ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

Σχολή Μηχανικών
Τμήμα Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής

PHD THESIS

Ανάπτυξη αλγορίθμων σε PLC για Fail-Safe συστήματα

Ευστάθιος Θεοχάρης

Αθήνα
Ιανουάριος 2024

Επιτροπή Διατριβής

Η παρούσα διπλωματική εργασία εγκρίθηκε ομόφωνα από την τριμελή επιτροπή αξιολόγησης, που ορίστηκε από τη Γενική Συνέλευση του Τμήματος Βιομηχανικού Σχεδιασμού και Μηχανικών Παραγωγής του Πανεπιστημίου Δυτικής Αττικής, σύμφωνα με το νόμο και τον εγκεκριμένο Οδηγό Σπουδών του τμήματος.

Επιβλέπων: Μιχαήλ Παπουτσιδάκης, Καθηγητής

Μέλη της Τριμερούς Συμβουλευτικής Επιτροπής συμπεριλαμβανομένου του Επιβλέποντα:

Digitally signed by Michail Papoutsidakis
Date: 2024.03.14 11:20:17 +02'00'

Georgios Chamilothoris
2024.03.14 19:45:53 +02'00'

Dimitrios Dimogiannopoulos
Digitally signed by Dimitrios Dimogiannopoulos
Date: 2024.03.14 12:57:14 +02'00'

Μιχαήλ Παπουτσίδακης	Γεώργιος Χαμηλοθώρης	Δημήτριος Δημογιαννόπουλος
Καθηγητής	Καθηγητής	Αναπληρωτής Καθηγητής
Επιβλέπων	Μέλος Επιτροπής	Μέλος Επιτροπής
Τμήμα Βιομηχανικής Σχεδίασης και Παραγωγής Πανεπιστήμιο Δυτικής Αττικής	Τμήμα Μηχανολόγων Μηχανικών Σχεδίασης και Παραγωγής Πανεπιστήμιο Δυτικής Αττικής	Τμήμα Βιομηχανικής Σχεδίασης και Παραγωγής Πανεπιστήμιο Δυτικής Αττικής

Μέλη της επταμελούς Εξεταστικής Επιτροπής:

α/α	Ονοματεπώνυμο	Βαθμός/Επαγγελματικός τίτλος/Τμήμα/Σχολείο/Πανεπιστήμιο
1	Μιχαήλ Παπουτσίδακης	Καθηγητής / Τμήμα Βιομηχανικής Σχεδίασης και Παραγωγής / Σχολή Μηχανικών / Πανεπιστήμιο Δυτικής Αττικής
2	Γεώργιος Χαμηλοθώρης	Καθηγητής / Τμήμα Μηχανολόγων Μηχανικών / Σχολή Μηχανικών / Πανεπιστήμιο Δυτικής Αττικής
3	Δημήτριος Δημογιαννόπουλος	Αναπληρωτής Καθηγητής / Τμήμα Βιομηχανικής Σχεδίασης και Παραγωγής / Σχολή Μηχανικών / Πανεπιστήμιο Δυτικής Αττικής
4	Παρασκευή Ζαχαρία	Επίκουρη Καθηγήτρια / Τμήμα Μηχανολόγων Μηχανικών / Σχολή Μηχανικών / Πανεπιστήμιο Δυτικής Αττικής
5	Χαράλαμπος Πατρικάκης	Καθηγητής του Τμήματος Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών / Πανεπιστήμιο Δυτικής
6	Δημήτριος Φραγκούλης	Επίκουρος Καθηγητής του Τμήματος Τεχνολογιών Ψηφιακής Βιομηχανίας του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών
7	Ηλίας Ξυδιάς	Επίκουρος Καθηγητής Τμ. Μηχανικών Σχεδίασης Προϊόντων και Συστημάτων, Πανεπιστήμιο Αιγαίου

Δήλωση _Συγγραφέα _Διδακτορικής _Διατριβής

Ο κάτωθι υπογεγραμμένος Θεοχάρης Ευστάθιος του Κωνσταντίνου υποψήφιος διδάκτορας του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι: «Είμαι συγγραφέας και δικαιούχος των πνευματικών δικαιωμάτων επί της διατριβής και δεν προσβάλλω τα πνευματικά δικαιώματα τρίτων. Για τη συγγραφή της διδακτορικής μου διατριβής δεν χρησιμοποίησα ολόκληρο ή μέρος έργου άλλου δημιουργού ή τις ιδέες και αντιλήψεις άλλου δημιουργού χωρίς να γίνεται αναφορά στην πηγή προέλευσης (βιβλίο, άρθρο από εφημερίδα ή περιοδικό, ιστοσελίδα κ.λπ.). 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 διδακτορικού διπλώματος μου».
Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της διατριβής μου μέχρι 3έτη και έπειτα από αίτηση μου στη Βιβλιοθήκη.

Ο δηλών

Ευχαριστίες

Καταρχάς θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα καθηγητή Δρ Μιχαήλ Παπουτσιδάκη για την αμέριστη υποστήριξή του που μου παρείχε για να περατώσω την Διδακτορική Διατριβή μου. Η επικοινωνία που είχαμε καθ' όλη την διάρκεια εκπόνησης της Διατριβής μου ήταν αδιάλειπτη και οι συμβουλές του στοχευμένες δίνοντάς μου ώθηση εκεί που πραγματικά τη χρειαζόμουν.
Εκτός από τον επιβλέποντα καθηγητή μου, θα ήθελα επίσης να ευχαριστήσω τον Καθηγητή Δρ. Γεώργιο Χαμηλοθώρη και τον Αναπληρωτή Καθηγητή Δρ. Δημήτριο Δημογιαννόπουλο, μέλη της επιτροπής εποπτείας της διατριβής μου, όπου με γνώσεις τους με καθοδήγησαν σε όλη τη διάρκεια της έρευνάς μου.
Ιδιαίτερα θα ήθελα να ευχαριστήσω τη σύζυγό μου Κωνσταντία και τα παιδιά μου Κωνσταντίνο και Θεοδώρα όπου με την κατανόηση και την ενθάρρυνσή τους μου έδιναν ώθηση για τη συνέχεια και την ολοκλήρωση της Διδακτορικής Διατριβής μου όταν πραγματικά το χρειαζόμουν.
Τέλος θα ήθελα να ευχαριστήσω τον ομότιμο Καθηγητή Κωνσταντίνο Αλαφοδήμο όπου για πάνω από 25 χρόνια ήταν ο καθοδηγητής μου στην επαγγελματική μου σταδιοδρομία.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κατάλογος Εξισώσεων

Περίληψη

Οι αυξανόμενες απαιτήσεις αυτοματισμού στην παραγωγή καθιστούν τα συστήματα ελέγχου πιο περίπλοκα και ευάλωτα σε βλάβες. Οι βλάβες μπορούν να προκαλέσουν καθυστερήσεις στην παραγωγή, υλικές ζημιές αλλά κυρίως και εργατικά ατυχήματα. Για το λόγο αυτό έχουν δημιουργηθεί οδηγίες (Directives) και Νομοθεσίες (Legislation) σε επίπεδο χώρας, ευρωπαϊκής ένωσης και παγκόσμιας κλίμακας που καθορίζουν την ουσιαστική ασφάλεια και τις απαιτήσεις του Βιομηχανικού εξοπλισμού. Οδηγίες που πρέπει να τηρούν όσοι ασχολούνται με τον σχεδιασμό, την προμήθεια, την αγορά ή τη χρήση βιομηχανικού εξοπλισμού στην Ευρωπαϊκή Ένωση αλλά και σε αρκετές χώρες εκτός Ευρωπαϊκής Ένωσης. Για το λόγο αυτό έχουν δημιουργηθεί κάποιες οδηγίες (CAT, SIL) που πρέπει να ακολουθούνται, ώστε να διασφαλίζεται η ασφαλής λειτουργία τους σε περίπτωση βλάβης τόσο του υλικού όσο και του λογισμικού. Για μια αξιόπιστη λειτουργία ενός συστήματος Fail Safety μαζί με ένα σύστημα που λειτουργεί σε SIL2 ή SIL3, πρέπει να διαθέτει Υλικό και Λογισμικό Ασφαλείας.
Οι κατασκευαστές βιομηχανικού εξοπλισμού ενσωματώνουν χαρακτηριστικά ασφαλείας σε μια ποικιλία συσκευών. Ανάλογα με τις απαιτήσεις Επιπέδου Ακεραιότητας Ασφαλείας (SIL), αυτά τα χαρακτηριστικά μπορούν να χρησιμοποιηθούν κατά τη φάση του σχεδιασμού προκειμένου να αυξηθεί η ασφάλεια σε περιπτώσεις αστοχιών ή δυσλειτουργιών. Με την κατάλληλη σχεδίαση, η διαδικασία καθώς και το περιβάλλον της (συμπεριλαμβανομένων των ανθρώπων) μπορούν να προστατευθούν με την είσοδο σε μια ελεγχόμενη ασφαλή κατάσταση. Οι κατασκευαστές έχουν προσεγγίσει αυτό το πρόβλημα με διάφορους τρόπους, συμπεριλαμβανομένης της προσθήκης περιττών Κεντρικών Μονάδων Επεξεργασίας (CPU), της χρήσης ειδικού υλικού για τη διασύνδεση σημάτων εισόδου και εξόδου καθώς και της ανάπτυξης πρωτοκόλλων δικτύου ασφαλείας για την επικοινωνία. πληροφοριών ασφαλείας σε όλες τις συσκευές. Δυστυχώς, αυτά τα χαρακτηριστικά δεν μπορούν να προστεθούν σε υπάρχοντα μηχανήματα, τουλάχιστον χωρίς αναβάθμιση κάποιου υλικού. Καθώς το σχετικό κόστος οδηγεί σε πιο αργή υιοθέτηση, οι κατασκευαστές βασίζονται σε προηγούμενες εργασίες προκειμένου να υποστηρίξουν ορισμένα χαρακτηριστικά ασφαλείας, ιδίως τον εντοπισμό σφαλμάτων στη CPU. Αυτό υλοποιείται με τη μορφή βιβλιοθηκών λογισμικού που λειτουργούν σε χαμηλό επίπεδο (λογική πύλη), σχεδιασμένες να εκτελούνται σε παλαιότερο υλικό (PLC) ώστε να μπορούν να προσφέρουν ένα αυξημένο επίπεδο ασφάλειας.
Η παρούσα μελέτη αναλύει τις απαιτούμενες οδηγίες και νομοθεσίες που πρέπει να τηρούνται για τη ασφαλή λειτουργία μιας παραγωγικής μονάδας. Περιγράφει την ασφάλεια λειτουργίας που διαθέτουν Βασικά και Εξειδικευμένα συστήματα με PLC για τη διασφάλιση της ασφάλειας ενός συστήματος αυτοματισμού. Αναπτύσσει αλγόριθμους για την καταγραφή μετρήσεων συμπεριφοράς ηλεκτρονικού εξοπλισμού και μετά από ανάλυση των μετρήσεων αξιολογεί εάν ο βασικός εξοπλισμός θα μπορούσε να χρησιμοποιηθεί σε αυτά τα συστήματα και να διασφαλιστεί η λειτουργία Ασφάλειας ταυτόχρονα. Ο στόχος είναι απλώς να αποδείξει ότι εάν υπάρξει μία διαφορετική προσέγγιση στην υλοποίηση του αυτοματισμού με εξοπλισμό

Basic PLC που είναι ήδη εγκατεστημένα στην παραγωγική διαδικασία, θα μπορούσε να αναβαθμίσει την ασφάλεια των συστημάτων αυτών. Ως εκ τούτου, με χαμηλό κόστος σε χρόνο και χρήμα, ιδιαίτερα στα υπάρχοντα συστήματα αυτοματισμού, θα μπορούσαν να υπάρξουν λειτουργίες Ασφάλειας Αστοχίας.

Abstract

Increasing requirements in production automation make control systems more complex and vulnerable to failures. Failures can cause delays in production, property damage and, above all, accidents at work. For this reason, Directives and Legislation have been created at country, European Union and global level to define the essential safety requirements for industrial equipment. These Directives that must be followed by those involved in the design, supply, purchase or use of industrial equipment in the European Union and in several countries outside the European Union. For this reason, specific guidelines (CAT, SIL) have been created that must be followed to ensure safe operation in case of failure of any hardware or software component. For a reliable operation of a Fail Safety system together with a system operating at SIL2 or SIL3, the Hardware and Software must be Safetty type.

Industrial equipment manufacturers incorporate safety features into a variety of devices. Depending on the Safety Integrity Level (SIL) requirements, these features can be used during the design phase to increase safety in the event of failures or malfunctions. With proper design, the process as well as its environment (including people) can be protected by entering a controlled safe state. Manufacturers have approached this problem in several ways, including adding redundant Central Processing Units (CPUs), using special hardware to interface input and output signals, and developing safety network protocols for the safe communication across devices. Unfortunately, these features cannot be added to existing machines, at least not without upgrading some hardware. As the associated costs lead to slower adoption, manufacturers rely on previous work to support certain security features, in particular CPU debugging. This is implemented in the form of low-level (logic gateway) software libraries designed to run on older hardware (PLCs) so that they can provide an increased level of security.

This thesis discusses the required guidelines and legislation that must be followed to ensure the safe operation of a production plant. It describes the safety of operation that Basic and Specialized systems with PLCs have to ensure the safety of an automation system. It further presents developed algorithms that record behavioral measurements of electronic equipment, analyze the measurements and evaluate whether the basic equipment could be used in these systems to ensure Safety operation at the same time. The objective is simply to demonstrate that if there is a different approach to implement automation with Basic PLC equipment already installed in production processes, the safety aspects can be improved. Most importantly it is demonstrated that Safety Failure Functions can be implemented in existing automation systems, at low cost in terms of time and money.

ΚΕΦΑΛΑΙΟ 1

Οδηγίες και Νομοθεσία για Fail –Safe Συστήματα

Στο κεφάλαιο αυτό αναλύονται οι ευρωπαϊκές οδηγίες (Directives) και η Νομοθεσία (Legislation) που καθορίζουν την ουσιαστική ασφάλεια και τις απαιτήσεις του Βιομηχανικού εξοπλισμού. Οδηγίες που πρέπει να τηρούν όσοι ασχολούνται με τον σχεδιασμό, την προμήθεια, την αγορά ή τη χρήση βιομηχανικού εξοπλισμού στην Ευρωπαϊκή Ένωση αλλά και σε αρκετές χώρες εκτός Ευρωπαϊκής Ένωσης.

Ο στόχος των συστημάτων ασφαλείας είναι η διατήρηση των πιθανών κινδύνων τόσο για τους ανθρώπους όσο και για το περιβάλλον όσο το δυνατόν χαμηλότερα με τη χρήση κατάλληλου τεχνικού εξοπλισμού. Η προστασία του ανθρώπου και του περιβάλλοντος πρέπει να τεθεί σε ίση βάση σε όλες τις χώρες εφαρμόζοντας κανόνες και κανονισμούς που έχουν εναρμονιστεί διεθνώς. Ταυτόχρονα, αυτό αποσκοπεί επίσης στην αποφυγή διαφορετικών απαιτήσεων ασφαλείας σε διαφορετικές χώρες που θα είχε αντίκτυπο στην ανταγωνιστική κατάσταση - δηλαδή η πρόθεση είναι να διευκολυνθούν οι διεθνείς εμπορικές συναλλαγές.

Υπάρχουν διαφορετικές έννοιες και απαιτήσεις για την εγγύηση της ασφάλειας στις διάφορες περιοχές και χώρες σε όλο τον κόσμο. Οι νομικές έννοιες και οι απαιτήσεις ως προς το πώς πρέπει να είναι η επαρκής ασφάλεια, είναι εξίσου διαφορετικές με την κατανομή των ευθυνών. Για παράδειγμα, στην ΕΕ υπάρχουν απαιτήσεις που τίθενται τόσο από τον κατασκευαστή μιας μονάδας-συστήματος καθώς και της εταιρείας εκμετάλλευσης (της μονάδας-συστήματος), οι οποίες ρυθμίζονται με τη χρήση των κατάλληλων Ευρωπαϊκών Οδηγιών, Νόμους και Πρότυπα. Από την άλλη πλευρά στις ΗΠΑ οι απαιτήσεις στον κατασκευαστή μιας μονάδας-συστήματος και της εταιρείας εκμετάλλευσης (της μονάδας-συστήματος) διαφέρουν σε περιφερειακό και ακόμη και σε τοπικό επίπεδο.

Ωστόσο, ισχύει η αρχή ότι ο εργοδότης πρέπει να διασφαλίζει την ασφάλεια στον τόπο εργασίας σε ολόκληρες τις ΗΠΑ. Οι νόμοι περί ευθύνης προϊόντων αναφέρουν ότι σε περίπτωση οποιασδήποτε ζημιάς ή τραυματισμό υπεύθυνος μπορεί να θεωρηθεί και ο κατασκευαστής του μηχανήματος.

