ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ

ΠΑΡΑΔΟΣΗ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

ΠΡΟΤΥΠΑ ΚΑΙ FAIL SAFE ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΛΕΙΤΟΥΡΓΙΑ ΣΥΣΤΗΜΑΤΩΝ ΑΥΤΟΜΑΤΙΣΜΟΥ

ΓΙΑΝΝΗΣ ΣΙΩΤΑΣ 47195

12ο ΕΞΑΜΗΝΟ

ΕΙΣΗΓΗΤΕΣ: κ. Θεοχάρης Ευστάθιος

κ. Short Andrew

ΑΘΗΝΑ 2022

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ/ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Σιώτας Γιάννης του Ευαγγέλου, με αριθμό μητρώου 47195 φοιτητής της Σχολής Πανεπιστημίου Δυτικής Αττικής του Τμήματος Βιομηχανικής Σχεδίασης και Παραγωγής, δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής/διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο/Η Δηλών/ούσα

ΠΡΟΤΥΠΑ ΚΑΙ FAIL SAFE ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΛΕΙΤΟΥΡΓΙΑ ΣΥΣΤΗΜΑΤΩΝ ΑΥΤΟΜΑΤΙΣΜΟΥ

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η πτυχιακή/διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
	Θεοχάρης Ευστάθιος	**ΕΔΙΠ Α'**	EFSTATHIOS THEOCHARIS Digitally signed by EFSTATHIOS THEOCHARIS Date: 2022.07.17 13:20:30 +03'00'
	Short Andrew	**ΕΔΙΠ Α'**	ANDREW-RONALD SHORT Digitally signed by ANDREW-RONALD SHORT Date: 2022.07.17 13:14:05 +03'00'
	Παπουτσιδάκης Μιχαήλ	**ΚΑΘΗΓΗΤΗΣ**	Michail Papoutsidakis Digitally signed by Michail Papoutsidakis Date: 2022.08.29 23:09:34 +03'00'

Περιεχόμενα

Contents

ΚΕΦΑΛΑΙΟ 1^{Ο}

1.1 ΕΙΣΑΓΩΓΗ

Στις μέρες μας, κάθε παραγωγικός κλάδος ο οποίος είναι υπεύθυνος για την σωστή και ασφαλή παραγωγή προϊόντων, είναι υποχρεωμένος να ακολουθεί βασικά πρότυπα τα οποία καθιστούν ασφαλή αυτή τη μονάδα προς το εργατικό προσωπικό όπου εργάζεται σε εκείνο τον χώρο.

Τι εννοούμε όμως με τον όρο ασφάλεια και με ποιόν τρόπο εκφράζουμε όλα αυτά τα πρότυπα;

Αρχικά, είναι σημαντικό να αναφερθεί πως ο λόγος ύπαρξης όλων των προτύπων είναι για την αποφυγή σοβαρών τραυματισμών μέχρι και θανάτων σε άκρως σοβαρές περιστάσεις, όπως πχ ηλεκτροπληξία λόγω μη υπάρχοντος επαγγελματικού εξοπλισμού, λανθασμένη κίνηση ενός ρομποτικού βραχίονα μέχρι και πυρκαγιά από κάποιο επεξεργαστή εισόδων-εξόδων όπως ένα PLC κλπ. Για την αποφυγή όλων αυτών, υπάρχουν πολλοί κλάδοι οι οποίοι κρίνουν αν το κάθε μηχάνημα καθίσταται ασφαλές για χρήση, λαμβάνοντας υπόψη κάποιους στοιχειώδης ¨νόμους¨. Θα ασχοληθούμε με δύο από τους πιο γνωστούς οργανισμούς προτύπων, οι οποίοι είναι οι: IEC(International Electrotechnical Commission) και ISO(International Organization for Standardization).

Όσον αφορά τον IEC, είναι ένας διεθνής οργανισμός που ασχολείται με τη δημοσίευση προτύπων όλων των ηλεκτρονικών και ηλεκτρολογικών συσκευών που χρησιμοποιούνται σε οικίες έως σε τεράστιες και πολύπλοκες παραγωγές, οι οποίες χρήζουν ύψιστη ασφάλεια. Το IEC έχει τη δυνατότητα να διαχειριστεί τέσσερα παγκόσμια συστήματα αξιολόγησης για τη συμμόρφωση όλων των ηλεκτρονικών εξοπλισμών που πιστοποιούνται με τα διεθνή πρότυπα. Επίσης, στο IEC συμπεριλαμβάνονται και οι τομείς για τη διανομή ηλεκτρικών, μαγνητικών, ηλεκτρομαγνητικών και τηλεπικοινωνιακών πολυμέσων.

Παρόμοια, ο ISO είναι ένας διεθνής οργανισμός για την δημιουργία και έκδοση διαφόρων ειδών προτύπων σε πολλών ειδών βιομηχανιών και παραγωγών. Επίσης υπάρχει συνεργασία της ISO με την IEC λόγω ίδιου ενδιαφέροντος σε πολλά πρότυπα ηλεκτρολογικού περιεχομένου, με λίγα λόγια είναι και τα δύο εργαλεία τα οποία χρησιμοποιούνται στο δημόσιο και ιδιωτικό τομέα για να γίνει όσο το δυνατόν πιο αποδοτικός ο έλεγχος

έγκρισης αυτών προτύπων και έτσι να χρησιμοποιείται ως κατευθυντήριο μέσο σε όλες τις παραγωγικές και βιοχημικές μονάδες. Παράλληλα πρέπει πάντα τα πρότυπα που εκδίδονται είτε από την ISO είτε από την IEC, να τηρούν τις διάφορες υποχρεώσεις όλου του παγκοσμίου εμπορίου, διότι κάθε όμιλος – εταιρία σε κάθε χώρα διαφέρει στον τρόπο πώλησης και τυποποίησης προτύπων, ανάλογα με τις απαιτήσεις. Αυτό γίνεται για να υπάρχει πάντα καλή συνεργασία, απόδοση και ισότητα. Τα διεθνή πρότυπα IEC και ISO αναπτύσσονται χρησιμοποιώντας μια διαδικασία πολυμερούς περιβάλλοντος που διασφαλίζει ότι ένα ευρύ φάσμα τεχνικών απόψεων εκπροσωπούνται, συμπεριλαμβανομένων εκείνων των οικονομικών και κοινωνικών ενδιαφερόντων.

1.2 ΠΡΟΤΥΠΑ

[1] Παραπάνω αναφερθήκαμε γενικά στα πρότυπα IEC και ISO και τη χρησιμότητά τους σε κάθε βιομηχανία. Παρακάτω θα γίνει αναφορά κάποιων βασικών ειδών προτύπων, δίνοντας παράδειγμα μια παραγωγική μονάδα που χρησιμοποιεί μια γραμμή παραγωγής, έναν φούρνο και στη συνέχεια έναν ανελκυστήρα ο οποίος θα τοποθετεί προσωρινά το προϊόν σε έναν χώρο ψύξης. Κατ΄αυτή τη διαδικασία, κρύβονται πολλοί μεγάλοι κίνδυνοι διότι πάντα πρέπει να βρίσκεται προσωπικό σε αυτό το χώρο για να πραγματοποιείτε συνεχής έλεγχος πως το προϊόν που παράγεται είναι στην εντέλεια και ταυτόχρονα να πραγματοποιείτε έλεγχος στα μηχανήματα σε περίπτωση βλάβης. Άρα θα αναλυθούν διάφορα πρότυπα έτσι ώστε να γίνει έγκριση αυτής της παραγωγής στον τομέα της ασφάλειας.

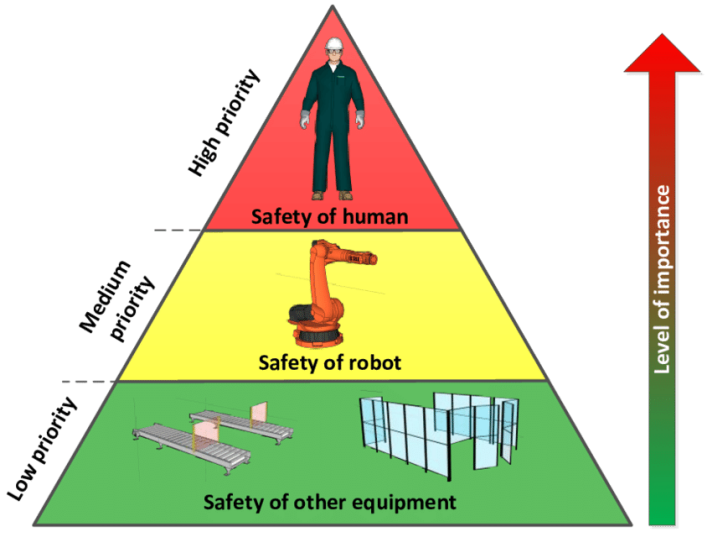
Παράλληλα, τα πρότυπα που αφορούν την ασφάλεια χωρίζονται σε κάποιες κατηγορίες λόγω της διαφοροποίησης τους στον κίνδυνο. Πιο συγκεκριμένα ο καθοριστικός ρόλος των προτύπων αυτών είναι στην παρουσίαση ενός πλαισίου το οποίο αφορά την καθοδήγηση και τις αποφάσεις που πρέπει να παρθούν όσον αφορά την σωστή συντήρηση των μηχανημάτων και τον κύκλο ζωής τους, έτσι ώστε να είναι πάντα προβλεπόμενη και ελεγχόμενη η ασφάλειά τους κατά τη χρήση. Υπάρχουν τρεις διαφορετικές κατηγορίες προτύπων και είναι οι εξής:

- Τύπου Α: Σε αυτή τη κατηγορία έπονται τα πρότυπα που αφορούν διάφορες βασικές έννοιες και μεθόδους σχεδιασμού που μπορούν να εφαρμοστούν. Στου τύπου Α, η ασφάλεια εξαρτάται από τη σωστή λειτουργία των μηχανημάτων στις βασικές ηλεκτρικές και ηλεκτρονικές αρχές. Κάποια από αυτά είναι και τα πρότυπα IEC 61508 (Λειτουργική ασφάλεια των ηλεκτρονικών συστημάτων), ISO

13849 και IEC 61511 (Συστήματα οργάνων για την διασφάλιση της ασφάλειας σε μια βιομηχανία).

- Τύπου Β: Στον δεύτερο τύπο υπάρχουν τα πρότυπα τα οποία ασχολούνται με την στρατηγική επιλογή μεθόδων για την ασφαλή ηλεκτρική ασφάλεια. Αυτό επιτυγχάνεται με τον σχεδιασμό διαφόρων μεθόδων για την αποφυγή επαφής γυμνών καλωδίων ή άλλων αγώγιμων στοιχείων όπως είναι η γείωση. Κάποια από αυτά τα πρότυπα είναι το EN 60947-5 (Διανομείς χαμηλής τάσης) και το ISO 12100 (Ασφάλεια των μηχανημάτων, εκτίμηση και μείωση κινδύνου).

- Τύπου Γ: Στην τελευταία κατηγορία έχουμε τα πρότυπα που ασχολούνται στην εξασφάλιση αποφυγής κάποιας πυρκαγιάς ή έκρηξης από κάποια ηλεκτρική συσκευή. Με βάση αυτών, κάποιοι τρόποι για τον περιορισμό και μείωση πυρκαγιών, είναι η χρήση των ‘’φρακτών Ζένερ’’ και γαλβανισμένων διόδων, έτσι ώστε η ροή του ρεύματος να κατευθύνεται μόνο προς μια κατεύθυνση. Ένα από αυτά τα πρότυπα είναι το IEC 60079-11 το οποίο βρίσκεται ακόμα σε εξέλιξη για την βέλτιστη λειτουργία μείωσης του κινδύνου από την κάθε πιθανή δυσλειτουργία που μπορεί να υπάρξει.



[1] Εικόνα 1: Οι τρεις κατηγορίες των προτύπων ασφάλειας.

ΚΕΦΑΛΑΙΟ 2Ο

2.1 ΠΡΟΤΥΠΟ IEC 61508

[2][3] Το IEC 61508 είναι το βασικό πρότυπο που αναλύει τη διαχείριση της λειτουργικής ασφάλειας στην ανάπτυξη των διαφόρων ηλεκτρονικών που σχετίζονται με αυτή. Πιο συγκεκριμένα, αποτελείται από μεθόδους για τον τρόπο σχεδίασης, ανάπτυξης, εφαρμογής και επίβλεψης των διαφόρων μηχανημάτων αυτοματισμού με την εξής ερμηνεία:

(Electrical/Electronic/Programmable Electronic Safety-related Systems).

Το IEC 61508 είναι το πιο αναγκαίο και βασικό λειτουργικό πρότυπο ασφάλειας που ισχύει σε όλες τις βιομηχανικές παραγωγές. Ορίζει τη σωστή λειτουργική ασφάλεια όπου σχετίζεται με το EUC(Equipment Under Control) και το σύστημα ελέγχου που εξαρτάται από τη λειτουργία όλων των συστημάτων που ασχολούνται με την ασφάλεια, αλλά και τη μείωση εξωτερικών κινδύνων. Άρα η λογική πίσω από τα πρότυπα αυτά είναι η σωστή λειτουργία του μηχανήματος ή σε περίπτωση που αποτύχει, να είναι προβλέψιμο χωρίς να υπάρχει κάποιος κίνδυνος.

Βασικός στόχος είναι η ευαισθητοποίηση του προσωπικού των τμημάτων ανάπτυξης και ποιότητας. Επίσης, εξίσου σημαντικό είναι η ενημέρωση των διευθυντών της εταιρίας, οι οποίοι έχουν πρωταγωνιστικό ρόλο στις επιπτώσεις μίας παραγωγής σε περίπτωση αμέλειας. Κατά το πρότυπο αυτό, υπάρχουν δύο θεμελιώδες αρχές:

- Μια διαδικασία όπου ονομάζεται κύκλος ζωής ασφάλειας, η οποία αναλύεται με γνώμονα τις βέλτιστες πρακτικές για την αναγνώριση και εξάλειψη των διαφόρων σφαλμάτων.
- Μια προσέγγιση πιθανής αστοχίας για να κατανοηθεί η κάθε επίπτωση στην ασφάλεια των αστοχιών της συσκευής-μηχανής.

Επιπλέον, το πρότυπο IEC 61508 έχει τις ακόλουθες ιδέες όσον αφορά τον κίνδυνο:

- Μπορεί μόνο να μειωθεί η πιθανότητα του κινδύνου, αλλά <u>ποτέ</u> ο μηδενικός κίνδυνος.
- Οι μη ανεκτοί κίνδυνοι πρέπει να μειώνονται
- Η καλύτερη, οικονομικά ασφάλεια επιτυγχάνεται όταν πραγματοποιείτε κατά τη διάρκεια όλου του κύκλου ζωής της ασφάλειας.

2.1.2 ΠΡΟΤΥΠΟ IEC 61508 & ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ

[4] Το συγκεκριμένο πρότυπο έχει ως απαίτηση να πραγματοποιείται πλήρης αξιολόγηση σε κάθε περίπτωση ύπαρξης κινδύνου σε όλα τα μηχανήματα, αλλά και σε περιπτώσεις συμβάντων. Έτσι, είναι καθοριστικό να γίνεται ποιοτική και ποσοτική ανάλυση η οποία παρουσιάζει τους διάφορους κινδύνους που μπορεί να προκύψουν και μια σειρά προσεγγίσεών τους.

Η συγκεκριμένη ανάλυση παρέχει ένα πλαίσιο 6 κατηγοριών πιθανότητας του κινδύνου και 4 των συνεπειών που μπορεί να προκαλέσει.

2.1.3 ΠΙΘΑΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ ΤΟΥ ΚΙΝΔΥΝΟΥ

ΠΙΘΑΝΟΤΗΤΑ	***ΕΠΕΞΗΓΗΣΗ***	***ΕΥΡΟΣ (ΣΕ ΧΡΟΝΙΑ)***
ΣΥΧΝΑ	*ΠΟΛΛΕΣ ΦΟΡΕΣ ΣΤΗ ΔΙΑΡΚΕΙΑ ΖΩΗΣ*	$>10^{-3}$
ΠΙΘΑΝΟ	*ΑΡΚΕΤΕΣ ΦΟΡΕΣ -//-*	$10^{-3}\ to\ 10^{-4}$
ΤΥΧΑΙΟ	*ΜΙΑ ΦΟΡΑ ΚΑΤΑ ΤΗ -//-*	$10^{-4}\ to\ 10^{-5}$
ΜΑΚΡΥΝΟ ΑΛΛΑ ΟΧΙ ΑΠΙΘΑΝΟ	*ΣΧΕΤΙΚΑ ΑΠΙΘΑΝΟ ΣΤΗ -//-*	$10^{-5}\ to\ 10^{-6}$
ΑΠΙΘΑΝΟ	*ΑΡΚΕΤΑ ΑΠΙΘΑΝΟ ΝΑ ΣΥΜΒΕΙ*	$10^{-6}\ to\ 10^{-7}$
ΑΔΥΝΑΤΟΝ	*ΑΠΙΣΤΕΥΤΑ ΑΔΥΝΑΤΟΝ ΟΤΙ ΥΠΑΡΧΕΙ ΠΕΡΙΠΤΩΣΗ ΝΑ ΣΥΜΒΕΙ*	$<10^{-7}$

2.1.4 ΣΥΝΕΠΕΙΕΣ ΠΕΡΙΠΤΩΣΕΩΝ

ΚΑΤΗΓΟΡΙΑ	***ΕΠΕΞΗΓΗΣΗ***

ΚΑΤΑΣΤΡΟΦΙΚΗ	*ΑΠΩΛΕΙΕΣ ΠΟΛΛΩΝ ΖΩΩΝ*
ΚΡΙΣΙΜΗ	*ΑΠΩΛΕΙΑ ΜΙΑΣ ΖΩΗΣ*
ΟΡΙΑΚΗ	*ΚΡΙΣΙΜΟΙ ΤΡΑΥΜΑΤΟΣΜΟΙ ΕΝΟΣ Ή ΠΟΛΛΩΝ ΑΤΟΜΩΝ*
ΑΜΕΛΗΤΕΑ	*ΕΛΑΧΙΣΤΟΙ ΤΡΑΥΜΑΤΙΣΜΟΙ ΣΤΗΝ ΧΕΙΡΟΤΕΡΗ ΠΕΡΙΠΤΩΣΗ*

Και αυτοί οι δυο πίνακες συνδυάζονται για να μας δώσουν έναν ενιαίο, ο οποίος θα καθορίσει κάποιες κλάσεις οι οποίες μας δείχνουν αν είναι ανεκτό να υπάρχει κάτι τέτοιο ή χρίζει αλλαγή και προσοχή.

	ΣΥΝΕΠΕΙΑ			
ΠΙΘΑΝΟΤΗΤΑ	*ΚΑΤΑΣΤΡΟΦΙΚΗ*	*ΚΡΙΣΙΜΗ*	*ΟΡΙΑΚΗ*	*ΑΜΕΛΗΤΕΑ*
ΣΥΧΝΑ	*1*	*1*	*1*	*2*
ΠΙΘΑΝΟ	*1*	*1*	*2*	*3*
ΤΥΧΑΙΟ	*1*	*2*	*3*	*3*
ΜΑΚΡΥΝΟ	*2*	*2*	*3*	*4*
ΑΠΙΘΑΝΟ	*3*	*3*	*4*	*4*
ΑΔΥΝΑΤΟΝ	*4*	*4*	*4*	*4*

Παραπάνω, έχουμε τον πίνακα με τις κλάσεις, οι οποίες έχουν μια συγκεκριμένη έννοια.

1. Αδιανόητο να συμβεί σε κάθε περίπτωση.
2. Μη επιθυμητό. Για να γίνει ανεκτό, πρέπει να έχει εξακριβωθεί πως ο κίνδυνος δεν μπορεί να μειωθεί περεταίρω.
3. Ανεκτό, εάν υπάρχει περίπτωση μείωσης του κινδύνου.
4. Δεκτό, παρόλο που μπορεί να χρειαστεί κάποια βελτίωση στο μέλλον και μόνιμη παρακολούθηση.

Το IEC 61508 μας παρουσιάζει επίσης ένα μέσο το οποίο χρησιμοποιούμε για να εντοπίσουμε την απόδοση του συστήματος ασφάλειας και ονομάζεται Επίπεδο Ακεραιότητας Ασφάλειας (Safety Integrity Level, SIL). Το SIL μας δείχνει τις πιθανότητες να αστοχήσει ένα μηχάνημα κατά τη ζήτηση. Υπάρχουν τέσσερα διαφορετικά SIL 1-4, όπου το υψηλότερο($4^{ο}$) σημαίνει ύψιστη ασφάλεια και ελάχιστες πιθανότητες εμφάνισης κινδύνου, άρα μικρότερο ρίσκο. Είναι κατανοητό πως όσο πιο υψηλό SIL υπάρχει, τόσο και μεγαλύτερο το κόστος, κάτι που πολλές φορές το καθιστά και δύσκολο στην αγορά του σε πολλές παραγωγές. Παρακάτω υπάρχει ένας πίνακας

όπου παρουσιάζονται όλα τα SIL ανάλογα με την πιθανότητα να υπάρξει κάποια ζημιά που να προκαλεί κίνδυνο στους εργαζόμενους.

SIL	*ΧΑΜΗΛΗ ΖΗΤΗΣΗ*	*ΥΨΗΛΗ & ΣΥΝΕΧΟΜΕΝΗ ΖΗΤΗΣΗ (ΖΗΜΙΑ/ΩΡΑ)*
1	$\geq 10^{-2} to < 10^{-1}$	$\geq 10^{-6} to < 10^{-5}$
2	$\geq 10^{-3} to < 10^{-2}$	$\geq 10^{-7} to < 10^{-6}$
3	$\geq 10^{-4} to < 10^{-3}$	$\geq 10^{-8} to < 10^{-7}$
4	$\geq 10^{-5} to < 10^{-4}$	$\geq 10^{-9} to < 10^{-8}$

Έχοντας κάποια μηχανήματα σε μια βιομηχανική παραγωγή, θα γίνει αναφορά του κατάλληλου SIL σε σχέση με την επικινδυνότητα. Αρχικά υπάρχει ένας φούρνος στον οποίο ψήνεται το προϊόν, ύστερα υπάρχει μια γραμμή παραγωγής που προωθεί το προϊόν σε έναν ανελκυστήρα για την ψύξη του και τέλος έχουμε το μηχάνημα για την πακετοποίηση και συσκευασία. Όλα τα μηχανήματα έχουν έναν συγκεκριμένο βαθμό επικινδυνότητας και είναι ανάλογος με την πιθανότητα να βρίσκεται κάποιος εργαζόμενος σε εκείνο τον χώρο. Στον φούρνο υπάρχει ελάχιστη πιθανότητα κάποιος χειριστής να βρίσκεται κοντά σε αυτόν, με αποτέλεσμα να υπάρχουν σχεδόν ελάχιστες πιθανότητες κάποιος να καεί. Παρόλα αυτά, οι ελάχιστες πιθανότητες υπάρχουν διότι σε περίπτωση που κάποιος από τους φούρνους πάθει κάποια βλάβη, θα χρειαστεί ο χειριστής να παρευρεθεί εκεί και να πραγματοποιήσει κάποια αλλαγή, άρα μπορεί να πάθει κάποιο έγκαυμα ψηλού βαθμού (οριακή). Στη συνέχεια έχουμε τον ανελκυστήρα, ο οποίος έχει διάφορους οδοντωτούς τροχούς, εκεί απαγορεύεται να έχουμε κάποιον χειριστή διότι η επικινδυνότητα είναι αρκετά υψηλή. Στην περίπτωση που υπάρξει κάποια βλάβη, πρέπει πρώτα να σταματήσει όλη η παραγωγή για να επισκευαστεί, κάτι που το καθιστά ασφαλές σε συνθήκες επισκευής. Τέλος, έχουμε το πακετάρισμα του προϊόντος στο οποίο υπάρχει ένας ρομποτικός βραχίονας ο οποίος τοποθετεί το προϊόν σε κούτες και ύστερα τις κλείνει. Εδώ υπάρχει πάντα κάποιος χειριστής για να επιβλέπει αν υπάρχει ο σωστός αριθμός προϊόντων σε κάθε κούτα, παρόλα αυτά είναι και πολύ αυξημένος ο κίνδυνος κάποιος να χάσει πχ το χέρι του και παράλληλα είναι αρκετά πιθανό κάτι τέτοιο να συμβεί.

Συλλέγοντας όλα τα μηχανήματα και τον κίνδυνο που μπορεί να προξενήσουν σε κάποιο χειριστή, βρισκόμαστε το SIL 3, δηλαδή πρέπει να πιστοποιηθεί το πρότυπο IEC 61508 με SIL 3, στο οποίο έχουμε ύψιστους κινδύνους, κάποιους μη αντιστρέψιμους, παρόλα αυτά δεν χάνουμε ζωές χειριστών.

