő weboldalon találhatók meg:

https://ics-cert.us-cert.gov/advisories

A sérülékenységek részletes leírását, a megoldási javaslatokat, és az érintett termékek teljeskörű listáját a sérülékenységhez tartozó linken lehet megtalálni.

## ICS riasztások

2019. szeptember hónapban az ICS-CERT nem adott ki riasztást.

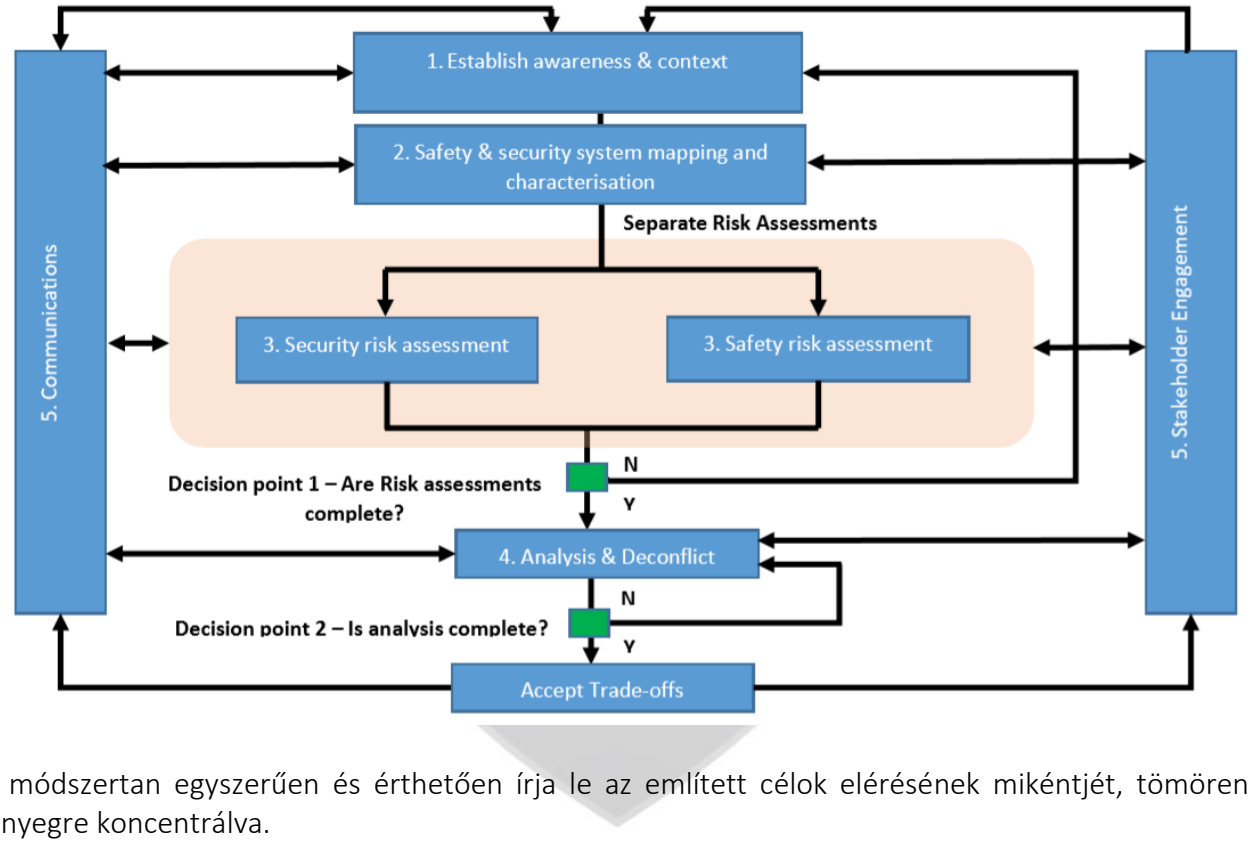
A riasztások részletezve a kapcsolódó linkeken, illetve összesítve a következő weboldalon találhatók meg:

https://www.us-cert.gov/ics/alerts

## ICS jó gyakorlatok, javaslatok

Gyakran igényként jelentkezik az ipari irányító rendszerek üzemeltetőinél a biztonságos működés és az információbiztonság kapcsolatának megfelelő összhangban történő kezelése. Az összhang megteremtése nem könnyű feladat, sokszor akadályokba ütközik a megvalósítás, vagy előfordul, hogy az üzemeltető nem tudja miként kezdjen hozzá a feladathoz.

