|  |  | |
| --- | --- | --- |
| ***ELEKTRIZITATEA ETA ELEKTRONIKA*** | | |
| ***AUTOMATIZAZIOA ETA ROBOTIKA, ( MEKATRONIKA….)*** | | |
| ***ZIBERSEGURTASUN INDUSTRIALA (ZEHARKAKOA)*** | | |
| ***Iraupena: x orduko n saio*** | | ***Antolaketa: n pertsonatako taldeak*** |

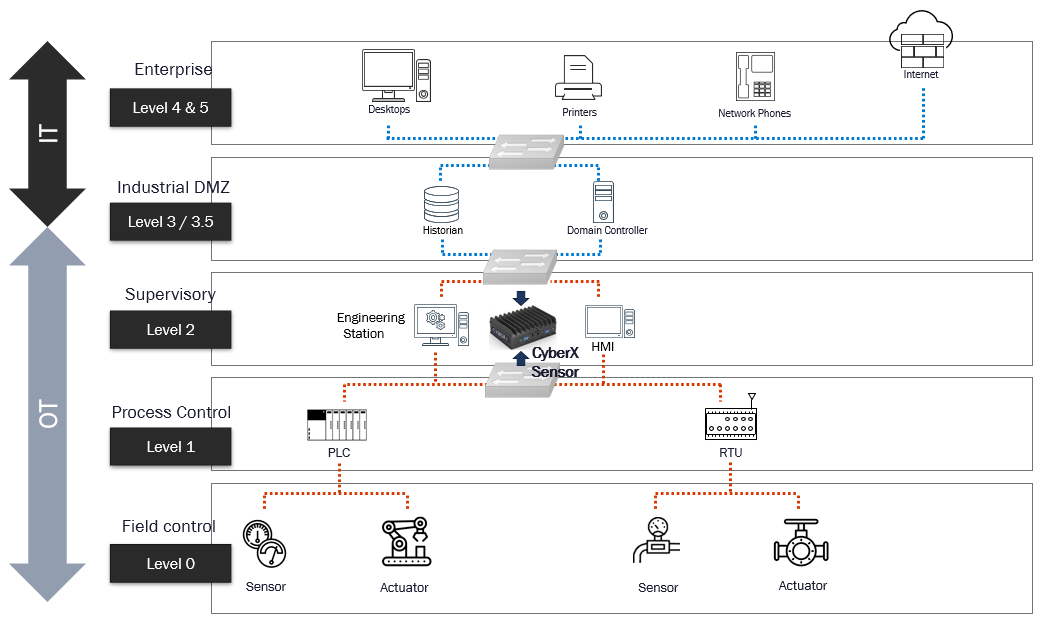
| ***n Erronka***  ***Zibersegurtasun industrialeko jarduerak ezartzea sistema automatizatuetan*** |
| --- |
| ***Azalpen laburra***  Zikloan egin duzun sistema automatikoaren erronkan edo proiektuan zibersegurtasun industrialeko jarduerak txertatu. |

| **Erronka** |
| --- |

4.0 industriak fabrikazio adimenduna eta interkonektatutako gailuak ditu ezaugarri. Baina interkonektatutako beste edozein sistema bezala, helburu potentzialak dira zibererasoentzat. Instalazioetan sartzeak arrisku handiko ondorioak izan ditzake industria-erakundeentzat.

Erronka honetan, zibersegurtasun-jarduerak txertatu beharko dituzu gaur egun zure heziketa-zikloaren barruan lanean ari zaren instalazio automatizatuan. Jarduera horiek txertatuz, ikasgelaren inguruan industria-instalazioak babesteko beharrari buruzko kontzientziazioa sortuko duzu, zibersegurtasunaren munduko terminologiara ohituko zara eta jarduera horiek egiteko moduari buruzko ezagutza teknikoak eskuratuko dituzu.

Zibersegurtasuna: ordenagailuak, zerbitzariak, gailu mugikorrak, sistema elektronikoak, sareak etab, asmo txarreko erasoetatik babesteko praktika da.



| **Helburuak / Ikasketa emaitzak** |
| --- |

*TEKNIKOAK*

*1- IT (Informazioaren Teknologiak) eta OT (Eragiketaren Teknologiak) teknologien konbergentziarako aldaketak zehazten ditu, ingurune horiek erakundeetan duten egoera aztertuz.*

*2- Industria-sistema seguruen kontrolean esku hartzen duten gailu programagarriak ezagutzen ditu.*

*3- Arrisku teknologikoko egoerak ebaluatzen ditu industria-instalazioak kontrolatzeko sistemetan.*

*4- Kontrol industrialeko sistemak konfiguratzen ditu, egon daitezkeen arrisku-egoerak minimizatuz.*

*5- Industria-kontroleko sistemetan anomaliak detektatzen ditu.*

*ZEHARKAKOAK (*[*Errubrikak*](https://drive.google.com/file/d/1uNcwrLVx2o8hYf5tCzoew4FgdMgA5Vsf/view?usp=sharing)*)*