2.2 ΠΡΟΤΥΠΟ IEC 61511

[5][6] Το IEC 61511 είναι το πρότυπο που σχετίζεται στο τεχνικό κομμάτι μίας παραγωγικής μονάδας και καθορίζει διάφορες πρακτικές στη μηχανική των διαφόρων συστημάτων που εξακριβώνουν την ασφάλεια με τη βοήθεια οργάνων. Το συγκεκριμένο πρότυπο ορίζει όλες τις απαιτήσεις της λειτουργική ασφάλειας που καθορίζονται από πρότυπο IEC 61508 και έτσι εστιάζεται σε έναν τύπο οργανωμένου συστήματος ασφάλειας στον τομέα διεργασιών. Αυτό ονομάζεται Σύστημα με Όργανα Ασφάλειας (SIS).

Το IEC 61511 καλύπτει τις απαιτήσεις του σχεδιασμού και της διαχείρισης για το SIS, το οποίο περιλαμβάνει τα εξής: Την αρχική ιδέα, τον σχεδιασμό, την υλοποίηση, τη λειτουργία και συντήρηση έως και τον παροπλισμό. Αρχίζει στην πιο πρώιμη φάση ενός έργου και ανέρχεται μέχρι την εκκίνηση του.

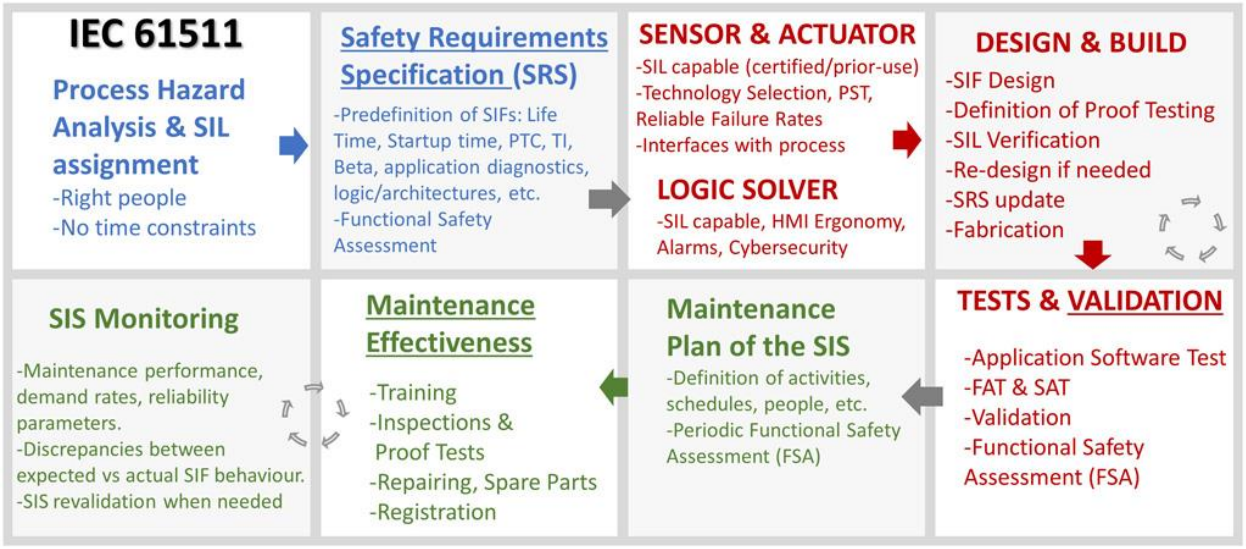
Το πρότυπο αυτό αποτελείται από τέσσερα βασικά μέρη για την απόδοση του SIL:

- Απαιτήσεις πλαισίου, διερμηνείες, σύστημα, υλικό και λογισμικό.
- Οδηγίες για την εφαρμογή του προτύπου.
- Οδηγίες για τον προσδιορισμό των απαιτήσεων όσον αφορά τα επίπεδα ακεραιότητας ασφάλειας.
- Απόδειξη συμμόρφωσης.

[7] Επίσης το πρότυπο IEC 61511 προσφέρει κάποιες μεθόδους για την απεικόνιση της ασφάλειας με βάση τη συμμόρφωσή της στο πρότυπο :

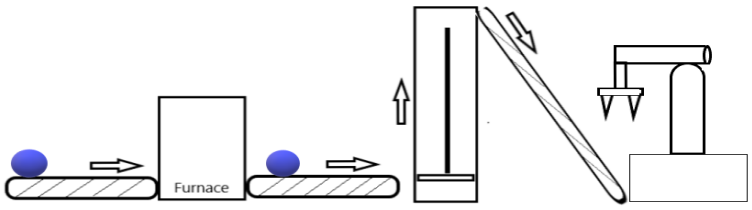
- Γράφημα βαθμονόμησης του κινδύνου, ως ημιποσοτική μέθοδος.
- Γράφημα κινδύνου, ως ποιοτική μέθοδος.

- Επίπεδο ανάλυσης ασφάλειας (LOPA).



[7] Εικόνα 2: Συμμόρφωση του προτύπου IEC 61511 στην παραγωγή.

Είναι κατανοητό πως όταν η ανάλυση κινδύνου προσδιορίζει ότι απαιτείται SIS, η απαιτούμενη μείωση του κινδύνου γίνεται στόχος για την απόδοση του SIS . Παρακάτω θα δούμε έναν πίνακα της συμμόρφωσης του IEC 61511 στον παραγωγικό χώρο.

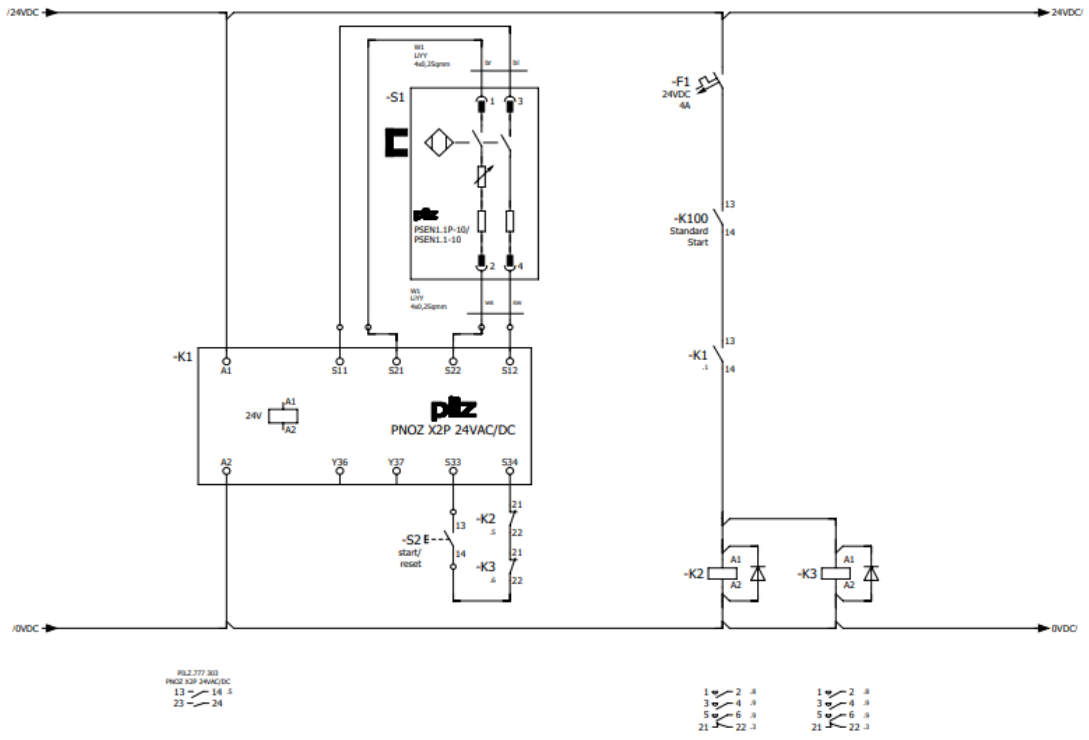


Εικόνα 3: Απεικόνιση της παραγωγικής μονάδας.

[8] Στο προηγούμενο πρότυπο αναφέρθηκε πως με βάση την παραγωγική διαδικασία που υπάρχει βρισκόμαστε σε SIL 3 και με τη βοήθεια του προτύπου IEC 61511, θα γίνει προσπάθεια μείωσης του SIL και ταυτόχρονα να υπάρχει μεγαλύτερη ασφάλεια στο χώρο των εργαζομένων. Αρχικά το πιο σημαντικό εργαλείο που θα βοηθήσει σε περίπτωση ανάγκης είναι ένα safety relay το οποίο θα απενεργοποιεί τα μηχανήματα όπως είναι ο φούρνος και ο βραχίονας που πακετάρει τα κιβώτια. Αυτό είναι αναγκαίο διότι ανά πάσα στιγμή, όταν παρατηρηθεί κάποια περίπτωση που φέρνει σε κίνδυνο τον εργαζόμενο, να σωθεί.

Τα συγκεκριμένα relay είναι της εταιρία Pilz, τα οποία είναι κατασκευασμένα και πιστοποιημένα με πολλά πρότυπα για να εξασφαλίζουν την ασφάλεια. Ειδικότερα, καλύπτουν το πρότυπο IEC 61511 και IEC 62061. Πραγματοποιείται ελεγχόμενη και αυτόματη επαναφορά ανάλογα με τις απαιτήσεις της παραγωγής, αλλά στη προκείμενη περίπτωση θα χρειαστούμε αυτόματη για ευνόητους λόγους. Η λειτουργία του relay θα έχει την εξής λογική: Το άνοιγμα και κλείσιμο των διακοπτών θα πραγματοποιείται με το safety relay k1 PNOZ X2P μέσω επαφής ασφάλειας s1. Οι επαφές στον διακόπτη s1 ανοίγουν από την στιγμή που η πύλη ασφάλειας είναι ανοιχτή k1, με αποτέλεσμα να διακόπτεται το εσωτερικό κύκλωμα εισόδων αλλά και τις επαφές ασφάλειας k2,k3. Με τη βοήθεια αυτών των safety relay, γίνεται να μειωθεί κατά πολύ ο κίνδυνος και έτσι από SIL 3 που βρισκόμασταν, να χρειαστούμε SIL 2.

Πιο συγκεκριμένα θα γίνει η ανάλυση του safety relay pilz X2P μετά το διάγραμμα στο οποίο απεικονίζεται η συνδεσμολογία και οι διάφοροι διακόπτες, χρονικά και επαφές.



[8] Εικόνα 4: Κύκλωμα safety relay pilz.

Η λειτουργία ασφάλειας του ρελέ είναι ως εξής: Το άνοιγμα και το κλείσιμο της πύλης ασφάλειας είναι σηματοδοτημένο στο ρελέ μέσω των επαφών του διακόπτη ασφάλειας PSEN 1,1p(S1). Οι επαφές του PSEN ανοίγουν μόλις ανοίξει η πύλη ασφάλειας. Έτσι, διακόπτεται το κύκλωμα της εισόδου και οι επαφές K1 ανοίγουν. Τέλος, οι K2,3 απενεργοποιούνται.

Είναι σημαντικό να αναφερθεί πως οι πλέον fail safe relays χρησιμοποιούν διπλό κανάλι συνδεσμολογίας σε περίπτωση που το ένα από τα δύο αποτύχει σε περίπτωση διακοπής του ρεύματος είτε σε περίπτωση απενεργοποίησης του συστήματος λόγω κινδύνου.

Βάση του προτύπου, υπάρχει πάντα μια κοινή αιτία αποτυχίας του συστήματος του ρελέ και υπολογίζεται περίπου στο 2%, παρόλα αυτά το μηχάνημα πάντα θα τίθεται σε ασφαλή απενεργοποίηση χωρίς να εκθέσει σε κίνδυνο τον χρήστη.

Για να εκκινήσουμε το ρελέ πρέπει το κουμπί επαναφοράς S2 να τηρεί τις εξής προϋποθέσεις: 1) Η πύλη ασφάλειας 1,1p να είναι κλειστή και 2) Οι επαφές του S1 να είναι κλειστές καθώς και οι επαφές K2,3. Αυτό διότι οι K2,3 είναι κανονικά κλειστές επαφές, δηλαδή δίνουν έξοδο 1 όταν έχουν τιμή εισόδου 0.

Παράλληλα, θα είναι χρήσιμο να τοποθετηθούν και μπάρες προστασίας κοντά στο ρομποτικό βραχίονα έτσι ώστε να μειώσουμε τον κίνδυνο ακόμα

παραπάνω σε περίπτωση που κάποιο προσωπικό χρίζει να περάσει στο χώρο της παραγωγής. Παρακάτω θα αναπτυχθεί ένας πίνακας ο οποίος θα απεικονίζει την επικινδυνότητα του κάθε μηχανήματος βάση των SIL. Οι πίνακες φτιάχνονται πριν χρησιμοποιηθεί κάποιο μέτρο προστασίας.

ΣΟΒΑΡΟΤΗΤΑ	ΠΙΘΑΝΟΤΗΤΑ 1	-//- 2	-//- 3	-//- 4
Χρήση πρώτων βοηθειών				
Παραπομπή σε ιατρική επίβλεψη				
Κομμένο δάχτυλο/ σπάσιμο χεριού				
Θανατηφόρο ατύχημα	×			

Πίνακας επικινδυνότητας ρομποτικού βραχίονα.

ΣΟΒΑΡΟΤΗΤΑ	ΠΙΘΑΝΟΤΗΤΑ 1	-//- 2	-//- 3	-//- 4
Χρήση πρώτων βοηθειών				
Παραπομπή σε ιατρική επίβλεψη				
Κομμένο δάχτυλο/ σπάσιμο χεριού		×		
Θανατηφόρο ατύχημα				

Πίνακας επικινδυνότητάς μεταφορικού μέσου του προϊόντος στην παραγωγή.

ΣΟΒΑΡΟΤΗΤΑ	ΠΙΘΑΝΟΤΗΤΑ 1	-//- 2	-//- 3	-//- 4

Χρήση πρώτων βοηθειών				
Παραπομπή σε ιατρική επίβλεψη			×	
Κομμένο δάχτυλο/ σπάσιμο χεριού				
Θανατηφόρο ατύχημα				

Πίνακας επικινδυνότητας φούρνου παραγωγής.

Βάση των πινάκων, είναι κατανοητό πως βρισκόμαστε σε μια περίπτωση όπου υπάρχει αρκετά υψηλός κίνδυνος λόγω του ρομποτικού βραχίονα και της γραμμής παραγωγής, παρόλα αυτά ο φούρνος είναι πιο ασφαλής. Άρα, βάση των στοιχείων που έχουμε αποκομίσει από τους πίνακες, μπορούμε να θέσουμε περιπτώσεις για την μείωση του κινδύνου, κάτι που πραγματοποιήθηκε παραπάνω.

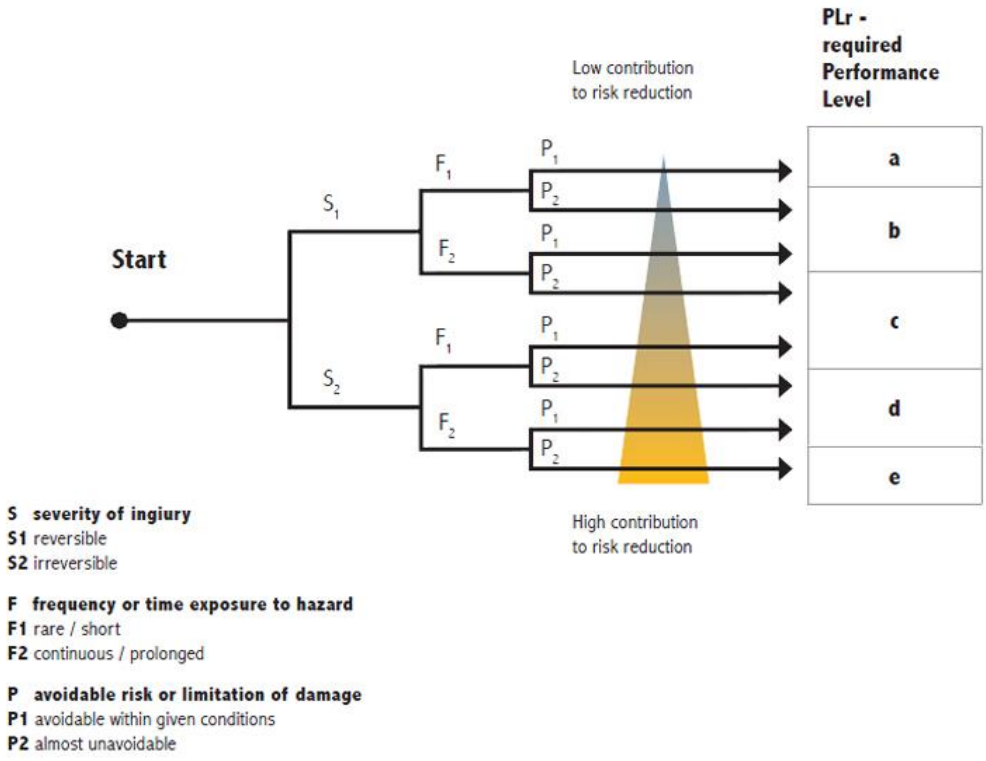
2.3 ΠΡΟΤΥΠΟ ISO 13849

Στη συνέχεια θα γίνει αναφορά για το πρότυπο ISO 13849, το οποίο είναι διαφορετικών εκδοτών πρότυπο, αλλά έχει και αυτό προκαθοριστικό ρόλο στην ασφάλεια σε μία μονάδα.

[9] Το συγκεκριμένο πρότυπο ασχολείται και αυτό με την ασφάλεια που παρέχουν διάφορα μηχανήματα ελέγχου. Αποτελείται από δύο μέρη τα οποία έχουν το καθένα μια διαφορετική λειτουργία όσον αφορά την ασφάλεια.

- 1ο Στάδιο: Βασικές αρχές για τη βοήθεια στον σχεδιασμό αλλά και διάφορες απαιτήσεις στην ασφάλεια και ταυτόχρονα καθοδήγηση όσον αφορά την ενοποίηση των συστημάτων ελέγχου στην ασφάλεια.
- 2ο Στάδιο: Γίνεται επικύρωση και καθορίζονται οι διαδικασίες που πρέπει να επικυρωθούν με δοκιμές. Επίσης, πραγματοποιούνται λειτουργίες ασφάλειας του συστήματος και τέλος το επίπεδο απόδοσης που επιτυγχάνεται με την ασφάλεια.

Βασικό στοιχείο που χρησιμοποιεί το πρότυπο αυτό είναι το Performance Level required (PLr), το οποίο χρησιμοποιείται για την μείωση του απαιτούμενου κινδύνου. Το μέσον αυτό είναι σημαντικό διότι γίνεται πάντα σύγκριση του PL που χρειαζόμαστε με το PL το οποίο τελικά εκτιμάτε. Για να πραγματοποιηθεί αυτό, χρησιμοποιείται ένα γράφημα το οποίο υπολογίζει τις εκτιμώμενες παραμέτρους του ίδιου του κινδύνου και πιο συγκεκριμένα την αυστηρότητα του κινδύνου, τη συχνότητα και τους τρόπους αποφυγής του, έτσι ώστε να φτάσουμε σε στάδιο να καλύπτουμε το απαιτούμενο βαθμό ασφάλειας του PLr.



Εικόνα 5: Εκτίμηση ρίσκου & κινδύνου με τη βοήθεια του Performance level.

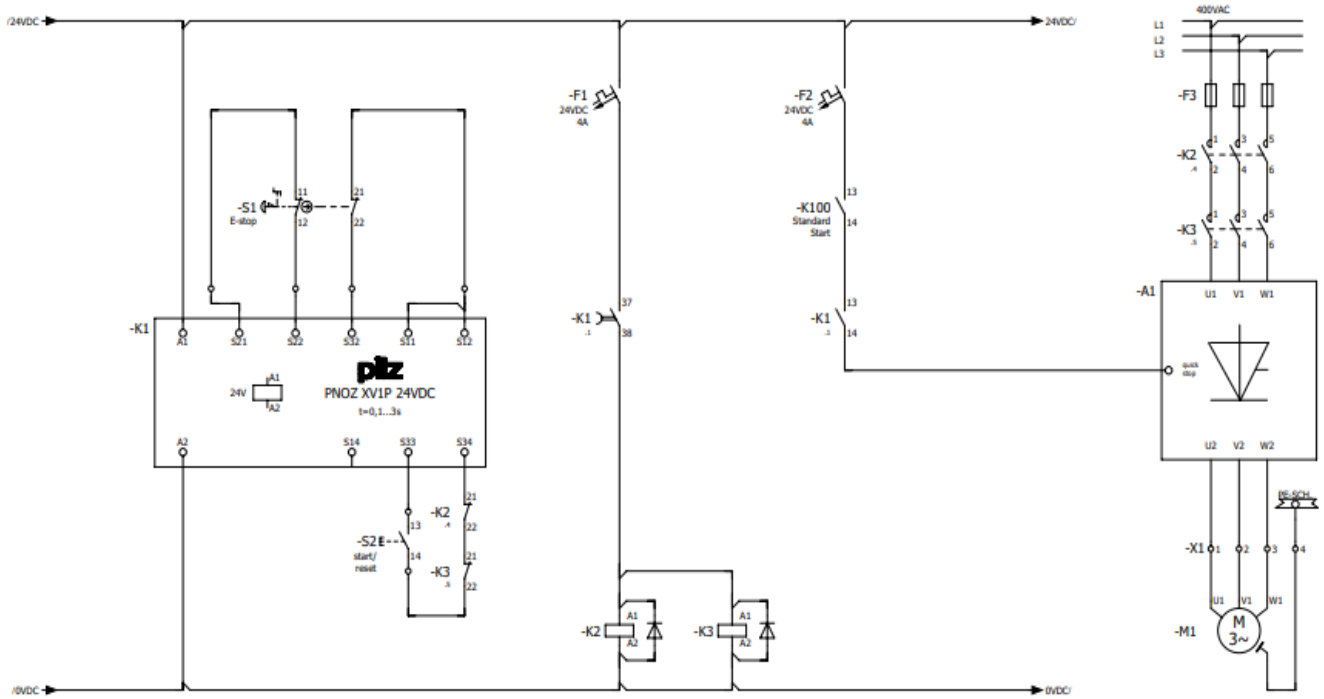
Στην παραπάνω εικόνα παρατηρούμε το σχήμα του Βαθμού Απόδοσης, που χρησιμοποιείται στο πρότυπο ISO 13849 το οποίο βασίζεται σε μία προσέγγιση πιθανοτήτων για να πραγματοποιηθεί η αξιολόγηση των συστημάτων στην ασφάλεια.

Ο βαθμός απόδοσης καθορίζεται με βάση τις κατηγορίες οι οποίες είναι οι εξής:

- Δομική απαίτηση
- Μέσος χρόνος της επικίνδυνης αποτυχίας ενός μηχανήματος
- Τη διαγνωστική κάλυψη
- Την αποτυχία κοινής αιτίας

Παράλληλα, η λογική πίσω από το σχήμα είναι πως όσο πιο ψηλά βρισκόμαστε στην πυραμίδα τόσο μικρότερο θα είναι το ρίσκο αυστηρότητας του κινδύνου, η συχνότητα έκθεσης σε κάποιον κίνδυνο αλλά και αν υπάρχει τρόπος αποφυγής του ή όχι.

Με βάση το συγκεκριμένο πρότυπο, θα γίνει αναφορά πάνω σε έναν ακόμα safety relay. Το συγκεκριμένο relay είναι της εταιρίας Pilz και πιο συγκεκριμένα το XV1P. Το συγκεκριμένο εξάρτημα χρησιμοποιείται για μια ασφαλή ακινητοποίηση ενός κινητήριου μηχανήματος.



[9] Εικόνα 6: Κύκλωμα safety relay pilz με βάση το πρότυπο ISO 13849.

Με βάση το διάγραμμα παρατηρείτε πως υπάρχει διπλό κανάλι με ανίχνευση σε όλες τις επαφές, συνεχής παρακολούθηση επαναφοράς, ηλεκτρονική λειτουργία STOP για απομακρυσμένη χρήση και κύκλωμα ανάδρασης για τις επεκτάσεις των επαφών.

Η λειτουργία του E-STOP έχει ως εξής: Από τη στιμγή που θα πατηθεί το S1 (button) τότε κλείνει η παροχή του κυκλώματος με μια καθυστέρηση του χρόνου. Αυτό σημαίνει πως όταν πατηθεί το κουμπί αυτό, το ρελέ με επαφή K1 και πιο συγκεκριμένα οι επαφές 13-14 ανοίγουν και ταυτόχρονα η λειτουργία του απότομου σταματήματος λαμβάνεται στη cpu που βρίσκεται στο A1. Κατά την ενεργοποίηση της καθυστέρησης χρόνου με την επαφή delay-on (επαφή 37-38) (ξεκινάει η καθυστέρηση του χρόνου με το πάτημα του κουμπιού) απενεργοποιούνται οι επαφές K2,K3 μετά το πέρασμα του καθορισμένου χρόνου.

Για την εκκίνηση του συστήματος πρέπει να πατηθεί το κουμπί S2, αν πρώτα το S1 δεν λειτουργεί και οι επαφές K2, K3 είναι κλειστές.

Βάση του προτύπου ISO 13849 και με τη βοήθεια του εργαλείου βαθμού απόδοσης το συγκεκριμένο ρελέ ασφαλείας μπορεί να βαθμολογηθεί με d, δηλαδή υπάρχει υψηλή συμβολή στη μείωση του κινδύνου.

2.4 ΠΡΟΤΥΠΟ IEC 62443

[10] Το πρότυπο 62443 ασχολείται στα δίκτυα επικοινωνίας των βιομηχανιών και πιο συγκεκριμένα στην ασφάλεια της πληροφορικής στα συστήματα, δηλαδή περιλαμβάνει την έννοια των επιπέδων διασφάλισης της ασφάλειας. Το συγκεκριμένο πρότυπο παρέχει μια σειρά από διάφορες απαιτήσεις, οι οποίες καθορίζουν σε τι στάδιο ασφάλειας βρίσκεται το σύστημά μας. Υπάρχουν τέσσερα διαφορετικά επίπεδα που ασχολούνται με την κυβερνασφάλεια των συστημάτων. Παρακάτω θα αναλυθούν τα επίπεδα ασφάλειας όσον αφορά τον κίνδυνο στον κυβερνοχώρο μιας βιομηχανίας.

ΣΤΑΔΙΟ ΑΣΦΑΛΕΙΑΣ	***ΣΤΟΧΟΣ***	***ΙΚΑΝΟΤΗΤΕΣ***	***ΠΗΓΗ***
SL1	*Συνήθης παράβαση*	*Ελάχιστες*	*Ατομική συνεισφορά*
SL2	*Παράβαση από hacker*	*Γενικές*	*Ελαχίστων*

SL3	*χακτιβισμός*	*Προδιαγραφές ελέγχου διεπαφής*	*Πλήθος διαφόρων hacker*
SL4	*Εθνικό κράτος*	*-//-*	*Επεκταμένης ομάδας διαφόρων ειδών*

Είναι σημαντικό να υπάρχει πάντα ασφάλεια και στο μέρος του κυβερνοχώρου λόγω ύπαρξης διαφόρων πληροφοριών που είναι πολύ σημαντικά για να λειτουργεί σωστά μια παραγωγική μονάδα. Στον παραπάνω πίνακα έχουμε μια σειρά από διάφορα εγκλήματα που μπορεί να πραγματοποιηθούν και ταυτόχρονα η καθοδήγηση των εργαζομένων όσον αφορά την επικινδυνότητα. Πολλές φορές δεν εγγυάται πως μπορεί ένα σύστημα να αμυνθεί ενάντιας σε επιδέξιους χάκερ ή κυβερνοεγκληματίες και γι΄αυτό τον λόγο πρέπει να ακολουθούνται κάποια συγκεκριμένα στάδια για την διασφάλιση του συστήματος να παραμένει άθικτη.

[11] Υπάρχουν έξι βασικά βήματα για την αποφυγή κάποιας επίθεσης στον κυβερνοχώρο.

1. Η δημιουργία ενός πλάνου ασφάλειας στο οποίο το εξειδικευμένο προσωπικό θα ελέγχει λεπτομερώς όλο τον εξοπλισμό και τις φυσικές συνδεσμολογίες(καλώδια σε routers), σε όλο το συνδεδεμένο σε δίκτυο σύστημα καθώς και τις πιθανές ευπάθειες του. Η δημιουργία ενός ολοκληρωμένου πλάνου είναι το Α και το Ω πριν πραγματοποιηθεί οποιαδήποτε πράξη.

2. Οριοποίηση ξεχωριστών δικτύων για την διευκόλυνση των χρηστών να εισέρχονται σε αυτό, χωρίς να υπάρχει κομφούζιο σε όλο το δίκτυο. Είναι σημαντική διαχώριση του δικτύου σε ζώνες επιχείρησης και ταυτόχρονα ο προσδιορισμός της κάθε μίας, για την ασφαλέστερη επεξεργασία σε περίπτωση κάποιας αλλαγής αλλά και μεγαλύτερη ασφάλεια σε περίπτωση κάποιας επίθεσης από χάκερ, λόγω ότι θα βρίσκεται σε συγκεκριμένο domain και όχι σε όλο το δίκτυο, κάτι που θα ήταν καταστροφικό για μια βιομηχανία.

3. Ύπαρξη περιμετρικής προστασίας μεταξύ των ζωνών για να γνωρίζουμε ανά πάσα στιγμή πού μπορεί να παρουσιαστεί κάποιο πρόβλημα και ταυτόχρονα να εξασφαλίσουμε την απομακρυσμένη πρόσβαση.

4. Στο τέταρτο βήμα μπορούμε να χωρίσουμε τα τμήματα του σταδίου 2^{ου} σε μικρότερα για μεγαλύτερη ασφάλεια. Αρχικά μπορούμε σε κάθε

ζώνη να την κατατάξουμε με βάση την ασφάλεια στον εξοπλισμό ως 1^{o}, μετά την ασφάλεια που αποδίδεται στο σύστημα ως 2^{o}. Έτσι όταν υπάρξει κάποια απρόσμενη επίθεση, να είναι ακόμα πιο εύκολη η εντόπισή του προβλήματος.

5. Χρήση σκλήρυνσης συσκευών (ICS). Στο στάδιο αυτό πραγματοποιείται μια διαδικασία με την οποία ασφαλίζουμε ένα σύστημα μειώνοντας την επιφάνεια της επίθεσης, έτσι ώστε να μειώσουμε τον κίνδυνο σε σημεία τα οποία είναι ευάλωτα. Έτσι μειώνεται η πιθανότητα αυτά τα στοιχεία να αποκτηθούν από κάποιον έμπειρο χάκερ.

6. Τέλος, η συνεχής παρακολούθηση όλων των συστημάτων θα βοηθήσει την αποτροπή οποιουδήποτε κινδύνου. Με την συνεχή εισαγωγή νέων ενημερώσεων και υλικολογισμικού, χτίζεται το τείχος ασφάλειας του συστήματος μιας βιομηχανίας.

Ως παράδειγμα θα θέσουμε πάνω στην παραγωγική μονάδα που προαναφέρθηκε κι αυτό για να γίνει κατανοητό πως κάθε παραγωγική μονάδα μικρή είτε μεγάλη πρέπει να καλύπτει το πρότυπο ασφάλειας του κυβερνοχώρου.

Αρχικά, για την σωστή λειτουργία των PLC που είναι το βασικότερο σύστημα για να πραγματοποιούνται ορθά όλες οι εντολές που θα λαμβάνει ο ρομποτικός βραχίονας, διότι χωρίς τον σωστό έλεγχο θα υπάρξουν σίγουρα λάθη και ως αποτέλεσμα πιθανοί κίνδυνοι προς το εργατικό προσωπικό. Οπότε για τη σωστή λειτουργία ενός PLC πρέπει να εξασφαλιστεί πως το δίκτυο για τη μεταφορά των δεδομένων που αλληλοεπιδρά με τις μηχανές είναι ασφαλές, δηλαδή να ελεγχτούν πρώτα όλες οι φυσικές συνδέσεις. Ύστερα, το δίκτυο να χωριστεί σε ζώνες που αφορούν την παραγωγή ξεχωριστά, δηλαδή η γραμμή παραγωγής, οι φούρνοι, οι ανελκυστήρες και ο ρομποτικός βραχίονας να ελέγχονται ξεχωριστά σε διάφορες ζώνες του δικτύου για μην υπάρξει εμπλοκή σε περίπτωση κάποιο από τα υπόλοιπα συστήματα παρουσιάσουν βλάβη.

Πιο πρακτικά, στην δική μας περίπτωση η ασφάλεια πρέπει να παρέχεται στα συστήματα Scada (Supervision control and data acquisition). Το σύστημα αυτό είναι αναγκαίο σε μια παραγωγή με αυτοματισμούς διότι, μπορεί ο διακομιστής που το χρησιμοποιεί, να ελέγχει ανά πάσα στιγμή όλες τις μονάδες των μηχανημάτων από απόσταση, μέσω μιας συσκευής που θα διαθέτει το λογισμικό αυτό. Εξίσου σημαντικό είναι πως μπορούν να πραγματοποιηθούν ρυθμίσεις σε περίπτωση που υπάρξει ανάγκη.

Τέλος, η συνεχής παρακολούθηση του δικτύου μαζί με τη βοήθεια των συστημάτων ICS, θα μειώσουν την πιθανότητα κάποιας επίθεσης πάνω στο σύστημα, με αποτέλεσμα να μην χαθούν σημαντικά αρχεία που στηρίζουν τη λογική λειτουργία των PLC και ταυτόχρονα με τη χρήση των Scada να πραγματοποιούνται παρατεταμένοι έλεγχοι, για να έχουμε κάλυψη των καθοριστικών ζητουμένων του προτύπου IEC 62443.

2.5 ΠΡΟΤΥΠΟ ISO 12100

[12] Το πρότυπο 12100 είναι ένα διεθνές πρότυπο το οποίο ασχολείται πάνω στην ασφάλεια των μηχανημάτων. Η λογική πίσω από το πρότυπο είναι η ικανότητα ενός μηχανήματος να εκτελεί την προκαθορισμένη του λειτουργία και παράλληλα καθ΄ όλη τη διάρκεια του κύκλου ζωής του, να μειώνεται ο κίνδυνος. Επίσης, το ISO 12100 λαμβάνει διάφορες αποφάσεις για τη μέγιστη ασφάλεια των μηχανημάτων και τα διάφορα έγγραφα που είναι αναγκαία για την επιτυχής αξιολόγηση του κινδύνου. Οι ενδείξεις αυτές παρέχουν σημαντικές πληροφορίες που κάθε βιομηχανία πρέπει να γνωρίζει και είναι οι εξής: Η εμπειρία του προσωπικού βάση σχεδιασμού, τα διάφορα ατυχήματα που μπορεί να προκύψουν, οι τραυματισμοί αυτών και ο κίνδυνος που προμηνύει το κάθε μηχάνημα. Το συγκεκριμένο πρότυπο κατά την εφαρμογή του, δεν αρκεί για την συμμόρφωση με τις απαιτήσεις της υγείας και την ασφάλειας, παρόλα αυτά ακολουθεί ένα πλαίσιο για την μερικώς ορθή εφαρμογής.

[13] Επιπλέον, το ISO 12100 παρουσιάζει όλους τους τύπους κινδύνου και τις διαφορές τους σε σύγκριση με την απλή έννοια του κινδύνου.

- Αποδεκτός κίνδυνος: Αποδεκτό επίπεδο κάποιου κινδύνου ύστερα από την σωστή αξιολόγηση του.
- Υπολειπόμενος κίνδυνος: Παρόλη την προσπάθεια εξάλειψης του κινδύνου με προστατευτικά μέτρα, παραμένει ακόμα.
- Ρίσκο: Ο συνδυασμός της πιθανότητας να συμβεί κάποια βλάβη και ταυτόχρονα η σοβαρότητά της.
- Επικίνδυνη περίπτωση: Η κατάσταση στη οποία κάποιος εργαζόμενος εκτίθεται σε έναν ή παραπάνω κινδύνους.
- Απειλή: Είναι η πιθανή πηγή της κάθε βλάβης.
- Βλάβη: Είναι ο τραυματισμός ή κάποια ζημιά στην υγεία.

Μετά την επεξήγηση των διαφόρων τύπων κινδύνων που μπορεί να παρουσιάσουν τα μηχανήματα, υπάρχουν δύο σημαντικά βήματα τα οποία το συγκεκριμένο όπως και πολλά πρότυπα ακολουθούν.

2.5.1 RISK ASSESSMENT

Η εκτίμηση του κινδύνου είναι ένα μέσο το οποίο πρότυπο ακολουθεί για την ανάλυση και αξιολόγηση του κινδύνου σε ένα μηχάνημα. Βάση λογικής, όταν υπάρχει μεγάλη ζήτηση και συνεχόμενη επανάληψη αυτής της διαδικασίας είναι αντιληπτό πως υπάρχει ανάγκη μείωσης του κινδύνου με εφαρμογή προστατευτικών μέτρων. Το μέτρο αυτό βοηθά στη μείωση του κινδύνου και γίνεται εφαρμοστό από τους σχεδιαστές που ασχολούνται με το κάθε μηχάνημα. Επίσης το risk assessment απαιτεί επιπλέον πληροφορίες όπως είναι η αναλυτική περιγραφή του κάθε μηχανήματος, τα πρότυπα που χρησιμοποιούνται και η εμπειρία που απαιτείται για τη χρήση του. Τέλος, με βάση το ISO 12100, ο τύπος του κινδύνου που προαναφέρθηκε μπορεί να υπολογιστεί με τον εξής τρόπο:

ΤΥΠΟΣ ΚΙΝΔΥΝΟΥ = ΠΙΘΑΝΟΤΗΤΑ * ΒΛΑΒΗ

Άρα, είναι πλέον κατανοητό πως αυτά τα στοιχεία είναι αλληλένδετα για τον τύπο του κινδύνου που παρουσιάζει το κάθε μηχάνημα.

2.5.2 RISK ANALYSIS-EVALUATION-REDUCTION

Μόλις πραγματοποιηθεί η εκτίμηση, συνεχίζουν κατά σειρά τρείς ακόμα διαδικασίες οι οποίες είναι σημαντικές για την περεταίρω εξασφάλιση μείωσης του κινδύνου.

Η ανάλυση του ρίσκου πραγματοποιεί μια διαδικασία για την παρακολούθηση των ορίων μίας μηχανής, δηλαδή μετά από ποιες περιστάσεις θα αποτελεί επικίνδυνο στον χρήστη και κατά σειρά την συχνότητα εμφάνισής του.

Η αξιολόγηση το ρίσκου είναι η διαδικασία κατά την οποία αποφασίζεται πόσο σημαντική είναι η μείωση του κινδύνου βάση της ανάλυσης που προηγείται. Η μείωση είναι η τελευταία διαδικασία κατά την οποία εξαλείφεται ο κίνδυνος ή μειώνεται η σοβαρότητά του.

2.6 ΠΡΟΤΥΠΟ ISO/IEC 15408

[14] Το πρότυπο ISO/IEC 15408 ασχολείται με την ασφάλεια που πρέπει να επικρατεί στην τεχνολογία της πληροφορικής και πιο συγκεκριμένα για την πιστοποίηση ασφάλειας υπολογιστών. Η ονομασία του προτύπου αυτού είναι τα κοινά κριτήρια (Common Criteria), τα οποία είναι ένα πλαίσιο στο οποίο οι διάφοροι χρήστες να ορίσουν τις απαιτήσεις που πρέπει να τεθούν σε λειτουργία για την επίτευξη της ασφάλειας και τη διασφάλιση σε ένα στόχο ασφάλειας μέσω των προφίλ προστασίας. Παράλληλα, ένας πωλητής μπορεί να θέσει τα δικά του χαρακτηριστικά ασφάλειας στα προϊόντα που πουλάει και ύστερα να πραγματοποιηθεί αξιολόγηση εάν τα προϊόντα αυτά ανταποκρίνονται στα πρότυπα ασφάλειας. Τα κοινά πρότυπα παρέχει μια σειρά πιστοποιημένων προϊόντων συμπεριλαμβανομένων των λειτουργικών συστημάτων, των συστημάτων ελέγχου πρόσβασης, βάσης δεδομένων και διαχείρισης κλειδιών.

2.6.1 ΕΙΔΗ ΠΕΡΙΠΤΩΣΕΩΝ – ΚΛΕΙΔΙΑ

[14][15] Το μεγαλύτερο πλήθος των περιπτώσεων που αξιολογούνται, χρησιμοποιούν αιτιολόγηση βάση διαφόρων στοιχείων και ισχυρισμών των οποίων πρέπει να πληρούν σε κάθε συγκεκριμένο τομέα της ασφάλειας. Το κομμάτι των περιπτώσεων έχει ως βάση την λογική την οποία μοιράζονται μεταξύ τους αλλά παράλληλα τη δομή η οποία διαφέρει σε κάθε περίπτωση. Παρακάτω θα γίνει αναφορά στα περιεχόμενα του Common Criteria και από ποια μέρη αποτελείται, καθώς και τα διάφορα ‘’κλειδιά΄΄ που χρησιμοποιούνται για την εξασφάλιση της ασφάλειας.

- Προφίλ Προστασίας: Είναι η εφαρμογή ανεξάρτητης δήλωσης των απαιτήσεων ασφάλειας του στόχου αξιολόγησης που ανταποκρίνεται σε συγκεκριμένες ανάγκες χρηστών οι οποίες ανταποκρίνονται σε ιδιαίτερο περιβάλλον ασφάλειας.
  Ένα τέτοιο είδος προφίλ αναφέρεται στο σύνολο των απαιτήσεων των οποίων προκαθοριστικός ρόλος είναι η αντιμετώπιση συγκεκριμένων απειλών στο εργασιακό περιβάλλον .
- Στόχος Ασφάλειας: Αποτελεί ως βασικό στοιχείο για την αξιολόγηση. Επίσης χρησιμοποιεί τη λογική πίσω από τον στόχο της εκτίμησης (Target of Evaluation) και ταυτόχρονα τις απειλές για την ασφάλεια, καθώς και τα μέτρα διασφάλισης.
  Ο στόχος ασφάλειας είναι μια δήλωση αξιώσεων ασφάλειας για ένα σύστημα πληροφορικής. Η δομή του είναι παράλληλη με του προφίλ

προστασίας, αν και ο στόχος ασφάλειας περιέχει ένα σύνολο απαιτήσεων ασφάλειας για το σύστημα το οποίο μπορεί να πραγματοποιήσει απ' ευθείας αναφορά πάνω στη λογική του CC.

- Σύνολο: Αποτελεί ένα σχετικό συνδυασμό των απαιτήσεων ασφάλειας και ονομάζεται πακέτο. Ανταποκρίνεται σε κάποια ιδιαίτερη ανάγκη που εκφράζεται ως το σύνολο των στόχων πάνω στην ασφάλεια. Το πακέτο έχει τη δυνατότητα επαναχρησιμοποίησης για να ορίζει απαιτήσεις οι οποίες θα είναι πιο αποτελεσματικές στην ικανοποίηση των στόχων.
- Στόχος εκτίμησης: Ο στόχος εκτίμησης είναι ένα σύστημα πληροφορικής προς αξιολόγηση τα στοιχεία του οποίου περιγράφονται με συγκεκριμένους όρους από ένα αντίστοιχο στόχο ασφάλειας. Η αξιολόγηση αυτή αποτελείται από αυστηρή ανάλυση και δοκιμές που διεκπεραιώνονται από κάποιο εμπιστευμένο εργαστήριο. Εν ολίγοις, ο στόχος εκτίμησης είναι ένα προϊόν πληροφορικής για την καθοδήγηση του χρήστη που αποτελεί αντικείμενο μιας αξιολόγησης.

2.7 ΠΡΟΤΥΠΟ IEC 61131

Το πρότυπο 61131 ασχολείται πάνω στους προγραμματιζόμενους ελεγκτές ή αλλιώς PLC. Αποτελείται από πέντε μέρη τα οποία συνοψίζουν τις απαιτήσεις που πρέπει να καλύπτουν τα σύγχρονα PLC. Το συγκεκριμένο πρότυπο είναι μια κατευθυντήρια γραμμή για τον σωστό προγραμματισμό ενός PLC και ανάλογα τις περιπτώσεις ζήτησης, μπορεί κάποιος χρήστης να επιλέξει σε πιο από τα μέρη του προτύπου μπορεί να συμμορφωθεί, χωρίς να χρειαστεί να το εφαρμόσει όλο. Παρόλα αυτά είναι πολύ σημαντικό να γνωρίζουν οι χρήστες και οι κατασκευαστές σε ποια μέρη καλύπτουν τα στάνταρ και ποια όχι. Αυτό πρέπει να γίνει λόγω ότι ο κατασκευαστής χρησιμοποιεί ένα σύνολο πινάκων στους οποίους σημειώνει αν εφαρμόζεται σε κάθε μέρος το πρότυπο. Από τη στιγμή που τα PLC έχουν επεκταθεί πια σε κάθε βιομηχανία και εξελίσσονται συνεχώς, πρέπει να υπάρχουν και κάποια αντίβαρα που πρέπει να ισοσταθμιστούν για να συμμορφώνονται τα πρότυπα:

- Συνεχής εκπαίδευση του προσωπικού που εργάζεται πάνω στον προγραμματισμό και την συντήρηση των PLC.
- Την επέκταση των προγραμμάτων, όσον αφορά την περιπλοκότητα και τις απαιτήσεις.
- Ανάπτυξη του κλάδου προγραμματισμού, έτσι ώστε να υπάρχει επαρκές προσωπικό το οποίο να μπορεί να διαχειριστεί μια βλάβη σε περίπτωση ανάγκης.

Πρώτο μέρος: Στο πρώτο μέρος έχουμε όλες τις βασικές πληροφορίες, ορισμούς και χαρακτηριστικά των PLC. Επίσης υπάρχουν τα εγχειρίδια χρήσης αυτών, στα οποία απεικονίζονται οι είσοδοι-έξοδοι των PLC, τα χρονικά και όλα τα συστήματα που παρέχουν για τον χρήστη.

Δεύτερο μέρος: Στο δεύτερο μέρος αναλύονται όλες οι απαιτήσεις που έχουν τα μηχανήματα και οι διάφοροι έλεγχοι που πρέπει να προκριθούν όπως είναι η άσκηση διαφόρων καταπονήσεων στους ελεγκτές των PLC για να είναι σίγουροι οι χρήστες πως θα λειτουργήσουν σωστά κάτω από αντίξοες συνθήκες.

Τρίτο μέρος: Το τρίτο μέρος ασχολείται ξεκάθαρα στο κομμάτι των γλωσσών προγραμματισμού. Πιο συγκεκριμένα, ποιες γλώσσες χρησιμοποιούνται (*πχ* ladder, stl), ποιοι οι ορισμοί των λεξιλογίων που χρησιμοποιούνται, πως γίνεται η σύνταξή τους και τέλος οι σημασιολογικές τους περιγραφές.

Τέταρτο μέρος: Στο τέταρτο μέρος έχουμε τις οδηγίες χρήσης των μηχανημάτων. Κατευθύνει τον χρήστη του PLC πως να πραγματοποιήσει ορθά το έργο στον αυτοματισμό, προσανατολίζοντάς τον πάντα με πληροφορίες διαφόρων παραδειγμάτων από παρόμοια θέματα και ταυτόχρονα την επιλογή του κατάλληλου εξοπλισμού.

Πέμπτο μέρος: Στο πέμπτο μέρος έχουμε την υπηρεσία συναλλαγής μηνυμάτων. Αυτή η επικοινωνία αφορά συγκεκριμένα τα PLC παρόλο που μπορεί να κατασκευάζονται από διαφορετικές εταιρίες και να χρησιμοποιούν άλλου τύπου συσκευές. Αυτό πραγματοποιείται με τη βοήθεια ενός επιπλέον προτύπου ονομαζόμενου ISO 9505, το οποίο επιτρέπει στα PLC να επικοινωνούν μέσω δικτύου. Έτσι, θα καλύπτονται οι επιλογές συσκευών ανάμεσα σε μια βιομηχανική παραγωγή, η ανταλλαγή σημαντικών δεδομένων και η διαχείριση όσων έχουν πρόσβαση στο σύστημα του δικτύου, κάτι που θα εξασφαλίσει μέγιστη ασφάλεια.

Άρα, για να εξασφαλίσουμε πως θα υπάρχει ασφάλεια στο κομμάτι παραγωγής και πιο συγκεκριμένα στην αλληλεπίδραση ανθρώπου – PLC, πρέπει να τηρούνται αυτά τα πέντε μέρη έτσι ώστε να υπάρχει συμμόρφωση με το πρότυπο ή αν δεν τηρούνται όλα, να σημειώνεται.

2.8 ΠΡΟΤΥΠΟ ΕΝ 1037

[16]Το πρότυπο ΕΝ 1037 ασχολείται με την ασφάλεια πάνω στις απροσδόκητες εκκινήσεις των μηχανημάτων από διάφορες αιτίες. Το συγκεκριμένο πρότυπο βρίσκει διάφορα μέτρα σχεδιασμού για την εξασφάλισης της ασφάλειας.

Το ΕΝ 1037 προτείνει διάφορους τρόπους για να μειωθεί ο κίνδυνος, ένας από αυτούς είναι η παροχή απομόνωσης και επαγωγής της ενέργειας, επίσης οι συνεχόμενες εργασίες συντήρησης στα διάφορα κυκλώματα ισχύος. Για να υπάρχει ασφάλεια στα μηχανήματα που χρησιμοποιούνται πρέπει ν όλες οι συσκευές να έχουν κάποια στοιχειώδη χαρακτηριστικά ώστε να μην θέτουμε σε κίνδυνο τους χρήστες.