2018-ban megjelent egy módszertan, amely segít a harmóniát megtalálni az említett „safety" és „security" között, melynek keretrendszerét az alábbi ábra mutatja meg:




A módszertan egyszerűen és érthetően írja le az említett célok elérésének mikéntjét, tömören a lényegre koncentrálva.

A 10 oldalas Pdf. dokumentum a következő webhelyről tölthető le:

https://www.sciencedirect.com/science/article/pii/S187705091831216X

## ICS képzések, oktatások

A teljeség igénye nélkül 2019. októberben ICS biztonság tárgyában a következő tréningek, oktatások kerülnek lebonyolításra:

2019. októberben a következő tréning, oktatás kerül lebonyolításra az ICS/SCADA biztonság kapcsán a SANS szervezésében:

- ICS410: ICS/SCADA Security Essentials SANS; San Diego, California, USA; 2019. október 7-11.
- ICS410: ICS/SCADA Security Essentials SANS; Szingapúr, Szingapúr; 2019. október 14-18.
- ICS410: ICS/SCADA Security Essentials SANS; Doha, Katar; 2019. október 13-17.
- ICS410: ICS/SCADA Security Essentials SANS; Denver, Colorado, USA; 2019.október 14-18.
- ICS410: ICS/SCADA Security Essentials SANS; Orlando, Florida, USA; 2019. október 28-november 1.

A részletek a következő web-helyen találhatók:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

### Időszakosan induló online kurzusok:

A https://www.coursera.org/ honlapon lehetőség van online elvégezni bizonyos ipari irányító rendszerek biztonságával kapcsolatos tanfolyamokat, melyek során video oktatásokon vehet részt a jelentkező, és feladatok megoldásával demonstrálhatja tudását a szakterületet érintően. Az online tanfolyam elvégzését követően a Univesity of Colorado Boulder tanúsítványt állít ki a végzettek részére. A következő kurzusok végezhetők el:

- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization

További részletek a következő webhelyen találhatók:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

Az említett oktatásokon felül az ICS-CERT is kínál Online kurzusokat (a következő online kurzusokra előre leghamarabb 2019. decemberre lehet regisztrálni):

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- ICS Cybersecurity

További részletek a következő webhelyen találhatók:

https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

A SANS nem kizárólag helyhez kötötten szervez képzéseket az ipari irányító rendszerek biztonságával kapcsolatban, hanem online kurzust is indít:

- ICS410: ICS/SCADA Security Essentials SANS

További részletek a következő webhelyen találhatók:

https://www.sans.org/find-training-beta/search?courses=2762&types=10&redirect=beta#__utma=195150004.1547647064.1563952209.1566466056.1568274011.4&__utmb=195150004.2.9.1568274014545&__utmc=195150004&__utmx=-&__utmz=195150004.1568274011.4.3.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=17428089

Az ipari irányító rendszerek és a SCADA rendszerek biztonságáról szóló Online kurzus érhető el az Udemy honlapján, ahol a jelentkező megtanulhatja az ICS/SCADA biztonság alapjait, technológiai megoldásokat, szoftver kezelést, szabályozási megoldásokat.

- ICS/SCADA Cyber Security

További részletek a következő webhelyen találhatók:

https://www.udemy.com/ics-scada-cyber-security/

A Department of Homeland Security 2 napos képzése során a résztvevők megismerhetik a különböző vezérlő rendszerek biztonságával kapcsolatos tudnivalókat.

- SCADA security training

További részletek a következő webhelyen találhatók:

https://www.tonex.com/training-courses/scada-security-training/

## ICS konferenciák

A hírlevélben bemutatott konferenciákon túl, az Európai Kiberbiztonsági hónap keretein belül számos konferencia kerül megrendezésre, ahol fellelhetők ipari irányító rendszerek kiberbiztonságával kapcsolatos előadások. Érdemes körülnézni az interneten!
A teljesség igénye nélkül a következő konferenciák kerülnek megrendezésre 2019. októberben:

### Industrial Control System Security 2019

A nemzetközi konferencián szó lesz többek között a kritikus infrastruktúrák nemzeti kockázatairól, a régi irányító rendszerek fenyegetettségi kitettségének csökkentéséről, valamint az ICS monitoringról is. Bemutatásra kerül az ausztrál kritikus infrastruktúra védelmi törvény (Security of Critical Infrastructure Act), továbbá a stratégia alkotás esszenciája is megvitatásra kerül.

