Implementació d'una CPU de seguretat a l'estació de la cèl·lula flexible del laboratori VGA104

Marc Planas Naz

Grau d'Enginyeria en Electrònica Industrial i Automàtica

Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú

Resum

Aquest Treball de Fi d'Estudis consisteix en una anàlisi d'una CPU de seguretat NX-SL3300, fabricat per OMRON i la seva posterior implementació en l'estació de la cèl·lula de producció flexible del laboratori VGA104 a l'EPSEVG. Per a dur a terme aquesta implementació es realitza un estudi de les seguretats de la cèl·lula flexible i seguint la metodologia que dicten les normes internacionals sobre seguretat funcional, es fa una avaluació i reducció de riscos. Durant aquest procés, és quan es realitza la configuració i el muntatge tant de la CPU de seguretat com dels diferents elements de seguretat. Posteriorment, es realitza un manual d'usuari en l'annex IV amb tots els passos de programació i configuració detallats. Per finalitzar, es fa una avaluació i verificació de la funció de seguretat per poder comprovar si la reducció de riscos s'ha aconseguit de manera òptima o no. En resum, aquest Treball de Fi d'Estudis contribueix al camp de l'Enginyeria Electrònica Industrial i Automàtica, amb la finalitat de millorar i donar a conèixer la seguretat en els entorns de la indústria 4.0.

1. Introducció

Aquest projecte es basa sobretot en la implementació de la CPU de seguretat de OMRON [1] amb les corresponents targetes d'entrades i sortides i els diferents elements de seguretat.

Un cop estudiada la cèl·lula flexible del laboratori es va començar a determinar quina seria la metodologia a seguir durant el transcurs del projecte. Aquest enfocament iteratiu i adaptatiu fa que sigui molt flexible i que es puguin afegir elements nous en funció de l'estudi teòric. Això permet adaptar les necessitats de les estacions de treball al projecte, per exemple, quan es va testejar la catifa de seguretat i es va observar que no funcionava, aquesta metodologia ens va permetre seguir la implementació dels elements de seguretat, sense haver de parar a buscar una catifa nova, o alguna altra alternativa, i a posterior realitzar el procés d'iteració estudiant el problema i tornant a la fase d'experimentació.

El context d'aquest projecte ens permet obrir les portes a l'àmbit de la seguretat en l'automatització, i ens permet aprendre conceptes com: estimació i anàlisis de risc, valoració del risc, nivell de prestacions, nivell d'integritat de la seguretat, temps mig fins a fallada perillosa, etc.

Tots aquests conceptes estan regits per una sèrie de normes per poder aconseguir els objectius de la seguretat funcional i aprofitar de forma eficaç i segura la tecnologia de la qual es disposa. És per això, que en aquest projecte es profunditza molt en aquestes normes però sobretot en les següents: IEC 61508 [2], ISO 13849 [3] i l'ISO 12100 [4].

Un cop es realitza l'avaluació de riscos, comença el procés de reducció de riscos que correspon a la configuració i implementació de la unitat NX-SL3300 conjuntament amb els diferents elements de seguretat. Una vegada implementades les mesures de reducció de riscos es realitza una avaluació i verificació de la funció de seguretat per poder comprovar si realment s'han reduït els riscos, i a partir d'això, en funció del resultat, o es tornen a analitzar els riscos que continuen actius (o els nous riscos apareguts) i tornem a realitzar tot el procés anteriorment descrit o es finalitza i es conclou el projecte declarant la cèl·lula flexible com a segura.

2. Seguretat en l'automatització

Aquest bloc del projecte està conformat pels conceptes bàsics en l'àmbit de la seguretat funcional, així com les principals normes internacionals utilitzades en el treball. També s'inclou un repàs sobre les característiques tècniques dels diversos elements de seguretat que s'implementen en la cèl·lula flexible i també sobre la CPU de seguretat NX-SL3300.

Estudiant la norma IEC 61508-1 ens adonem sobre la importància de garantir la seguretat funcional en la cèl·lula flexible la qual està composta per sistemes elèctrics, electrònics i electrònics programables. Veiem com té importància el nivell d'integritat de la seguretat així com la gestió d'aquesta seguretat funcional en tots els cicles de vida de la màquina. I aprenem que aquesta seguretat no només es refereix pel que fa el Hardware sinó que també fa referència al Software.