Αρχικά, είναι σημαντικό να πραγματοποιείται σωστή μόνωση σε διάφορα καλώδια και περιφερειακά στοιχεία που συνδέονται σε ένα μπουτόν ασφαλείας. Παράλληλα να μεταφέρονται οι λειτουργίες του απομονωτή μπουτόν μέσω διαφόρων συνδέσμων έτσι ώστε να μπορεί να χρησιμοποιηθεί σε πολλά διαφορετικά σημεία ενός χώρου εργασίας. Επίσης είναι σημαντική η ένδειξη και η θέση του διακόπτη, έτσι ώστε να γνωρίζει όλο το προσωπικό και τέλος η ασφάλιση του διακόπτη αυτού με κάποιο καπάκι είτε λουκέτο, για να μην υπάρχει απρόσμενη απενεργοποίηση και σύγχυση χωρίς λόγο, παρά μόνο όταν υπάρξει πραγματική ανάγκη.

Όσον αφορά τις συσκευές για την διαχείριση της ενέργειας, το συγκεκριμένο πρότυπο ασχολείται παράλληλα με τη διάχυση της αποθηκευμένης ενέργειας καθώς και τη συγκράτηση της σε διάφορες συσκευές. Κάποιες από αυτές είναι τα κυκλώματα εκφόρτισης πυκνωτών ή οι βαλβίδες σε δεξαμενές υψηλής πίεσης. Επίσης το πρότυπο παρέχει κάποια βήματα έτσι ώστε όταν χρησιμοποιείται κάποιο PLC να γίνεται πάντα ελεγχόμενη η χρήση του.

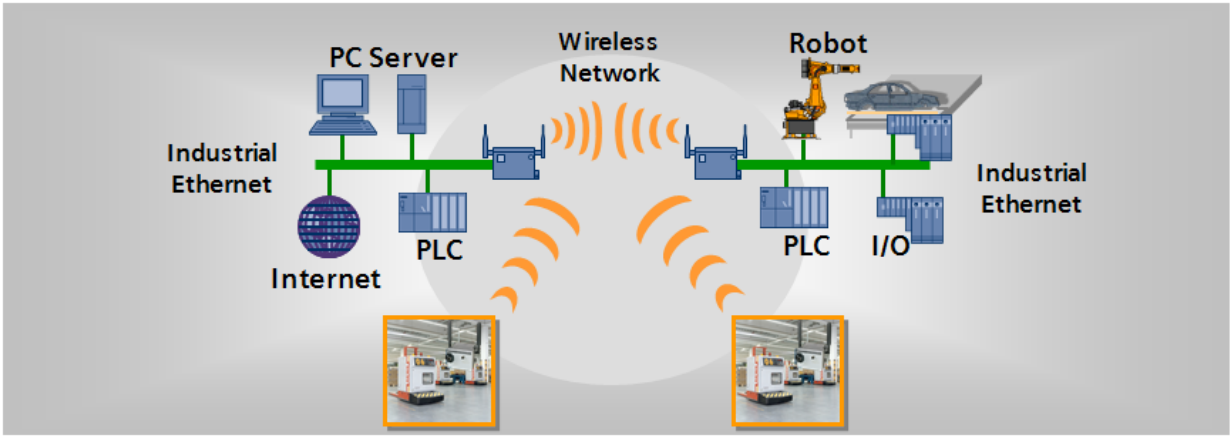
Πάντα κατά τη διάρκεια που πραγματοποιείται διασπορά ή διατήρηση της ενέργειας πρέπει:

- Να συμβαίνει ταυτόχρονα η ενεργειακή απομόνωση.
- Να μην παροτρύνει η ενέργεια αυτή σε πιο επικίνδυνες καταστάσεις.
- Να περιγράφονται με ακρίβεια οι οδηγίες λειτουργίας.
- Να πραγματοποιείται έλεγχος για την αποτελεσματικότητα της διαδικασίας με όργανα όπως μανόμετρα κλπ.
- Αυτόματη απενεργοποίηση του συστήματος πριν παρουσιαστεί σοβαρός κίνδυνος.

2.9 ΔΙΑΔΙΚΤΥΑΚΟ ΠΡΟΤΥΠΟ PROFINET

Σε μια παραγωγική μονάδα θα υπάρξουν πολλά παρελκόμενα συστήματα με τα οποία θα πραγματοποιείται ένας κύκλος επικοινωνίας – παραγωγής μεταξύ μηχανών. Αυτό σημαίνει πως υπάρχουν πρότυπα με τα οποία μπορεί ένας ελεγκτής να επικοινωνεί με όλα τα αισθητήρια, μοτέρ, servo drive κλπ έτσι ώστε να εξασφαλιστεί πως όλα λειτουργούν κάτω από ορισμένες συνθήκες ή αν υπάρξει κάποια επιπλοκή να εντοπιστεί το γρηγορότερο δυνατό όσον αφορά την επικοινωνία όλων των περιφερειακών συσκευών.

[17] Όπως υπάρχουν οι φυσικές συνδεσμολογίες καλωδίων, εισόδων και εξόδων σε περιφερειακές συσκευές όπως PLC, I/O blocks, αισθητήρες κλπ., έτσι υπάρχει ένα πρότυπο που υποστηρίζει τις συνδεσμολογίες του Ethernet σε μια παραγωγική μονάδα και ονομάζεται Profinet. Το Profinet είναι από τα πιο γνωστά πρότυπα ανταλλαγής δεδομένων κάτω από συνθήκες πραγματικού χρόνου και δυνατότητας πραγματοποίησης διαφόρων πράξεων σε περίπτωση βλάβης όσον αφορά τη μεταφορά δεδομένων, πχ εκκίνηση ενός μηχανήματος και επικοινωνίας αυτού με ένα PLC. Το Profinet προέρχεται από την παλαιότερη έκδοση μετάδοσης και σειριακής επικοινωνίας το Profibus. Το Profibus μπορεί να πραγματοποιήσει επικοινωνία μεταξύ ελεγκτών και συσκευών μέσω ενός καλωδίου RS-485 το οποίο χρησιμοποιείται μέχρι και σήμερα και πολλές μονάδες παραγωγής λόγω φθηνότερου υλικού όσον αφορά τις εγκαταστάσεις των καλωδίων αλλά και την συντήρηση. Παρόλα αυτά, το Profinet επιλέγεται από τις περισσότερες εταιρίες λόγω διαφοράς καλωδίου, πιο συγκεκριμένα το UDP το οποίο είναι πιο ανθεκτικό στις παραγωγικές μονάδες αλλά και λόγω μεγαλύτερης ευελιξίας στις τοπολογίες συνδέσεις πχ αστέρας, δέντρο, γραμμή και δακτύλιο. Η μόνη προϋπόθεση είναι η σταθερή σύνδεση δικτύου 100MB/PS το λιγότερο. Είναι κατανοητό πως με τη βοήθεια αυτού του προτύπου είναι δυνατή και λειτουργία όλων των αυτοματισμών λόγω συνεχούς επικοινωνίας όλων των μηχανημάτων με τα PLC. Επίσης, η χρήση του είναι πολύ οικονομική διότι έχει τη δυνατότητα να ενσωματωθεί σε κάποιο υπάρχον δίκτυο χωρίς κάποια στοιχειώδη τροποποίηση.



[17] Εικόνα 7: Profinet συνδεσμολογία μέσα σε παραγωγική μονάδα με χρήση Ethernet.

Όσον αφορά την ασφάλεια το Profinet έχει τρεις βασικούς στόχους για να μπορεί επιτυχώς να εξασφαλίσει την ασφαλή λειτουργία:

- Αν ένα μηχάνημα εμφανίσει βλάβη, το πρότυπο αυτό να θέσει γρήγορα την ασφαλή λειτουργία.
- Σε περίπτωση που υπάρξει πάλι κάποιο σφάλμα, να μπορεί η οποιαδήποτε μηχανή να πραγματοποιήσει την ελάχιστη απαιτούμενη εντολή που θα της δοθεί.
- Η επιτυχής προστασία όλων των δεδομένων – πληροφοριών με τα οποία είναι δυνατή η επικοινωνία.

Το πρωτόκολλο αυτό έχει κάποια συγκεκριμένη θέση στο μοντέλο OSI. Πιο συγκεκριμένα στο 7ο επίπεδο που ασχολείται με τις εφαρμογές και πιο ειδικότερα στην αποστολή μηνυμάτων και παρουσίαση πομπού με δέκτη. Το Ethernet από την άλλη βρίσκεται στο 1ο και το 2ο επίπεδο, όπου 1ο είναι οι φυσικές συνδέσεις καλωδίων, σύνδεση τάσης κλπ. και το 2ο η λογική σύνδεση ελέγχου, η χρήση της MAC address και ο έλεγχος λαθών. Το Profinet μεταδίδει πληροφορία μέσω καναλιών TCP/IP, Real Time, Isochronous Real Time και Time Sensitive Networking.

Το Profinet λειτουργεί κατά βάση με τον πραγματικό χρόνο, αλλά κάποιες φορές υπάρχουν καταστάσεις πιο κρίσιμες σε μια μονάδα και κάποιες πιο ανεκτές στην καθυστέρηση αλλά πιο κρίσιμες στη μείωση του θορύβου που μπορεί να διαστρεβλώσει τη πληροφορία. **TCP/IP** είναι για εφαρμογές που δεν υπάρχει ανάγκη να υπάρχει μηδαμινός χρόνος μετάδοσης όπως διάγνωση προβλήματος μιας μηχανής. **RT** χρησιμοποιείται για εφαρμογές

εξαιρετικά κρίσιμες με τον χρόνο κύκλου 512ms έως 250μs και παράλληλα η πληροφορία μεταφέρεται από το 2ο επίπεδο OSI απευθείας στο 7ο, παραλείποντας το TCP/IP για να κερδίσει χρόνο, γενικά το RT είναι το πιο χρησιμοποιημένο μέσο μετάδοσης πληροφορίας και καλύπτει κατά 90% όλες τις παραγωγικές μονάδες. **IRT** αναφέρεται σε εφαρμογές που έχουν την ανάγκη μιας ιδιαίτερης τιμής που μπορεί να καθορίσει όλη τη λειτουργία, κάτι το οποίο μπορεί να επηρεαστεί από τον θόρυβο, εκεί χρησιμοποιείται το IRT για να πραγματοποιήσει διαφορετικούς κανόνες ανάμεσα στο OSI έτσι ώστε να υπάρχει εξασφαλισμένη μεταφορά της ιδιαίτερης αυτής πληροφορίας. Οι χρόνοι κύκλου μηχανής μπορούν να φτάσουν στα 31.25μs.

Βάση αυτών των χαρακτηριστικών, υπάρχουν δύο είδη Profinet και χρησιμοποιούνται σε επικοινωνίες μεταξύ plc και συσκευών εισόδων/εξόδων βάση RT και IRT.

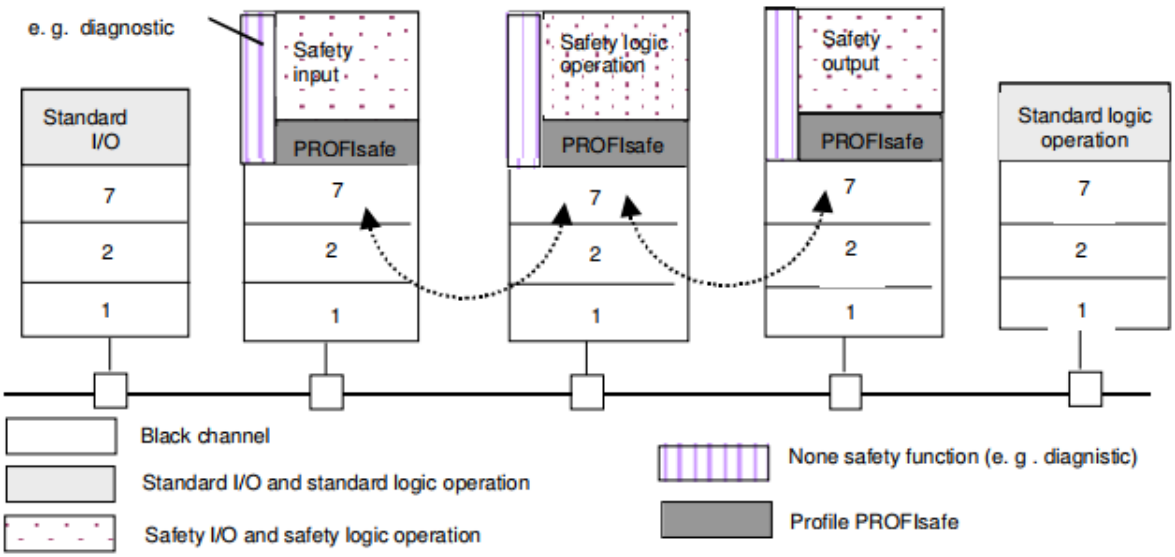
- CBA: Η συγκεκριμένη κατηγορία ονομάζεται και αλλιώς κλάσης Α και χρησιμοποιείται για επικοινωνίες μεταξύ δύο ή περισσοτέρων μηχανών με TCP/IP. Η λογική είναι να μπορεί ένα σύστημα να μαθαίνει με την πάροδο του χρόνου να επεξεργάζεται αυτόνομες διεργασίες και να τις υλοποιεί σαν έναν αυτοματισμό χρησιμοποιώντας επικοινωνία μέσω διαφόρων ελεγκτών.
- I/O: Η συγκεκριμένη κατηγορία χρησιμοποιεί συσκευές εισόδων/εξόδων για να την απευθείας σύνδεσή τους με το Ethernet. Στη περίπτωση αυτή υπάρχει επικοινωνία μεταξύ I/O ελεγκτή με συσκευή και I/O επόπτη με συσκευή. Ο ελεγκτής χρησιμοποιεί στη μνήμη του το πρόγραμμα του αυτοματισμού. Τα δεδομένα εξόδου των συσκευών επέρχονται από τους ελεγκτές και ανάμεσα σε αυτή την επικοινωνία μεταφέρονται δεδομένα όπως διαμόρφωση, ανάλυση πληροφορίας και ειδοποιήσεις. Επίσης οι συσκευές I/O χρησιμοποιούνται ως πεδία για τη σύνδεση περισσοτέρων ελεγκτών μέσω του Profinet I/O. Παράλληλα μέσω του Ethernet υπάρχει μια σύνδεση μεταξύ επόπτη και συσκευών I/O, όπου εκεί πραγματοποιούνται διαγνώσεις για διάφορα σφάλματα, έλεγχοι και παραμετροποιήσεις αν κάτι χρίζει αλλαγή.

2.9.1 PROFISAFE

[18] [19] [20] Με στήριγμα το Profinet, υπάρχει ένα λογισμικό το οποίο είναι επιπρόσθετο αυτού και ονομάζεται Profisafe. Το λογισμικό αυτό ασχολείται ξεκάθαρα ,με την λειτουργική ασφάλεια μεταξύ των επικοινωνιών, δηλαδή διασφαλίζει την ακεραιότητα των fail safe σημάτων στις διάφορες συσκευές ασφάλειας και των ελεγκτών τους. Το Profisafe

λειτουργεί με βάση τα πρότυπα IEC 61508 (μέχρι και επίπεδο SIL 3) και ISO 13849 (PL “e”). Το λογισμικό αυτό βοηθάει επίσης στη μείωση χρήσης επιπλέον καλωδίων για τη μετάδοση πληροφορίας καθώς χρησιμοποιεί απευθείας μετάδοση στους ελεγκτές διεργασίας.

Το Profisafe εξασφαλίζει τις ασφαλείς λειτουργίες μέσω ενός τυπικού συστήματος μετάδοσης, χρησιμοποιώντας πάντα ένα επίπεδο υψηλότερο από το μοντέλο του OSI, έτσι ώστε να υπάρχει άμεση επικοινωνία σε περίπτωση αστοχίας, χωρίς να υπάρχει καθυστέρηση από τα υπόλοιπα επτά επίπεδα.



Εικόνα 10: Απεικόνιση της ασφάλειας του Profinet βάση του μοντέλου OSI.

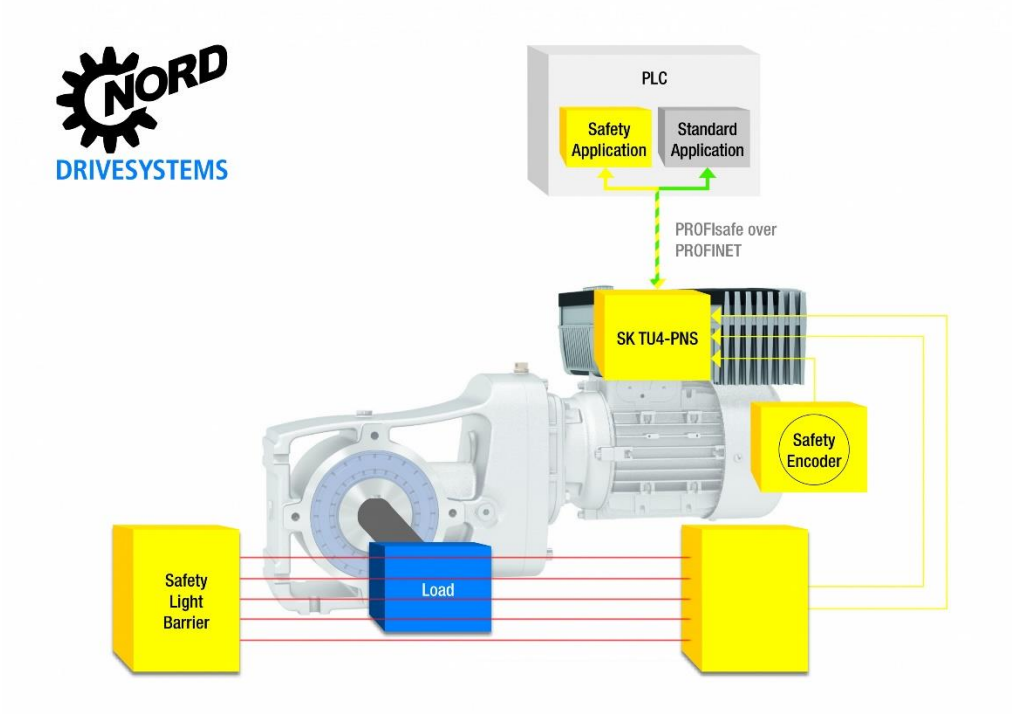
Με βάση την παραπάνω εικόνα υπάρχει ένα bus το οποίο ενώνεται με όλες τις διαφορετικές εισόδους/εξόδους, ελεγκτές κλπ και ονομάζεται μαύρο κανάλι. Το συγκεκριμένο κανάλι χρησιμοποιεί την κυκλική επικοινωνία μεταξύ συσκευών-ελεγκτών και η λειτουργία ψηφοφορίας θα μπορέσει απευθείας να εντοπίσει κάποια ελλαττωματική συσκευή. Επίσης, ένα ακόμα χαρακτηριστικό, είναι η 1:1 επικοινωνία μεταξύ ενός συνόλου συσκευών πάνω στο bus του ελεγκτή. Παράλληλα, υιοθετεί την αρχή αυθεντικότητας των μηνυμάτων για να εξασφαλίσει πως ότι στέλνεται και έρχεται μέσα στο σύστημα είναι αληθές.

Ένα μαύρο κανάλι έχει τη δυνατότητα να χρησιμοποιεί διάφορα στοιχεία δικτύου όπως κανάλια ασύρματης μετάδοσης, routers, switches κλπ. Όμως

λόγω ότι πρέπει να είναι δυνατή η συμμόρφωση σε SIL 3 επίπεδο, υπάρχουν κάποιες περιοριστικές αλλαγές οι οποίες είναι οι εξής:

- Επιτρεπτοί όλοι των ειδών διακόπτες, αλλά χρήση το πολύ μέχρι εκατό στη σειρά.
- Οι ονομασίες των τμημάτων του Profisafe πρέπει υποχρεωτικά να ονομάζονται με διαφορετικές ονομασίες, ενώ αν αυτό δεν είναι ανεκτό να γίνεται χρήση router πολλών θυρών που θα χρησιμοποιούν την ίδια ονομασία.

Οι αλλαγές πραγματοποιούνται με σκοπό τη μέγιστη κατάταξη όλων των περιφερειακών συσκευών και την ευκολία εντοπισμού λαθών και σφαλμάτων σε περίπτωση βλάβης/επισκευής.



[21] Εικόνα 11: Χρήση του προτύπου Profisafe πάνω σε ένα μοτέρ με ασφαλιστικό.

Στην παραπάνω εικόνα είναι μια απλή περίπτωση που πρέπει το controller – servo του κινητήρα να επικοινωνήσει με τον βασικό controller PLC σε περίπτωση που υπάρξει κάποια επιπλοκή στο φωτοκύτταρο κουρτίνα. Η διαφορά εδώ είναι πως λόγω χρήσης αυτού του προτύπου, παραλείπονται υποχρεωτικά κάποια τμήματα του επιπέδου OSI ώστε να λάβει και να αποστείλει εντολή το PLC όσο το δυνατόν πιο γρήγορα, έτσι ώστε να μην υπάρξουν τραυματισμοί σε περίπτωση που κάποιος εργαζόμενος περάσει τα όρια της κουρτίνας και πάει να ακουμπήσει κάποιο τμήμα της μηχανής.

2.10 AS – INTERFACE

[22] Το ASi (Actuator Sensor Interface) είναι μια διαφορετική μέθοδος δικτύωσης διαφόρων συσκευών πιο συγκεκριμένα γτα αισθητήρια και τους ενεργοποιητές με έναν ελεγκτή. Αρχικά υπάρχει η ευκολία μείωσης των πολλαπλών καλωδίων, διότι το ASi χρησιμοποιεί ελάχιστα για να παράξει πολλές ταυτόχρονα φυσικές συνδέσεις χωρίς αυτό να σημαίνει χάσιμο πληροφορίας. Επίσης χρησιμοποιεί τη λογική Master – Slave έτσι ώστε να μέσα στο κύκλωμα ο Master να μπορεί να ανταλλάσσει πληροφορίες μέχρι τέσσερις εισόδους και εξόδους της κάθε slave συσκευής είτε αυτό μεταφέρεται αναλογικά είτε ψηφιακά, αλλά ο master μπορεί συνολικά να συνδεθεί μέχρι και εξήντα δύο συσκευές slave. Είναι πολύ πιο οικονομικό σε σχέση με μια τυπική καλωδίωση και χρήση συσκευών όπως ρελέ, θερμικά, κ.α. και παράλληλα πιο αποδοτική στη χρήση καθώς είναι πολύ πιο εύκολο να πραγματοποιηθεί κάποια αλλαγή σε περίπτωση βλάβης λόγω τεράστιας μείωσης καλωδίων. Επιπλέον, είναι πολύ πιο γρήγοροι οι χρόνοι απόκρισης των συσκευών slave με τον master από ότι του ίδιου του ελεγκτή. Ταυτόχρονα μπορεί πολύ εύκολα και ακριβές να υπολογιστεί ο χρόνος αναμονής ενεργοποίησης κάποιου αισθητήρα ή ενεργοποιητή. Η ιεραρχία του ASi έχει τρία μέρη:

Τη συσκευή Master όπου ενώνεται με τις υψηλότερες συσκευές ελεγκτών και πραγματοποιεί ελέγχους στο σύστημα, διάγνωση αν όλες οι πληροφορίες που διέρχονται και εξέρχονται είναι σωστές και διαμόρφωση των παραμέτρων αν είναι ανάγκη. Το δεύτερο μέρος είναι οι καλωδιώσεις οι οποίες χωρίζονται σε δύο τμήματα, πρώτα είναι η καλωδίωση που θα μεταφέρει ρεύμα και δεδομένα στους αισθητήρες και δεύτερον η καλωδίωση που μεταφέρει ρεύμα μόνο στους ενεργοποιητές. Βασικό είναι να γνωρίζουμε πως οι τάσεις τροφοδοσίας διαφέρουν στους αισθητήρες και στους ενεργοποιητές. Το τρίτο μέρος είναι τα τροφοδοτικά που μεταφέρουν τάση σε όλες τις συσκευές του συστήματος και παράλληλα μπορούν να πραγματοποιήσουν μέσω του καλωδίου τη διαχώριση της πληροφορίας με την τάση. Μια ASi συσκευή ως σύνολο μπορεί να φτάσει μέχρι εκατό μέτρα, αλλά αν υπάρχει διάθεση επέκτασης μπορεί να γίνει χρήση κάποιου επαναλήπτη και ειδικές φίσες επέκτασης όπου θα διαδίδει περαιτέρω την πληροφορία μέχρι τα εξακόσια μέτρα.