* Pertsonalak:
  + Autonomia
  + Inplikazioa
  + Ekimen sortzailea
* Komunikazioa:
  + Ahozko komunikazioa
  + Idatzizko komunikazioa
* Digitala:
  + Informazioan eta datuetan alfabetatzea
  + Komunikazioa eta lankidetza
  + Eduki digitalak sortzea
  + Segurtasuna
  + Arazoak konpontzea
* Lankidetzakoa:
  + Talde-lana
  + Arazoak konpontzea
  + Erabakiak hartzea



| 1. **Egin beharreko lanak** |
| --- |

Zibersegurtasun-jarduera hauek sartu lanean ari zaren automatizazio-erronkan :

* Industrian gertatzen ari diren IT&OT teknologiak integratzea eskatzen duten aldaketak justifikatu.
* Industria-instalazioak zergatik dauden arriskuan eta arrisku-egoerak zeintzuk diren identifikatu.
* Aztertu zer arazo sortzen dituen komunikazio-portuak irekitzeak edo webserver-a gaituta edukitzeak... Arriskupean dauden eta seguruak ez diren industria-ekipoak aurkitu. Kontuan izan portu horiek alde batetik irekita edukitzeak eta beste batetik beste instalazio batean sartzeak dakartzan arazoak.
* Aztertu, orain dela gutxi,eta instalazio industrialen aurka , mundu mailan izan den eraso informatiko esaguratsuren bat, ransomware motakoa edo antzekoa.
* Gehien erabiltzen diren komunikazio-protokoloak identifikatu. Erabili Wireshark aplikazioa zure instalazio industrialean sortzen diren komunikazioen trafikoa bistaratzeko.
* Erabili Tknikan sortutako panela zure instalazio industrialaren memoria-eremuei buruzko datuak lortzeko eta datuak idazteko. Enpresaren sarean sartzeak ekar dezakeen arazoaz sentsibilizatzea, bai eta enpresaren industria-komunikazioak testu lauan eta monitorizazio-tresna informatikoen bidez eskuragarri jartzeaz ere.
* SCI kontrol industrialeko instalazioetan dauden mehatxuak eta ahuleziak identifikatu.
* 4.0 industria-jarduera gisa, atera zure ekoizpen-sistemako datuak teknika hauetakoren bat edo ezagutzen dituzun beste batzuk erabiliz: OPC UA, Keepserver, Siemesn IOT , Nodered, Tknikaren panela
* Egizu zure sarea nola segmentatuko zenuen ariketa simulatua, konfigurazio segurua emateko. Marraztu instalazioa babesteko egitura aproposaren eskema bat, kontuan hartu segmentazioa vlan, switch, router edo suebakien bidez.

| 1. **Ebaluazio irizpideak** |
| --- |

* Gaitasun teknikoak %70
* Zeharkako gaitasunak %30

Ebaluazio-proposamena. Erabili ohiko duzun proiektu/erronken ebaluazio-orria , egindako zibersegurtasun-jarduerekin lotutako itemak txertatuz.

| **PROIEKTU ZenbX** | **Taldea:** |  |
| --- | --- | --- |
| **EBALUAZIO IRIZPIDEAK** | **202X/2X Urtea** |  |
| **Ikaslea :** | **Proiektu zenbk :** |  |
| **GAITASUN TEKNIKOEN BALORAZIOA: ( 7 puntu )** | |  |
| Industria-instalazioak zergatik dauden arriskuan eta arrisku-egoerak zein diren identifikatzen du. | |  |
| PLCan programazio segurua egiteko beharra justifikatzen duten artikuluak aurkitu eta aztertzen ditu. | |  |
| Aztertu PLC Security Top 20 zerrenda, eta aukeratu zure proiektuan aplikatzeko bideragarrienak iruditzen zaizkizun 10 neurriak | |  |
| Inplementatu zure PLCren programan modu erreal eta eraginkorrean sar daitezkeen praktikak | |  |
| * Praktika1 | |  |
| * Praktika2 | |  |
| * Praktika3 | |  |
| **ZEHARKAKO GAITASUNEN EBALUAZIOA (3 puntos)** | |  |
| Pertsonalak: Autonomia, inplikazioa, ekimen ekintzailea. | |  |
| Komunikazioa: ahozko komunikazioa, idatzizko komunikazioa. | |  |
| Digitala: informazioa eta datuak alfabetatzea, Komunikazioa eta lankidetza, eduki digitalak sortzea, Segurtasuna eta arazoen konponketa | |  |
| Elkarlana: talde-lana, arazoak konpontzea, erabakiak hartzea | |  |
| **Gaitasun Teknikoak (7)** | |  |
| **Zeharkako gaitasunak (3)** | |  |
| **NOTA** | |  |

| 1. **Baliabideak** |
| --- |

1. Centro Vasco de Ciberseguridad <https://www.basquecybersecurity.eus/es/>
2. Centro de Ciberseguridad Industrial de Gipuzkoa <https://www.ziur.eus/es/>
3. Industrias de Ciberseguridad del País Vasco. <https://www.cybasque.eus/>
4. INCIBE Insituto nacional de Ciberseguridad <https://www.incibe.es/>
5. CCI Centro de Ciberseguridad Industrial <https://www.cci-es.org/>
6. Bibliografía: <https://infolibros.org/libros-de-seguridad-informatica-gratis-pdf/>

| 1. **Denboraren antolaketa** |
| --- |

| **Astelehena** | **Asteartea** | **Asteazkena** | **Osteguna** | **Ostirala** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |