



HackEPS 9^a edició

Nov. 25

bonÀrea

Comunicació industrial

THE FUTURE IS ALREADY HERE

it.bonarea.com

INDEX

1.	Quin repta es planteja	2
1.1.	Per què és important comunicar-se correctament amb un PLC industrial?	2
1.2.	En què consisteix el repte?	2
3.	Informació prèvia per realitzar la prova	3
4.	Restriccions.....	3
5.	Interfície gràfica del panell	4
6.	Format d'entrega.....	4
7.	Premi	5

1. Quin repta es planteja

1.1. Per què és important comunicar-se correctament amb un PLC industrial?

En el món industrial actual, molts processos depenen de PLCs que controlen màquines, línies de producció i sistemes crítics. Per poder supervisar i controlar aquests equips, cal comunicar-se amb ells mitjançant diferents protocols, com OPC UA, S7 o a través d'un navegador web.

Tot això s'ha de fer mantenint sempre la seguretat dels equips. Una comunicació mal configurada o poc protegida pot posar en risc el funcionament de la planta i obrir la porta a possibles atacs de ciberseguretat. Per això és essencial verificar que les comunicacions funcionen correctament i que continuen sent robustes.

1.2. En què consisteix el repte?

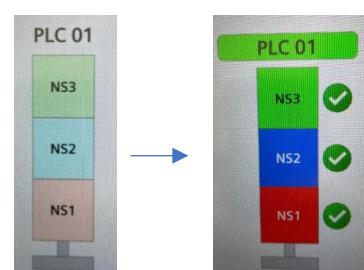
El repte consisteix a desenvolupar una aplicació o conjunt de proves que permeti comunicar-se amb un PLC industrial utilitzant diferents protocols de comunicació, haureu de ser prou hàbil per saber quin protocol utilitzar en cada bloc de dades. En resum, l'usuari ha de demostrar que és capaç d'establir comunicacions industrials correctament i entendre la importància de mantenir aquests equips protegits.

Els objectius són:

- Llegir i escriure dades al PLC a través de cadascun dels mètodes de comunicació.
- Validar que les connexions són fiables i segures, comprovant si hi ha configuracions febles o punts vulnerables.
- Assegurar que la ciberseguretat del PLC continua sent robusta, revisant aspectes com l'autenticació, el xifrat i els permisos d'accés.

Objectius principals:

- 1- Activar el pilot vermell del semàfor corresponent a NS1.
- 2- Activar el pilot blau del semàfor corresponent a NS2.
- 3- Activar el pilot verd del semàfor corresponent a NS3.



El repte queda superat quan s'aconsegueix activar els 3 pilots utilitzant una seqüència en concret.

3. Informació prèvia per realitzar la prova

Abans de poder iniciar qualsevol comunicació amb els diferents PLCs, és imprescindible conèixer la seva adreça IP. Sense aquesta informació, no és possible establir cap tipus de connexió amb el PLC.

Per tal que pugueu descobrir la IP de cada PLC i posteriorment realitzar la comunicació, s'ha habilitat una xarxa Wi-Fi específica per a la prova.

Dades de la xarxa Wi-Fi:

- **SSID:** BonHack_2025
- **Contrasenya:** b0nH@ckLle1d@

4. Restriccions

Un cop hagueu identificat les diferents adreces IP dels PLCs disponibles, cal tenir en compte les següents restriccions per tal de garantir que la prova es desenvolupa de manera ordenada i sense interferències entre grups:

1. Cada grup treballarà només amb un dels 5 PLCs.
Un cop trieu un PLC i la seva IP, haureu de mantenir-vos-hi durant tota la prova. Això evita conflictes i reescritures involuntàries en altres dispositius.
2. Formeu grups el més reduïts possible.
Com més petit sigui el grup, menor serà el risc que diferents usuaris modifiquin al mateix temps les dades del PLC, cosa que podria alterar els resultats o interferir amb el treball d'altres participants.
3. Respecteu el treball dels altres grups.
Eviteu accedir o modificar un PLC que no sigui el vostre. Qualsevol canvi indegit pot afectar directament el progrés d'altres participants.
4. No es pot utilitzar software amb llicències piratejades.

4. Interfície gràfica del panell

Al panell de la prova hi ha instal·lada una pantalla HMI de Siemens, configurada per mostrar en temps real l'estat del procés associat als cinc PLCs disponibles. Aquesta interfície us permet visualitzar:

- L'estat de comunicació de cada PLC
- Les variables més rellevants durant la prova
- Els possibles canvis que els usuaris realitzen
- El progrés general del repte

Així, mentre treballieu, podreu veure sempre en quin punt es troba cada dispositiu i si la comunicació està funcionant correctament.