Συμπληρωματικά, υπάρχει μια ακόμα εναλλακτική λύση στις συνδεσμολογίες μέσω του ASi και ονομάζεται ASi Safety at Work. Η συγκεκριμένη μέθοδος ακολουθεί τα πρότυπα EN ISO μέχρι κατηγορίας e και IEC 61508 μέχρι SIL 3. Στο συγκεκριμένο σύστημα γίνεται καθορισμός του σωστού συνδυασμού στοιχείων ασφάλειας και κατά σειρά η ρύθμιση της οθόνης ασφάλειας βάση την προεπιλεγμένη κατηγορία ελέγχου. Αυτή η

οθόνη παρομοιάζεται με ένα ρελέ ασφαλείας καθώς ελέγχει συνεχώς κάποιες καταστάσεις και δρα αναλόγως σε περίπτωση βλάβης ή κινδύνου. Επιπροσθέτως, λόγω της μεγάλης συμβατότητας της, μπορεί να αντικαταστήσει πολλαπλά ρελέ εξοικονομώντας έτσι χώρο, χρόνο εγκατάστασης – αλλαγής και χρήμα. Αν είναι αναγκαία η μέγιστη ασφάλεια, τότε ο σχεδιαστής πρέπει πολύ προσεκτικά να διασφαλίσει πως τα περιφερειακά εξαρτήματα που χρησιμοποιούνται συντονίζονται και λειτουργούν ανάλογα με τις ρυθμίσεις της οθόνης, έτσι ώστε να πραγματοποιείται η ύψιστη λειτουργία του ASi SaW.

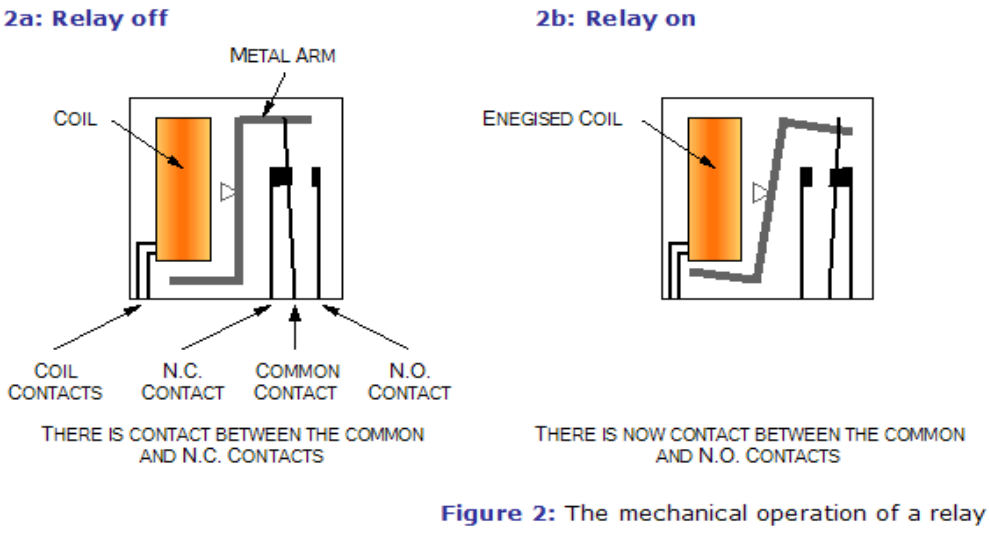
ΚΕΦΑΛΑΙΟ 3^{Ο}

3.1 ΕΡΓΑΛΕΙΑ ΧΡΗΣΗΣ ΣΕ FAIL SAFE ΣΥΣΤΗΜΑΤΑ

Σε μία παραγωγική μονάδα υπάρχουν διάφορα πρότυπα τα οποία πρέπει να χρησιμοποιούνται για να θεωρηθεί ασφαλές το εργατικό περιβάλλον και παράλληλα τη βέλτιστη μείωση των πιθανών κινδύνων. Για να είναι αυτό εφικτό, είναι σημαντικό να χρησιμοποιούνται διάφορα εργαλεία τα οποία θα μειώνουν τον κίνδυνο και τις διάφορες περιπτώσεις ανάγκης.

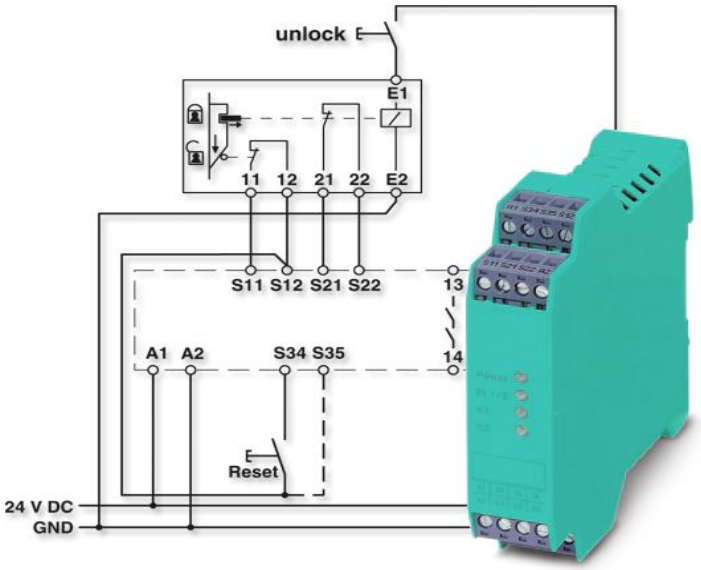
3.2 SAFETY RELAY

Τα ρελέ ασφαλείας είναι οι κατάλληλες συσκευές για να εξασφαλιστεί η ασφάλεια σε μια παραγωγική μονάδα και όχι μόνο. Όταν υπάρξει κατάσταση που θα θέσει σε κίνδυνο τον εργαζόμενο ή το ίδιο το μηχάνημα, τότε ο διακόπτης αυτός θα ενεργοποιήσει την λειτουργία να ‘’ανοίξει΄΄ και να μειώσει έτσι τον κίνδυνο, παρόλο που δεν είναι πάντα σίγουρο πως θα εξαλειφθεί. Κάθε ρελέ ασφάλειας παρακολουθεί μια συγκεκριμένη λειτουργία και με τη βοήθεια πολλαπλών τέτοιων στοιχείων, μπορεί να καλυφθεί μια μεγάλη έκταση των παραγωγικών μονάδων. Τείνουν να έχουν αντοχή στον χρόνο και εκτεταμένη αποτελεσματικότητα καθώς αποτελεί προτεραιότητα σε όλες τις βιομηχανικές επιχειρήσεις για την αποφυγή ατυχημάτων, είτε αυτό μπορεί να προκληθεί από προσωπικό είτε από κάποια δυσλειτουργία του ηλεκτρικού κυκλώματος. Μερικές από τις πιο δημοφιλές λειτουργίες ενός ρελέ ασφαλείας είναι η διακοπή μιας κίνησης με ελεγχόμενο τρόπο, η παρακολούθηση της θέσης των κινητών φρουρών και η απενεργοποίηση σε περίπτωση έκτακτης ανάγκης.



[23] Εικόνα 2: Λογική πίσω από ένα τυπικό ρελέ ασφάλειας.

Για να μπορέσει κάποιος να χρησιμοποιήσει επιτυχώς ένα τέτοιο στοιχείο, είναι σημαντική η γνώση βασικού ηλεκτρολογικού σχεδίου και τα πρότυπα που πρέπει να καλυφθούν. Παρόλα αυτά δεν χρειάζεται κάποια περαιτέρω εκπαίδευση, λόγω απλότητας και αποτελεσματικότητας.



[24] Εικόνα 3: Συνδεσμολογία ενός ρελέ ασφαλείας.

Παραπάνω είναι ένα τυπικό σχεδιάγραμμα ενός ρελέ ασφαλείας. Η συνδεσμολογία έχει ως εξής: Το A1 συνδέεται στην παροχή 24 vdc και το A2 στη γείωση. Η επαφές 11.12 και 21.22 χρησιμοποιούνται ως μπουτόν έκτακτης ανάγκης και είναι Normally Closed επαφές, δηλαδή είναι κανονικά κλειστές επαφές πριν τους δοθεί κάποιο ερέθισμα. Επίσης, οι

επαφές S34 και S35 χρησιμοποιούνται για χειροκίνητη επανεκκίνηση του συστήματος πατώντας το μπουτόν Reset.

Υπάρχουν πολλά είδη ρελέ τα οποία είναι πολύ διαδεδομένα και εύχρηστα. Κάποια από αυτά είναι είναι οι κουρτίνες, τα ταπέτα ασφάλειας, οι συσκευές τριών θέσεων, οι συσκευές με χρήση δύο χεριών, οι μαγνητικές επαφές, τα μπουτόν έκτακτης ανάγκης καθώς και οι αισθητήρες χωρίς επαφή.

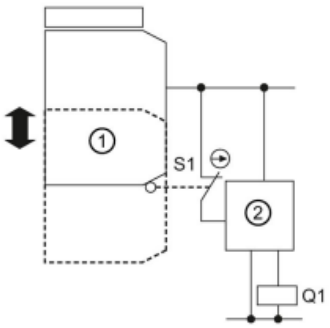
3.3 SINGLE CHANNEL OR DUAL CHANNEL SAFETY RELAY

Στην αγορά υπάρχουν πολλά διαδεδομένα είδη ρελέ ασφαλείας τα οποία χρησιμοποιούνται σε πολλές εφαρμογές είτε αυτά είναι απλοί ηλεκτρολογικοί πίνακες ή μια διάταξη ολόκληρης βιομηχανικής παραγωγής. Μια βασική κατηγορία αυτών είναι τα μονού καναλιού και διπλού καναλιού ρελέ.

Ένα ρελέ με μονό κανάλι είναι μια αξιόπιστη λύση για να εξασφαλιστεί η ασφάλεια σε ένα κύκλωμα καθώς δεν χρειάζεται κάποια παρακολούθηση σε περίπτωση που πρέπει να κλείσει μια βασική λειτουργία. Αυτό σημαίνει πως υπάρχει ενσωματωμένη στο κύκλωμα του ρελέ η ‘’παρακολούθηση’’ και παράλληλα παραπέμπει αποτελεσματικά αν υπάρξει βλάβη κάποιου εξαρτήματος. Επίσης η ενεργοποίηση και απενεργοποίηση του ρελέ πραγματοποιείται αυτόματα με ασφαλές τρόπο αφού ακολουθεί ένα συγκεκριμένο εύρος παλμών, δηλαδή ελέγχεται αυτόματα στο τέλος κάθε κύκλου ενεργοποίησης/απενεργοποίησης. Υπάρχει περίπτωση ένα ρελέ τέτοιου είδους να παρουσιάσει πρόβλημα κατά την λειτουργία του και να μην πραγματοποιηθεί πχ η αναγκαία απενεργοποίηση του κυκλώματος. Πώς μπορεί να αποφευχθεί κάτι τέτοιο;

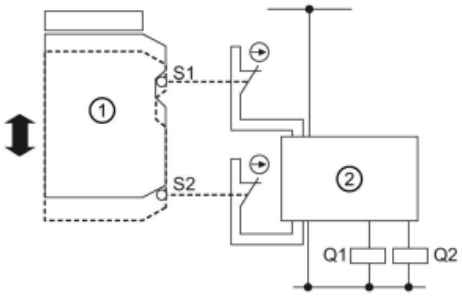
Μια ιδανική λύση στο πρόβλημα αυτό είναι η χρήση ενός ρελέ το οποίο χρησιμοποιεί διπλό κανάλι και είναι το ίδιο χρήσιμο όσον αφορά τις εφαρμογές, καθώς μπορεί και αυτό να ελέγχει αυτόματα το κύκλωμα σε περίπτωση βλάβης. Επιπλέον, μπορεί να χρησιμοποιηθεί σε συμπλεκόμενα προστατευτικά, σε κουρτίνες, σαρωτές λέιζερ και διάφορα χαλιά ασφαλείας.

Το βασικό πλεονέκτημα που έχει το διπλό κανάλι σε σύγκριση με το μονό είναι στο ίδιο το κύκλωμα όπου θα πραγματοποιηθεί η διέγερση της επαφής όταν θα χρειαστεί να ασφαλίσει. Το διπλό έχει τη δυνατότητα αν υπάρξει κάποια βλάβη στο ίδιο το ρελέ να λειτουργήσει η πρώτη ή δεύτερη επαφή, εξασφαλίζοντας σχεδόν πάντα πως δεν θα υπάρχει ελλαττωματικό ρελέ.



① Mechanical position switches
② Safety relay

Figure 3-10 Single-channel safety-related control system



① Mechanical position switches
② Safety relay

Figure 3-11 Two-channel safety-related control system

Εικόνα 4: Βασική διαφορά ενός single & dual channel ρελέ.

Παραπάνω είναι φανερό πως ένα διπλού τύπου ρελέ ασφάλειας είναι πολύ πιο αξιόπιστο από ένα μονό, παρόλο που είναι αρκετά πιο ακριβά όσον αφορά τη τιμή τους. Βασικό κριτήριο πάντα είναι η ασφάλεια, άρα πιο ιδανικό είναι του διπλού καναλιού ρελέ.

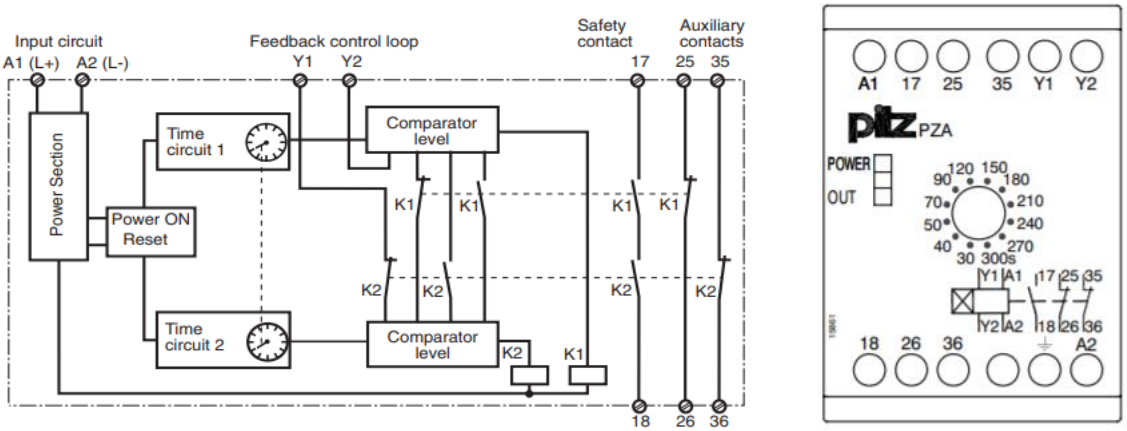
3.4 SAFETY RELAY WITH DELAY TIMER

[25] Τα ρελέ με χρονιστή πραγματοποιούν τις ίδιες βασικές λειτουργίες που πραγματοποιεί ένα τυπικό ρελέ ασφαλείας, παρόλα αυτά παρέχει μια επιπλέον λειτουργία η οποία χρησιμοποιείται στην έξοδο. Αυτή η λειτουργία είναι η χρονοκαθυστέρηση και χρησιμοποιείται σε εφαρμογές που πρέπει η ισχύς να διατηρείται για ένα συγκεκριμένο χρονικό διάστημα μετά τη λήψη της εισόδου.

Ένα χρονικό έχει διάφορους τρόπους να λειτουργήσει την χρονοκαθυστέρηση, είτε delay on, δηλαδή όταν τεθεί σε λειτουργία η είσοδος, τότε υπάρχει μια καθυστέρηση μέχρι να ενεργοποιηθεί η έξοδος και αντίστοιχα το delay off,

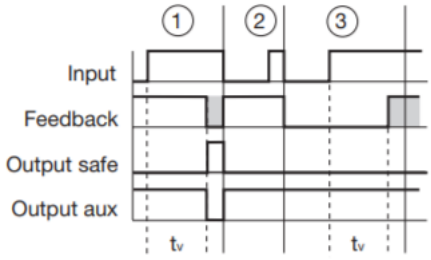
όταν η είσοδος τεθεί εκτός λειτουργίας, τότε υπάρχει μια καθυστέρηση μέχρι να σβήσει και η έξοδος. Επίσης το time bypass όπου ενεργοποιεί την έξοδο ασφάλειας για μέγιστο προκαθορισμένο χρονικό διάστημα όταν η είσοδος ασφάλειας είναι σβηστή. Μία ακόμα είναι η επαναφορά του χρόνου που ενεργοποιεί την έξοδο ασφάλειας για μέγιστο χρονικό διάστημα που είναι προκαθορισμένο όταν ανοίξει η είσοδος.

Ένα χρονικό ρελέ μπορεί να ρυθμιστεί από 0 έως 999 δευτερόλεπτα και είναι λογικό να έχει κάποια μικρή ακρίβεια που μπορεί για κάποιο ρελέ να είναι ± 1 κλπ.



[25] Εικόνα 5: Μπλόκ διάγραμμα και τερματικός μηχανισμός.

Παραπάνω απεικονίζεται ένα ρελέ με χρονικό της εταιρίας pilz στο οποίο αριστερά έχουμε την συνδεσμολογία του κυκλώματος και δεξιά είναι φανερό πως ο χρόνος επιλέγεται στο κυκλικό επιλογέα ο οποίος θέτει πόση χρονοκαθυστέρηση θα υπάρξει στο σύστημα. Πιο συγκεκριμένα, οι επαφές A1 και A2 είναι οι είσοδοι τροφοδοσίας(+,-) και όταν πατηθεί το start έχοντας την είσοδο ασφαλείας 17 κλειστή, το PZA απενεργοποιείται και παράλληλα η επαφή ασφαλείας δεν ανοίγει. Αν πατηθεί το στοπ, ενεργοποιείται το ρελέ κ1 και οι NC επαφές κ1 κλείνουν. Ύστερα την πάροδο του χρονικού διαστήματος που έχει καθοριστεί, η επαφή ασφαλείας του PZA κλείνει και ανοίγει η επαφή ασφαλείας 17.



[25] Εικόνα 6: Διάγραμμα χρόνου.

Στο παραπάνω σχήμα φαίνεται ο τρόπος με τον οποίο λειτουργεί το ρελέ, αλλά προσωποποιημένο με τον χρόνο. Τν είναι ο χρόνος της καθυστέρησης, input είναι η είσοδος που τροφοδοτείται με ρεύμα, feedback η ανατροφοδότηση, output safe είναι η επαφή ασφαλείας 17-18 και output aux είναι οι βοηθητικές επαφές.

3.5 SAFETY PLC

[26] Τα PLC (Programmable Logic Controller) ασφαλείας είναι προγραμματιζόμενα μηχανήματα τα οποία ενσωματώνονται με διάφορες διαγνωστικές λειτουργίες οι οποίες πραγματοποιούν ανίχνευση πιθανών βλαβών για την αποφυγή κάποιας επικίνδυνης κατάστασης που μπορεί να τραυματίσει κάποιον χρήστη είτε να προκαλέσει κάποια βλάβη στο ίδιο το μηχάνημα.

Ένα τέτοιου είδος PLC είναι μέλος στο SIS(Safety Instrumental Systems), το οποίο σύστημα αποτελείται από λογισμικό και συσκευές(μαζί με το safety PLC) οι οποίες είναι ειδικές στην αντιμετώπιση μιας κρίσιμης κατάστασης. Όταν εντοπιστεί μια τέτοια κατάσταση τότε το plc θα θέσει σε ασφαλή κατάσταση το οποιοδήποτε μηχάνημα. Όσον αφορά τον προγραμματισμό του συγκεκριμένου λογικού μηχανήματος είναι ίδιος με ένα τυπικό PLC, παρόλο που χρησιμοποιεί μια τεχνική που ονομάζεται SIL(Safety Integrity Level) και αξιολογεί την ασφάλεια σε ένα σύστημα με βάση πόσο επικίνδυνο είναι και ποια τα στάδια μείωσης του.

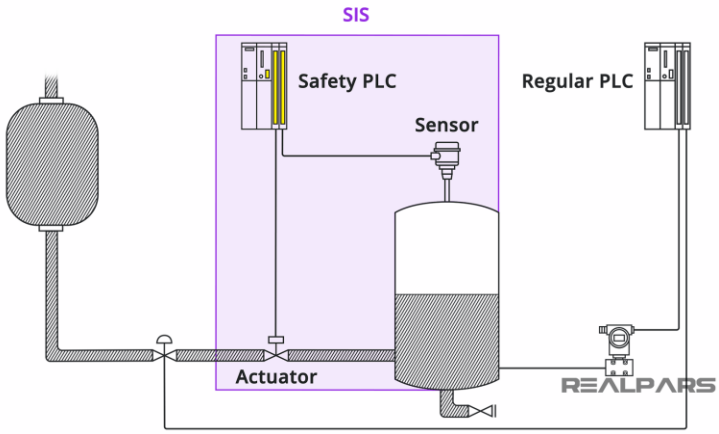
Επίσης σε αυτά τα PLC η λογική του κώδικα είναι κλειδωμένη έτσι ώστε να εξασφαλιστεί η ασφάλεια και ταυτόχρονα γίνεται αναγνώριση ότι όλα λειτουργούν κάτω από σωστές καταστάσεις. Επιπλέον, σε περιπτώσεις που μπορεί να υπάρχει κάποιο ελλαττωματικό στοιχείο πχ καλώδια, επαφές κλπ. γίνεται άμεση ενημέρωση της κατάστασης για την αλλαγή τους.

[27] Ένα safety PLC βασίζεται πάνω σε δύο επεξεργασίες οι οποίες είναι υπεύθυνες για την παρακολούθηση του προγράμματος και την επικοινωνία του με εξωτερικές συσκευές εισόδων – εξόδων. Πρώτα, η επεξεργασία που υποστηρίζει είναι διπλή (1oo2D), η μια ονομάζεται ARM και η άλλη RISC. Πάντα και οι δύο λειτουργούν βάση της λογικής καλύτερης λύσης, ανάλογα με τις πληροφορίες που λαμβάνουν από τα αισθητήρια και τα διάφορα περιφερειακά συστήματα. Ως βάση, η ARM εκτελεί όλες τις βασικές λογικές εντολές του προγράμματος και η RISC μόνο τις κρίσιμες σε χρόνο εντολές που ασχολούνται σε πραγματικό χρόνο. Επίσης η RISC χρησιμοποιεί 32bit πυρήνα για να μην πιάνει μεγάλο χώρο κατά την επεξεργασία των πληροφοριών μιας κρίσιμης κατάστασης. Αν υπάρξει κάποιο πρόβλημα με τον επεξεργαστή ARM, τότε αναλαμβάνει ο RISC και αποθηκεύει μέσα στο

FPGA τα αποτελέσματα της διάγνωσης. Το κομμάτι της εκτέλεσης εντολών σε ένα τέτοιο PLC αποτελείται από τέσσερα μέλη, το στρώμα της διοίκησης, το κομμάτι των συσκευών, την αποθήκευση και το μηχάνημα που πραγματοποιεί μια εικονική λειτουργία στο πρόγραμμα που τρέχει στο PLC.

Όσον αφορά το τμήμα σχεδίασης στη μονάδα εκτέλεσης, υπάρχει το PLCVM όπου είναι το πιο βασικό στοιχείο ενός plc ασφαλείας διότι μπορεί και διαβάζει τη γλώσσα προ/μού ladder που προέρχεται από τον χρήστη και ύστερα το VM μεταφράζει τη γλώσσα σε δικά του δεδομένα κατάλληλα για να καταλάβει και μόλις πραγματοποιηθεί αυτή η διαδικασία, τα δεδομένα αποστέλλονται σε μια εξωτερική πηγή I/O και καταλήγει σε μια μνήμη όπου και εκεί εκτελείται το πρόγραμμα.

Η λειτουργία του τμήματος διοίκησης είναι να εξακριβώνει πως όλες οι προηγούμενες ψηφιακές συνδέσεις μεταξύ μεταφραστή, λογικού προ/τος και ελέγχου σωστής λειτουργίας προ/τος (start/stop/emergency stop). Κατά σειρά, το τμήμα hardware έχει βασικό σκοπό να συνδέει τις φυσικές συνδέσεις του PLC με το πληκτρολόγιο και όλα τα περιφερειακά. Τέλος, το τμήμα μνήμης έχει τη δουλειά του προγραμματισμού της μνήμης όσον αφορά τα δεδομένα που δέχεται να κρατήσει.