Αυτό που είναι σημαντικό για τους κατασκευαστές μηχανημάτων και τις εταιρείες κατασκευής εγκαταστάσεων είναι ότι ισχύουν πάντα η νομοθεσία και οι κανόνες του τόπου όπου λειτουργεί το μηχάνημα ή η εγκατάσταση. Για παράδειγμα, το σύστημα ελέγχου ενός μηχανήματος το οποίο λειτουργεί και χρησιμοποιείται στις ΗΠΑ πρέπει να πληροί τις απαιτήσεις των ΗΠΑ, ακόμα κι αν ο κατασκευαστής του μηχανήματος (δηλαδή ο OEM) εδρεύει στην Ευρώπη.

Τα αίτια των κινδύνων και τα τεχνικά μέτρα για την αποφυγή τους μπορεί να διαφέρουν και αυτός είναι ο λόγος που γίνεται διαφοροποίηση μεταξύ διαφόρων τύπων ασφάλειας, π.χ. προσδιορίζοντας τη συγκεκριμένη αιτία ενός κινδύνου. Για παράδειγμα, ο όρος "ηλεκτρική ασφάλεια" χρησιμοποιείται εάν πρέπει να παρέχεται προστασία έναντι ηλεκτρικών κινδύνων και ο όρος "λειτουργική ασφάλεια" χρησιμοποιείται εάν η ασφάλεια εξαρτάται από τη σωστή λειτουργία. Αυτή η διαφοροποίηση αντικατοπτρίζεται πλέον στα πιο πρόσφατα πρότυπα και υπάρχουν ειδικά πρότυπα που σχετίζονται με τη λειτουργική ασφάλεια. Όσον αφορά την

ασφάλεια των μηχανημάτων σχετικά πρότυπα είναι το EN ISO 13849 και το IEC 62061 που περιέχουν ειδικές διατάξεις σχετικά με τις απαιτήσεις σε συστήματα ελέγχου που σχετίζονται με τη λειτουργική ασφάλεια. Το βασικό πρότυπο ασφάλειας IEC 61508 (επίσης EN 61508 και DIN EN 61508 / VDE 0803) απευθύνεται στη λειτουργική ασφάλεια ηλεκτρικών, ηλεκτρονικών και προγραμματιζόμενων ηλεκτρονικών συστημάτων, ανεξάρτητα από το πεδίο εφαρμογής τους. [1] [2] [3]

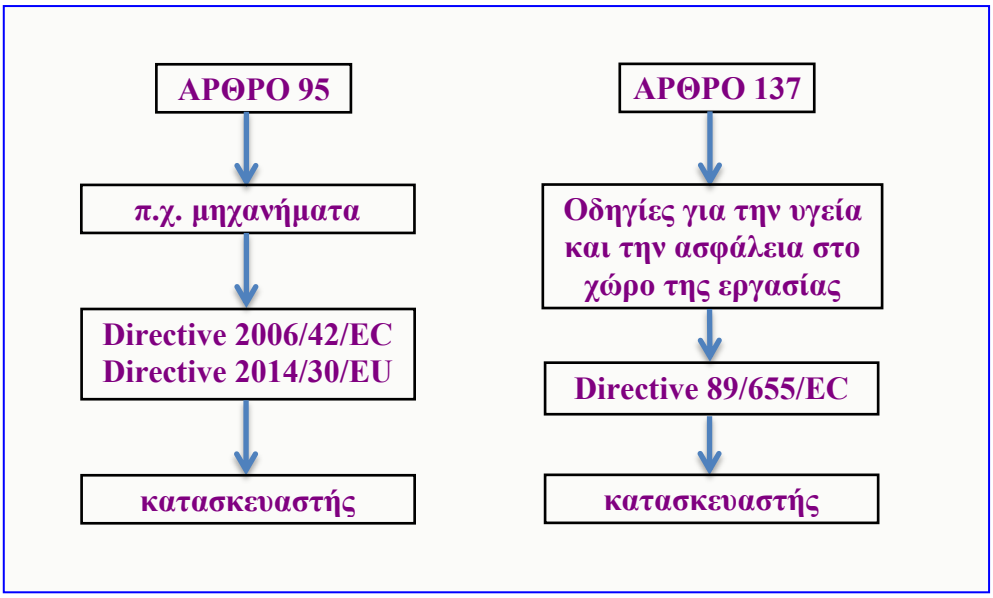
Για τη διασφάλιση της λειτουργικής ασφάλειας ενός μηχανήματος ή μιας εγκατάστασης τα μέρη της προστασίας που σχετίζονται με την ασφάλεια και οι συσκευές ελέγχου πρέπει πιστοποιημένα να λειτουργούν σωστά και αξιόπιστα. Επιπλέον, τα συστήματα πρέπει να συμπεριφέρονται με τέτοιο τρόπο ώστε η μηχανή είτε να παραμένει σε ασφαλή κατάσταση είτε να μεταβαίνει σε ασφαλή κατάσταση σε περίπτωση που λάβει χώρα μία βλάβη. Για να επιτευχθεί αυτό απαιτείται εξειδικευμένη τεχνολογία η οποία να πληροί τις απαιτήσεις που περιγράφονται στα σχετικά πρότυπα. Οι απαιτήσεις για την επίτευξη λειτουργικής ασφάλειας βασίζονται στους ακόλουθους βασικούς στόχους:

- Αποφυγή συστηματικών βλαβών
- Έλεγχος συστηματικών βλαβών
- Έλεγχος τυχαίων βλαβών ή αστοχιών

Το μέτρο για το επίπεδο της επιτυγχανόμενης λειτουργικής ασφάλειας είναι η πιθανότητα εμφάνισης επικίνδυνων αστοχιών, η ανοχή των σφαλμάτων και η ποιότητα που πρέπει να διασφαλίζεται με την αποφυγή συστηματικών σφαλμάτων. Τα βασικά πρότυπα που σχετίζονται με την ασφάλεια είναι το IEC 61508:«Επίπεδο ακεραιότητας ασφαλείας» (SIL) και EN ISO 13849-1 «Επίπεδο απόδοσης» (PL) και «Κατηγορίες».

Στην απαίτηση να γίνουν οι εγκαταστάσεις, οι μηχανές και ο λοιπός εξοπλισμός όσο το δυνατόν ποιο ασφαλής οι επιχειρηματικοί εταίροι περιγράφουν την κατάσταση που σχετίζεται με όλες τις σημαντικές πτυχές της ασφάλειας. Με τη διατήρηση και την εκπλήρωση αυτών προτύπων μπορεί να διασφαλιστεί ότι μια εταιρεία που κατασκευάζει μια μονάδα ή ένας κατασκευαστής που παράγει μια μηχανή ή μια συσκευή έχει εκπληρώσει την ευθύνη του για τη διασφάλιση της ασφάλειας. Οι απαιτήσεις Ασφάλειας της Ευρωπαϊκής Ένωσης βάση του άρθρου 95 για την ελεύθερη διακίνηση προϊόντων και του άρθρου 137 για την ασφαλή εργασία ορίζονται με τις παρακάτω οδηγίες όπως φαίνονται στον Πίνακα 1:

Πίνακας 1. Οδηγίες Ασφαλής Λειτουργίας



Η νομοθεσία απαιτεί ότι η ποιότητα του περιβάλλοντος και η υγεία των ανθρώπων πρέπει να προστατεύονται με προληπτικά μέτρα «Οδηγία 2012/18/ΕΕ». Επίσης απαιτεί να επιτευχθούν αυτός και παρόμοιοι στόχοι και θέτει απαιτήσεις στους χειριστές, τους χρήστες των εγκαταστάσεων και στους κατασκευαστές εξοπλισμού και μηχανές, αναθέτοντας την ευθύνη για ενδεχόμενο τραυματισμό ή ζημιά. [4]

Οι οδηγίες της ΕΕ περιέχουν μόνο γενικούς στόχους ασφάλειας και:

- καθορίζουν τις απαιτήσεις για τις εγκαταστάσεις/συστήματα και τις εταιρείες εκμετάλλευσης για τη διασφάλιση της υγείας και την ασφάλεια του προσωπικού και την ποιότητα του περιβάλλοντος
- καθορίζουν τις απαιτήσεις προϊόντων (π.χ. για μηχανές) για τη διασφάλιση της υγείας και της ασφάλειας του χρήστη.
- περιλαμβάνουν κανονισμούς σχετικά με την υγεία και την ασφάλεια στο χώρο εργασίας (ελάχιστες απαιτήσεις).

Οι Ενώσεις Προτύπων που έχουν την κατάλληλη εντολή της Επιτροπής της ΕΕ (CEN, CENELEC) μπορούν να ορίσουν τις τεχνικές λεπτομέρειες. Αυτά τα πρότυπα είναι εναρμονισμένα σύμφωνα με μία συγκεκριμένη οδηγία και παρατίθενται στην επίσημη Εφημερίδα της ΕΕ.

Η νομοθεσία δεν προσδιορίζει ότι πρέπει να τηρούνται συγκεκριμένα πρότυπα. Ωστόσο, όταν τηρούνται συγκεκριμένα πρότυπα, τότε μπορεί να «υποτεθεί» ότι τηρούνται η σχετική ασφάλεια και οι στόχοι των οδηγιών της ΕΕ.

Οι οδηγίες της ΕΕ έχουν τον ίδιο βαθμό σημασίας, δηλαδή εάν ισχύουν πολλές οδηγίες για ένα συγκεκριμένο κομμάτι εξοπλισμού ή συσκευής, τότε έχουν τις απαιτήσεις όλων των

σχετικών οδηγιών που πρέπει να πληρούνται (π.χ. για ένα μηχάνημα με ηλεκτρικό εξοπλισμό πρέπει να τηρείται η οδηγία για τα μηχανήματα και η οδηγία για τη χαμηλή τάση).

1.1 Υγεία και ασφάλεια στο χώρο εργασίας στην ΕΕ

Οι απαιτήσεις για την υγεία και την ασφάλεια στο χώρο εργασίας βασίζονται στο άρθρο 137 (προηγούμενο 118α) της σύμβασης Ε.Ε. Η βασική οδηγία Υγεία και ασφάλεια στο χώρο εργασίας (89/391/ΕΕC) καθορίζει τις ελάχιστες απαιτήσεις για την ασφάλεια στο χώρο εργασίας. Οι τελικές απαιτήσεις υπόκεινται στην εθνική νομοθεσία και μπορεί να υπερβαίνουν τις απαιτήσεις των βασικών οδηγιών. Αυτές οι απαιτήσεις περιλαμβάνουν τη λειτουργία και τη χρήση προϊόντων (π.χ. μηχανές, χημικά εργοστάσια).

1.2 Ασφάλεια μηχανημάτων στην Ευρώπη

Με την εισαγωγή μιας κοινής ευρωπαϊκής αγοράς ελήφθη απόφαση για την εναρμόνιση της εθνικών οδηγιών και κανονισμών όλων των κρατών μελών της ΕΕ που περιλαμβάνουν την τεχνική υλοποίηση μηχανημάτων. Συνέπεια αυτού είναι ότι τα μηχανήματα πρέπει να εφαρμόζουν τις οδηγίες σε εθνικό δίκαιο έχοντας έτσι ως στόχο την ύπαρξη ενιαίων προστατευτικών στόχων και τη μείωση των εμπορικών φραγμών. Ένα σύνολο μηχανών οι οποίες λειτουργούν ως ένα αναπόσπαστο σύνολο για μία γραμμή παραγωγής θεωρείται «μηχανή». Επομένως, ο τομέας εφαρμογής των οδηγιών για τις μηχανές κυμαίνεται από ένα "ημιτελές" μηχάνημα μέχρι σε ένα πλήρες.

Για τη λειτουργική ασφάλεια των νέων μηχανήματων από τις 29 Δεκεμβρίου 2009 ισχύουν οι οδηγίες 2006/42/ΕΚ. [5]

Η εκτίμηση κινδύνου, οι απαιτήσεις που τίθενται στην τεκμηρίωση, τα κατάλληλα συστήματα ασφαλείας, η αξιολόγηση συμμόρφωσης καθώς και οι κατασκευαστές μηχανημάτων εκτός Ευρωπαϊκής Ένωσης τροποποιήθηκαν στην οδηγία για τα νέα μηχανήματα. Για την αξιολόγηση του κινδύνου ενός μηχανήματος πρέπει να διατίθενται ικανό και κατάλληλα εκπαιδευμένο προσωπικό. Η εκτίμηση κινδύνου πρέπει να περιγράφεται στην τεχνική τεκμηρίωση του μηχανήματος και πρέπει να αναφέρεται στις οδηγίες λειτουργίας.

Επίσης έχουν ορισθεί νέες διαδικασίες για την αξιολόγηση της συμμόρφωσης CE. Αυτές ισχύουν για μηχανές οι οποίες περιλαμβάνονταν στο παράρτημα IV της οδηγίας για τα μηχανήματα, καθώς και για τις "ημιτελείς μηχανές". Οι κατασκευαστές που επιθυμούν να εισάγουν μηχανές στην ΕΕ πρέπει να διαθέτουν τεχνική τεκμηρίωση της μηχανής τους όπου θα παράγεται στην ΕΕ, π.χ. από εξουσιοδοτημένο αντιπρόσωπο. Αυτό απλοποιεί τη διαδικασία συμμόρφωσης CE για τις αρμόδιες αρχές και παρέχει στους χρήστες υψηλότερο βαθμός ασφάλειας κατά την αγορά και τη λειτουργία ενός μηχανήματος.

Οι βασικές απαιτήσεις υγείας και ασφάλειας πρέπει να πληρούνται απόλυτα για την ασφάλεια των μηχανών. Ο κατασκευαστής πρέπει να τηρεί τα ακόλουθα βασικά για ενσωμάτωση της ασφάλειας:

- Τα μηχανήματα πρέπει να είναι κατασκευασμένα με τέτοιο τρόπο ώστε να μπορούν να εγκατασταθούν, να λειτουργούν και να διατηρούνται χωρίς να τίθεται σε κίνδυνο το προσωπικό.
- Κατά την κατασκευή της μηχανής ο κατασκευαστής πρέπει να εφαρμόσει τις βασικές ακόλουθες αρχές με τη σειρά που δίνονται:
  - Πρέπει να εξαλειφθούν ή να μειωθούν όσο το δυνατόν περισσότερο οι κίνδυνοι (ενσωμάτωση των αρχών ασφάλειας στην ανάπτυξη και κατασκευή της μηχανής).
  - Πρέπει να λαμβάνονται τα απαραίτητα προστατευτικά μέτρα σε σχέση με κινδύνους που δεν μπορούν να εξαλειφθούν.
  - Οι χρήστες πρέπει να ενημερώνονται για τους εναπομείναντες κινδύνους που οφείλονται στη μη δυνατότητα εξάλειψης αυτών.

Οι προστατευτικοί στόχοι πρέπει να εφαρμόζονται με υπευθυνότητα προκειμένου να εκπληρωθεί η σχετική απαίτηση συμμόρφωσης με την οδηγία.

Ο κατασκευαστής ενός μηχανήματος πρέπει να παρέχει απόδειξη ότι έχουν τηρηθεί οι βασικές απαιτήσεις. Αυτή η απόδειξη γίνεται ευκολότερη με την εφαρμογή εναρμονισμένων προτύπων (π.χ. EN ISO 13849-1 ή EN 62061).

1.3 Πρότυπα

Για να διατεθούν τα προϊόντα στην αγορά ή να λειτουργήσουν πρέπει να πληρούν τη βασική ασφάλεια των οδηγιών της ΕΕ. Τα πρότυπα μπορεί να είναι εξαιρετικά χρήσιμα όταν οδηγούν στην εκπλήρωση των απαιτήσεων ασφαλείας. Στην περίπτωση αυτή πρέπει να γίνει διαφοροποίηση μεταξύ εναρμονισμένων Ευρωπαϊκών προτύπων και άλλων προτύπων τα οποία αν και έχουν επικυρωθεί δεν έχουν ακόμη εναρμονιστεί με βάση ειδικής οδηγίας καθώς και άλλων τεχνικών κανόνων και κανονισμών που είναι γνωστά και ως «εθνικά πρότυπα».

Με την εφαρμογή των επικυρωμένων προτύπων οι κατασκευαστές μπορούν να αποδείξουν ότι έχει τηρηθεί η αναγνωρισμένη τελευταία λέξη της τεχνολογίας για την ασφάλεια.

Όλα τα πρότυπα επικυρώνονται καταρχήν ως ευρωπαϊκά πρότυπα και στη συνέχεια πρέπει να υιοθετούνται αμετάβλητα ως εθνικά πρότυπα των κρατών μελών. Τα υπάρχοντα εθνικά πρότυπα για το ίδιο θέμα πρέπει στη συνέχεια να ανακληθούν.

1.3.1 Εναρμονισμένα ευρωπαϊκά πρότυπα

Τα εναρμονισμένα ευρωπαϊκά πρότυπα καταρτίζονται από δύο οργανισμούς τυποποίησης τον CEN (Comité Européen de Normalisation) και τον CENELEC (Comité Européen de Normalization Electrotechnique), ως εντολή από την Ε.Ε.