Industrial Control System Security 2019; Sidney, Ausztrália; 2019. október 1-2.

További részletek a következő webhelyen találhatók:

https://www.iqpc.com/events-ics-security

### CEE Scada Security conference

Az első CEE Scada biztonsági konferencia a következőkre fókuszál: jelenlegi és jövőbeli fenyegetettségek és megoldások. Bemutatásra kerülnek új technológiai trendek az ICS biztonság területén. Részletezésre kerül, hogy a kiberbiztonság megteremtése egy befektetés a szervezetek és az egész társadalom számára. Szó lesz továbbá az Ipar 4.0-ról, és üzleti lehetőségekről a kiberbiztonság területén.

SCADA SECURITY CEE Conference; Prága, Csehország; 2019. október 12-13.

További részletek a következő webhelyen találhatók:

https://cybersecuritymonth.eu/ecsm-countries/czech-republic/scada-security-cee-conference

### Cyber Security in SCADA and Industrial Control Systems

A konferencia számos érdekes előadást tartogat, ráadásul **ingyenesen is lehet regisztrálni!** A rendezvényen szó lesz többek között ICS tesztelésről, ICS digital forensic tevékenységekről, ellátási lánc okozta problémákról, SOC tevékenységekről, SCADApocalipszisről, DMA támadásokról és még számos ICS és SCADA biztonságot érintő újdonságról.

The Premier Cyber Security Conference for ICS/SCADA and Critical Infrastructure; Stokholm, Svédország; 2019. október 21-24.

További részletek a következő webhelyen találhatók:

https://cs3sthlm.se/

## Industrial Control Systems (ICS) Cyber Security Conference

A konferencia összehozza az ICS üzemeltetőket, gyártókat, biztonsági kutatókat, és állami szereplőket, akik érdekeltek az ICS biztonságban. Lehetősége lesz a résztvevőknek a legutóbbi kiber incidensek okainak elemzésére, valamint annak megvitatására, hogy miként kellene együttműködni az érintetteknek. A 2002 óta megrendezésre kerülő konferencián a kritikus infrastruktúrák védelmére is nagy figyelem irányul.

Industrial Control Systems (ICS) Cyber Security Conference; Atlanta, USA; 2019. október 21-24.

További részletek a következő webhelyen találhatók:

https://www.icscybersecurityconference.com/

# ICS incidensek

## Ukrán atomerőműből érzékeny adatok kerülhettek nyilvánosságra

A szervezetben dolgozó személyek által végrehajtott illegális kriptovaluta bányászat okozta az érzékeny adatok nyilvánosságra hozatalát. Az eset vizsgálata során kiderült, hogy olyan berendezések voltak elhelyezve a szervezeten belül, melyeket a szabályozás szerint nem lehetett volna.

A kriptovaluta bányászat tehát saját berendezésekkel zajlott, de a szervezet villamos hálózatát használták az érintettek a művelet végrehajtása során. A berendezések a szervezet intranetjéhez, illetve a világhálóhoz is csatlakoztatásra került, amely által a szervezet fizikai biztonságáról szóló minősített dokumentumok is nyilvánosságra kerültek.

A szakértők szerint hónapokig, vagy még tovább is nyilvánosan elérhetőek voltak az említett dokumentumok, ezzel veszélyeztetve egy katasztrófa bekövetkezését.

A cikk megemlíti, hogy a szervezeti információbiztonsági politikák és szabályzatok mit sem érnek, ha a megfelelő kontroll környezet nincs kialakítva.

Egy kapcsolódó cikk megemlíti, hogy a kriptovaluta bányászat az ipari rendszerekre hatalmas veszélyt jelent, és ilyen esetekben nem ritka az sem, hogy rosszindulatú szoftverek jutnak be az üzemeltetési környezetbe.

Forrás: https://www.securityweek.com/illegal-cryptocurrency-mining-ukraine-nuclear-plant-exposed-sensitive-data

Szerző: A cikk által említett kontroll környezet hiánya valóban hatalmas gond. Ilyen esetekben szokták azt mondani, hogy „Minden szabályzat annyit ér, amennyi megvalósul belőle!”. Ebben az esetben a szabályzat nem sokat ért…

Felvetődik a kérdés, hogy a megnövekedett energiafelhasználás, illetve a nem szokványos tevékenységtől eltérő informatikai cselekmények miért nem tűntek fel senkinek, miért nem generáltak riasztást? Ennek számos oka lehet, érdemes rajta elgondolkodni.