[26] Εικόνα 7: Απεικόνιση ενός Safety PLC σε σύστημα

3.6 ΜΕΘΟΔΟΙ ΣΥΝΔΕΣΜΟΛΟΓΙΑΣ SAFETY PLC ΜΕ CPU

[28] Διάφορα συστήματα τα οποία χρησιμοποιούν safety PLC πρέπει να χρησιμοποιούν μεθόδους παρακολούθησης και τρόπους συνδεσμολογίας των εισόδων – εξόδων του PLC με την CPU, έτσι ώστε να είναι προκαθορισμένο το κάθε SIL που χρησιμοποιείται σε κάθε εφαρμογή και ταυτόχρονα την

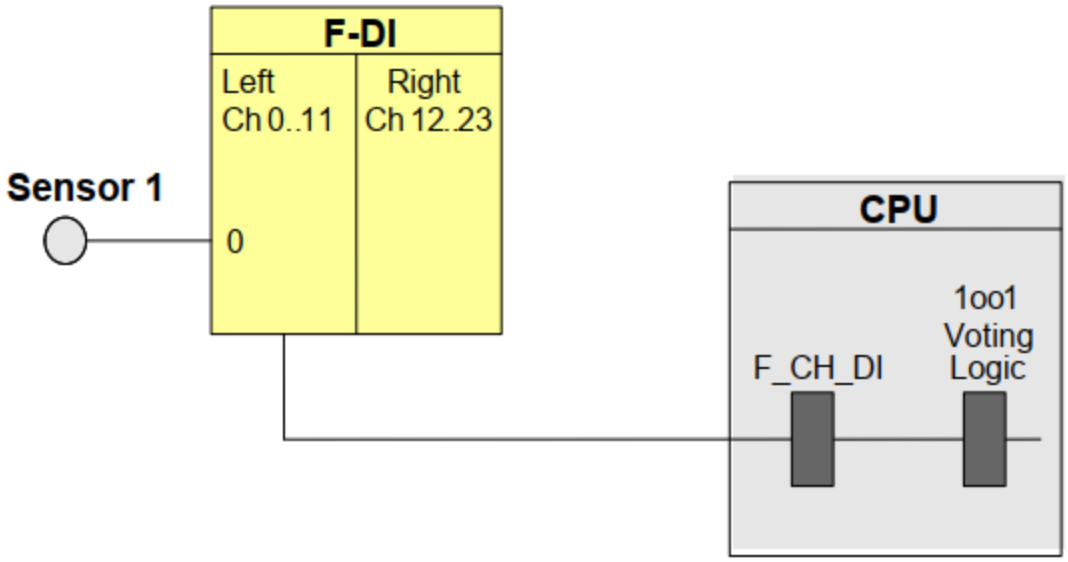
αναγκαιότητα του ρίσκου όσον αφορά τον κίνδυνο. Υπάρχουν πάρα πολλοί τρόποι συνδεσμολογίας ενός PLC με μία CPU και κάποιες από αυτές είναι F-Di, F-Do, F-Ai, F-Ao. Παρακάτω θα γίνει παρουσίαση όλων των βασικών αρχιτεκτονικών:

- Ένας αισθητήρας (1oo1) και μια F-Di (1oo1).
- Ένας αισθητήρας (1oo1) και δύο F-Di (2oo2).
- Δύο αισθητήρες (1oo2) και μια F-Di με αξιολόγηση (1oo1).
- Δύο αισθητήρες (1oo2) και δύο F-Di με αξιολόγηση (2oo2).
- Δύο αισθητήρες (1oo2) με αξιολόγηση ενός προγράμματος χρήστη.
- Δύο αισθητήρες (1oo2) με δύο F-Di (2oo2) και αξιολόγηση μέσω προγράμματος χρήστη.
- Έλεγχος ενός ενεργοποιητή (1oo1) σε μια έξοδο F-Do (1oo1).
- Έλεγχος ενός ενεργοποιητή (1oo1) σε δύο F-Do(2oo2).

Σημαντική παρατήρηση είναι πως οι παραπάνω τεχνικές χρησιμοποιούνται σε διάφορα PLC της Siemens.

3.7 ΔΙΑΜΟΡΦΩΣΗ ΥΛΙΚΟΥ ΕΝΟΣ ΑΙΣΘΗΤΗΡΑ (1oo1) & ΜΙΑΣ F-Di(1oo1)

[28] Η προκειμένη διάταξη αφορά τις εφαρμογές οι οποίες δεν απαιτούν υψηλή διαθεσιμότητα. Η 1oo1 σημαίνει πως χρησιμοποιείται μόνο ένα αισθητήριο και αν αυτό λάβει κάποιο σήμα, τότε σηματοδοτείται η ενεργοποίηση της λογικής ασφάλειας. Σε περίπτωση που η λογική του προγράμματος εντοπίσει κάποια ανάγκη για ασφαλή λειτουργία, τότε μπορεί να ενεργοποιηθεί με διάφορους τρόπους. Αν δεν εντοπιστεί ελλαττωματικό αισθητήριο ή fail safe ψηφιακή έξοδος, τότε είναι δυνατή η ασφαλής λειτουργία αλλά όχι αναγκαία. Αν έχουμε ψηφιακή έξοδο με βλάβη(X-NAI) ή αν υπάρχει σφάλμα στο αισθητήριο (NAI-X) τότε οπωσδήποτε τίθεται η ασφαλής λειτουργία μείωσης κινδύνου. Επίσης η συγκεκριμένη διάταξη μπορεί να εξασφαλίσει μέχρι SIL 2.



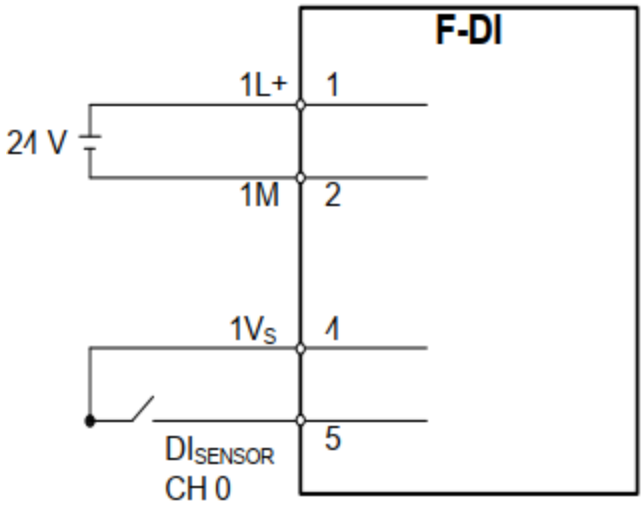
[28] Εικόνα 8: Απεικόνιση Sensor(1oo1) & F-Di(1oo1).

Η διάταξη αυτή όπως και οι υπόλοιπες έχουν μια τιμή η οποία αντιπροσωπεύει την πιθανότητα να υπάρξει αποτυχία της ασφαλούς λειτουργίας(PFD – Probability of Failure on Demand) και υπάρχει μέθοδος υπολογισμού αυτής της τιμής. PFD EIN = PFDsensor + PFDfdi + PFDcpu.

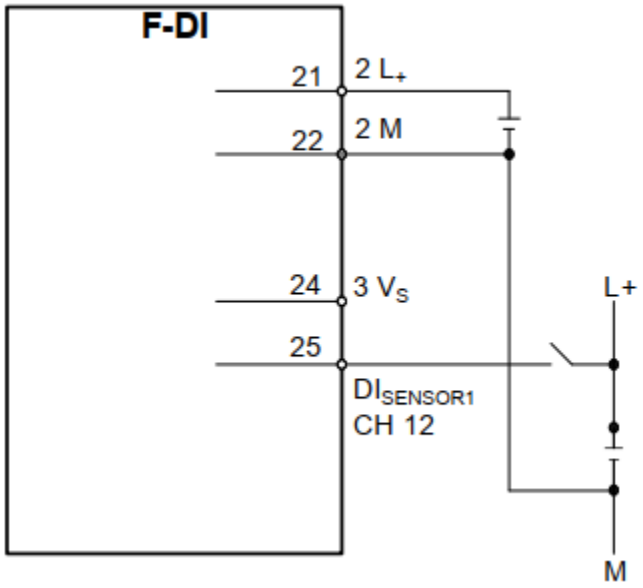
PFDsensor = $\lambda DU \times \frac{T1}{2}$. Το PFD F-Di βάση πινάκων είναι περίπου < $1.00E^{-4}$, το PFD CPU -//- έχει πολλές τιμές οι οποίες ποικίλουν ανάλογα με τα χρόνια χρήσης, δηλαδή <$1.9E^{-4}$~$2.8E^{-4}$ (Στα 10 χρόνια) και <$3.8E^{-4}$~$5.6E^{-4}$ (Στα 20 χρόνια).

Όσον αφορά τη συνδεσμολογία αυτής της διάταξης ισχύει το εξής: Το αισθητήριο μπορεί να τροφοδοτηθεί με δύο τρόπους, η μια είναι το F-Di να τροφοδοτήσει το αισθητήριο και η δεύτερη είναι η χρήση μιας εξωτερικής πηγής. Όταν το αισθητήριο είναι στην πρώτη περίπτωση, τότε είναι συνδεδεμένο στο 0ο κανάλι και τροφοδοτείτε από το 1Vs, ενώ η παροχή όλου του F-Di είναι 24Vdc.

Στην δεύτερη περίπτωση, το αισθητήριο τροφοδοτείται από το 12^{ο} κανάλι και τη βοήθεια μιας επαφής N.O., ενώ το F-Di μέσω της εξωτερικής πηγής L+.



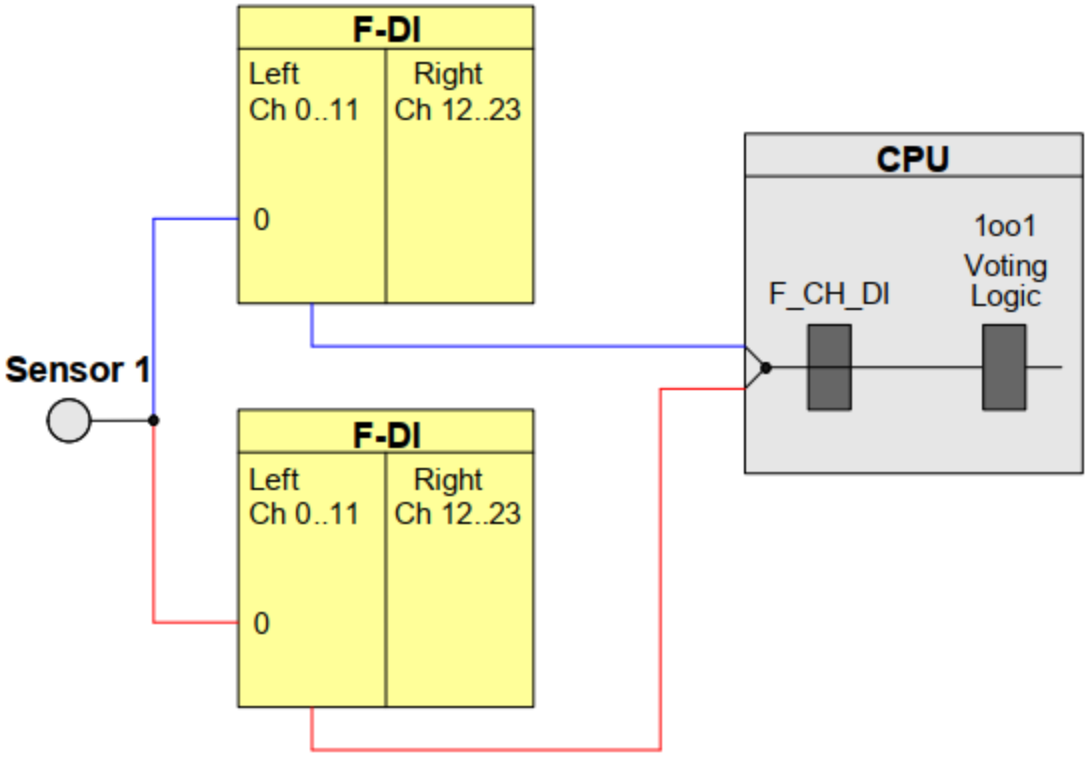
[28] Εικόνα 9: Τροφοδότηση μέσω του F-Di.



[28] Εικόνα 10: Τροφοδότηση με εξωτερική πηγή/γραμμή.

3.8 ΔΙΑΜΟΡΦΩΣΗ ΥΛΙΚΟΥ ΕΝΟΣ ΑΙΣΘΗΤΗΡΑ(1oo1) & ΠΕΡΙΣΣΟΤΕΡΩΝ F-Di(2oo2)

[28] Στη συγκεκριμένη αρχιτεκτονική υπάρχει μεγαλύτερη διαθεσιμότητα σε εξόδους F-Di και παράλληλα ποιες θα διαχειριστεί η CPU στο F_CH_Di, καθώς είναι πλέον 2oo2. Με βάση αυτό, ο ένας αισθητήρας συδέεται και στις δύο F-Di's στο 0 κανάλι και στη CPU υπάρχει μόνο μια είσοδος καναλιού η οποία θα κρίνει μέσω του προγράμματος ποια από τις δυο F-Di είναι αληθής για να λάβει εκείνης το σήμα.

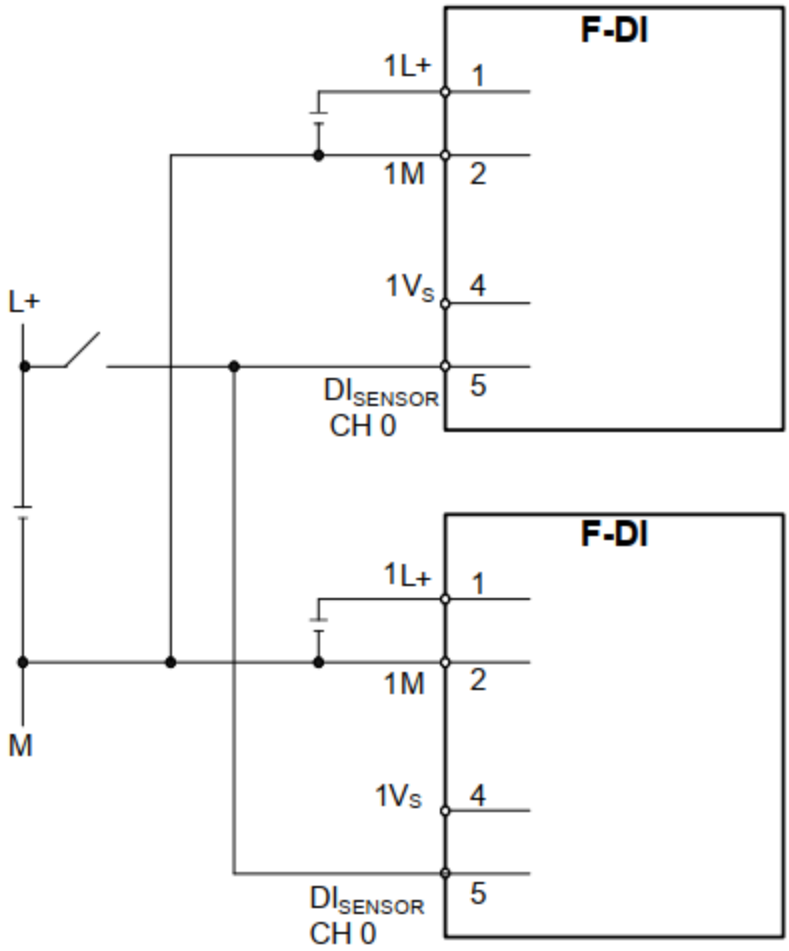


[28] Εικόνα 11: Απεικόνιση sensor(1oo1) & δύο F-Di(2oo2), εκ των οποίων η μια θα κριθεί περιττή.

Ο τρόπος με τον οποίο η αρχιτεκτονική ενεργοποιεί την ασφαλή λειτουργία είναι ως εξής: Όταν δεν υπάρχει κάποια ελλαττωματική F-Di κ αισθητήριο, τότε δεν υπάρχει ανάγκη ενεργοποίησης της ασφαλούς λειτουργίας, αυτό παραμένει ως έχει όταν έχει πρόβλημα μια από τις δύο F-Di, αφού η CPU παίρνει πάντα μια από τις δύο. Αν όμως παρουσιάσουν σφάλμα και οι δύο είτε μόνο το αισθητήριο, τότε μπαίνει αυτόματα σε ασφαλή λειτουργία. Επίσης εξίσου σημαντικό είναι ότι παρόλο που υπάρχουν δυο έξοδοι, δεν σημαίνει πως αυξάνεται το SIL.

Για να υπολογιστεί η πιθανότητα σφάλματος κατά τη χρήση, χρησιμοποιείται η ίδια εξίσωση με την προηγούμενη παρόλο που υπάρχει μια μικρή αλλαγή. PFDein = PFDsensor + 2PFDfdi + PFDcpu.

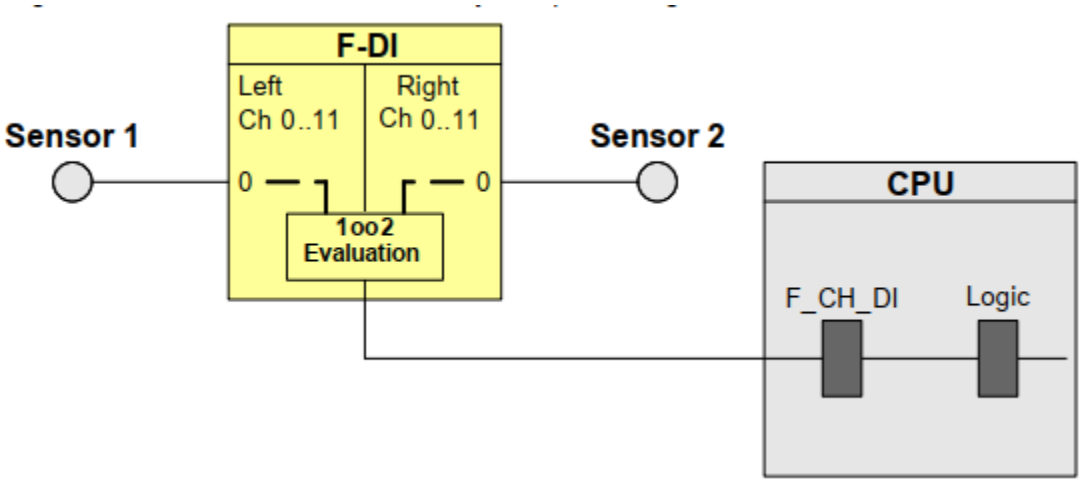
Η συνδεσμολογία τους πραγματοποιείται μόνο με εξωτερική πηγή, χρησιμοποιώντας το 0 κανάλι για τον αισθητήρα ο οποίος λαμβάνει ρεύμα από την L+, ενώ τα F-Di παίρνουν από το L/M.



[28] Εικόνα 12: Απεικόνιση συνδεσμολογίας του 1oo1 σε 2oo2.

3.9 ΔΙΑΜΟΡΦΩΣΗ ΥΛΙΚΟΥ ΜΕ ΔΥΟ ΑΙΣΘΗΤΗΡΕΣ(1oo2) ΚΑΙ F-Di ΜΕ ΑΞΙΟΛΟΓΗΣΗ

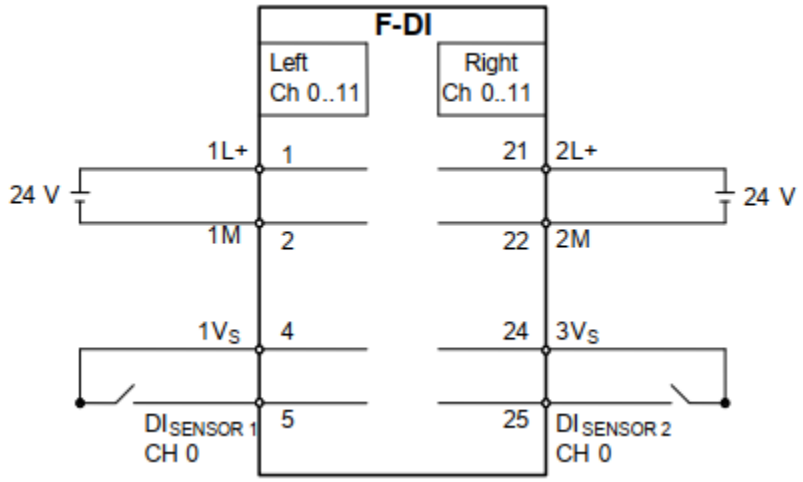
[28] Η συγκεκριμένη διαμόρφωση χρησιμοποιείται σε εφαρμογές που χρήζουν παραπάνω από ένα αισθητήριο για να υπάρχει η κατάλληλη ασφάλεια. Επίσης, για να μπορέσει να λειτουργήσει η λογική του προγράμματος για την ασφάλεια, πρέπει να εντοπίσει τουλάχιστον ένα από τα δύο αισθητήρια και ύστερα θα κριθεί η διαδικασία από την F-Di. Μέσω αυτής συνδέονται και τα αισθητήρια, το 1^{ο} στο αριστερό κανάλι 0 και το 2^{ο} στο δεξί κανάλι 0. Όσον αφορά τη λειτουργία ασφάλειας, πρέπει να υπάρξει βλάβη σε οποιαδήποτε από τους δύο αισθητήρες και F-Di για να τεθεί στο ON. Με τη διαμόρφωση του συγκεκριμένου υλικού μπορεί να χρησιμοποιηθεί για την επίτευξη έως και SIL 3.



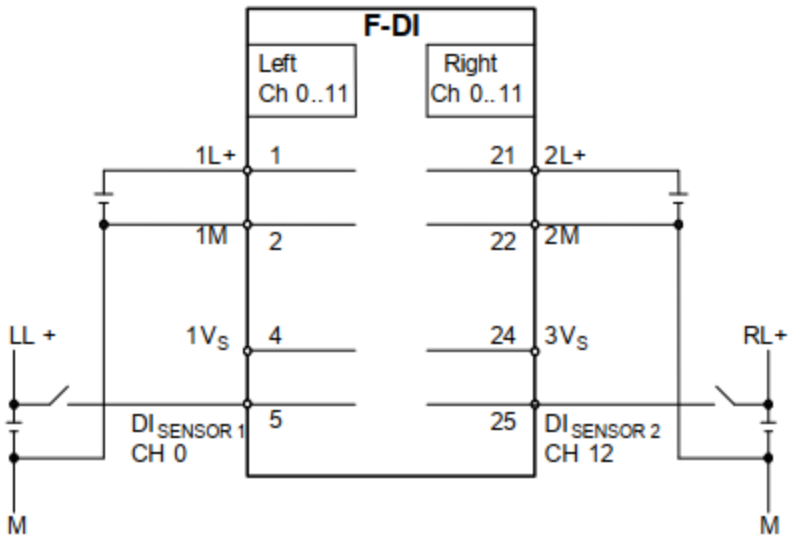
[28] Εικόνα 13: Απεικόνιση του 1oo2 σε 1oo1 F-Di.

Ο υπολογισμός της πιθανότητας σφάλματος σε αυτή την περίπτωση έχει κάποιες διαφοροποιήσεις. Το PFDein υπολογίζεται με τον ίδιο τρόπο, αλλά το PFDsensor υπολογίζεται ως εξής: $\frac{\lambda du^2 \times T1^2}{3} + \beta \times \lambda du \times \frac{T1}{2}$.

Για τη τροφοδοσία αυτής της διάταξης υπάρχουν δύο τρόποι εφαρμογής, πρώτα έχουμε την τροφοδότηση των αισθητήρων μέσω του F-Di και η δεύτερη με χρήση εξωτερικής πηγής. Στην πρώτη περίπτωση γίνεται χρήση των εισόδων 1Vs & 3Vs για την τροφοδοσία στα κανάλια 0 αριστερά κ δεξιά αντίστοιχα, καθώς στο F-Di δίνεται παροχή 24v από τις γραμμές 1L+ 1M & 2L+ & 2M. Στη δεύτερη περίπτωση γίνεται χρήση μιας εξωτερικής πηγής LL+ & RL+ που συνδέονται στον πρώτο αισθητήρα στο 0 κανάλι και στο δεύτερο αισθητήρα στο 12ο κανάλι.



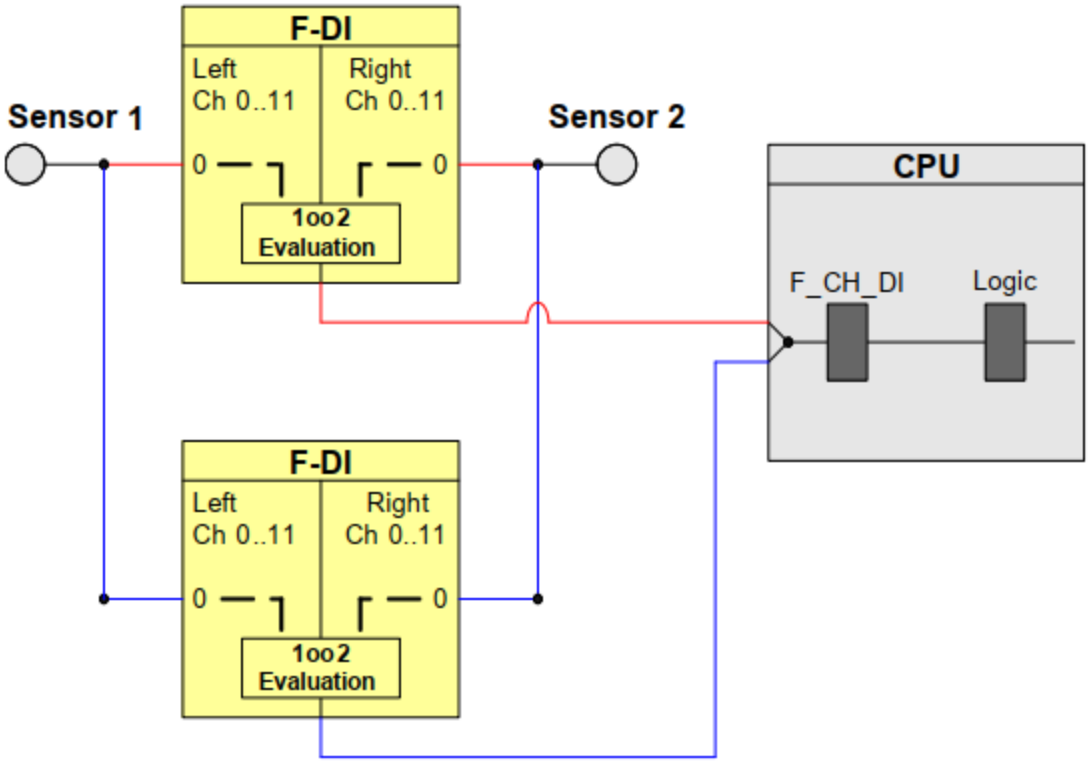
[28] Εικόνα 14: Συνδεσμολογία κ τροφοδοσία με εσωτερική πηγή.