Τα πρότυπα (πρότυπα EN) δημοσιεύονται στην επίσημη Εφημερίδα του Συμβουλίου της Ευρωπαϊκής Ένωσης και στη συνέχεια γίνονται αποδεκτά στα εθνικά πρότυπα χωρίς καμία αλλαγή. Χρησιμοποιούνται για την εκπλήρωση των βασικών απαιτήσεων υγείας και

ασφάλειας των καθορισμένων προστατευτικών στόχων της οδηγίας για τα μηχανήματα. Στη Γερμανία, ο υπεύθυνος για την CEN/CENELEC είναι ο DIN και ο DKE.

Με την εκπλήρωση τέτοιων εναρμονισμένων προτύπων, υπάρχει ένα "αυτόματο τεκμήριο συμμόρφωσης", π.χ. ο κατασκευαστής μπορεί να υποθέσει ότι έχει εκπληρώσει όλες τις πτυχές ασφάλειας της οδηγίας (για όσο διάστημα όπως καλύπτονται στο συγκεκριμένο πρότυπο). Τα ευρωπαϊκά εναρμονισμένα πρότυπα πρέπει να έχουν καταχωρηθεί στην Εφημερίδα του Ευρωπαϊκού Συμβουλίου. Τα εναρμονισμένα ευρωπαϊκά πρότυπα για την ασφάλεια των μηχανημάτων είναι ιεραρχικά δομημένα ως εξής

1. Πρότυπα τύπου Α γνωστά και ως βασικά πρότυπα.
2. Πρότυπα τύπου Β γνωστά και ως Πρότυπα Ομάδας.
3. Πρότυπα τύπου C γνωστά και ως Πρότυπα Προϊόντος.

Η δομή φαίνεται στο παρακάτω Πίνακα 2.

Πίνακας 2. Ευρωπαϊκά πρότυπα για την ασφάλεια μηχανών

<table>
<tr><td>Safety basic standards</td><td>Πρότυπο τύπου Α, βασικές προδιαγραφές για όλα τα μηχανήματα.</td><td colspan="5">EN ISO 12100
Ασφάλεια μηχανημάτων
- Βασική ορολογία, γενικές οδηγίες
- Οδηγίες για την εκτίμηση κινδύνου</td></tr>
<tr><td>Safety group standards</td><td>Πρότυπα τύπου Β1, Θέματα ασφάλειας υψηλότερου επιπέδου</td><td>EN349
Αποφυγή σύνθλιψης τμημάτων του ανθρώπινου σώματος</td><td>EN62061, EN ISO 13849-1
Εξοπλισμός ελεγκτών που σχετίζονται με την ασφάλεια</td><td>DIN EN ISO 13857
Ασφάλεια μηχανημάτων - αποστάσεις ασφαλείας για την αποφυγή πρόσβασης σε επικίνδυνες ζώνες από τον άνθρωπο</td><td>EN60204-1
Ηλεκτρικός εξοπλισμός μηχανών</td><td>EN ISO 14119
Μηχανήματα ασφαλείας, συσκευές αλληλασφάλισης που σχετίζονται με προστατευτικά</td></tr>
<tr><td></td><td>Πρότυπα τύπου Β2, απαιτήσεις για εξοπλισμό ασφαλείας (αναφορά σε ειδικό προστατευτικό εξοπλισμό)</td><td>EN574
Έλεγχος δύο χεριών</td><td colspan="2">EN ISO 13850
Λειτουργικές αρχές Emergency Stop</td><td colspan="2">EN 61496-1
Φωτεινές μπάρες, φωτεινές κουρτίνες</td></tr>
<tr><td>Technical standards</td><td>Πρότυπα τύπου C, τεχνικά πρότυπα, ειδικές απαιτήσεις που τίθενται σε ορισμένους τύπους μηχανημάτων</td><td>EN 81-3
Ανελκυστήρες</td><td>EN201
Μηχανήματα χύτευσης</td><td colspan="2">EN692, EN693
Πρέσες και μηχανήματα κοπής</td><td>EN ISO 23125
Τόρνοι</td></tr>
</table>

1.3.2 Πρότυπα τύπου Α/Βασικά πρότυπα

Το Πρότυπο Α (EN ISO 12100) περιέχει την Ασφάλεια μηχανών, βασική ορολογία και γενικές κατευθυντήριες γραμμές σχεδιασμού. [6]

Το Πρότυπο καθορίζει τεχνικές και μεθόδους για την ελαχιστοποίηση των κινδύνων, που μπορούν επίσης να είναι χρήσιμες για τους κατασκευαστές εάν δεν υπάρχουν ισχύοντα Πρότυπα τύπου Γ.

1.3.3 Πρότυπα τύπου Β/Πρότυπα ομάδας

Αυτά περιλαμβάνουν όλα τα πρότυπα που σχετίζονται με την ασφάλεια και που μπορούν να αντιμετωπίσουν διάφορους τύπους μηχανών.
Τα Πρότυπα τύπου Β απευθύνονται επίσης κυρίως σε εκείνα τα μέρη που ορίζουν τα Πρότυπα τύπου Γ. Ωστόσο, μπορούν επίσης να είναι χρήσιμα στους κατασκευαστές κατά το σχεδιασμό και την κατασκευή μιας μηχανής, εάν δεν υπάρχουν Πρότυπα τύπου Γ.
Για τα Πρότυπα Β έχει γίνει μια πρόσθετη υποδιαίρεση και πιο συγκεκριμένα σε:

- Πρότυπα τύπου Β1 για πτυχές ασφάλειας υψηλότερου επιπέδου, π.χ. αρχές εργονομικού σχεδιασμού, ασφαλής αποστάσεις από πιθανές πηγές κινδύνου, ελάχιστες αποστάσεις για την αποφυγή σύνθλιψης του σώματος από τον εξοπλισμό.
- Πρότυπα τύπου Β2 για τον εξοπλισμό ασφαλείας για διάφορους τύπους μηχανών, π.χ. εξοπλισμός για στάση έκτακτης ανάγκης, κυκλώματα δύο χεριών, λειτουργίες αλληλασφάλισης, εξοπλισμός ανέπαφης προστασίας και εξαρτήματα συστημάτων ελέγχου που σχετίζονται με την ασφάλεια.

1.3.4 Πρότυπα τύπου Γ/Πρότυπα προϊόντων

Αυτά περιλαμβάνουν πρότυπα για συγκεκριμένα μηχανήματα - π.χ. για εργαλειομηχανές, μηχανές επεξεργασίας ξύλου, ανελκυστήρες, μηχανήματα συσκευασίας, μηχανήματα εκτύπωσης και πολλά άλλα.

Τα ευρωπαϊκά πρότυπα είναι δομημένα έτσι ώστε οι γενικές δηλώσεις που περιλαμβάνονται ήδη στα πρότυπα τύπου Α ή τύπου Β να μην επαναλαμβάνονται.

Τα Πρότυπα Προϊόντων περιλαμβάνουν απαιτήσεις για τα μηχανήματα. Αυτές οι απαιτήσεις, υπό ορισμένες περιστάσεις αποκλίνουν από τα βασικά και τα ομαδικά πρότυπα. Το Πρότυπο Γ έχει απολύτως την υψηλότερη προτεραιότητα για τους κατασκευαστές μηχανών (OEM). Οι κατασκευαστές μπορούν κάνοντας χρήση το πρότυπο Γ να υποθέσουν ότι πληρούν τις βασικές απαιτήσεις των οδηγιών για τα μηχανήματα (αυτόματο τεκμήριο συμμόρφωσης). Εάν δεν υπάρχει Πρότυπο προϊόντος για ένα συγκεκριμένο μηχάνημα, τότε τα πρότυπα τύπου Β μπορούν να εφαρμοστούν για λόγους προσανατολισμού όταν σχεδιάζεται και κατασκευάζεται μία μηχανή.

Προκειμένου να παρασχεθεί μια μέθοδος εναρμόνισης των βασικών απαιτήσεων μίας οδηγίας, με εντολή της επιτροπής της ΕΕ καταρτίστηκαν εναρμονισμένα πρότυπα στις τεχνικές επιτροπές της CEN και της CENELEC για μηχανήματα ή ομάδες μηχανημάτων για όλους σχεδόν τους τομείς.

Η κατάρτιση των προτύπων περιλαμβάνει ουσιαστικά εκπροσώπους από κατασκευαστές των συγκεκριμένων μηχανημάτων, ρυθμιστικών φορέων όπως οι Ενώσεις Ασφαλίσεων Εργοδοτών καθώς και χρήστες. Μια πλήρης λίστα με όλα τα αναφερόμενα πρότυπα καθώς και τις σχετικές δραστηριότητες με πρότυπα – και με υποχρεωτικά νέα πρότυπα για το μέλλον παρέχονται στο Διαδίκτυο κάτω από: (http://www.newapproach.org/).

Πρέπει να σημειωθεί ότι δεν είναι υποχρεωτική η εφαρμογή του προτύπου, αλλά αντίθετα, πρέπει να επιτευχθούν οι στόχοι ασφάλειας.

1.3.5 Εθνικά πρότυπα

Εάν δεν υπάρχουν εναρμονισμένα ευρωπαϊκά πρότυπα ή δεν μπορούν να εφαρμοστούν για συγκεκριμένους λόγους, τότε ένας κατασκευαστής μπορεί να εφαρμόσει τα «Εθνικά Πρότυπα». Όλοι οι άλλοι τεχνικοί κανόνες εμπίπτουν στις οδηγίες για τα μηχανήματα, π.χ. στους κανονισμούς πρόληψης ατυχημάτων τα οποία δεν αναφέρονται στην Εφημερίδα του Ευρωπαϊκού Συμβουλίου (επίσης πρότυπα IEC ή ISO, τα οποία επικυρώθηκαν ως EN). Εφαρμόζοντας επικυρωμένα πρότυπα ο κατασκευαστής μπορεί να αποδείξει ότι η κατασκευή του μηχανήματος ολοκληρώθηκε κάνοντας χρήση τεχνολογία αιχμής. Ωστόσο όταν εφαρμόζονται τέτοια πρότυπα δεν αποδεικνύεται αυτόματα το τεκμήριο συμμόρφωσης όπως με ένα εναρμονισμένο πρότυπο.

1.4 Εκτίμηση κινδύνου (Risk assessment)

Ως αποτέλεσμα του σχεδιασμού και της λειτουργικότητάς τους τα μηχανήματα και οι εγκαταστάσεις παράγουν πιθανούς κινδύνους. Ως εκ τούτου η οδηγία για τα μηχανήματα απαιτεί αξιολόγηση του κινδύνου για κάθε μηχανή και εάν χρειάζεται μείωση του κινδύνου ώστε ο κίνδυνος να είναι μικρότερος από τον ανεκτό κίνδυνο.

Τα ακόλουθα πρότυπα θα πρέπει να εφαρμόζονται για τις τεχνικές αξιολόγησης και της αξιολόγησης αυτών των κινδύνων:

- EN ISO 12100, Ασφάλεια μηχανημάτων - Γενικές αρχές σχεδιασμού - Εκτίμηση κινδύνου και μείωση κινδύνου. Το EN ISO 12100 περιγράφει κυρίως τους κινδύνους που πρέπει να ληφθούν υπόψη και τις αρχές σχεδιασμού για τη μείωση του κινδύνου καθώς και την επαναληπτική διαδικασία με εκτίμηση κινδύνου και μείωση κινδύνου προκειμένου να επιτευχθεί η ασφάλεια.
- ANSI B11.0 - 2015, Γενικές Απαιτήσεις και Αξιολόγηση Κινδύνων (για Η.Π.Α μόνο). Αυτό το πρότυπο ισχύει για νέα, τροποποιημένα ή ανακατασκευασμένα μηχανήματα που λειτουργούν με ηλεκτρισμό που δεν είναι φορητά από άνθρωπο, που χρησιμοποιούνται για τη διαμόρφωση και/ή τη διαμόρφωση μετάλλου με κοπή, κρούση, πίεση, ηλεκτρική ή άλλες τεχνικές επεξεργασίας ή συνδυασμός αυτών των διαδικασιών. Περιλαμβάνει τα πρότυπα ANSI B 11.19 - 2010 (R2008) και ANSI B11.TR3.

1.4.1 Διαδικασία εκτίμησης κινδύνου (Risk assessment process)

Η αξιολόγηση κινδύνου είναι μια ακολουθία βημάτων που επιτρέπει να διερευνηθεί συστηματικά η ύπαρξη κινδύνων που προκαλούνται από μηχανήματα. Όπου είναι απαραίτητο στη φάση της αξιολόγησης κινδύνου ακολουθείται από μείωση κινδύνου.

Η εκτίμηση κινδύνου περιλαμβάνει τα ακόλουθα:

- Ανάλυση κινδύνου (Risk Analysis)
- Καθορισμός των ορίων του μηχανήματος (EN ISO 12100)
- Προσδιορισμός των κινδύνων (EN ISO 12100)
- Αξιολόγηση κινδύνου (Risk Evaluation) (EN ISO 12100:2010-03 Ενότητα 5.6)

Αφού εκτιμηθούν οι κίνδυνοι πραγματοποιείται αξιολόγηση κινδύνου ως μέρος μιας επαναληπτικής διαδικασίας για την επίτευξη της ασφάλειας. Σε αυτό το σημείο πρέπει να ληφθεί απόφαση εάν είναι απαραίτητο να μειωθεί ένας κίνδυνος. Αν ένας κίνδυνος πρέπει να μειωθεί περαιτέρω πρέπει να επιλεγούν και να εφαρμοστούν κατάλληλα προστατευτικά μέτρα και η αξιολόγηση κινδύνου θα πρέπει στη συνέχεια να επαναληφθεί.

Τα στοιχεία κινδύνου ορίζονται ως ένα εργαλείο για την αξιολόγηση των κινδύνων. Ο παρακάτω Πίνακας 3 δείχνει την αλληλεξάρτηση μεταξύ των στοιχείων κινδύνου.

Τα στοιχεία κινδύνου (S, F και W) χρησιμεύουν ως ποσότητες εισροών και για τα δύο πρότυπα. Αυτά τα στοιχεία κινδύνου αξιολογούνται με διαφορετικούς τρόπους. Σύμφωνα με το EN 62061καθορίζεται ένα απαιτούμενο επίπεδο ακεραιότητας ασφάλειας (SIL), ενώ με το EN ISO 13849-1 καθορίζεται ένα Επίπεδο Απόδοσης (PL).

Πίνακας 3. Στοιχεία Κινδύνου (Risk Elements)

Κίνδυνος που σχετίζεται με τον εντοπισμένο κίνδυνο	Κρισιμότητα της ζημιάς	Fr, Συχνότητα και διάρκεια της έκθεσης στον κίνδυνο
		Pr, Πιθανότητα του κινδύνου
		Av, πιθανότητα αποφυγής ή μείωσης της βλάβης

Εάν δεν έχει ακόμη επιτευχθεί ο απαιτούμενος βαθμός ασφάλειας απαιτούνται μέτρα για περαιτέρω μείωση του κινδύνου. Ο κίνδυνος πρέπει να μειωθεί με τον κατάλληλο σχεδιασμό και εφαρμογή του μηχανήματος. Για παράδειγμα χρησιμοποιώντας κατάλληλα μέτρα ελέγχου ή προστασίας για τις λειτουργίες ασφαλείας.

1.4.2 Υπολειπόμενος κίνδυνος (Residual risk) (EN ISO 12100)

Η ασφάλεια είναι ένας σχετικός όρος στο τεχνικό μας περιβάλλον. Δυστυχώς δεν γίνεται να εφαρμόσει τη λεγόμενη «εγγύηση μηδενικού κινδύνου» όπου τίποτα δεν μπορεί να συμβεί σε καμία περίπτωση. Ο υπολειπόμενος κίνδυνος ορίζεται ως: Κίνδυνος που παραμένει μετά

την εφαρμογή των προστατευτικών μέτρων. Σε αυτή την περίπτωση τα προστατευτικά μέτρα αντιπροσωπεύουν όλα τα μέτρα για την μείωση του κινδύνου.

1.4.3 Μείωση ρίσκου (Risk reduction)

Εκτός από την εφαρμογή δομικών μέτρων μείωσης κινδύνου, μείωση κινδύνου μπορεί να επιτευχθεί σε ένα μηχάνημα χρησιμοποιώντας λειτουργίες ελέγχου που σχετίζονται με την ασφάλεια. Πρέπει να τηρούνται ειδικές απαιτήσεις όταν εφαρμόζοντας αυτές οι λειτουργίες ελέγχου, κλιμακούμενες ανάλογα με το μέγεθος του κινδύνου. Αυτές οι λειτουργίες ελέγχου για ηλεκτρικά συστήματα ελέγχου ορίζονται στο EN ISO 13849-1 και στο IEC 61508 για ειδικά προγραμματιζόμενα ηλεκτρονικά συστήματα.

Οι απαιτήσεις που τίθενται σχετικά με την ασφάλεια των συστημάτων ελέγχου ταξινομούνται σε κατηγορίες, ανάλογα με το επίπεδο κινδύνου και την απαραίτητη μείωση αυτού. Με το EN ISO 13849-1 έχει εισαχθεί ένα νέο διάγραμμα κινδύνου σε κατηγορίες ιεραρχικά διαβαθμισμένες σε επίπεδα απόδοσης (PL). Το EN 62061 χρησιμοποιεί το "Επίπεδο Ακεραιότητας Ασφαλείας" (SIL) για την ταξινόμηση των κινδύνων, αυτό είναι ένα ποσοτικοποιημένο μέτρο για την απόδοση που σχετίζεται με την ασφάλεια μιας ασφαλούς λειτουργίας. Το απαιτούμενο SIL προσδιορίζεται επίσης με βάση την αρχή αξιολόγησης κινδύνου σύμφωνα με το EN ISO 12100.