Amb la norma ISO 13849-1 es mostra tot el que es relaciona inherentment amb el disseny dels sistemes de control, el nivell de prestacions requerit per la màquina i el que es determina, s'explica detalladament les diferents classes d'arquitectura i les diferents categories que presenten els elements de seguretat. I finalment aquesta norma explica pas per pas com realitzar l'avaluació de riscos i com fer correctament la validació del nivell de prestacions. El nivell de prestacions més baix equival a Pla mentre que el nivell més alt correspon a PLe.

Performance Level (PL) según EN ISO 13849-1
a
b
c

Fig. 1. *Nivells de prestacions.*

Amb la norma ISO 12100 ens permet analitzar i valorar de manera sistemàtica els riscos que presenta la cèl·lula flexible. Aquesta norma explica com realitzar una avaluació de riscos i explica que aquesta avaluació, va acompanyada si és necessari d'una reducció dels riscos.

Fig. 2. CPU de seguretat NX-SL3300.

El centre d'aquest projecte és la CPU de seguretat, la CPU (**Fig. 2**) que s'implementa en la cèl·lula flexible és l'element principal que conformarà la reducció de riscos. Aquest element aconsegueix una transferència d'informació segura gràcies al protocol FSoE, a més, assegura uns requisits per aconseguir el nivell de SIL 3 i PLe per una categoria 4 de seguretat, tot això, conforme amb les normatives internacionals anteriorment descrites.

A partir d'aquesta unitat, l'acompanyen els mòduls d'entrades i sortides de seguretat que també asseguren els mateixos requisits que la CPU i permeten la connexió dels elements de seguretat necessaris per a la funció de seguretat.

3. Elements de seguretat

Els elements de seguretat implementats en aquest projecte es poden classificar en dos tipus, segons la classe de parades de seguretat: la parada d'emergència i la parada de protecció.

Polsador "bolet" d'emergència

El polsador "bolet" d'emergència és un element d'entrada al sistema de seguretat dissenyat per aturar de manera immediata la màquina o el procés industrial quan es pressiona. Quan s'activa es provoca en la lògica del sistema el que coneixem com a **parada d'emergència**.

Fig. 3. Polsador "bolet" d'emergència.

Barrera fotoelèctrica F3S-B

La barrera fotoelèctrica és un dispositiu d'entrada al sistema de seguretat que utilitza un feix de llum per a detectar objectes o persones que la traspassen mitjançant un emissor i un receptor. Aquest tipus d'elements de seguretat són equips de protecció electrosensible (ESPE) formats per un dispositiu de detecció, un de control i una commutació del senyal de sortida i realitzen una **parada de protecció**.

Fig. 4. Barrera fotoelèctrica.

Contactors o relés de seguretat

Els contactors o relés de seguretat són també elements de seguretat i formen part de la sortida del sistema de seguretat, s'encarreguen en la majoria de vegades de realitzar la desconnexió total de la zona de risc. Perquè aconsegueixin la funció de seguretat es connecten dos en sèrie per si un es queda clavat que el sistema talli la connexió de totes formes gràcies al segon contactor.

Balisa de senyalització

També es disposa d'una balisa de senyalització la qual forma part del sistema de seguretat, ja que és l'element encarregat de comunicar l'estat de la màquina als operaris, i moltes vegades, avisa dels perills actuant com un protector més del sistema. Aquest element també és un requeriment obligatori segons les normes internacionals sobre seguretat funcional.

4. Avaluació de riscos

Com s'ha explicat en la introducció, l'inici del projecte és situa en l'avaluació de riscos de la cèl·lula flexible. L'avaluació de riscos està conformada per dues etapes, la primera, un anàlisis del risc, i la segona etapa, una valoració del risc [5].

Anàlisis del risc

Per dur a terme correctament l'anàlisi del risc segons les normes internacionals, s'ha de fer una fixació dels límits de la màquina, en aquest cas, la cèl·lula flexible sencera. Aquests límits, no només fan referència als espacials, sinó que també es tenen en compte els límits temporals. Aquests límits temporals s'estableixen considerant tota la vida útil de la cèl·lula flexible, es a dir, els possibles riscos que sorgeixen, mentre s'està muntant la cèl·lula flexible, no seran els mateixos quan està treballant, o quan s'està realitzant un manteniment. És per això, que en l'anàlisi dels riscos, es tenen en compte totes aquestes etapes de la vida útil de la màquina.

Una vegada es fixen els límits de la màquina, passem al procés d'identificació dels perills en la cèl·lula flexible, tals com: col·lisions amb el robot o altres elements mòbils, atrapaments amb les cintes transportadores o altres com per exemple el perill elèctric.