[28] Εικόνα 15: Συνδεσμολογία κ τροφοδοσία με εξωτερική πηγή.

3.10 ΔΙΑΜΟΡΦΩΣΗ ΥΛΙΚΟΥ ΜΕ ΧΡΗΣΗ ΔΥΟ ΑΙΣΘΗΤΗΡΩΝ(1oo2) ΚΑΙ ΔΥΟ F-Di ΜΕ ΑΞΙΟΛΟΓΗΣΗ

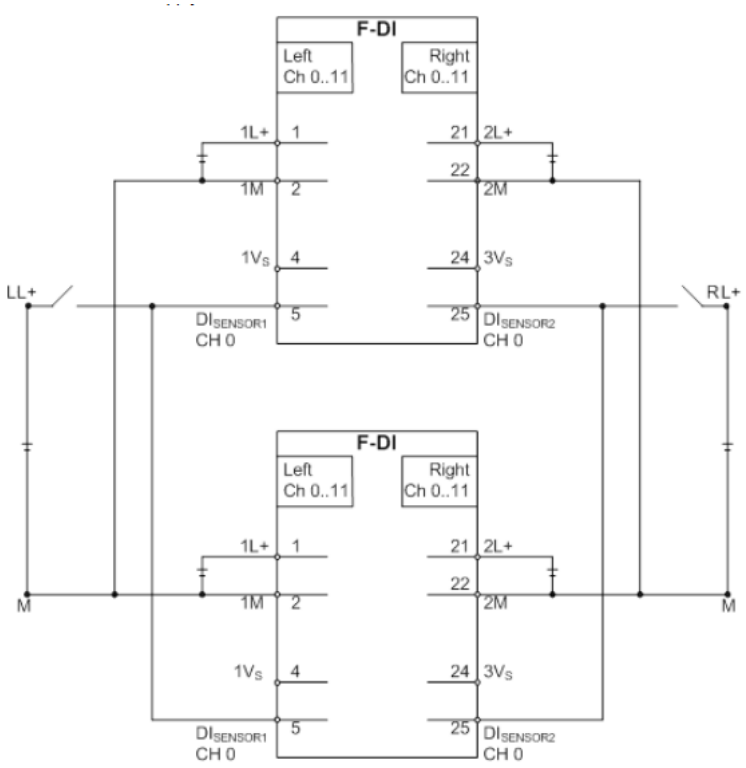
[28] Στην συγκεκριμένη διαμόρφωση υλικού η CPU μπορεί να κρίνει ποια από τις δύο F-Di είναι περιττή με τη χρήση εκτίμησης 2oo2. Οι αισθητήρες χρησιμοποιούνται και στα δύο F-Di καθώς συνδέονται στα 0 κανάλια και των δύο. Η κάθε είσοδος F-Di πραγματοποιεί εκτίμηση 1oo2 λαμβάνοντας σήμα από τα αισθητήρια και ύστερα μέσω της CPU κρίνεται ποια από τις δύο εισόδους θα χρησιμοποιηθεί στη λογική για την ασφάλεια.



[28] Εικόνα 16: Απεικόνιση δύο αισθητήρων (1oo2) με δύο εισόδους F-Di(2oo2) με εκτίμηση.

Για να μπορέσει το πρόγραμμα να τεθεί σε ασφαλή λειτουργία κατά τη βλάβη κάποιου στοιχείου, πρέπει να υπάρχει βλάβη είτε στον πρώτο αισθητήρα είτε στον δεύτερο καθώς και αν έχουμε ελλαττωματικές και τις δύο εισόδους F-Di1,2. Ο υπολογισμός της πιθανότητας παρουσίασης βλάβης υπολογίζεται ως εξής: PFDein = PFDsensor + 2PFDfdi + PFDcpu. Το PFDsensor υπολογίζεται όπως στην προηγούμενη περίπτωση ενώ τα άλλα δύο παραμένουν ίδια.

Κατά τη συνδεσμολογία παρατηρείται πως γίνεται χρήση μόνο εξωτερικής πηγής η οποία τροφοδοτεί και τα δύο αισθητήρια με τους ακροδέκτες LL+ & RL+ στα 0 κανάλια και των δύο F-Di.

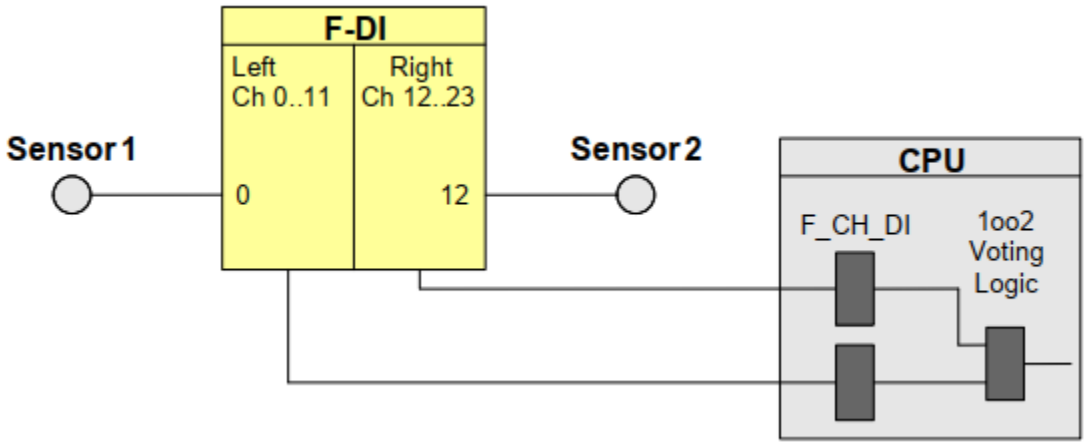


[28] Εικόνα 17: Απεικόνιση του κυκλώματος και τροφοδοσίας αισθητηρίων μέσω εξωτερικής πηγής.

3.11 ΔΙΑΜΟΡΦΩΣΗ ΥΛΙΚΟΥ ΜΕ ΔΥΟ ΑΙΣΘΗΤΗΡΕΣ(1oo2) ΜΕ ΕΚΤΙΜΗΣΗ ΣΤΟ ΠΡΟΓΡΑΜΜΑ ΧΡΗΣΤΗ

[28] Στη συγκεκριμένη περίπτωση χρησιμοποιείται αξιολόγηση 1oo2 για εφαρμογές που απαιτούν δύο αισθητήρια για την επιτυχία της αυξημένης ασφάλειας. Η αξιολόγηση πραγματοποιείται στην CPU η οποία χρησιμοποιεί δύο εισόδους για να διευκολύνεται η διάγνωση σε περίπτωση εμφάνισης κάποιας βλάβης. Η διαμόρφωση της συγκεκριμένης διάταξης πραγματοποιείται με δύο τρόπους, είτε με μία F-Di ή με δύο F-Di.

Όσον αφορά τη διαμόρφωση με μια F-Di και τα δύο αισθητήρια συνδέονται πάνω στο F-Di, το πρώτο στο κανάλι 0 της αριστερής πλευράς παρομοίως το δεύτερο στης δεξιάς πλευράς. Ύστερα από το F-Di φεύγουν δύο έξοδοι και μπαίνουν στις δύο εισόδους της CPU. Η λογική του προγράμματος για ασφάλεια ενεργοποιείται μόλις παρουσιαστεί βλάβη είτε στον πρώτο αισθητήρα είτε στον δεύτερο είτε στην F-Di. Ο υπολογισμός της πιθανότητας βλάβης υπολογίζεται : PFDein = PFDsensor + PFDfdi + PFDcpu, ενώ τα υπόλοιπα παραμένουν ίδια με την προηγουμένη περίπτωση. Επίσης, η συγκεκριμένη αρχιτεκτονική υποστηρίζει συστήματα μέχρι SIL 3 κάτω.

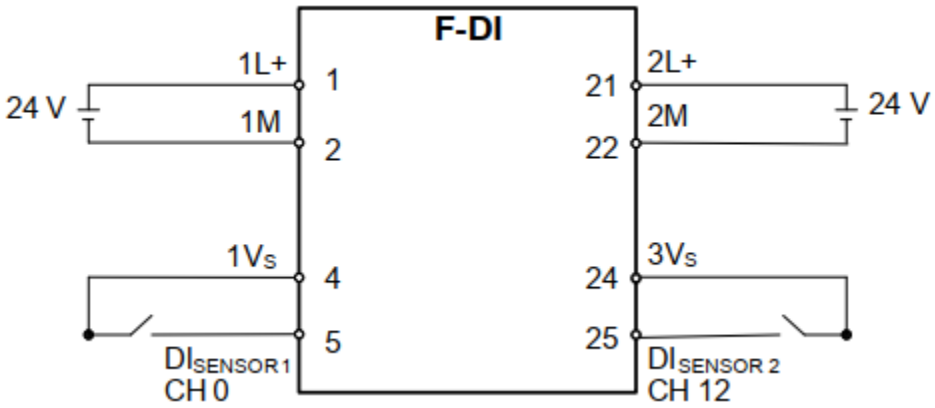


[28] Εικόνα 18: Απεικόνιση συστήματος δύο αισθητηρίων(1oo2) με χρήση μίας F-Di και αξιολόγηση μέσω χρήστη.

Στη δεύτερη περίπτωση γίνεται χρήση δύο F-Di στις οποίες συνδέονται τα αισθητήρια στη κάθε μια από ένα και στις εξόδους των F-Di συνδέονται τα F_CH_DI της CPU. Για να ενεργοποιηθεί αυτόματα η ασφαλή λειτουργία του προγράμματος, πρέπει να παρουσιαστεί βλάβη σε κάθε μια F-Di ή αισθητήριο ξεχωριστά. Όσον αφορά τη πιθανότητα κάποιας βλάβης που υπολογίζεται με μαθηματικές εξισώσεις υπάρχουν αρκετές αλλαγές στην προκειμένη περίπτωση. PFDein = (PFDsensor + PFDfdi)1oo2 + PFDcpu.

Το PFDsensor,fdi = PFDsensor + PFDfdi. Το (PFDsensor + PFDfdi)1oo2 = $(\frac{4}{3} \times \text{PFDsensor, fdi}^2)$ + $(\beta \times \text{PFDsensor, fdi})$. Τέλος, το PFDsensor = $\lambda du \times \frac{T1}{2}$.

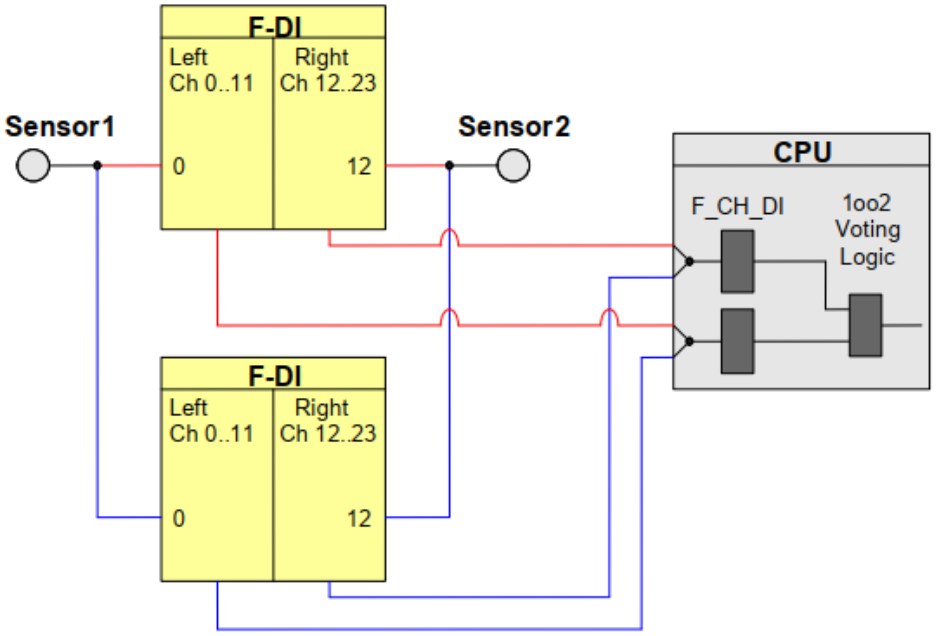
Η συνδεσμολογία της δεύτερης περίπτωσης γίνεται με χρήση εσωτερικής πηγής 24v η οποία τροφοδοτεί και τους δύο αισθητήρες. Στο 1Vs συνδέεται το πρώτο αισθητήριο και στο κανάλι 0, ενώ το δεύτερο στην επαφή 3Vs και κανάλι 12, ενώ το ίδιο το F-Di τροφοδοτείται από τις 1L+,1M στο αριστερό μέλος και δεξιά το 2L+,2M.



[28] Εικόνα 19 : Συνδεσμολογία τροφοδοσίας 1oo2 με εκτίμηση της CPU.

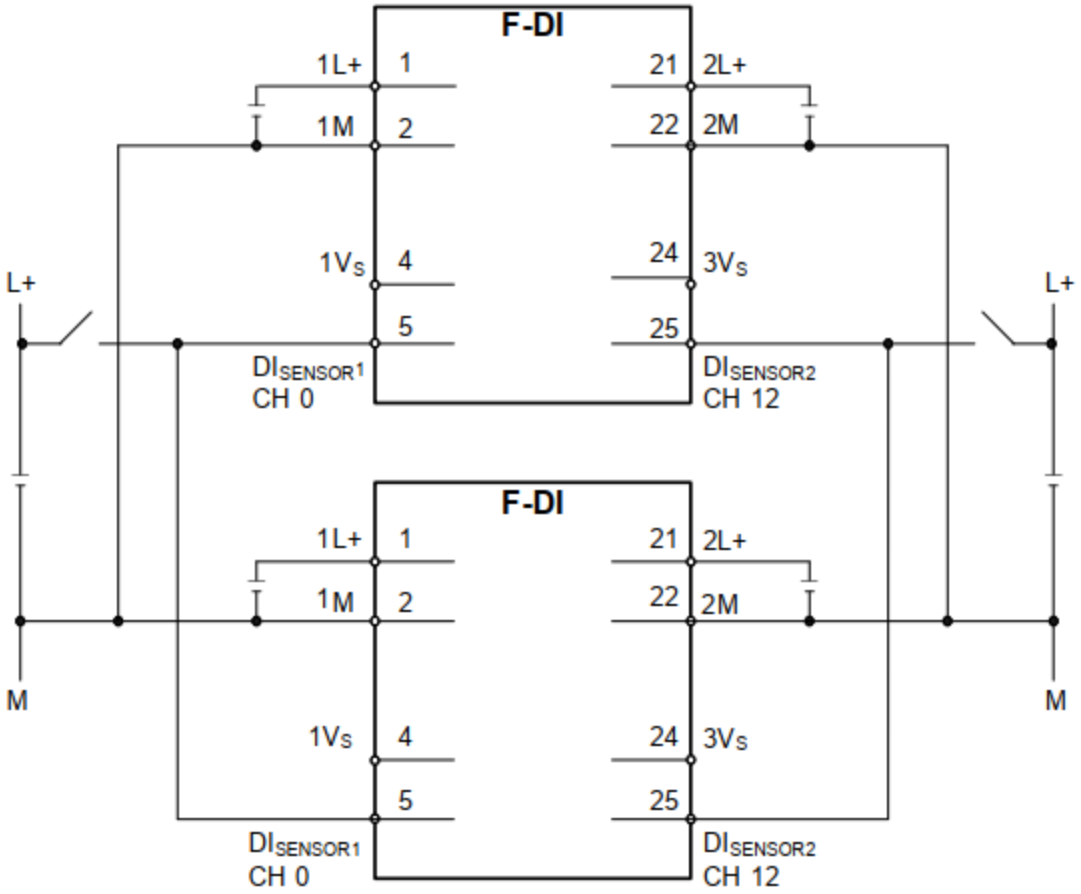
3.12 ΔΙΑΜΟΡΦΩΣΗ ΥΛΙΚΟΥ ΜΕ ΧΡΗΣΗ ΔΥΟ ΑΙΣΘΗΤΗΡΩΝ ΔΥΟ F-DI ΚΑΙ ΕΚΤΙΜΗΣΗ ΜΕΣΩ CPU

[28] Στην προκειμένη διαμόρφωση υλικού γίνεται χρήση δύο αισθητήρων που συνδέονται παράλληλα και στις δύο F-Di. Το πρόγραμμα που χρησιμοποιείται έχει ως λογική να λαμβάνει διαφορετικό οδηγό F_CH_DI για κάθε αισθητήρα ως σήμα.



[28] Εικόνα 20: Απεικόνιση συστήματος με δύο αισθητήρια(1oo2) παράλληλα στα δύο F-Di με εκτίμηση μέσω CPU.

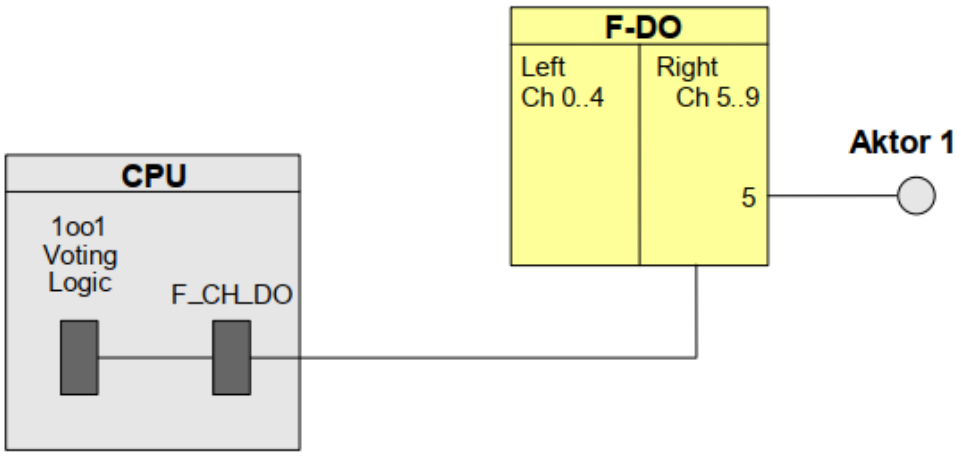
Η λογική του προγράμματος ξεκινάει να λειτουργεί μόλις εντοπιστεί κάποιο σφάλμα σε ένα από τα δύο αισθητήρια είτε στις δύο F-Di συγχρόνως. Για τον υπολογισμό χρησιμοποιείται η εξής μαθηματική εξίσωση: PFDein = PFDs + 2PFDfdi + PFDcpu. Οι PFDfdi και PFDcpu υπολογίζονται με σταθερές τιμές που είχαν προαναφερθεί στις αρχικές αρχιτεκτονικές, ενώ το PFDs όπως την προηγούμενη περίπτωση. Η συνδεσμολογία πραγματοποιείται μόνο με τη χρήση εξωτερικής πηγής η οποία τροφοδοτεί τα αισθητήρια στα κανάλια 0 και 12 της κάθε F-Di.



[28] Εικόνα 21: Συνδεσμολογία κυκλώματος 1oo2 με περιττή F-Di καθώς και χρήση CPU ως εκτιμητή.

3.13 ΔΙΑΜΟΡΦΩΣΗ ΥΛΙΚΟΥ ΜΕ ΧΡΗΣΗ ΕΝΕΡΓΟΠΟΙΗΤΩΝ

[28] Όπως τα συστήματα εισόδων, έτσι και τα συστήματα εξόδων υπάρχουν συνδυασμοί αυτών για την αξιολόγηση. Όλοι οι ενεργοποιητές λειτουργούν ανάλογα με τη λογική πίσω από το πρόγραμμα ασφάλειας. Υπάρχουν αρκετά είδη σχηματισμών των ενεργοποιητών ανάλογα την ανάγκη, πχ 1oo1, 2oo2 ή 1oo3. Η πιο απλή περίπτωση είναι με τη χρήση μιας εξόδου F-Do η οποία προηγείται από την CPU που καθορίζει τα σήματα και τις λογικές του προγράμματος. Η 1oo1 μπορεί να καλύψει μέχρι και SIL 3.

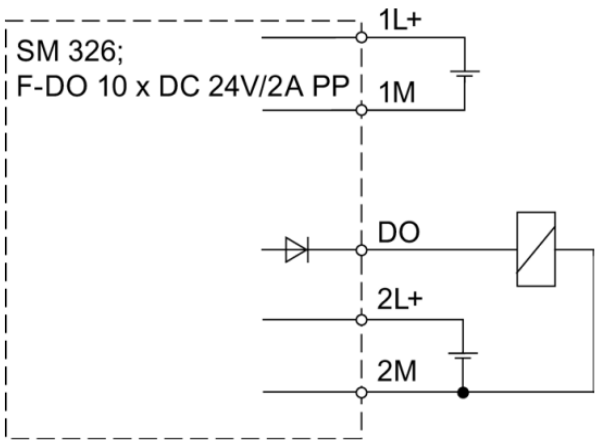


[28] Εικόνα 22: Αρχιτεκτονική με χρήση μιας F-Do 1oo1.

Με τη χρήση των εξόδων αυτών, είναι δυνατό να παρακολουθείται πάνω στο safety PLC οι ενδείξεις οι οποίες αναφέρονται στη σωστή λειτουργία όσον αφορά την ¨ασφαλή λειτουργία¨ του προγράμματος καθώς και τις διάφορες βλάβες που μπορεί να προκύψουν κατά τη διαδικασία χρήσης. Επίσης, πίσω από αυτές τις ενδείξεις γίνονται και όλες οι κατάλληλες συνδεσμολογίες των εξόδων και τροφοδοσίας αυτών. Σε κάθε ενεργοποιητή της F-Do τροφοδοτείται 24Vdc. Όπως στις F-Di έτσι και στις F-Do υπάρχει μέθοδος υπολογισμού της πιθανότητας βλάβης και βρίσκεται με τον εξής τρόπο:

PFDout = PFDfdo + PFDfinal element, όπου το PFDfdo είναι μια σταθερά περίπου $< 1E^{-5}$ και το PFDfinal element = λdu$\times \frac{T1}{2}$.

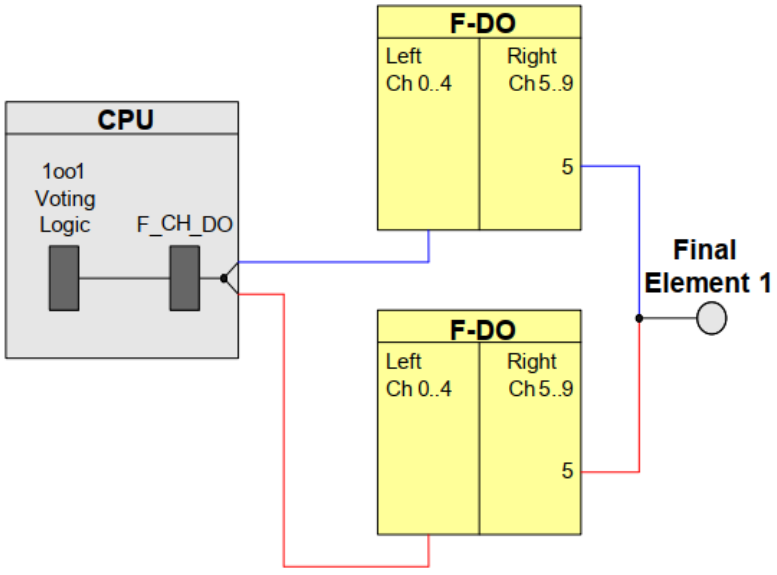
Για την τροφοδοσία της F-Do, χρησιμοποιούνται οι ακροδέκτες 1L+/1M, ενώ η τροφοδοσία του φορτίου τάσης του αριστερού καναλιού γίνεται στο 2L+/2M.



[28] Εικόνα 23: Συνδεσμολογία κυκλώματος F-Do.

3.14 ΔΙΑΜΟΡΦΩΣΗ ΥΛΙΚΟΥ ΜΕ ΧΡΗΣΗ ΕΝΟΣ ΕΝΕΡΓΟΠΟΙΗΤΗ ΚΑΙ ΔΥΟ F-Do

[28] Η συγκεκριμένη διαμόρφωση χρησιμοποιείται για μεγαλύτερη διαθεσιμότητα εξόδων καθώς και η χρήση του ενεργοποιητή ελέγχεται με το ζεύγος των εξόδων. Χρησιμοποιώντας την F_CH_DO της CPU είναι δυνατή η μετάδοση του σήματος στις F-Do. Ο ενεργοποιητής συνδέεται στις δύο F-Do στα κανάλια 5.