További hibák és/vagy hibák sorozata is oka lehet az incidens megvalósulásának, itt a nem megfelelő szegregáció, vagy a riasztás false pozitívként való kezelése is szóba jöhet, de számos további kérdés is megfogalmazódat az olvasókban…

## Könyvajánló

A SCADA és más ipari irányító rendszerek kiberbiztonságáról szóló könyv bemutatja az ipari irányító rendszerek (ICS) rendszerek komponenseit, a hálózat nélküli ICS infrastruktúrát, az üzemeltetés és az IT kapcsolatát (IT vs. OT), az ICS rendszerek fenyegetettségeit, támadásokat az ICS rendszerek ellen, továbbá az ICS biztonság taxonómiáját.

A könyv részletezi az ICS rendszerek kiber kockázatait, a biztonság mérőszámait az ICS rendszerekben, a szituációs tudatosságot, az ICS rendszerekbe történő behatolás észlelést, valamint a fizikai behatolás észlelést, a vezérlő rendszerek biztonsággal kapcsolatos kutatásainak módszertanait.

A szerzők rávilágítanak arra, hogy milyen módon szükséges szabályozni az ICS rendszerek működését és azt milyen stratégia mentén kell megtenni, illetve az ICS és SCADA rendszerek elleni támadásokra történő reagálás milyen módon valósulhat meg.

A könyv záró része a dolgok internetének- (Internet of Things – IoT), és az ICS rendszereknek a jövőképét mutatja be.

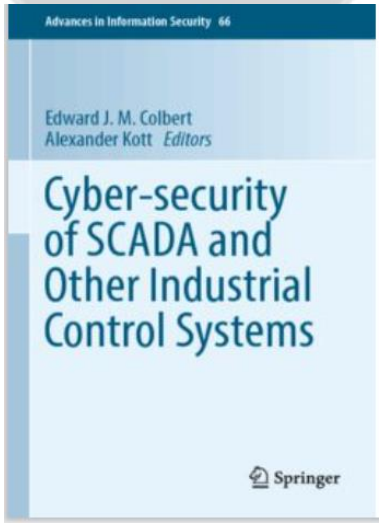
A könyv címe: Cyber-Security of SCADA and Other Industrial Control Systems

Szerzők: Edward J. M. Colbert; Alexander Kott

Kiadás éve: 2016.

A kiadvány letölthető a következő linken:

https://www.pdfdrive.com/cyber-security-of-scada-and-other-industrial-control-systems-e60132591.html



## Black Cell javaslatok

A sérülékenységek sokszor megkeserítik a szervezetek életét, főleg, ha esetleg azok kihasználásra kerülnek.

**Sérülékenység:** Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.

A sérülékenységek felfedezése, és azok befoltozása valamely javítócsomag (patch) által, egy olyan időtartamot eredményez (abban az esetben, ha egyáltalán készül patch az adott sérülékenységre), melyet a szakirodalom sérülékenységi ablaknak hív.

A sérülékenységi ablak általában hosszú időtartamot ölel fel, gyakran hónapokat, azonban előfordul, hogy éveket is.

Az IPS rendszerek (Intrusion Prevention Systems – Behatolás Megelőző Rendszerek) meghatározó módon csökkenthetik az elektronikus információs rendszerek, vagy alkalmazások sérülékenységi ablakát „virtuális patch”-ként viselkedve, a Windows alapú-, és a SCADA rendszerek vonatkozásában.

Javasolt az ipari irányító rendszerek üzemeltetőinek nagyobb hangsúlyt fektetni a sérülékenység menedzsmentre, és a sérülékenységi ablak időket a lehető legalacsonyabbra csökkenteni.

Javasolt továbbá megfelelően működtetett információbiztonság irányítási rendszerben az IPS rendszerek alkalmazása, ezzel is csökkentve a sérülékenységi ablakok okozta kockázatokat.

A Balck Cell következő weboldalán további információkat találhat a menedzselt IDS/IPS szolgáltatásokról:

https://blackcell.hu/termekek/

Ha bizonytalan abban, hogy szervezete érettségi szintje nem áll készen egy IPS rendszer megfelelő szintű üzemeltetésére, akkor tanácsadási szolgáltatásaink keretében megállapítjuk, hogy mit kell tennie a szervezetnek, hogy alkalmas legyen egy ilyen rendszer implementálására. További információk a következő weboldalon:

https://blackcell.hu/tanacsadas/