Un cop identificats tots els perills per a totes les situacions perilloses, es realitza una estimació del risc on es determina un nivell de prestacions requerit per a cada situació de perill, seguint la metodologia que descriu la **Fig. 5**. [6].

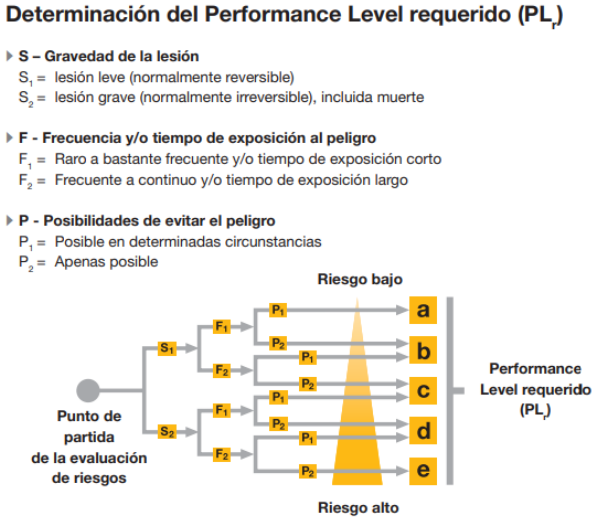

Fig. 5. Determinació del nivell de prestacions requerit.

Valoració del risc

En la valoració del risc s'estudia si realment és necessari realitzar una reducció de riscos, en aquest projecte, un cop

realitzat l'anàlisi del risc, es conclou la necessitat d'un nivell PLrC i, per tant, en el procés de reducció de riscos, que si és necessari, s'ha d'aconseguir aquest nivell de prestacions requerit.

5. Configuració de la CPU de seguretat NX-SL3300

Configuració del Hardware

La unitat NX-SL3300 té diverses configuracions possibles que varien en funció del sistema on s'implementa i els mòduls dels quals es disposen. En aquest projecte aquesta CPU de seguretat es configura de la forma "CPU Rack" mitjançant el NX Bus a un PLC també de OMRON del model NX102-9020, que és el que es disposa a l'estació 4 de la cèl·lula flexible. Aquesta connexió via NX Bus és el mètode de connexió modular dels PLC i mòduls de la marca OMRON, que es munten al carril DIN del quadre elèctric. En aquest projecte, es connecten i configuren dues targetes d'entrades de seguretat (NX-SID800) i dues targetes de sortides de seguretat (NX-SOD400).

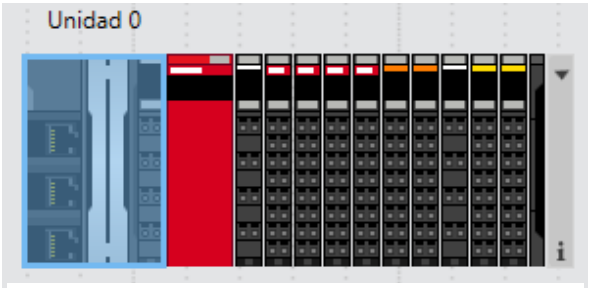

Fig. 6. *Bastidor de la CPU*

Configuració del Software

Un cop estan totes les unitats alimentades correctament a 24 V DC, i mitjançant el software d'OMRON "Sysmac Studio" es comença la configuració del Software de la CPU de seguretat. Per començar, s'ha d'aconseguir una comunicació entre el PLC al qual està connectada la CPU i un PC. Una vegada s'ha establert correctament, es passa al següent pas, que és aconseguir la correcta comunicació entre la CPU del PLC i la CPU de seguretat. Configurant tots els paràmetres i ajustant les unitats correctes al bastidor el resultat es pot observar en la **Fig. 7**.

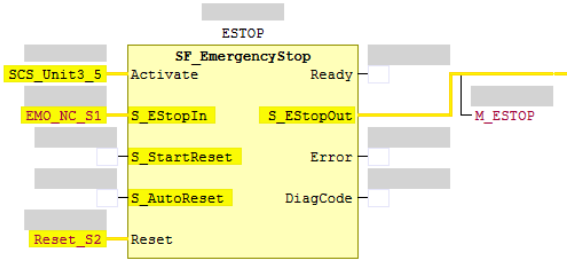

Fig. 7. *Funció SF_EmergencyStop utilitzada pel polsador de parada d'emergència.*

Programació de la unitat NX-SL3300

Una vegada s'ha aconseguit configurar tots els elements necessaris correctament, el següent pas és començar amb la programació. La CPU de seguretat és programa d'una forma diferent dels PLC "normals" i és que, utilitza un llenguatge de programació anomenat FBD, que és un llenguatge gràfic i consisteix en la utilització de blocs de funcions units per línies de connexió. Aquest llenguatge està definit per la norma IEC 61131-3 [7] per a autòmats programables i està enfocada en funcions de seguretat.