[28] Εικόνα 24: Αρχιτεκτονική με δύο F-Do.

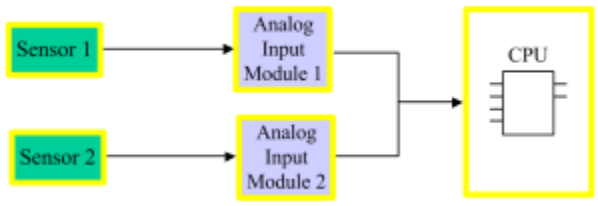
Τέλος, το PFD υπολογίζεται με τις ίδιες παραμέτρους της προηγούμενης περίπτωσης αλλά αλλάζει ο γενικός τύπος: PFDout = 2PFDfdo + PFDfe. Παρομοίως, με την συνδεσμολογία της προηγούμενης περίπτωσης

πραγματοποιείται η συνδεσμολογία του κυκλώματος παρά μόνο με τη διαφορά ενός παραπάνω F-Do.

3.15 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΝΑΛΟΓΙΚΩΝ ΕΙΣΟΔΩΝ

[29] Έχοντας μια αναλογική είσοδο, υπάρχει διαφορά από μια ψηφιακή όπως έγινε μεγάλη αναφορά προηγουμένως και αυτό οφείλεται στον τρόπο που λαμβάνει το σήμα. Μια αναλογική είσοδος μπορεί να λάβει πχ 4-20mAmp ή 0-10 volt dc. Αυτό σημαίνει πως το PLC δεν λαμβάνει σταθερά μια τιμή διότι οι τιμές μιας θερμοκρασίας ή η στάθμη νερού μιας δεξαμενής αλλάζουν ανάλογα με τις καταστάσεις, κάτι που ενδεικτικά θα αλλάξει και τις τιμές τάσεων κ ρευμάτων στις αναλογικές εισόδους τους. Το PLC είναι γνωστό πως μπορεί να διαβάσει μόνο 0 κ 1 με αποτέλεσμα να μην είναι εύκολη η μετάφραση ενδιάμεσων τιμών 0-10volt ή 4-20 m A. Το αναλογικό σήμα μπορεί να μεταφραστεί με τη βοήθεια ενός μετατροπέα A/D, ο οποίος θα λάβει το αναλογικό σήμα και με τη βοήθεια των ψηφιακών στοιχείων bits θα μεταφραστεί το σήμα σε ψηφιακό για να αντιληφθεί το PLC τι ακριβώς λαμβάνει στην είσοδό του. Τη συγκεκριμένη λειτουργία πραγματοποιεί και σε εφαρμογές όπως αισθητήρια θερμοκρασίας, αντιστάσεις τύπου ποτενσιόμετρο του οποίου η τιμή μπορεί να μεταβληθεί, σε επαγωγικούς αισθητήρες με τους οποίους είναι δυνατή η μέτρηση απόστασης από ένα μεταλλικό αντικείμενο, άρα με τάση-ρεύμα να μεταδοθεί ένα σήμα στην αναλογική είσοδο του controller.

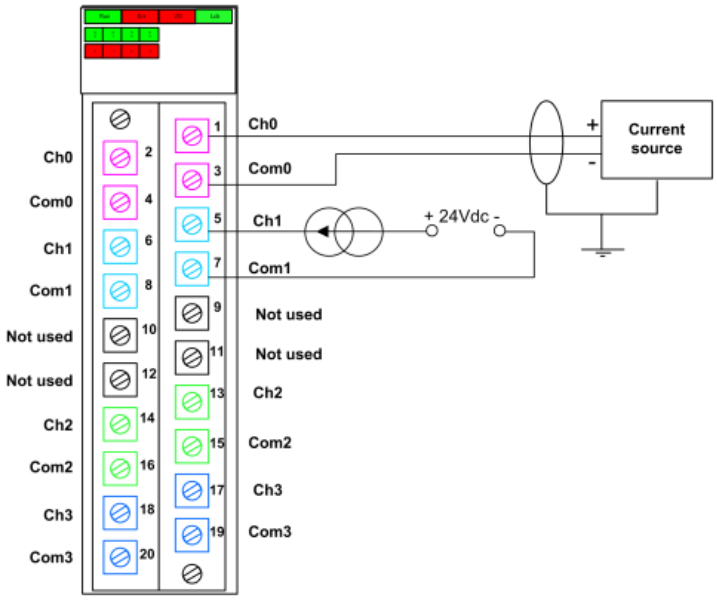
Πιο συγκεκριμένα, το Module x80 της Schneider electric, είναι ένα σύστημα αναλογικών εισόδων κ εξόδων που διαχειρίζεται διάφορες τιμές όπως πίεση, θερμοκρασία, κενό αέρος και αντιστάσεις. Οι έξοδοι βγάζουν τιμές σημάτων για την διαχείριση του τελευταίου στοιχείου, όπως ηλεκτρονικές βαλβίδες, τρόμπες-αντλίες, ενεργοποιητές κλπ. Το συγκεκριμένο module χρησιμοποιεί 4 αναλογικές εισόδους των 4-20mAmp και βάση το πρότυπο IEC 61508 μπορεί να καλύψει εφαρμογές έως και SIL3 σε θέμα ασφάλειας.



[29] Εικόνα 25: Απεικόνιση λογικής αναλογικών εισόδων

Στη παραπάνω *εικόνα φαίνεται ο τρόπος λειτουργίας του συστήματος διαχείρισης αναλογικών εισόδων. Όταν το πρώτο αισθητήριο μπορεί και παραδίδει δεδομένα εντός των ορίων όπου έχει ρυθμιστεί το PLC να δέχεται για να λειτουργεί, τότε χρησιμοποιείται η πρώτη αναλογική είσοδος προς επεξεργασία. Εάν υπάρξει κάποια βλάβη ή κάποιο λανθασμένο δεδομένο που εισέρχεται στο πρώτο module, αλλά το δεύτερο διαβάζει σωστά, τότε η CPU χρησιμοποιεί αυτό για επεξεργασία. Αν και τα δύο module δεν λαμβάνουν σωστά δεδομένα, τότε ενεργοποιείται η λειτουργία ασφάλειας με την οποία σειρά της θα ασφαλίσει το PLC το οποίο θα απενεργοποιήσει κάποιο μηχάνημα από πιθανή επικίνδυνη κατάσταση.*

Όσον αφορά τη συνδεσμολογία αυτού του module, έχει τέσσερις αναλογικές εισόδους στις οποίες κάθε είσοδος αποτελεί ένα ζεύγος θετικών Pin (Chanel) και ένα ζεύγος αρνητικών (Com). Σε αυτές τις εισόδους είναι δυνατή και η σύνδεση των διαφόρων αναλογικών αισθητηρίων που προαναφέρθηκαν.

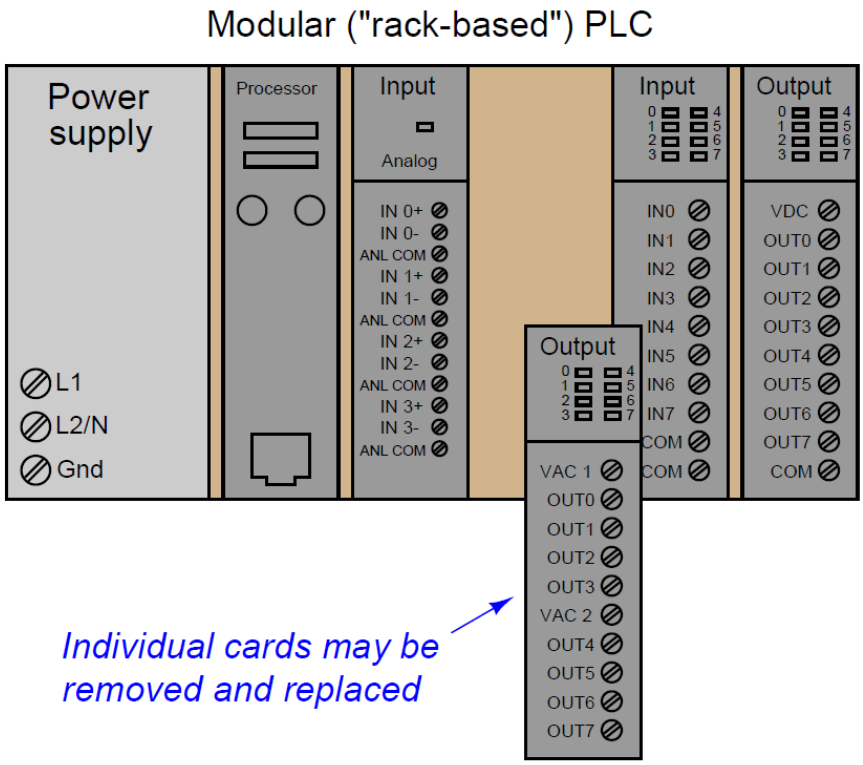


[29] Εικόνα 26: Συνδεσμολογία κυκλώματος του block αναλογικών εισόδων της Schneider.

Παραπάνω είναι μια μικρή αναπαράσταση για το πως μπορεί να πραγματοποιηθεί κάποια συνδεσμολογία ενός αισθητήρα, δηλαδή θα χρησιμοποιηθεί για παράδειγμα το CH2 και COM2 με Pin 13-15 στα οποία το 13 θα δώσει θετική τάση και το 15 θα το ενώσει με την αρνητική.

3.16 PLC MODULE I/O

[30] Βάση των παραπάνω πληροφοριών ένα PLC μπορεί να χρησιμοποιήσει ψηφιακά και αναλογικά bus ταυτόχρονα με τα οποία θα συνδεθούν όλα τα αναγκαία αισθητήρια με τα οποία το controller θα λαμβάνει πληροφορίες για να μπορεί να πράξει ανάλογα με τα 0-1 για ψηφιακά και 0-5volt για αναλογικά σήματα.



[30] Εικόνα 27: Απεικόνιση του bus εισόδων/εξόδων πάνω σε ένα τυπικό PLC.

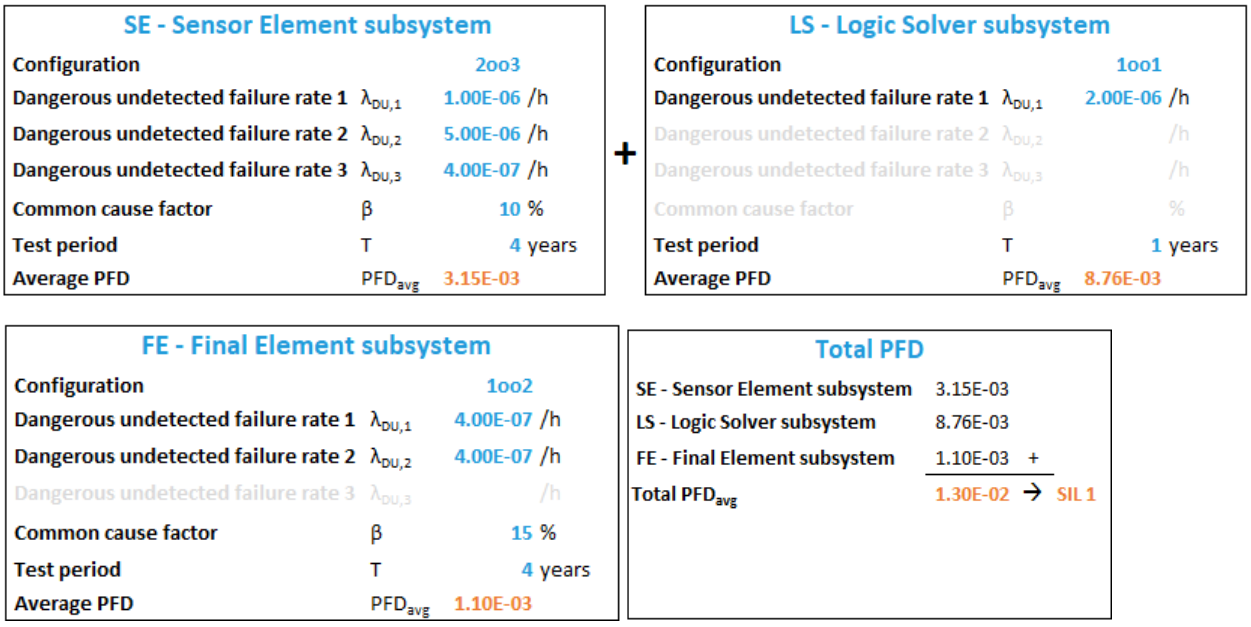
Στις αναλογικές εισόδους μπορούν να συνδεθούν αισθητήρες θερμοκρασίας, υγρασίας, ροής, μετρητές τάσης/ρεύματος και διάφορους αναμεταδότες ρεύματος. Παράλληλα στις ψηφιακές εισόδους μπορούν να συνδεθούν διάφορα push buttons είτε αυτά είναι για εκκίνηση/διακοπή, για έκτακτη ανάγκη κλπ. Επίσης, μπορούν να συνδεθούν όλων των διαφόρων τύπων ρελέ για τον έλεγχο και την προστασία του συστήματος, όπου σε σειρά είναι δυνατή η συνδεσμολογία ενός περιοριστή τάσης. Είναι πολύ απλή η σύνδεση αυτών των συσκευών πάνω στο PLC διότι είναι αρκετά κατανοητό εφόσον το κάθε bus που συνδέεται πάνω στο rack έχει αναγραφόμενη την ονομασία Analog και Digital. Όσον αφορά τις εξόδους, είναι πιο απλή η συνδεσμολογία των μοτέρ, λαμπών κλπ. αφού συνδέονται πάνω στα out

ανάλογα αν είναι AC ή DC. Το VAC/DC είναι τροφοδοσία των εξόδων και το out είναι εκεί που θα συνδεθεί κάποιο μοτέρ ή κάποια φωτεινή ένδειξη.

3.17 PFD CONSILATOR

[31] Προηγουμένως, έγινε αναφορά του SIL και του PFD σε κάθε κατηγορία αρχιτεκτονικής, τα οποία μπορούν να δείξουν πόσο ασφαλές είναι το σύστημα που χρησιμοποιείται και ποιες πιθανότητες υπάρχουν στην εμφάνιση κάποιας βλάβης. Υπάρχουν διάφορα λογισμικά και εφαρμογές που μπορούν να τα υπολογίσουν αυτόματα, αλλά χρειάζεται να τοποθετήσουμε κάποια στοιχειώδη δεδομένα έτσι ώστε να μας δείξει σε τί SIL ¨βρισκόμαστε¨.

Το PFD CONSILATOR της CONSILTANT, μπορεί να πραγματοποιήσει αυτές τις λειτουργίες και βάση των χαρακτηριστικών πχ μιας μηχανής, είναι δυνατός ο υπολογισμός του SIL & PFD. Η λογική πίσω από αυτόν τον solver είναι η πρόσθεση όλων των υποσυστημάτων που αποτελούνται από αισθητήρια, λογική προγράμματος και τελικού στοιχείου. Το κάθε υποσύστημα βγάζει ένα μέσο PFD και στο τέλος προστίθενται μεταξύ τους για το ολικό.



[31] Εικόνα 28: Πρόσθεση των τριών υποσυστημάτων του consilator και το αποτέλεσμα.

Παραπάνω, φαίνονται τρία πινακάκια που απεικονίζουν το κάθε υποσύστημα ξεχωριστά. Στο πρώτο πινακάκι ασχολείται με τους αισθητήρες

όπου επιλέγουμε πόσους χρησιμοποιούνται στο σύστημα πχ 1oo2 δύο αισθητήρες, μετά εισάγουμε τις πιθανότητες εμφάνισης επικίνδυνης κατάστασης όσον αφορά τον εξοπλισμό, ύστερα εισάγεται ο παράγοντας κοινής αιτίας, ο οποίος αυτός υπολογίζεται βάση το ποσό των αισθητηρίων που χρησιμοποιεί το σύστημα και της βοήθειας του πίνακα D.5 του προτύπου IEC 61508. Επίσης, πρέπει να εισαχθούν και τα στοιχεία που απεικονίζουν πόσο καιρό θα γίνει δοκιμή του συστήματος, το ποσό κάλυψης όσον αφορά την απόδειξη δοκιμής. Από όλες αυτές τις πληροφορίες βγαίνει μια μέση τιμή του PFDaverage της κάθε περίπτωσης και τέλος προστίθενται όλα μαζί όπου και υπολογίζεται αυτόματα το SIL που ανήκει το ολικό σύστημα. Το SIL εννοείται πως μπορεί να αυξηθεί αν τεθούν κατάλληλοι μέθοδοι υπό λειτουργία. Παρακάτω θα πραγματοποιηθεί ένα μικρό παράδειγμα για να δούμε σε τί SIL θα βρισκόμαστε με τις ανάλογες αρχιτεκτονικές.

Κάνοντας μια υπόθεση πως γίνεται χρήση αρχιτεκτονικής 1oo2 όσον αφορά τους αισθητήρες (δύο αισθητήρες) και αυτοί οι δύο αισθητήρες έχουν μια μηδαμινή πιθανότητα να παρουσιάσουν κάποια επικίνδυνη βλάβη μέσα σε χρονικό διάστημα του ενός έτους που θα πραγματοποιηθούν οι δοκιμές και βάση του στοιχείου β (παράγοντας κοινής αιτίας που υπολογίζεται αυτόματα βάση της πιθανότητας βλάβης δύο ή περισσοτέρων αισθητήρων) θα έχουμε ένα μέσο όρο περίπου 5.4^{-8} PFD συστημάτων αισθητήρων. Τώρα προστίθεται και το υποσύστημα του ενός λογικού ελεγκτή που θα λαμβάνει τα σήματα των αισθητήρων. Η πιθανότητα βλάβης του ελεγκτή έχει τεθεί 1^{-6}/h με δοκιμαστικό χρόνο ενός έτους, τότε θα υπολογιστεί ο μέσος όρος του PFD 4.38^{-3} για το υποσύστημα αυτό. Τέλος, υπάρχει και το υποσύστημα ενός ενεργοποιητή που παρουσιάζει πιθανότητα βλάβης 6^{-10}/h σε χρονικό διάστημα ενός έτους υπολογίζεται το PFD περίπου 2.63^{-6} . Αν γίνει πρόσθεση των τριών M.O θα παρουσιαστεί πως το ολικό σύστημα βρίσκεται σε SIL 2, κάτι που το καθιστά σχετικά επικίνδυνο και θα χρειαστεί να χρησιμοποιηθούν περισσότερα αισθητήρια και διάφορα είδη για να μπορέσει το σύστημα να είναι ασφαλέστερο προς του εργαζομένους και τη μείωση παρουσίασης βλαβών.

ΕΠΙΛΟΓΟΣ

Με τη λέξη πρότυπο δηλώνουμε το έγγραφο με το οποίο εξασφαλίζονται κάποια συγκεκριμένα στάνταρ σε μια βιομηχανία και όχι μόνο. Για να μπορεί κάποια εταιρία να συμβαδίζει με τις οδηγίες και τις απαιτήσεις του προτύπου που επιθυμεί να χρησιμοποιήσει, είναι υποχρεωτικό να καλύπτει κάποιες προϋποθέσεις. Παραπάνω παρουσιάστηκαν οι δύο βασικές ναυαρχίδες των προτύπων ασφάλειας, η ISO και IEC. Κάθε οργανισμός μπορεί να παρέχει διαφορετικού είδους πρότυπα όσον αφορά την ασφάλεια και γι' αυτό είναι σημαντικό σε μια βιομηχανία να βλέπουμε την τήρηση πολλών από τα πρότυπα αυτά, διότι όσο περισσότερα πρότυπα μπορεί και καλύπτει τόσο μεγαλύτερη και πιο ελεγχόμενη θα είναι η ασφάλεια χρήσης μηχανημάτων αλλά και σε περιπτώσεις κινδύνου να μην τραυματιστεί κάποιος εργαζόμενος. Το κάθε πρότυπο έχει τη δυνατότητα να εστιάσει την ασφάλεια σε συγκεκριμένα μέρη μιας παραγωγής, όπως κάποια ασχολούνται με τις ίδιες τις μηχανές, άλλα μπορούν και εστιάζουν στην επικοινωνία των μηχανημάτων με τις κεντρικές μονάδες επεξεργασίας δεδομένων, όπου κι αυτές οι μονάδες έχουν σημαντικό ρόλο στον εντοπισμό κάποιου προβλήματος αλλά και τον περιορισμό του ίδιου του κινδύνου. Άρα, τα πρότυπα ασφάλειας όπως και οι διάφορες περιφερειακές συσκευές έχουν ως προκαθοριστικό σκοπό να δώσουν στον εργαζόμενο έναν ασφαλή χώρο εργασίας στον οποίο τα πάντα θα είναι ελεγχόμενα και σε καταστάσεις επικινδυνότητας να μπορούν να τον κατευθύνουν έτσι ώστε να μην υπάρχουν άσχημες καταλήξεις για τον ίδιον-α αλλά και τα μηχανήματα τα οποία παρέχουν σημαντικά μέλη σε μια βιομηχανική παραγωγική.

ΠΑΡΑΠΟΜΠΕΣ

Σε αυτή τη λίστα αναφέρονται όλα τα παραδείγματα επιστημονικού υποβάθρου που χρησιμοποιήθηκαν κατά τη δημιουργία της εργασίας(επιστημονικές ομάδες, άρθρα, βιβλία, εκδότες) και στους οποίους ανήκουν τα πνευματικά δικαιώματα αποκλειστικά.

[1] SICK Sensor Intelligence: Selecting Safety Standards for Machine Safeguarding Requirements.

[2] MTL Instruments Group plc: An introduction to Functional Safety and IEC 61508 (2002).

[3] *Control Systems Safety Evaluation and Reliability*. ISA. (2010). ISBN 978-1-934394-80-9.

[4] E. Theocharis, M. Papoutsidakis, C. Drosos, G. Chamilothoris: Safety Standards in Industrial Applications: A Requirement for Fail-Safe Systems (2019).

[5] Bernd Schrörs: Functional Safety: IEC 61511 and the industrial Implementation.

[6] Wikipedia: IEC 61511 (2017).

[7] A G Foord, W G Gulland, C R Howard, T Kellacher, W H Smith (4-sight Consulting): Applying the latest standard for Functional Safety – IEC 61511.

[8] Functional Safety: Compliance with IEC 61511 (2019).

[9] Johan Hedberg, Andreas Söderberg, Jan Tegehall: How to design safe machine control systems – a guideline to EN ISO 13849.

[10] Daniel DesRuisseaux: Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications.

[11] Atkins Ltd, UK: Development of industrial cyber security standards, IEC 62443 for Scada and Industrial control system security.

[12] Martin J. Rosernstrauch, Jörg Krüger: Safe Human-Robot-Collaboration-Introduction and Experiment Using ISO/TS 15066 (2017).

[13] GM International: ISO 12100 definitions and steps in assessing the safety of machinery (2019).

[14] Ariffuddin Aizuddin: The Common Criteria ISO/IEC 15408- The insight, some thoughts, questions and issues (2001).

[15] Oleksandr Potii, Oleg Illiashenko, Dmitry Komin: Advanced security assurance case based on ISO/IEC 15408 (2015).

[16] EATON Powering Business Worldwide: Safety technology for machines and systems in accordance with international standards EN ISO 13849-1 and IEC 62061 (2019).

[17] Joachim Feld Siemens AG: Profinet – Scalable Factory Communication for All Applications (2004).

[18] Jami Sivén: Securing Profinet Networks, Par 5(11 May 2015).

[19] J.Rofár, M.Franeková: Functional Safety Specification of Communication Profile Profisafe.

[20] Michael Bowne: The Difference Between Profinet and Profisafe (Dec 3, 2020). Link: https://us.profinet.com/the-difference-between-profinet-and-profisafe.

[21] Power Transmission World: PROfisafe module for increased safety (photo).

[22] RealPars: What is AS-Interface?

(video: https://www.youtube.com/watch?v=S97rhReEnbo).

[23] Global Spec Engineering 360: Safety Relays Information(photo).

[24] Galco: Operating a Safety Relays(photo).

[25] Pilz: Safety timer relays, Pza (10/2009).

[26] Realpars: What is a Safety PLC (6/2020).

[27] Mingshi Li: Design of Safety PLC Execution Unit Based on Redundancy Structure of Heterogeneous Dual-Processor (October 2019).

[28] SIEMENS: Wiring and Voting Architectures for failsafe Digital Input(F-Di) and Output Modules(F-Do) of the ET 200M (2018).

[29] Schneider Electric: Modicom M580 Safety Manual, BMXSAI0410 Analog Input Module.

[30] Inst Tools by Editorian Staff: PLC Input Output Modules.

[31]CONSILANT:PFD Calculator (https://www.consiltant.com/en/tool/pfd-calculator/).