A més, quan un grup superi totes les tasques de comunicació amb èxit, la pantalla HMI mostrarà automàticament un missatge **d' enhorabona**, indicant que el repte ha estat completat!

Seguiu les regles esmentades en el següent apartat per preparar la documentació d'entrega dels resultats!

6. Format d'entrega

El guanyador serà el primer equip en aconseguir resoldre el repte. En cas d'empat o que cap equip pugui aconseguir el repte, es resoldrà en presentacions a porta tancada de les solucions provades per l'equip de bonÀrea. S'evaluarà com d'aprop han estat els participants d'arribar a la solució, els bloquejos identificats, la capacitat resolutiva, les solucions proposades entre d'altres.

- Heu de fer una foto de tots els membres del grup amb la pantalla HMI de fons, on es vegi clarament el missatge d' enhorabona.
- Heu d'enregistrar i anotar l'hora i el minut exactes en què heu completat la prova.
- Pujar documentació (utilitzant el canal que ens proporcionarà l'organització) sobre els mètodes de comunicació que heu utilitzat per accedir als diferents blocs de dades NS1-NS2-NS3.
- Utilizeu una explicació el més clara i completa possible del procediment seguit per cadascun d'ells. Podeu ajudar-vos de captures de pantalla que mostrin la comunicació establerta, les eines utilitzades i el resultat obtingut.

Aquest material permetrà validar tant la correcte realització del repte com la comprensió de les diferents vies de comunicació amb els PLC. Recordeu que cada pas que es superi té valor i pot ajudar positivament en l'avaluació final.

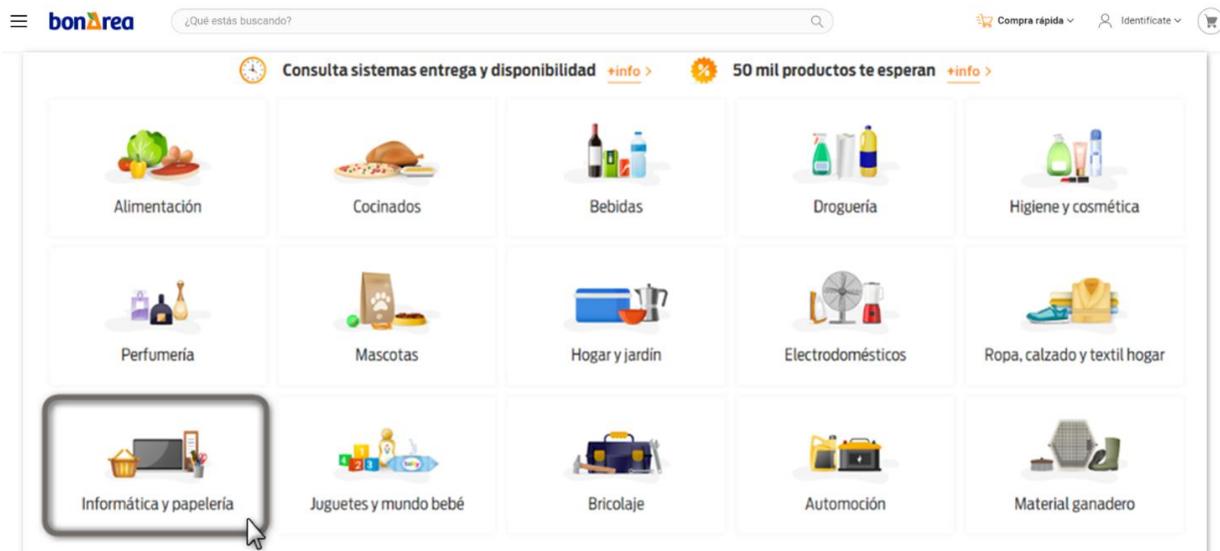
7. Premi

El premi consisteix en un val de 1000€ per gastar en la botiga online de bonÀrea. Si l'equip guanyador del premi desitja algun dispositiu o component tecnològic en concret que no aparegui a la web, el departament de compres d'enginyeria s'encarregarà de buscar-lo.



Si voleu veure tots els productes disponibles, podeu donar un cop d'ull a la pàginan web:

<https://www.bonarea-online.com/es>



*No dubteu en visitar la secció de productes d'informàtica.