Aquest llenguatge de programació segueix una lògica d'execució que depèn de les diferents xarxes, funcions i instruccions que fan que es pugui dinamitzar un programa, amb salts de programa, o instruccions de retorn (**Fig. 8**). Els blocs de funció que s'utilitzen en el programa d'aquest projecte són els següents:

- SF_EmergencyStop
- SF_ESPE
- SF_EDM

A més també s'utilitzen algunes portes lògiques i alguns operadors i variables especials. Aquestes funcions venen pre-definides pel software "Sysmac Studio" i només cal unir els blocs amb les línies de connexió i establir les diferents variables que s'utilitzen. En funció de la complexitat del programa i la quantitat de programes (POU's) s'ha d'establir una configuració de l'assignació dels programes ("Safety Task").

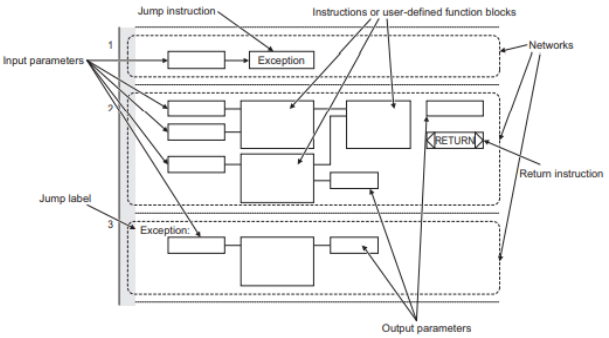

Fig. 8. *Esquema on es mostren els diferents elements que formen una xarxa en la programació FBD.*

6. Avaluació i verificació de la funció de seguretat

En aquest apartat, es realitza l'avaluació i verificació de la funció de seguretat. Després d'identificar els perills i reduir els riscos, s'avalua la funció de seguretat per obtenir els valors de PL o SIL. Aquests valors es comparen amb els requerits inicialment; si són iguals o superiors, la funció de seguretat compleix la normativa, indicant que els perills s'han eliminat o reduït.

Element de seguretat	Segons EN ISO 13849-1	Segons IEC 61508
CPU NX-SL3300	PLe/CAT4	SIL3
Targetes SID/SOD	PLe/CAT4	SIL3
Polsador d'emergència	ND	ND
Barrera fotoelèctrica F3S-B	CAT2,1,B	ND
Contactors	ND	ND

Taula 1. *Categories, nivells de prestacions i SIL donats pels fabricants dels diferents elements de seguretat en l'avaluació de la funció de seguretat.*

Com es pot observar, alguns elements no tenen un valor de la funció de seguretat donat pels fabricants i, per tant, s'ha de calcular. Per realitzar l'avaluació del nivell de prestacions s'han d'estimar i/o calcular diversos aspectes.

En aquest projecte és avalua el nivell de prestacions del polsador d'emergència, de la barrera fotoelèctrica F3S-B i els contactors.

Estimació de l'arquitectura

El polsador d'emergència i els contactors tenen una arquitectura de categoria 3, mentre que la barrera fotoelèctrica correspon com a màxim a una categoria 2.

Estimació del $MTTF_D$

El temps mig fins a fallada perillosa és una dimensió de temps per caracteritzar la fiabilitat bàsica dels components utilitzats. El seu càlcul es fa amb la següent fórmula:

$$MTTF_D = \frac{B_{10d}}{0{,}1 \times n_{op}} \qquad (1)$$

On n_{op} és nombre total d'operacions que un component realitza durant la seva vida útil esperada.

I el B10d representa el nombre de cicles o operacions després del qual el 10% dels components d'un conjunt han fallat de manera perillosa.

En el cas que el fabricant no proporcioni un valor de n_{op} es pot calcular de la següent manera:

$$n_{op} = \frac{d_{op} \times h_{op} \times 3.600 \ \frac{s}{h}}{t\ cycle} \qquad (2)$$

On d_{op} és el nombre mig de dies d'operació per any, i h_{op} és el nombre mig d'hores d'operació per dia.