Είναι πάντα σημαντικό - ανεξάρτητα από το ποιο πρότυπο εφαρμόζεται - όλα τα μέρη του ελέγχου του μηχανήματος που εμπλέκονται στην υλοποίηση των λειτουργιών που σχετίζονται με την ασφάλεια να πληρούν αυτές τις απαιτήσεις.

Κατά το σχεδιασμό και την εφαρμογή του ελέγχου είναι απαραίτητο να ελεγχθεί εάν πληρούνται οι απαιτήσεις του επιλεγμένου PL ή SIL.

Πρέπει δηλαδή να τηρούνται όλες οι πτυχές στα πρότυπα έτσι ώστε:

- Να ελέγχονται οι τυχαίες αστοχίες υλικού,
- Να αποφεύγονται συστηματικά σφάλματα/λάθη στο υλικό και το λογισμικό
- Να ελέγχονται συστηματικά σφάλματα/λάθη στο υλικό και το λογισμικό.

Επικύρωση (Validation)

Επικύρωση σημαίνει ότι ελέγχεται και αξιολογείται η λειτουργικότητα της ασφαλείας που πρέπει να επιτευχθεί. Ο σκοπός της επικύρωσης είναι να επιβεβαιωθούν οι ορισμοί και το επίπεδο συμμόρφωσης των σχετικών με την ασφάλεια μερών του ελέγχου, εντός του γενικού ορισμού των απαιτήσεων ασφαλείας της μηχανής. Επιπλέον, η επικύρωση πρέπει να υποδεικνύει ότι κάθε εξάρτημα που σχετίζεται με την ασφάλεια πληροί τις απαιτήσεις του σχετικού προτύπου.

Παρακάτω περιγράφονται οι ακόλουθες απαιτήσεις για την επικύρωση:

- Λίστες σφαλμάτων.
- Επικύρωση λειτουργιών ασφαλείας.
- Επικύρωση των καθορισμένων και των επιτευχθέντων επιδόσεων ασφαλείας.
- Επικύρωση των περιβαλλοντικών/περιβαλλοντικών απαιτήσεων.

- Επικύρωση των απαιτήσεων συντήρησης.

Οι απαιτήσεις για την επικύρωση των καθορισμένων λειτουργιών ασφαλείας πρέπει να περιγράφονται σε ένα σχέδιο επικύρωσης.

1.5 Ενσωματωμένη ασφάλεια (Safety Integrated)

Τα μέτρα τα οποία απαιτούνται για να γίνει ένας σύνθετος έλεγχος επαρκώς και λειτουργικά ασφαλής για εργασίες ασφαλείας είναι εξαιρετικά εκτεταμένες. Αυτός είναι ο λόγος που παράγονται συσκευές ειδικά σχεδιασμένες για λειτουργίες ασφαλείας.

1.5.1 Λειτουργίες που σχετίζονται με την ασφάλεια (Safety-related functions)

Οι λειτουργίες που σχετίζονται με την ασφάλεια περιλαμβάνουν εκτός από τις συμβατικές λειτουργίες:

- Διακοπή λειτουργίας.
- Διαδικασίες σε κατάσταση έκτακτης ανάγκης.
- Αποτροπή ανεπιθύμητης εκκίνησης.

Και πιο σύνθετες λειτουργίες όπως:

- Εμπλοκές που εξαρτώνται από την κατάσταση.
- Περιορισμός ταχύτητας.
- Περιορισμός θέσης.
- Ελεγχόμενη απενεργοποίηση.
- Ελεγχόμενη στάση κ.λπ.

Οι κλασικές λειτουργίες ορίζονται στο EN 60204-1 και μέχρι τώρα υλοποιούνται με χρήση ηλεκτρομηχανικών εξαρτημάτων. Τα ηλεκτρονικά προγραμματιζόμενα συστήματα μπορούν επίσης να χρησιμοποιούνται για την υλοποίηση πιο περίπλοκων λειτουργιών εάν πληρούν τα σχετικά πρότυπα. Σύνθετες λειτουργίες, π.χ. που περιλαμβάνουν τη συμπεριφορά ηλεκτροκινητήρων μεταβλητής ταχύτητας περιγράφονται στο EN 61800-5-2.

Στάση (Stopping)

Τρεις κατηγορίες στάσεων ορίζονται στο EN 60204-1, το οποίο ορίζει τον έλεγχο της ακολουθίας για τερματισμό της λειτουργίας, ανεξάρτητα από την κατάσταση της έκτακτης ανάγκης και φαίνονται στον Πίνακα 4.

Πίνακας 4. Κατηγορίες στάσεων στο EN 60204-1

Κατηγορία Στάσης 0 (Stop Category 0)	Ανεξέλεγκτη διακοπή αφαιρώντας αμέσως την τροφοδοσία ρεύματος του μηχανήματος.
Κατηγορία Στάσης 1 (Stop Category 1)	Ελεγχόμενη στάση, η τροφοδοσία δεν αποσυνδέεται μέχρι να επιτευχθεί η στάση.
Κατηγορία Στάσης 2 (Stop Category 2)	Ελεγχόμενη στάση όπου η τροφοδοσία ρεύματος εξακολουθεί να διατηρείται ακόμη και σε στάση. Η απενεργοποίηση διακόπτει μόνο την τροφοδοσία που μπορεί να προκαλέσει την κίνηση.

Διαδικασία σε κατάσταση έκτακτης ανάγκης (Procedure in an Emergency situation)

Οι διαδικασίες σε κατάσταση έκτακτης ανάγκης (EN 60204-1) περιγράφονται ως εξής:

- Διακοπή σε περίπτωση έκτακτης ανάγκης (Emergency Stop).
- Έναρξη σε περίπτωση έκτακτης ανάγκης (Emergency Start).
- Απενεργοποίηση σε περίπτωση έκτακτης ανάγκης (Emergency Off).
- Ενεργοποίηση σε περίπτωση έκτακτης ανάγκης (Emergency On).

Στάση έκτακτης ανάγκης (Emergency Stop)

Η στάση έκτακτης ανάγκης είναι μια ενέργεια που έχει σκοπό να σταματήσει μια διαδικασία ή κίνηση που θα είχε ως αποτέλεσμα έναν κίνδυνο (EN 60204-1).

Οι απαιτήσεις σε περίπτωση έκτακτης στάσης είναι:

- Πρέπει να έχει προτεραιότητα έναντι όλων των άλλων λειτουργιών και ενεργειών του χειριστή σε όλες τις καταστάσεις λειτουργίας.
- Η τροφοδοσία στα στοιχεία κίνησης του μηχανήματος, η οποία θα μπορούσε να οδηγήσει δυνητικά σε επικίνδυνη κατάσταση ή δυνητικά σε επικίνδυνες συνθήκες πρέπει να αποσυνδεθεί το συντομότερο δυνατό χωρίς τη δημιουργία άλλων κινδύνων.

Απενεργοποίηση έκτακτης ανάγκης (Emergency Off)

Αυτή είναι μια ενέργεια σε περίπτωση έκτακτης ανάγκης που αποσκοπεί στην αποσύνδεση της ηλεκτρικής ενέργειας σε ολόκληρη την εγκατάσταση ή μέρος μιας εγκατάστασης εάν υπάρχει κίνδυνος ηλεκτροπληξίας ή άλλος κίνδυνος με ηλεκτρική αιτία. Οι λειτουργικές πτυχές για την απενεργοποίηση σε περίπτωση έκτακτης ανάγκης ορίζονται στο IEC 60204-1.

Η απενεργοποίηση σε περίπτωση έκτακτης ανάγκης θα πρέπει να εφαρμόζεται για:

- Προστασία από την άμεση επαφή (π.χ. με καλώδια επαφής, συγκροτήματα επαφής, μεταγωγές, συσκευές σε δωμάτια που φιλοξενούν ηλεκτρικό εξοπλισμό) μπορεί να επιτευχθεί μόνο με την παροχή κατάλληλων αποστάσεων ή με κατάλληλα εμπόδια.
- Την ύπαρξη πιθανότητας άλλων κινδύνων ή ζημιών που προκαλούνται από την ηλεκτρική ενέργεια.

1.5.2 Συσκευές για απενεργοποίηση έκτακτης ανάγκης και διακοπή έκτακτης ανάγκης

Για τη διακοπή του εξοπλισμού και των μηχανημάτων σε περίπτωση έκτακτης ανάγκης πρέπει να παρέχονται συσκευές που χρησιμοποιούνται σε κάθε θέση ελέγχου χειριστή αλλά και σε άλλες θέσεις όπου μπορεί να είναι απαραίτητο να ξεκινήσει η ‘στάση’ σε περίπτωση έκτακτης ανάγκης.

Προκειμένου να εκπληρωθούν οι προστατευτικοί στόχοι που καθορίζονται στο EN 60204-1 καθώς και στο EN ISO 13850 πρέπει να ικανοποιούνται ακόλουθες απαιτήσεις και για τις δύο λειτουργίες: [7] [8]

- Όταν ενεργοποιηθεί έστω και λίγο η έκτακτη ανάγκη τότε το μηχάνημα παραμένει μόνιμα σε στάση.
- Πρέπει να είναι αδύνατη η επανεκκίνηση του μηχανήματος από ένα τηλεχειριστήριο κεντρικής μονάδας πριν ο κίνδυνος έχει απομακρυνθεί. Η συσκευή διακοπής έκτακτης ανάγκης πρέπει να απελευθερωθεί τοπικά από τον υπεύθυνο.

Προκειμένου να απλοποιηθεί η αλληλεπίδραση μεταξύ ανθρώπου και μηχανής, τα πρότυπα EN 60073 και DIN EN 60204-1 καθορίζουν την κατάλληλη σήμανση και κωδικοποίηση.

Σήμανση διακοπτών, μπουτόν και λυχνιών

Οι διακόπτες, τα κουμπιά και οι ενδεικτικές λυχνίες είναι τα κύρια εξαρτήματα του μηχανήματος που χρησιμοποιούνται ως τη διεπαφή μεταξύ ανθρώπου και μηχανής. Αυτά τα στοιχεία ελέγχου χειριστή προσδιορίζονται σαφώς και κωδικοποιούνται με τυπικό τρόπο χρησιμοποιώντας χρώματα που έχουν πολύ συγκεκριμένη σημασία. Αυτό εγγυάται ότι ο βαθμός ασφάλειας για το προσωπικό χειρισμού αυξάνεται και είναι επίσης απλούστερο για τη λειτουργία και συντήρηση του εξοπλισμού και των συστημάτων.

Τα χρώματα των κουμπιών, η σημασία αυτών των χρωμάτων, επεξηγήσεις και εφαρμογή φαίνονται στον παρακάτω Πίνακα 5:

Πίνακας 5. Χρώματα κουμπιών

Χρώμα	Περιγραφή	Επεξήγηση	Παραδείγματα
Κόκκινο	Έκτακτη ανάγκη	Ενεργοποίηση σε περίπτωση επικίνδυνης κατάστασης ή έκτακτης ανάγκης	Emergency Off
Κίτρινο	Ασυνήθιστη κατάσταση	Ενεργοποίηση σε περίπτωση μη φυσιολογικής κατάστασης	Παρέμβαση για την καταστολή μίας μη φυσιολογικής κατάστασης, Παρέμβαση για επανεκκίνηση ενός διακοπτόμενου αυτόματου κύκλου
Πράσινο	Κανονική Κατάσταση	Ενεργοποίηση για εκκίνηση σε κανονική κατάσταση	Έναρξη/Ενεργοποίηση Ωστόσο, προτείνεται να χρησιμοποιείται και το λευκό χρώμα
Μπλε	Επιτακτική ανάγκη	Ενεργοποίηση για μια συνθήκη που απαιτεί υποχρεωτική δράση	Λειτουργία επαναφοράς
Άσπρο Γκρι Μαύρο	Δεν έχει αποδοθεί συγκεκριμένο νόημα	Για γενική εκκίνηση λειτουργιών εκτός από έκτακτη στάση	Start/On Stop/Off

Τα χρώματα για τις ενδεικτικές λυχνίες, η σημασία τους σε σχέση με την κατάσταση του μηχανήματος ως καθώς και παραδείγματα χειρισμού και εφαρμογών παρατίθενται στον Πίνακα 6 σύμφωνα με το EN 60204-1.

Πίνακας 6. Χρώματα λυχνιών

Χρώμα	Περιγραφή	Επεξήγηση	Ενέργειες Χειριστή	Παραδείγματα
Κόκκινο	Έκτακτη ανάγκη	Επικίνδυνη κατάσταση	Άμεση δράση για απάντηση σε μία επικίνδυνη κατάσταση (π.χ. πατώντας το Emergency Stop	Πίεση/θερμοκρασία εκτός ασφαλών ορίων, μεταγωγή σε θέση στάσης
Κίτρινο	Ασυνήθιστη κατάσταση	Μη φυσιολογική κατάσταση Σε εκκρεμότητα κρίσιμη κατάσταση	Παρακολούθηση ή/και παρέμβαση (π.χ. μετάβαση στη προβλεπόμενη λειτουργία)	Πίεση/θερμοκρασία υπέρβαση του κανονικού ορίου
Πράσινο	Κανονική Κατάσταση	Κανονική Κατάσταση	Προαιρετική	Πίεση/θερμοκρασία εντός φυσιολογικών ορίων
Μπλε	Επιτακτική ανάγκη	Υποδεικνύει μια κατάσταση που απαιτεί ενέργεια από τον χειριστή	Υποχρεωτική Ενέργεια	Προτροπή για λειτουργία σε καθορισμένες τιμές
Άσπρο	Δεν έχει αποδοθεί συγκεκριμένο νόημα	Ουδέτερες καταστάσεις	Παρακολούθηση	Γενική πληροφόρηση

Σήμανση καλωδίων (Marking Cables)

Το EN 60204-1 επιτρέπει υψηλότερο βαθμό ευελιξίας όσον αφορά τη σήμανση και την κωδικοποίηση των καλωδίων. Η αρίθμηση των ακροδεκτών που ταιριάζουν με το ηλεκτρολογικό σχέδιο είναι επαρκής εάν είναι δυνατό να γίνει οπτικά και εύκολα ανιχνεύσιμο καλώδιο. Για πολύπλοκους ελέγχους, συνιστάται τα εσωτερικά καλώδια που χρησιμοποιούνται για την καλωδίωση καθώς και τα εξερχόμενα καλώδια να είναι κωδικοποιημένα έτσι ώστε μετά την αποσύνδεση του καλωδίου από το τερματικό να μπορεί εύκολα να επανασυνδεθεί στο ίδιο τερματικό. Αυτό συνιστάται επίσης και για θέσεις τερματικών που πρέπει να αποσυνδεθούν κατά τη μεταφορά του εξοπλισμού.

Με τη διατύπωση στο IEC 60204-1 2016 η επιτροπή προτύπων ήθελε να εκφράσει τα ακόλουθα σημεία:

- Κάθε μεμονωμένος αγωγός πρέπει να μπορεί να αναγνωριστεί αλλά με απόλυτη βεβαιότητα μόνο σε συνδυασμό με την τεκμηρίωση. Δεν ορίζεται ότι κάθε καλώδιο πρέπει να μπορεί να αναγνωριστεί χωρίς την κατάλληλη τεκμηρίωση.
- Ο κατασκευαστής και η εταιρεία εκμετάλλευσης θα πρέπει να συμφωνήσουν για τον τύπο κωδικοποίησης/σήμανσης και ως εκ τούτου και στις τεχνικές αναγνώρισης που θα χρησιμοποιούνται.

Δεν είναι πρόθεση του προτύπου να προσδιορίσει έναν συγκεκριμένο τύπο κωδικοποίησης που πρέπει να εφαρμοστεί Παγκοσμίως. Για παράδειγμα, για λόγους

ασφαλείας, οι εργοστασιακές εσωτερικές προδιαγραφές μπορεί να έχουν υψηλότερη προτεραιότητα, προκειμένου να αποφευχθεί η σύγχυση σε τομείς που διαχειρίζεται το ίδιο προσωπικό. Αυτοί οι ορισμοί δεν μπορούν να γενικευτούν λόγω του μεγάλου εύρους εφαρμογής του συγκεκριμένου προτύπου από μικρές μεμονωμένες μηχανές έως μεγάλα, πολύπλοκα εργοστάσια.

Κατά κύριο λόγο, θα πρέπει να χρησιμοποιούνται οι κατάλληλες δοκιμές για την αποφυγή σφαλμάτων εγκατάστασης/συναρμολόγησης.

Θα πρέπει να χρησιμοποιείται μια τυπική χρωματική κωδικοποίηση για τα καλώδια. Συνήθως προτείνονται τα παρακάτω χρώματα:

- Μαύρο για κύρια κυκλώματα AC και DC
- Κόκκινο για κυκλώματα ελέγχου AC
- Μπλε για κυκλώματα ελέγχου DC
- Πορτοκαλί για κυκλώματα μπλοκαρίσματος, τα οποία τροφοδοτούνται από εξωτερική πηγή ρεύματος.

Η παραπάνω αντιστοίχιση χρώματος συνιστάται εάν ληφθεί απόφαση να χρησιμοποιηθεί απλώς χρωματική κωδικοποίηση, η μόνη υποχρεωτική προδιαγραφή είναι η χρωματική κωδικοποίηση του προστατευτικού αγωγού και του ουδέτερου αγωγού. Για όλες τις άλλες καλωδιώσεις μία από τις μεθόδους που αναφέρονται στο πρότυπο IEC 60204 μπορεί να επιλεγούν (χρώμα, αριθμοί ή γράμματα, ή συνδυασμός χρωμάτων και αριθμούς ή χρώματα και γράμματα).

Κωδικοποίηση/σήμανση προστατευτικού αγωγού (Protective conductor coding/marking)

Ο προστατευτικός αγωγός πρέπει να μπορεί να αναγνωρίζεται μοναδικά ως αποτέλεσμα του σχήματος, της θέσης της σήμανσης ή του χρώματος. Εάν προσδιορίζεται μόνο ως αποτέλεσμα του χρώματός του, τότε ένας συνδυασμός δύο χρωμάτων πράσινο/κίτρινο πρέπει να χρησιμοποιείται σε όλο το μήκος του καλωδίου. Το πράσινο/κίτρινο χρώμα ο συνδυασμός μπορεί να χρησιμοποιηθεί μόνο για προστατευτικούς αγωγούς.

Κωδικοποίηση/σήμανση ουδέτερου αγωγού (Neutral conductor coding/marking)

Εάν ένα κύκλωμα έχει έναν χρωματικά κωδικοποιημένο ουδέτερο αγωγό, τότε πρέπει να χρησιμοποιείται ανοιχτό μπλε. Το ανοιχτό μπλε δεν μπορεί να χρησιμοποιηθεί για την κωδικοποίηση άλλων καλωδίων εάν υπάρχει κίνδυνος τυχαίας εναλλαγής τους.

Εάν δεν χρησιμοποιείται ουδέτερος αγωγός, μπορεί να χρησιμοποιηθεί ανοιχτό μπλε αγωγός για άλλους σκοπούς, αλλά όχι ως προστατευτικός αγωγός.

1.5.3 Δομή της ασφαλής λειτουργίας και προσδιορισμός της ασφαλής ακεραιότητας (Structure of the safety function and determining the safety integrity)

Παρόλο που τα δύο πρότυπα ασφαλείας EN 62061 και EN ISO 13849-1 χρησιμοποιούν διαφορετικές μεθόδους αξιολόγησης για μια ασφαλή λειτουργία, χρησιμοποιούν παρόμοιους

όρους και ορισμούς. Η προσέγγιση και των δύο προτύπων σε ολόκληρη την αλυσίδα ασφαλείας είναι συγκρίσιμη.

1.6 Ηλεκτρομαγνητική Συμβατότητα (Electromagnetic Compatibility), EMC

Ο όρος EMC (Ηλεκτρομαγνητική Συμβατότητα) αρχικά αναφερόταν κυρίως σε παρεμβολές ραδιοσυχνοτήτων, χρησιμοποιούταν γενικά για να περιγράψει την ενέργεια που εκπέμπεται, ακτινοβολείται ή που προκαλείται από ηλεκτρικό εξοπλισμό και έχει αρνητικό αντίκτυπο στη λειτουργία ενός ραδιοφωνικού συστήματος.

Με αυτήν την ερμηνεία της EMC, το μόνο σχετικό θέμα που μπορεί να εξεταστεί σε σχέση με τον έλεγχο συστημάτων ήταν εάν τα φαινόμενα που περιγράφονται παραπάνω (ακτινοβολία, εκπομπή ή επαγωγή) που προκαλούνται από εξαρτήματα ηλεκτρομηχανικής σε συγκεκριμένο εξοπλισμό θα είχε αρνητικό επιπτώσεις στις ραδιοεπικοινωνίες.

Καθώς ο όγκος των ηλεκτρονικών κυκλωμάτων που είναι ενσωματωμένα σε έναν ηλεκτρικό εξοπλισμό αυξήθηκε γρήγορα, το θέμα της ηλεκτρομαγνητικής συμβατότητας πήρε μία εντελώς νέα έννοια. Κατά την αξιολόγηση της ηλεκτρομαγνητικής συμβατότητας του εξοπλισμού στα οποία είναι ενσωματωμένα ηλεκτρονικά κυκλώματα είναι σημαντικό να ληφθούν υπόψη το σύνολο όλων των ηλεκτρικών, μαγνητικών και ηλεκτρομαγνητικών παρεμβολών που μπορούν να φτάσουν σε εξοπλισμό που περιέχει ηλεκτρονικά κυκλώματα και να έχει αντίστοιχα αρνητική επίδραση στη λειτουργία του.

Η ηλεκτρομαγνητική συμβατότητα είναι δηλαδή ο κλάδος της ηλεκτρικής μηχανικής που ασχολείται με τη δυσλειτουργία ηλεκτρικού ή ηλεκτρονικού εξοπλισμού που προκαλείται για παράδειγμα από ηλεκτρικά, μαγνητικά ή ηλεκτρομαγνητικά πεδία ή φαινόμενα. Βασικός παράγοντας για τη διασφάλιση της ηλεκτρομαγνητικά συμβατής λειτουργίας ηλεκτρολογικού εξοπλισμού είναι η σωστή κατασκευή και σχεδιασμός του εξοπλισμού.

Οι εκπομπές παρεμβολών EMC και η ατρωσία παρεμβολών ρυθμίζονται παγκοσμίως από πρότυπα, κατευθυντήριες γραμμές και νομοθεσία.

Στην περίπτωση συσκευών που παρέχονται έτοιμες προς χρήση συνήθως αρκεί να λειτουργούν σύμφωνα με την τεκμηρίωση του κατασκευαστή προκειμένου να τηρούνται οι οριακές τιμές EMC και να επιτυγχάνει μια ικανοποιητική λειτουργία. Για τη διασφάλιση της τήρησης EMC η ευρωπαϊκή Ένωση έκδωσε την οδηγία 2014/30/EU για πίνακες ελέγχου και οι διαδικασίες επαλήθευσης που ορίζονται από τα παρακάτω πρότυπα στον Πίνακα 7: [9] [10] [11] [12]

Πίνακας 7. Πρότυπα EMC

Πρότυπο	Τίτλος
EN 61439-	Συστήματα διακοπτών και ελέγχου χαμηλής τάσης (Low-voltage switchgear and controlgear assemblies)
EN 61000-6-	Ηλεκτρομαγνητική συμβατότητα (Electromagnetic compatibility), EMC • Ανοσία για κατοικίες, επαγγελματικούς χώρους και ελαφρά-βιομηχανικά περιβάλλοντα. • Ανοσία για βιομηχανικά περιβάλλοντα. • Πρότυπο εκπομπών για κατοικίες, εμπορικά και ελαφρά-βιομηχανικά περιβάλλοντα. • Πρότυπο εκπομπών για βιομηχανικά περιβάλλοντα
EN 61800-3	Συστήματα ηλεκτρικής ισχύος ρυθμιζόμενης ταχύτητας (Adjustable speed electrical power drive systems) Απαιτήσεις και ειδικές μέθοδοι δοκιμών
EN 55011 / CISPR11	Βιομηχανικός, επιστημονικός και ιατρικός (ISM) εξοπλισμός ραδιοσυχνοτήτων • Χαρακτηριστικά ηλεκτρομαγνητικής διαταραχής • Όρια και μέθοδοι μέτρησης

Φαινόμενα EMC

Οι ηλεκτρομαγνητικά επαγόμενες παρεμβολές μπορούν να έχουν διάφορες επιπτώσεις σε ηλεκτρικές εγκαταστάσεις όπως:

- Ασταθή συστήματα ελέγχου
- Σποραδικά δυσλειτουργίες
- Βλάβες του εξοπλισμού μέτρησης
- Δυσλειτουργίες του εξοπλισμού επικοινωνίας
- Αστοχία ή ανεπανόρθωτη ζημιά σε συσκευές και τμήματα εγκαταστάσεων

Αιτίες παρεμβολών

- Αναπήδηση μηχανικών επαφών
- Ενεργοποίηση και απενεργοποίηση λαμπτήρων φθορισμού
- Σύνδεση ανοιχτού κυκλώματος καλωδίων
- Διαδικασία ανάφλεξης σε εξοπλισμό συγκόλλησης
- Αποσύνδεση επαγωγικών φορτίων, μετασχηματιστών, αντιδραστήρων κ.λπ. που εγκαθίστανται παράλληλα στην πηγή τάσης
- Συσκευές μεταγωγής υψηλής συχνότητας (μετατροπείς συχνότητας, μονάδες τροφοδοσίας κ.λπ.)
- Ηλεκτρονικά συστήματα ελέγχου υψηλής συχνότητας (π.χ. οθόνες LCD)

- Εναλλασσόμενη τάση τροφοδοσίας 50 Hz
- Αλλαγές σήματος στα καλώδια ελέγχου και δεδομένων
- Σήματα ρολογιού υψηλής και χαμηλής συχνότητας
- Φαινόμενα που σχετίζονται με απενεργοποίηση επαγωγικών φορτίων, π.χ. ρελέ πάνω σε πλακέτες τυπωμένων κυκλωμάτων
- Μαγνητικά πεδία που προκαλούνται από μονάδες αποθήκευσης
- Σπινθήρα όταν ανοίγουν και κλείνουν επαφές

1.6.1 Βασικοί κανόνες EMC

Εάν ακολουθηθούν οι βασικοί κανόνες και τηρηθούν οι προδιαγραφές στην τεχνική τεκμηρίωση για τη συγκεκριμένη συσκευή που αναφέρονται παρακάτω τότε ένας πίνακας ελέγχου θα μπορεί είναι συμβατός με EMC και να λειτουργεί ικανοποιητικά.

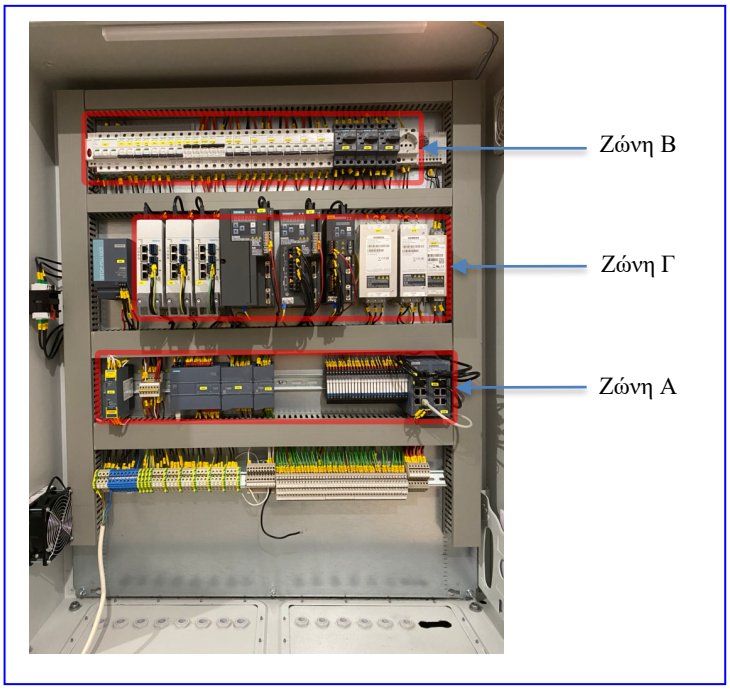
- Διαχωρισμός πηγών και θυμάτων παρεμβολών
  - Ζώνη EMC
  - Ξεχωριστή δρομολόγηση καλωδίων
- Λειτουργική γείωση και ισοδυναμική σύνδεση
- Χρήση θωρακισμένων καλωδίων
- Φίλτρα και κυκλώματα καταστολής

<u>Διαχωρισμός πηγών και θυμάτων παρεμβολών</u>

Ο ευκολότερος τρόπος εφαρμογής μέτρων καταστολής παρεμβολών σε έναν πίνακα ελέγχου είναι να διασφαλιστεί ότι οι πηγές παρεμβολών και τα θύματα παρεμβολών διαχωρίζονται χωροταξικά ως εξής:

- Κατηγοριοποιήση κάθε συσκευής ως πηγή παρεμβολών ή ως θύμα παρεμβολών.
- Διαχωρισμός ολόκληρου του πίνακα ελέγχου σε ζώνες EMC και αντιστοίχιση των συσκευών σε αυτές τις ζώνες.
- Αποτροπή της εκπομπής παρεμβολών από τις πηγές παρεμβολών:
  - Ισοδυναμική συγκόλληση
  - Θωράκιση
  - Φίλτρα και κυκλώματα καταστολής
- Παροχή προστασίας στα θύματα παρέμβασης:
  - Ισοδυναμική συγκόλληση
  - Θωράκιση

<u>Ζώνες EMC σε έναν πίνακα ελέγχου</u>

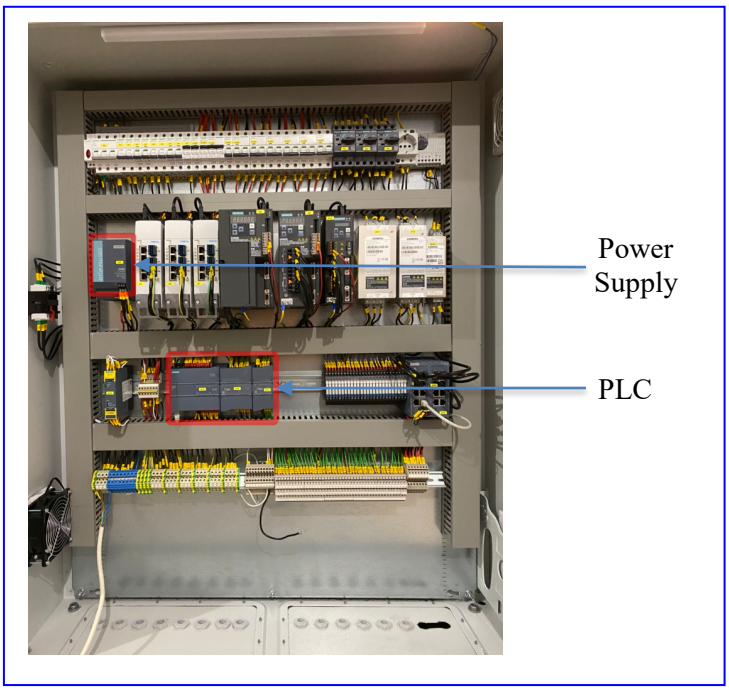


Εικόνα 1. Πίνακας ελέγχου

Ζώνη Α	Σύστημα ελέγχου και αισθητήρες (θύματα) π.χ. PLC, ρελέ ασφαλείας, εξοπλισμός αισθητήρων
Ζώνη Β	Χειριστήρια και σύνδεση δικτύου (πηγές και θύματα) π.χ. SIRIUS, ασφάλειες, διακόπτες, επαφές, σύνδεση ρεύματος
Ζώνη Γ	Ηλεκτρονικά ισχύος (πηγές) π.χ. Inverter που περιλαμβάνει ανορθωτή, μονάδα πέδησης, μετατροπέα και διακόπτες κυκλώματος άκρου κινητήρα, αντιδραστήρες και φίλτρα

1.6.2 Ζώνη Α: "Σύστημα ελέγχου και αισθητήρες (θύματα)"

Στη Ζώνη Α αντιστοιχούν συσκευές που είναι επιρρεπείς σε παρεμβολές του πίνακα ελέγχου μας με κυριότερο το σύστημα αυτοματισμού. Το επιτρεπόμενο περιβάλλον EMC για έναν ελεγκτή ορίζεται σύμφωνα με το πρότυπο EN 61000-6-4-2011. [13]



Εικόνα 2. PLC-Power Supply

Η Ζώνη Α στο παράδειγμά μας περιέχει επίσης μια μονάδα τροφοδοσίας Power Supply. Οι μονάδες τροφοδοσίας μερικές φορές αποτελούν πηγή ουσιαστικών παρεμβολών λόγω της παλμικής τάσης συνεχούς ρεύματος. Δεν έχει όμως νόημα να εγκατασταθεί σε ξεχωριστή θέση γιατί τότε θα ήταν απαραίτητα να γίνει διαχωρισμός της δρομολόγησης των καλωδίων 24VDC.

Πίνακας 8. Αξιολόγηση για επαλήθευση EMC

EMC περιβάλλον	Πληροφορίες του συστήματος αυτοματισμού PLC		Αξιολόγηση για επαλήθευση EMC
	EN 61000-6-2 / EN 61000-6-4	EN 55011	
Βιομηχανικό περιβάλλον	Βιομηχανικό περιβάλλον	Ζώνη Α	Ο εξοπλισμός μπορεί να χρησιμοποιηθεί σε βιομηχανικά περιβάλλοντα.
Οικιστικό περιβάλλον	-	Ζώνη Β εάν τα ακόλουθα πληρούνται οι προϋποθέσεις: • Τοποθέτηση γείωσης σε πίνακες ελέγχου, χειριστήρια	Ο εξοπλισμός μπορεί να χρησιμοποιηθεί σε οικιστικά περιβάλλοντα υπό συγκεκριμένες συνθήκες.

		• Χρήση φίλτρων στις ηλεκτρικές γραμμές τροφοδοσίας	

1.6.2.1 Φαινόμενα EMC που σχετίζονται με ελεγκτές

Ο εξοπλισμός ενός ελεγκτή και τα εξαρτήματά τους πρέπει να έχουν αναπτυχθεί για χρήση σε βιομηχανικό περιβάλλον και να πληρούν όλες τις νόμιμες απαιτήσεις EMC.

Ωστόσο, πριν την εγκατάσταση ενός ελεγκτή πρέπει να πραγματοποιηθεί αξιολόγηση EMC προκειμένου να εντοπιστούν τυχόν πιθανές πηγές παρεμβολών.

Οι ηλεκτρομαγνητικές παρεμβολές συνδέονται στο σύστημα αυτοματισμού από διάφορους δρόμους. Οι κύριες μορφές παρεμβολής παρατίθενται παρακάτω:

- Ηλεκτρομαγνητικά πεδία που έχουν άμεση επίδραση στο σύστημα.
- Παρεμβολές που συνδέονται στο σύστημα μέσω δικτύων επικοινωνίας.
- Παρεμβολές που συνδέονται μέσω καλωδίωσης της διεργασίας.
- Παρεμβολές που φτάνουν στο σύστημα μέσω του τροφοδοτικού ή/και της προστατευτικής γείωσης.

1.6.2.2 Μέτρα EMC για ελεγκτές

<u>Δρομολόγηση καλωδίων με προστασία από παρεμβολές</u>

Οι παρεμβολές μπορούν να φτάσουν στο σύστημα αυτοματισμού μέσω διαφόρων μηχανισμών ζεύξης ανάλογα με το μέσο διάδοσης και την απόσταση μεταξύ της πηγής παρεμβολής και του θύματος. Για την αποφυγή των παρεμβολών πρέπει να υλοποιηθούν τα παρακάτω:

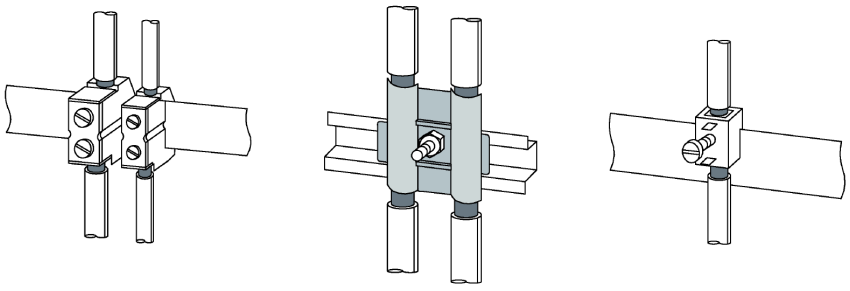
- Αντιστοίχιση των καλωδίων σε διαφορετικές κατηγορίες ανάλογα με την ευαισθησία τους στις παρεμβολές. Όσο μεγαλύτερη είναι η απόσταση που μπορεί να διατηρηθεί μεταξύ των διαφορετικών κατηγορίες καλωδίων, τόσο χαμηλότερο είναι το επίπεδο αμοιβαίας παρεμβολής μεταξύ των καλωδίων λόγω της χωρητικής και της επαγωγικής σύζευξης.
- Τα καλώδια που εισέρχονται στον πίνακα ελέγχου να μην οδεύουν παράλληλα.
- Εάν τα καλώδια εγκατασταθούν σε μεταλλικούς αγωγούς καλωδίων τότε μπορούν να τοποθετηθούν γειτονικά το ένα με το άλλο.
- Σύνδεση των μεταλλικών αγωγών στο σύστημα εξισορρόπησης δυναμικού.
- Εάν δεν μπορεί να αποφευχθεί η κατά μήκος διέλευση των καλωδίων, να τοποθετηθούν υπό γωνία 90° στα σημεία διέλευσης όπου είναι δυνατόν, προκειμένου έτσι να ελαχιστοποιηθούν οι παρεμβολές που προκαλούνται από τα ηλεκτρικά πεδία.

<u>Θωράκιση καλωδίων</u>

Ο σκοπός της θωράκισης των καλωδίων είναι η εξασθένηση (απόσβεση) των μαγνητικών, ηλεκτρικών ή των ηλεκτρομαγνητικών πεδίων παρεμβολής. Τα ρεύματα παρεμβολής στα προστατευτικά καλωδίων εκκενώνονται σε γείωση μέσω της σύνδεσης θωράκισης. Για να διασφαλιστεί ότι αυτά τα ρεύματα παρεμβολής δεν μπορούν να γίνουν μια πηγή παρεμβολής, είναι ιδιαίτερα σημαντικό να παρέχεται χαμηλή αντίσταση σύνδεσης με τον προστατευτικό αγωγό. Για την επίτευξη της θωράκισης πρέπει να υλοποιηθούν τα παρακάτω:

- Χρησιμοποίηση καλωδίων με πλεγμένη θωράκιση όπου είναι δυνατόν. Η θωράκιση πρέπει να κάνει περισσότερο από 80 % επαφή στο σημείο σύνδεσης.
- Σύνδεση των προστατευτικών καλωδίων στη γείωση και στα δύο άκρα του καλωδίου. Μόνο με σύνδεση της θωράκισης στη γείωση και στα δύο άκρα μπορούν οι παρεμβολές χαμηλής και υψηλής συχνότητας να μειωθούν.
- Εάν υπάρχει διαφορά δυναμικού μεταξύ των σημείων γείωσης ένα ρεύμα αντιστάθμισης μπορεί να ρέει κατά μήκος της γειωμένης θωράκισης. Σε αυτήν την περίπτωση θα πρέπει να εγκατασταθεί ένα πρόσθετο ισοδυναμικό καλώδιο.
- Εάν δεν υπάρχει η δυνατότητα εγκατάστασης ισοδυναμικού καλωδίου (π.χ. σε μεγάλης κλίμακας εγκατάσταση) τότε θα πρέπει να γίνει σύνδεση το ένα άκρο της θωράκισης στη γείωση μέσω ενός χωρητικού συνδέσμου. Αυτή η λύση είναι αποτελεσματική μόνο στη μείωση των παρεμβολών υψηλής συχνότητας.
- Οι ακόλουθοι τύποι σύνδεσης θωράκισης έχουν αποδειχθεί επιτυχείς για χρήση σε συσκευές που δεν είναι εξοπλισμένες με ειδικούς σφιγκτήρες θωράκισης:
  - Χρησιμοποίηση μεταλλικών λαβών για την στερέωση των θωρακίσεων των καλωδίων. Οι συνδέσεις πρέπει να παρέχουν μια καλή ηλεκτρική επαφή και μια σύνδεση μεγάλης επιφάνειας με την θωράκιση.
  - Στερέωση της θωράκισης σε μια προστατευτική ράβδο ακριβώς μετά το σημείο εισόδου του καλωδίου στο ερμάριο.

Η παρακάτω Εικόνα 3 δείχνει τους τύπους σύνδεσης θωράκισης που χρησιμοποιούνται συνήθως.



Εικόνα 3. Τύποι σύνδεσης θωράκισης

Ισοδυναμική συγκόλληση

Η ηλεκτρομαγνητική παρεμβολή μπορεί να προκαλέσει μεγάλες αποκλίσεις στο δυναμικό μεταξύ των εξαρτημάτων του πίνακα ελέγχου. Τα υψηλά αντισταθμιστικά ρεύματα που αναπτύσσονται μπορούν να έχουν σαν αποτέλεσμα ανεπιθύμητες ενέργειες (π.χ. δυσλειτουργίες ή ζημιές) στα εξαρτήματα. Μέσα στον πίνακα ελέγχουν πρέπει να γίνουν:

- Σύνδεση των καλωδίων σύνδεσης ισοδυναμικού σε μια μεγάλη περιοχή επαφής με τη γείωση.
- Προστασία των σημείων σύνδεσης από τη διάβρωση.
- Μη δημιουργία βρόχων γείωσης.
- Όδευση των καλωδίων ισοδυναμικής σύνδεσης όσο το δυνατόν πιο κοντά στα καλώδια σήματος.
- Όσο μικρότερη είναι η σύνθετη αντίσταση του καλωδίου σύνδεσης ισοδυναμικού, τόσο μεγαλύτερο είναι το ισοδυναμικό δεσμευτικό αποτέλεσμα. Η σύνθετη αντίσταση του επιπλέον εγκατεστημένου καλωδίου ισοδυναμικής σύνδεσης δεν πρέπει να υπερβαίνει το 10 % της σύνθετης αντίστασης θωράκισης.
- Προκειμένου να αποφευχθεί ο σχηματισμός βρόχων γείωσης, τα καλώδια ισοδυναμικής συγκόλλησης πρέπει να δρομολογούνται παράλληλα και όποτε είναι δυνατόν κοντά στο καλώδιο σήματος/διαύλου. Αυτό θα ελαχιστοποιήσει το μέγεθος της περιοχής μεταξύ των δύο καλωδίων.

1.6.3 Ζώνη Β: "Στοιχεία ελέγχου και σύνδεση δικτύου (πηγές παρεμβολών και θύματα)"

1.6.3.1 Επαφές και συγκροτήματα επαφών

Τα εξαρτήματα σύνδεσης στο δίκτυο αντιστοιχούν στη ζώνη Β του πίνακα ελέγχου. Οι επαφές με προστασία από παρεμβολές είναι ένα παράδειγμα ενός εξαρτήματος από τη ζώνη Β.

Εικόνα 4. Εξαρτήματα σύνδεσης

Τα ρελέ συζεύξης για κινητήρες μεταγωγής καθώς και για βοηθητικά κυκλώματα και κυκλώματα ελέγχου πρέπει να είναι ειδικά σχεδιασμένα για λειτουργία με ηλεκτρονικούς ελεγκτές. Τα βασικά χαρακτηριστικά αυτών των ρελέ σύζευξης πρέπει να έχουν χαμηλή κατανάλωση ενέργειας και εκτεταμένο εύρος λειτουργίας του πηνίου.

Η εξαιρετική αξιοπιστία επαφής των βοηθητικών επαφών εγγυάται ότι δεν θα υπάρχουν ψευδή σήματα ακόμη και σε χαμηλές ικανότητες μεταγωγής. Ένα ολοκληρωμένο σύστημα απόσβεσης υπέρτασης προστατεύει τα ευαίσθητα στάδια εξόδου από υπερτάσεις ανοίγματος πηνίου.

Εικόνα 5. Coupling Relay

Τα ρελέ σύζευξης μπορούν να αντικατασταθούν με στοιχεία RC ή Varistor για την απόσβεση των υπερτάσεων ανοίγματος στο πηνίο. Επίσης μπορούν να χρησιμοποιηθούν δίοδοι καταστολής θορύβου και δίοδοι Zener για σύντομους χρόνους διαλείμματος.

Εικόνα 6. Varistor

1.6.3.2 Περιβάλλον EMC για επαφές

Επαλήθευση EMC

Για να επιβεβαιωθεί η συμμόρφωση με την EMC πρέπει πρώτα να γίνει έλεγχος εάν ο εξοπλισμός έχει εγκριθεί για χρήση στο προβλεπόμενο περιβάλλον σύμφωνα με το συγκεκριμένο πρότυπο.

Δεδομένου ότι οι επαφές δεν περιέχουν κανένα ηλεκτρονικό κύκλωμα, δεν είναι ευαίσθητες σε ηλεκτρομαγνητικές παρεμβολές και επομένως δεν υπόκεινται σε κανένα πρότυπο προϊόντος EMC ή γενικό πρότυπο. Επομένως, δεν είναι απαραίτητο να πραγματοποιηθούν δοκιμές ανοσίας παρεμβολών για αυτά τα εξαρτήματα και καμία προδιαγραφή σχετικά με τη δοκιμή δεν περιλαμβάνεται στη τεκμηρίωση. Οι επαφές με μηχανισμό λειτουργίας στερεάς κατάστασης (solid-state) αναπτύσονται για το περιβάλλον Α σύμφωνα με το IEC/EN 60947-1, το IEC/EN 60947-4-1 ή την Κλάση Α σύμφωνα με το CISPR 11. [14]

Φαινόμενα EMC που σχετίζονται με επαφές

Τάσεις υπέρτασης

Οι υπερτάσεις εμφανίζονται όταν τα πηνία απενεργοποιούνται (επαγωγικά φορτία), κορυφές τάσης έως 4 kV μπορούν να προκύψουν με ρυθμό ανόδου της τάσης 1 kV/μsec. Αυτό οδηγεί σε:

- Ουσιαστική διάβρωση ως αποτέλεσμα της πρόωρης φθοράς των επαφών του πηνίου.
- Δημιουργία σημάτων παρεμβολής που οδηγούν σε ψευδή σήματα στους ηλεκτρονικούς ελεγκτές.

Επομένως όλα τα πηνία επαφής θα πρέπει να είναι εξοπλισμένα με στοιχεία απόσβεσης για εξασθένηση υπερτάσεων ιδιαίτερα όταν τα πηνία λειτουργούν σε συνδυασμό με ηλεκτρονικούς ελεγκτές. Επιπλέον ο υψηλός ρυθμός ανόδου των παραγόμενων κυματομορφών τάσης μπορεί να οδηγήσει σε χωρητική σύζευξη σημαντικών σημάτων παρεμβολής με γειτονικά συστήματα. Αυτό απαιτεί ένα κύκλωμα RC απευθείας στη θέση όπου προήλθε η πηγή παρεμβολής, δηλαδή στο πηνίο. Αυτό αποτρέπει την εμφάνιση υπερτάσεων απευθείας στη θέση προέλευσης και προστατεύει τα ηλεκτρονικά εξαρτήματα

που είναι επίσης ευαίσθητα στην τάση. Ακόμη αποτρέπει τη χωρητική σύζευξη των σημάτων παρεμβολής με τα καλώδια ελέγχου των ηλεκτρονικών κυκλωμάτων.

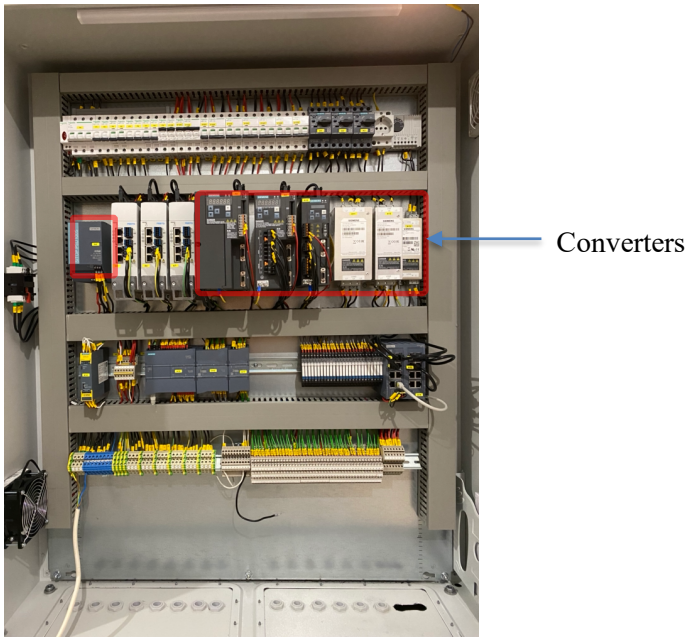
Μέθοδοι απόσβεσης

Τα ακόλουθα στοιχεία κυκλώματος RC χρησιμοποιούνται συνήθως για την απόσβεση υπερτάσεων και είναι συνδεδεμένα παράλληλα με το πηνίο:

- Δίοδος ελεύθερου τροχού (Freewheeling diode).
- Συνδυασμός διόδων (Diode combination).
- Βαρίστορς (Varistors).
- Δίοδος καταστολής (Suppressor diode).
- Στοιχείο RC (RC element).

1.6.4 Ζώνη Γ: "Ηλεκτρονικά ισχύος (πηγές)"

Η Ζώνη Γ του πίνακα ελέγχου περιέχει τον εξοπλισμό ηλεκτρονικών ισχύος όπως σύστημα κίνησης Converter.



Εικόνα 7. Converters

Για την επιβεβαίωση της ηλεκτρομαγνητικής συμβατότητας πρέπει πρώτα να γίνει έλεγχος εάν ο εξοπλισμός έχει εγκριθεί για χρήση στο προβλεπόμενο περιβάλλον. Στον

παρακάτω Πίνακα 9 φαίνεται η επαλήθευση EMC π.χ. για συστήματα οδήγησης κινητήρων (Drive Systems).