I "t cycle" és el temps mig d'operació entre l'inici de dos cicles successius.

Un cop calculat $MTTF_D$ és busca el seu índex (alt, mig o baix) en funció del valor obtingut. Aquest índex es consulta a la norma UNE-EN ISO 13849-1 a la Taula 6 de l'apartat 6.1.4.

Estimació del DC

La cobertura de diagnòstic (DC) és la relació entre la taxa de fallades perilloses detectades i la taxa total de fallades perilloses. És a dir, si aquest índex és un 0% significa que el component no té cap mecanisme de detecció de fallades i, per tant, la seva cobertura de diagnòstic és nul·la. A continuació s'exposa els diferents rangs de DC:

• Sense diagnòstic (DC = 0%): Cap mecanisme de detecció de fallades aplicat.

• Diagnòstic baix (DC = 60%): Monitoratge simple o proves manuals periòdiques.

• Diagnòstic mitjà (DC = 90%): Redundància amb comparació periòdica.

• Diagnòstic alt (DC = 99%): Redundància amb monitorització constant.

Realitzant l'estimació de la DC, s'obté que el polsador d'emergència, la barrera fotoelèctrica F3S-B i els contactors tenen una cobertura de diagnòstic mitjà, segons la Taula 7 de l'apartat 6.1.5 de la norma UNE-EN ISO 13849-1. Aquesta redundància amb comparació periòdica s'aconsegueix gràcies a la CPU de seguretat i les targetes d'entrades i sortides de seguretat.

Estimació del CCF

Les fallades de causa comuna és la probabilitat que dos o més defectes separats tinguin una causa comuna. Per realitzar aquesta estimació es consulta la taula F1 de la norma UNE-EN ISO 13849-1, es realitza un sumatori en funció de si es compleixen els requisits, i si aquest valor és igual o major a 65 punts, es pot afirmar que el component sí que aconsegueix la mesura contra CCF.

Mesura contra CCF (Punts)	**Component**		
	Contactor	**Barrera fotoelèctrica**	**Polsador d'emergència**
Separació (15)	X	X	X
Diversitat (20)			
Protecció contra sobretensions i sobreintensitats. (15)	X	X	X
Utilització de components de eficàcia comprovada (5)	X	X	X
Avaluació (5)	X	X	X
Formació (5)			
Prevenció de EMI o impureses de mitjans fluídics (25)	X	X	X
Altres influencies (10)	X	X	X
TOTAL	**75**	**75**	**75**
>65 Punts?	**Sí**	**Sí**	**Sí**

Taula 2. *Càlcul de la puntuació del CCF per comprovar si compleix els requisits.*

Aquestes mesures, són enumerades, en funció dels criteris tècnics, que representen la contribució de cada mesura en la reducció dels CCF.

En aquest projecte els tres components estudiats sí que compleixen els requeriments de les mesures contra les CCF.

Determinació del nivell de prestacions PL

Una vegada hem realitzat totes les estimacions, podem determinar el PL de cada component per finalment verificar si la funció de seguretat compleix els requisits establerts.

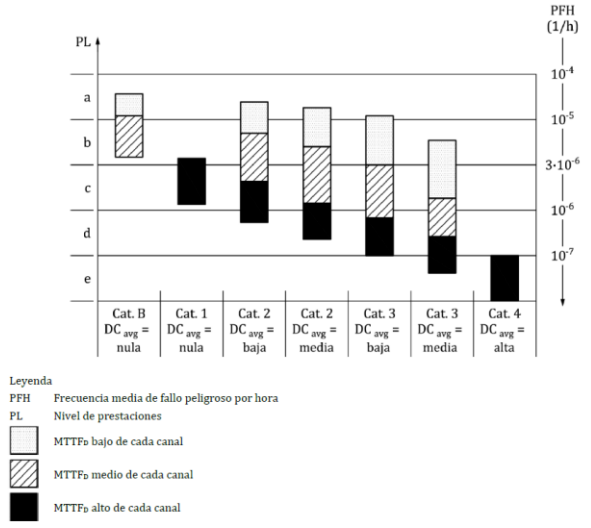

Fig. 9. *Relació entre les categories, la DC, el MTTFD, el PFH i el PL.*

Observant la **Fig. 9** obtenim els nivells de prestacions de cada component i és que, els contactors i el polsador d'emergència tenen un PLd (SIL2) mentre que la barrera fotoelèctrica té un PLc (SIL1).