Πίνακας 9. Επαλήθευση EMC

Περιβάλλον EMC	EN 61800-3	Αξιολόγηση για επαλήθευση EMC
Βιομηχανικό Περιβάλλον	Εκπληρώνεται με Κατηγορία C3	Ο εξοπλισμός μπορεί να χρησιμοποιηθεί σε βιομηχανικά περιβάλλοντα εάν έχει εγκατασταθεί και παραγγελθεί από ειδικό προσωπικό.
Οικιστικό Περιβάλλον	Εκπληρώνεται υπό όρους με Κατηγορία C2	Επιτρέπεται η χρήση σε κατοικημένες περιοχές με την επιφύλαξη της εκπλήρωσης των παρακάτω συνθηκών: • Ο εξοπλισμός έχει παραγγελθεί και εγκατασταθεί από ειδικό προσωπικό. • Έχει εγκατασταθεί ένα φίλτρο γραμμής στο διασφαλίζει τη συμμόρφωση με το όριο τιμές που ορίζονται σύμφωνα με EN 61800-3, Κατηγορία Γ2.

1.6.4.1 Φαινόμενα EMC που σχετίζονται με μετατροπείς (Converters)

Οι μετατροπείς συχνότητας είναι ισχυρές πηγές ηλεκτρομαγνητικών παρεμβολών. Τα συνήθης φαινόμενα που μπορούν να προκύψουν με την λειτουργία μιας μονάδας μετατροπέα δίνονται παρακάτω:

- Ξαφνικές δυσλειτουργίες μηχανημάτων και εξοπλισμού, συστημάτων πληροφορικής και τηλεφώνου χωρίς να είναι ευδιάκριτη η αιτία.
- Λανθασμένη ενεργοποίηση των προστατευτικών διακοπτών ή των αυτόματων διακοπτών.
- Συχνές βλάβες των τροφοδοτικών μεταγωγής, π.χ. σε συστήματα πληροφορικής.
- Καταστροφή των πυκνωτών, σε συστήματα αντιστάθμισης άεργου ισχύος και συστήματα φίλτρων.
- Υπερθέρμανση καλωδίων, κινητήρων, εξοπλισμού που συνδέονται απευθείας με το δίκτυο παροχής και εξοπλισμού όπως ασφάλειες, επαφές κ.λπ.
- Ανάπτυξη θορύβου (βουητό), για παράδειγμα σε διακόπτες, κινητήρες και μετασχηματιστές που είναι συνδέεται απευθείας με την παροχή ρεύματος.
- Υπερβολικό φορτίο στον ουδέτερο αγωγό, π.χ. στην τεχνολογία κτιρίων όταν πολλοί μονοφασικοί μετατροπείς/συσκευές λειτουργούν στην παροχή ρεύματος με ανορθωτές B2 ($3^{η}$ αρμονική).

Εκτός από τις άμεσες επιπτώσεις μπορεί να υπάρξουν μακροπρόθεσμες επιπτώσεις όπως:

- Ταχεία γήρανση των συσκευών για αντιστάθμιση άεργου ισχύος, σε συστήματα και ηλεκτρονικές συσκευές κ.λπ.
- Κακός συντελεστής ισχύος με αυξημένες απώλειες του συστήματος.

1.6.4.2 Μέτρα EMC για πίνακα ελέγχου

Οι διαδικασίες που πρέπει να υλοποιηθούν σε έναν πίνακα ελέγχου για να έχουμε EMC είναι τα παρακάτω:

- Αντιστοίχιση όλων των συσκευών που πρόκειται να εγκατασταθούν στον πίνακα ελέγχου στην κατηγορία "πηγή παρεμβολής" ή "θύμα παρεμβολής".
- Μετά την ολοκλήρωση της κατηγοριοποίησης των συσκευών, διαίρεση του πίνακα ελέγχου EMC.
- Λήψη μέτρων για την ηλεκτρομαγνητική αποσύνδεση των ζωνών. Τέτοια μέτρα αποσύνδεσης περιλαμβάνουν, για παράδειγμα, μεγάλες χωρικές αποστάσεις (περίπου 20cm). Καλύτερη και μεγαλύτερη εξοικονόμηση χώρου είναι η αποσύνδεση χρησιμοποιώντας ξεχωριστά μεταλλικά περιβλήματα ή μεγάλα μεταλλικά χωρίσματα. Εγκατάσταση όλων των εξαρτημάτων σε μια γυμνή και εξαιρετικά αγώγιμη μεταλλική πλάκα στήριξης. Σύνδεση της πλάκας στερέωσης έτσι ώστε να είναι ηλεκτρικά αγώγιμη με τη ράγα γείωσης και της ράγας θωράκισης EMC, π.χ. χρησιμοποιώντας πλεγμένες χάλκινες ταινίες
- Σύνδεση επίσης των πορτών του πίνακα ελέγχου στις πλαϊνές ράγες του πίνακα με μια πλεγμένη χάλκινη ταινία για βελτιωμένη εκφόρτιση παρεμβολών υψηλής συχνότητας.
- Γείωση ολόκληρου του πίνακα ελέγχου με τρόπο συμβατό με την ηλεκτρομαγνητική συμβατότητα.

1.6.4.3 Καλωδίωση συμβατή με EMC

Όλα τα καλώδια επικοινωνίας, αναλογικών σημάτων και τα καλώδια των κινητήρων από τους μετατροπείς πρέπει να θωρακίζονται μέσα και έξω από τον πίνακα ελέγχου. Το καλώδιο τροφοδοσίας του μετατροπέα πρέπει να είναι θωρακισμένο κατάντη του φίλτρου προς τον μετατροπέα.

Για τη συμβατότητα με EMC η δρομολόγηση καλωδίων στον πίνακα ελέγχου και στο σύστημα πρέπει να υλοποιηθεί ως εξής:

- Διατήρηση όλων των καλωδίων στον πίνακα ελέγχου όσο το δυνατόν πιο κοντά.
- Ξεχωριστή διέλευση των θωρακισμένων και των μη θωρακισμένων καλωδίων τροφοδοσίας και σήματος (εκτός από σύντομα τμήματα καλωδίου) και με ελάχιστη απόσταση μεταξύ τους 20cm. Επιτρέπεται η διασταύρωση καλωδίων.
- Μη δρομολόγηση καλωδίων από διαφορετικές ζώνες σε κοινόχρηστες πλεξούδες καλωδίων ή αγωγούς καλωδίων. Σύνδεση πάντα της θωράκισης και στα δύο άκρα χρησιμοποιώντας ένα στήριγμα θωράκισης συγκόλλησης 360°. Εάν είναι δυνατόν σύνδεση των θωρακισμένων καλωδίων στη συσκευή χωρίς ενδιάμεσους ακροδέκτες.
- Στερέωση της θωράκισης στον πίνακα ελέγχου και στον κινητήρα έτσι ώστε να έχει σύνδεση 360° με το στήριγμα θωράκισης ή την πλάκα στερέωσης.
- Οι θωρακίσεις των καλωδίων για αναλογικά σήματα πρέπει να συνδέονται και στα δύο άκρα με ισοδυναμική σύνδεση μεταξύ εξόδου και εισόδου.

1.6.4.4 Επαλήθευση συμμόρφωσης με την Οδηγία EMC 2014/30/ΕΕ

Παρακάτω περιγράφεται η διαδικασία για την επαλήθευση της συμμόρφωσης με το EMC 2014/30/ΕΕ σε συνδυασμό με τα εναρμονισμένα πρότυπα EN 61439-1 και EN 61439-2 (Πίνακας 10):

Πίνακας 10. Επαλήθευσης συμμόρφωσης με EMC

α/α	Συνθήκη	Εύρεση πληροφοριών	Εκτίμηση		Επαλήθευση / Τεκμηρίωση	
			Τήρηση Συνθηκών	Μη τήρηση Συνθηκών	Διαθέσιμη	Μη Διαθέσιμη
1	Είναι ο εξοπλισμός εγκεκριμένος για χρήση στο συγκεκριμένο περιβάλλον;	Τεκμηρίωση από τα χαρακτηριστικά του εξοπλισμού				
2	Έχει εγκατασταθεί ο εξοπλισμός σύμφωνα με τις προδιαγραφές του κατασκευαστή;	Τεκμηρίωση από τα χαρακτηριστικά του εξοπλισμού				
3	Εφαρμόζονται τα πιο πρόσφατα εναρμονισμένα πρότυπα;	Πρότυπα για πίνακες ελέγχου: Π.χ. EN 61439-1 και EN 61439-2				
4	Έχει γίνει ανάλυση και αξιολόγηση των κινδύνων της EMC;	Π.χ. με το CENELEC 32				
5	Συμμορφώνεται ο εξοπλισμός με τις απαιτήσεις της EMC 2014/30/ΕΕ;	Οδηγία EMC 2014/30/EU				

Σημείωση

Τα γενικά γνωστά μέτρα EMC δεν έχουν πάντα το επιθυμητό αποτέλεσμα σε όλες τις εφαρμογές. Εάν η θωράκιση των καλωδίων π.χ. ενός αναλογικού σήματος πρέπει να συνδεθεί στο ένα ή και στα δύο τα άκρα εξαρτάται από την πηγή παρεμβολής ή/και τη διαδρομή σύζευξης.

Επομένως ισχύουν τα εξής:

Η τεχνική τεκμηρίωση που παρέχεται με τις συσκευές ή τα εξαρτήματα που χρησιμοποιούνται είναι πάντα το δεσμευτικό έγγραφο σχετικά με τα μέτρα EMC. Πρέπει να τηρούνται οι οδηγίες που περιέχονται στην τεχνική τεκμηρίωση σχετικά με την εγκατάσταση, τη λειτουργία των εξαρτημάτων για την ηλεκτρομαγνητική συμβατότητα.

Πίνακας 11. Διαχωρισμός πηγών και θυμάτων παρεμβολών

α/α	Συνθήκη	Τήρηση Συνθηκών	Μη τήρηση Συνθηκών
1	Εφαρμόστηκαν οι ζώνες EMC;		
2	Λήφθηκαν τα κατάλληλα μέτρα (χωρίσματα, αποστάσεις, κ.λπ.) μεταφέρθηκαν ξεχωριστά οι πηγές και τα θύματα της παρεμβολής;		
3	Λήφθηκαν τα κατάλληλα μέτρα (μεταλλικοί αγωγοί καλωδίων, απόσταση, κ.λπ.) για την όδευση των καλωδίων ισχύος και σημάτων χωριστά;		
4	Διατηρήθηκαν τα καλώδια σε μήκος όσο το δυνατόν πιο κοντά;		
5	Τα καλώδια σημάτων είναι εγκατεστημένα όσο το δυνατόν πιο κοντά σε γειωμένα εξαρτήματα;		

Πίνακας 12. Λειτουργική γείωση και ισοδυναμική σύνδεση

α/α	Συνθήκη	Τήρηση Συνθηκών	Μη τήρηση Συνθηκών
6	Υπάρχει ανάγκη για ισοδυναμική σύνδεση και έχει εφαρμοστεί;		
7	Είναι όλα τα μεταλλικά μέρη ανενεργά συμπεριλαμβανομένου και του δίαυλου της θωράκισης και έχουν μεγάλη και αγώγιμη επαφή σύνδεσης;		
8	Έχει εφαρμοστεί η λειτουργική γείωση σύμφωνα με τις προδιαγραφές του κατασκευαστή;		

Πίνακας 13. Θωρακισμένα καλώδια

α/α	Συνθήκη	Τήρηση Συνθηκών	Μη τήρηση Συνθηκών
9	Έχουν ληφθεί τα κατάλληλα μέτρα για να θωρακίσουν τα καλώδια σήματος;		
10	Είναι η σύνδεση θωράκισης υψηλής αγωγιμότητας με μεγάλη περιοχή επαφής; • Καλώδια αναλογικού σήματος με θωράκιση συνδεδεμένη στο ένα άκρο εκτός εάν ορίζεται διαφορετικά από τον κατασκευαστή π.χ. για την αποφυγή βρόχων γείωσης. • Καλώδια ψηφιακού σήματος με θωράκιση συνδεδεμένη και στα δύο άκρα.		
11	Είναι οι θωρακίσεις συνεχείς, δηλαδή με όσο το δυνατόν λιγότερες διακοπές;		
12	Στηρίχθηκαν οι θωρακίσεις των καλωδίων σε μία μεγάλη περιοχή στην είσοδο του πίνακα ελέγχου;		
13	Έχει δρομολογηθεί ένα καλώδιο ισοδυναμικής σύνδεσης παράλληλα με το θωρακισμένο καλώδιο σήματος στις εγκαταστάσεις με διαφορές στο δυναμικό;		

Πίνακας 14. Φίλτρα και κυκλώματα καταστολής των παρεμβολών

α/α	Συνθήκη	Τήρηση Συνθηκών	Μη τήρηση Συνθηκών
14	Έχουν εγκατασταθεί φίλτρα και τα κυκλώματα καταστολής σύμφωνα με τις προδιαγραφές του κατασκευαστή;		
15	Είναι τα επαγωγικά φορτία, π.χ. τα πηνία επαφής εξοπλισμένα με στοιχεία προστασίας υπέρτασης?		

ΚΕΦΑΛΑΙΟ 2

Εφαρμογή Machinery Directive σε μία γραμμή παραγωγής

Οι φάσεις που απαιτούνται για την ασφαλή λειτουργία μίας γραμμής παραγωγής είναι:

1. Εκτίμηση Ρίσκου (Risk Assessment)
2. Μείωση Ρίσκου (Risk Estimation)
3. Επαλήθευση (Verification) βάση προτύπων

Για την καλύτερη κατανόηση των προτύπων θα σχεδιασθεί ένα μηχάνημα τηρώντας τα παραπάνω.

Στο παρακάτω σχήμα φαίνεται το μηχάνημα που πρέπει να σχεδιασθεί.

Η χρήση του μηχανήματος (γραμμή παραγωγής) είναι να μεταφέρονται τα κιβώτια (μέσω του ρομποτικού βραχίονα) από την παλέτα στην ταινία μεταφοράς, στην συνέχεια να οδηγούνται (μέσω της μεταφορικής ταινίας) στο σημείο γεμίσματος, εκεί να γεμίζουν και στη συνέχεια να οδηγούνται στο επόμενο μηχάνημα (γραμμή παραγωγής).

Το μηχάνημα έχει τα παρακάτω τεχνικά χαρακτηριστικά:

- Τριφασική παροχή: 400VAC , 50Hz.
- Θερμοκρασία λειτουργίας: από 0°C έως 50°C.
- Χρήση σε στεγασμένο χώρο: IP54.
- Μέγιστο βάρος κιβωτίου: 20 κιλά.
- Ακτίνα δράσης το ρομποτικού βραχίονα: 2,5μ Χ 2,5μ.
- Χρήση μόνο από εξειδικευμένο προσωπικό, ειδικευόμενοι μόνο με επιτήρηση και δεν υπάρχει πρόσβαση από επισκέπτες.
- Διάρκεια χρόνου λειτουργίας: 200.000 ώρες.

2.1 Εκτίμηση Ρίσκου (Risk Assessment) EN ISO 12100

Για την ανάλυση του Ρίσκου πρέπει να ορίσουν τα όρια της μηχανής, να προσδιορισθούν οι κίνδυνοι και να εκτιμηθούν. Οι κρίσεις αυτές θα πρέπει να υποστηρίζονται από ποιοτική ή ποσοτική εκτίμηση του κινδύνου που σχετίζονται με τους κινδύνους που παρουσιάζουν τα μηχανήματα. [6]

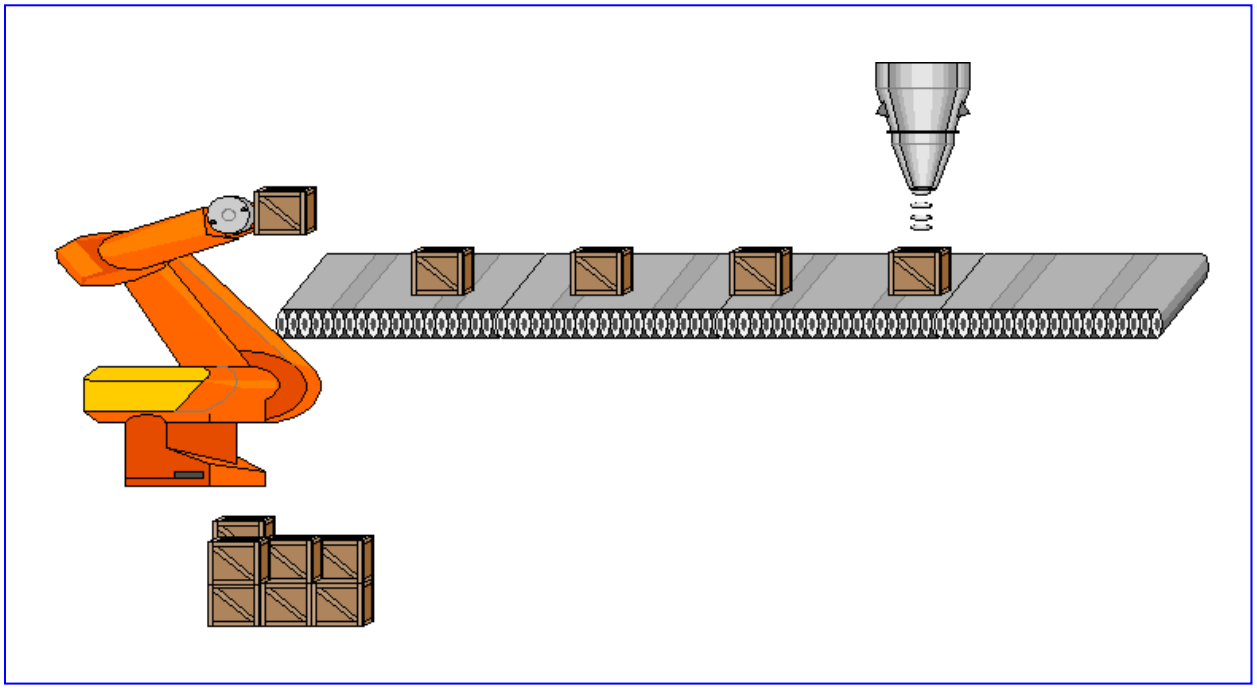
2.1.1 Καθορισμός της μηχανής

Η αξιολόγηση του κινδύνου αρχίζει με τον καθορισμό των ορίων των μηχανημάτων, λαμβανομένων υπόψη όλων των φάσεων της ζωής του μηχανήματος. Αυτό σημαίνει τα χαρακτηριστικά και τις επιδόσεις του μηχανήματος ή μιας σειράς των μηχανών σε μια ολοκληρωμένη διαδικασία και των συναφών ανθρώπων του περιβάλλοντος χώρου και των προϊόντων.