Verificació de la funció de seguretat

Aquesta verificació consisteix a comparar aquests valors de PL o SIL obtingut anteriorment amb els valors de PLr o SIL requerits segons l'avaluació de riscos inicial.

Si es donés la situació de què no s'aconsegueixen els nivells de PL o SIL requerits en l'avaluació de riscos, s'hauria d'iterar segons s'ha explicat en la metodologia del projecte i caldria tornar a realitzar una reducció de riscos des del començament.

En l'avaluació de riscos inicial havíem estimat un nivell de prestacions requerit PLrC i una vegada realitzada la reducció de riscos, en l'avaluació de la funció de seguretat estimada anteriorment, el resultat dels components que no es tenien dades de fabricant conclouen amb nivells de prestacions PLc el més baix i PLd.

Per tant, es pot afirmar que la reducció de riscos ha aconseguit els requeriments establerts.

7. Conclusions

En aquest projecte d'implementació de la CPU de seguretat a la cèl·lula flexible, s'han aconseguit els objectius principals, com el de posar en funcionament la CPU i assegurar-ne les funcions bàsiques de manera eficaç. S'ha realitzat la implementació de la CPU a l'estació 4 de manera exitosa, permetent la connexió segura de múltiples elements de seguretat segons les normatives internacionals. També s'ha integrat i comunicat la CPU amb els diversos controladors de manera efectiva. La programació de la CPU s'ha completat amb èxit, conjuntament amb la correcta configuració a nivell de Hardware i Software, i s'ha dut a terme una avaluació de riscos que ha permès implementar elements de seguretat com polsadors d'emergència i barreres fotoelèctriques. S'han complert les normatives de seguretat funcional, arribant als nivells de PL o SIL requerits. En resum, el projecte ha assolit els seus objectius i obre la porta a la implementació de noves tecnologies de seguretat en la indústria 4.0.

Tot i això, es va identificar una limitació en la implementació de la catifa de seguretat de Carlo Gavazzi, que estava malmesa, i a part, no disposava de les targetes NX-SIH400 necessàries [8]. Això va impedir la seva integració en l'estació automatitzada. En el futur, es planifica implementar aquesta catifa de seguretat juntament amb les targetes requerides, reforçant així la seguretat de l'estació i permetent una nova avaluació i reducció de riscos per comprovar la seguretat funcional del nou element implementat.

8. Agraïments

Vull agrair l'ajuda i el suport de tot l'equip de Serveis Tècnics de Laboratori de l'EPSEVG, especialment al meu tutor i mentor d'aquest projecte, l'Óscar De Sousa. Gràcies per la motivació i tots els moments compartits. També m'agradaria expressar el meu agraïment per haver tingut l'oportunitat de cursar els meus estudis a la universitat, i al personal docent que m'ha acompanyat en aquest camí. Finalment, voldria destacar el suport especial de la meva parella en els moments més difícils.

Referències

[1] Omron. Omron automatización industrial [en línia]. 2024. [consulta el 31/01/2024]. Disponible a: https://industrial.omron.es/es/home

[2] UNE-EN 61508-1, "Seguretat funcional dels sistemes elèctrics/ electrònics/electrònics programables relacionats amb la seguretat. Part 1: Requisits generals." 2011.

[3] UNE-EN ISO 13849-1, "Seguretat de les màquines. Parts dels sistemes de comandament relatius a la seguretat. Part 1: Principis generals pel disseny (ISO 13849-1:2023)." 2024.

[4] UNE-EN ISO 12100, "Seguretat de les màquines. Principis generals pel disseny. Avaluació del risc i reducció del risc (ISO 12100:2010)." 2012.

[5] Plassa, Josep. How to design integrated safety into machines from the start? [blog]. A: Industrial Omron [en línia]. 19 de setembre 2019 [consulta el 18/03/2024]. Disponible a: https://industrial.omron.eu/en/solutions/blog/how-to-design-integrated-safety-into-machines-from-the-start

[6] Pilz GmbH & Co. KG. Seguretat funcional. PILZ [en línia]. [Consulta: 5 d'abril de 2024]. Disponible a: https://www.pilz.com/es-ES/support/law-standards-norms/functional-safety

[7] EN 61131-3:2013, "Autòmats programables. Part 3: Llenguatges de programació" 2013.

[8] Carlo Gavazzi. Gavazzi Automation [en línia]. 2024. [consulta el 03/04/2024]. Disponible a: https://www.gavazziautomation.com/