Δηλαδή θα πρέπει να ορισθούν τα:

- όρια της μηχανής: φυσικά όρια της μηχανής, τις διεπαφές ανθρώπου / μηχανής, την παροχή του ηλεκτρικού ρεύματος,

- τα χρονικά όρια: διάρκεια ζωής, διαστήματα συντήρησης, φάσεις λειτουργίας
- και τις ομάδες χρηστών: εκπαίδευση, εμπειρία, δεξιότητες, επισκέπτες.



Εικόνα 8. Γραμμή παραγωγής γεμίσματος κιβωτίων

2.1.2 Προσδιορισμός κινδύνων

Ο προσδιορισμός των κινδύνων πρέπει να γίνει για όλες τις φάσεις της ζωής του μηχανήματος που είναι η συναρμολόγηση, η μεταφορά, η εγκατάσταση, η θέση σε λειτουργία και η λειτουργία. Οι πιθανοί κίνδυνοι που μπορούν να υπάρξουν είναι σπρώξιμο, συντριβή, κόψιμο, συμπίεση, τράβηγμα, τρίψιμο, λείανση.

Οι πιθανοί κίνδυνοι στο μηχάνημα του παραδείγματος είναι:

- Ρομποτικός Βραχίονας: σπρώξιμο και συντριβή
- Ταινία Μεταφοράς: σπρώξιμο και συντριβή
- Σύστημα Γεμίσματος: συντριβή και συμπίεση

2.1.3 Εκτίμηση κινδύνων

Για την εκτίμηση των κινδύνων θα πρέπει να είναι γνωστό εάν υπάρχει ανάγκη πρόσβασης στην επικίνδυνη περιοχή, η διάρκεια έκθεσης, ο αριθμός των ατόμων, η συχνότητα πρόσβασης, εάν η πιθανότητα ενός επικίνδυνου συμβάντος είναι μικρή, μεσαία ή μεγάλη, ο τύπος κίνησης των μηχανημάτων είναι ξαφνικός, γρήγορος ή αργός, ποια είναι τα προσόντα των ατόμων, δυνατότητα ενημέρωσης και διαφυγής.

2.1.4 Αξιολόγηση κινδύνων

Η αξιολόγηση των κινδύνων του μηχανήματος θα πρέπει αρχικά να γίνει ανά υποσύστημα. Στο συγκεκριμένο παράδειγμα υπάρχουν δύο υποσυστήματα και είναι:

Ρομποτικός Βραχίονας

Βαρύτητα Βλάβης	**Πιθανότητα εμφάνισης** A Πολύ Πιθανή	B Πιθανή	C Απίθανη	D Εξαιρετικά Απίθανη
1 Απαραίτητες πρώτες βοήθειες				
2 Απαραίτητη θεραπεία από γιατρό				
3 Σπασμένα άκρα ή κομμένα δάχτυλα				
4 Θάνατος ή χαμένα μάτια ή χαμένα άκρα		**4B**		

Μεταφορά και γέμισμα

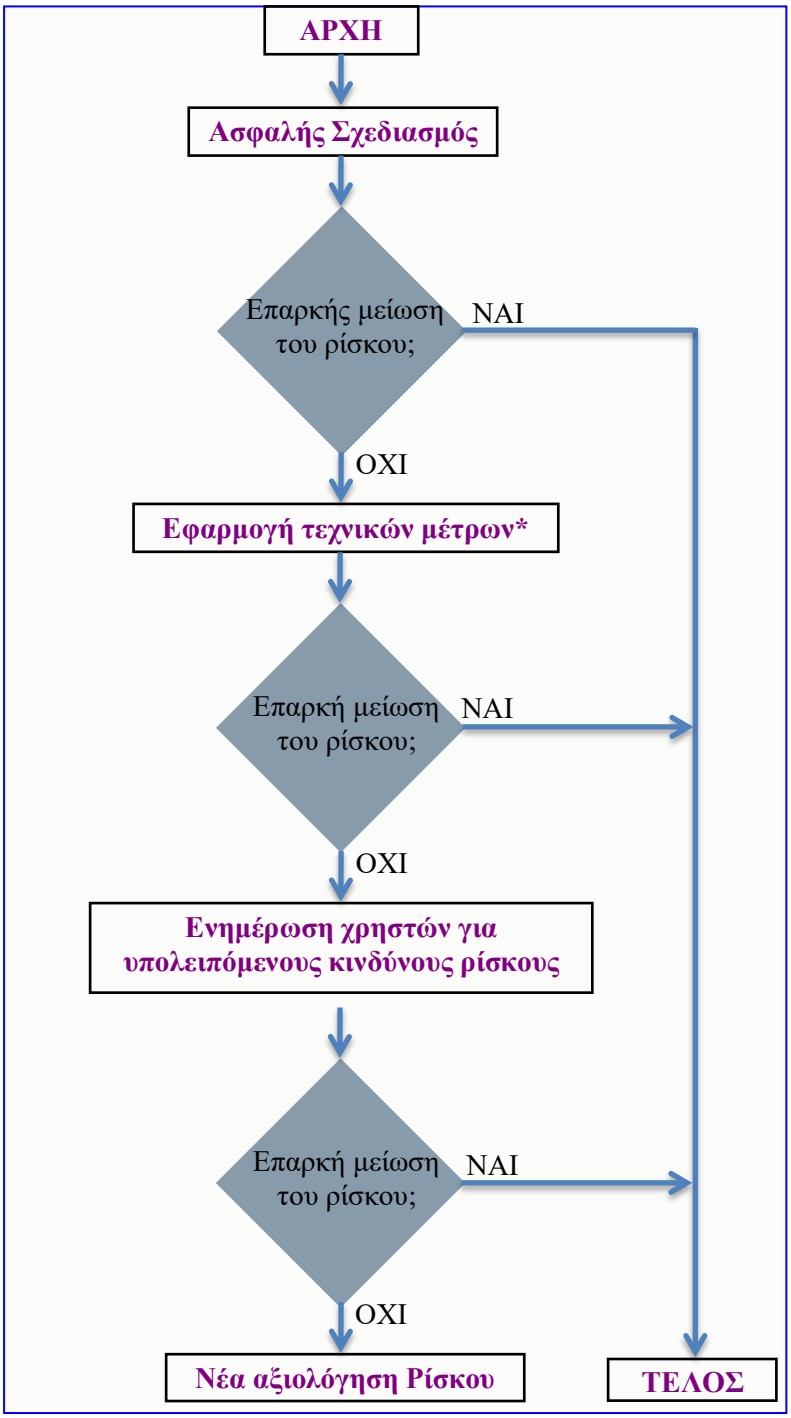
Βαρύτητα Βλάβης	**Πιθανότητα εμφάνισης** A Πολύ Πιθανή	B Πιθανή	C Απίθανη	D Εξαιρετικά Απίθανη
1 Απαραίτητες πρώτες βοήθειες				
2 Απαραίτητη θεραπεία από γιατρό				
3 Σπασμένα άκρα ή κομμένα δάχτυλα		**3B**		
4 Θάνατος ή χαμένα μάτια ή χαμένα άκρα				

Συνολικά για το μηχάνημα έχουμε:

Βαρύτητα Βλάβης	**Πιθανότητα εμφάνισης** A Πολύ Πιθανή	B Πιθανή	C Απίθανη	D Εξαιρετικά Απίθανη
1 Απαραίτητες πρώτες βοήθειες				
2 Απαραίτητη θεραπεία από γιατρό				
3 Σπασμένα άκρα ή κομμένα δάχτυλα		**3B**		
4 Θάνατος ή χαμένα μάτια ή χαμένα άκρα		**4B**		

2.1.5 Εκτίμηση Ρίσκου (Risk Estimation)

Μετά την εκτίμηση του ρίσκου θα πρέπει να εφαρμοσθούν τεχνικές με τις οποίες θα γίνει μείωση του ρίσκου. Στο παρακάτω σχήμα δίνεται η μεθοδολογία που πρέπει να ακολουθηθεί για την μείωση του ρίσκου σύμφωνα με το EN ISO 12100.



Εικόνα 9. Μεθοδολογία μείωσης του ρίσκου

*Τεχνικά μέτρα στο παράδειγμά μας θα μπορούσε να είναι τοποθέτηση προστατευτική περίφραξη για τον βραχίονα και το γεμιστικό.

2.2 Επαλήθευση (Verification) βάση προτύπων

Για τη λειτουργική ασφάλεια μηχανών υπάρχουν 2 πρότυπα με διαφορετικά επίπεδα ασφαλείας:

- EN ISO 13849-1 Performance Levels PL a - e
- IEC 62061 Safety Integrity Levels SIL 1- 3

Η χρήση του EN ISO 13849-1 επιλέγεται-προτείνεται για Safety συστήματα χαμηλής πολυπλοκότητας, ενώ το IEC 62061 επιλέγεται σε σύνθετα Safety συστήματα που κάνουν χρήση Safety PLCs. [1] [15]

Και τα δύο πρότυπα ακολουθούν τα ίδια βήματα:

Αξιολόγηση Κινδύνων (Asses the Risks)

- Κατανομή των μέτρων ασφάλειας (Allocate the safety measures)
- Αρχιτεκτονική Σχεδιασμού (Design Architecture)
- Επικύρωση (Validate)

2.2.1 EN ISO 13849-1 Performance Levels PL a – e

Το ISO 13849 είναι σχετικό ειδικότερα για τις ομάδες που εκπροσωπούν τους παράγοντες της αγοράς όσον αφορά την ασφάλεια των μηχανημάτων:

- κατασκευαστές μηχανών (μικρές, μεσαίες και μεγάλες επιχειρήσεις).
- φορείς υγείας και ασφάλειας (ρυθμιστικές αρχές, οργανισμοί πρόληψης ατυχημάτων, εποπτεία αγοράς κ.λπ.).

Επίσης και σε όσους μπορούν να επηρεαστούν από το επίπεδο ασφάλειας των μηχανημάτων όπως:

- χρήστες/εργοδότες μηχανών (μικρές, μεσαίες και μεγάλες επιχειρήσεις).
- χρήστες/εργαζόμενοι μηχανών (π.χ. συνδικάτα, οργανώσεις για άτομα με ειδικές ανάγκες).
- πάροχοι υπηρεσιών για συντήρηση (μικρές, μεσαίες και μεγάλες επιχειρήσεις).
- καταναλωτές (σε περίπτωση μηχανημάτων που προορίζονται για χρήση από καταναλωτές).

Το ISO 13849 προορίζεται να δώσει καθοδήγηση σε όσους εμπλέκονται στο σχεδιασμό και την αξιολόγηση συστημάτων ελέγχου, καθώς και στις Τεχνικές Επιτροπές που προετοιμάζουν πρότυπα τα οποία θεωρείται ότι συμμορφώνονται με τις Βασικές Απαιτήσεις Ασφάλειας του Παραρτήματος I του Οδηγίας (Directive) 2006/42/ΕΕ για τα μηχανήματα. Δεν παρέχει συγκεκριμένες οδηγίες για τη συμμόρφωση με άλλες οδηγίες της ΕΕ.

Ως μέρος της συνολικής στρατηγικής μείωσης κινδύνου σε ένα μηχάνημα, ένας σχεδιαστής συχνά επιλέγει να επιτύχει κάποιο μέτρο μείωσης του κινδύνου μέσω της εφαρμογής διασφαλίσεων που χρησιμοποιούν μία ή περισσότερες λειτουργίες ασφάλειας.

Τα μέρη των συστημάτων ελέγχου μηχανημάτων που έχουν ανατεθεί να παρέχουν λειτουργίες ασφαλείας ονομάζονται τμήματα συστημάτων ελέγχου που σχετίζονται με την ασφάλεια (SRP/CS) και αυτά μπορεί να αποτελούνται από υλικό και λογισμικό και μπορεί να

είναι είτε ξεχωριστά από το σύστημα ελέγχου μηχανής είτε αναπόσπαστο μέρος του. Εκτός από την παροχή λειτουργιών ασφαλείας, το SRP/CS μπορεί επίσης να παρέχει λειτουργικές λειτουργίες (π.χ. χειριστήρια με δύο χέρια ως μέσο έναρξης της διαδικασίας).

Η ικανότητα των εξαρτημάτων των συστημάτων ελέγχου που σχετίζονται με την ασφάλεια να εκτελούν μια λειτουργία ασφαλείας υπό προβλέψιμες συνθήκες εκχωρείται σε ένα από τα πέντε επίπεδα, που ονομάζονται επίπεδα απόδοσης (PL). Αυτά τα επίπεδα απόδοσης ορίζονται ως προς την πιθανότητα επικίνδυνης αστοχίας ανά ώρα.

Η πιθανότητα επικίνδυνης αποτυχίας της λειτουργίας ασφαλείας εξαρτάται από πολλούς παράγοντες, συμπεριλαμβανομένης της δομής υλικού και λογισμικού, την έκταση των μηχανισμών ανίχνευσης σφαλμάτων (διαγνωστική κάλυψη (DC)), την αξιοπιστία των εξαρτημάτων (μέσος χρόνος έως την επικίνδυνη αστοχία (MTTFD), η κοινή αιτία αποτυχίας (CCF)), διαδικασία σχεδιασμού, λειτουργική καταπόνηση, περιβαλλοντικές συνθήκες και διαδικασίες λειτουργίας.

Προκειμένου να βοηθηθεί ο σχεδιαστής και να διευκολυνθεί η αξιολόγηση του επιτυγχανόμενου PL, το ISO 13849 χρησιμοποιεί μια μεθοδολογία που βασίζεται στην κατηγοριοποίηση των κατασκευών σύμφωνα με συγκεκριμένα κριτήρια σχεδιασμού και συγκεκριμένες συμπεριφορές υπό συνθήκες σφάλματος. Σε αυτές τις κατηγορίες κατανέμεται ένα από τα πέντε επίπεδα, που ονομάζονται Κατηγορίες B, 1, 2, 3, 4 και 5.

Τα επίπεδα και οι κατηγορίες απόδοσης μπορούν να εφαρμοστούν σε μέρη συστημάτων ελέγχου που σχετίζονται με την ασφάλεια, όπως π.χ.:

- προστατευτικές συσκευές (π.χ. συσκευές ελέγχου με τα δύο χέρια, συσκευές αλληλομανδάλωσης), ηλεκτροευαίσθητες προστατευτικές διατάξεις (π.χ. φωτοηλεκτρικά φράγματα), συσκευές ευαίσθητες στην πίεση,
- μονάδες ελέγχου (π.χ. μια λογική μονάδα για λειτουργίες ελέγχου, επεξεργασία δεδομένων, παρακολούθηση, κ.λπ.), και στοιχεία ελέγχου ισχύος (π.χ. ρελέ, βαλβίδες κ.λπ.),
- καθώς και για συστήματα ελέγχου που εκτελούν λειτουργίες ασφαλείας σε όλα τα είδη μηχανημάτων από απλά (π.χ. μηχανές μικρών κουζινών ή αυτόματες πόρτες και πύλες) έως εγκαταστάσεις κατασκευής (π.χ. μηχανές συσκευασίας, μηχανές εκτύπωσης, πιεστήρια).

Το ISO 13849 προορίζεται να παρέχει μια σαφή βάση πάνω στην οποία μπορεί να αξιολογηθεί ο σχεδιασμός και η απόδοση οποιασδήποτε εφαρμογής του SRP/CS (και του μηχανήματος), για παράδειγμα από τρίτο μέρος, εσωτερικό ή ανεξάρτητο οίκο δοκιμών.

Το IEC 62061 και το ISO 13849 καθορίζουν απαιτήσεις για το σχεδιασμό και την εφαρμογή συστημάτων ελέγχου μηχανημάτων που σχετίζονται με την ασφάλεια. Η χρήση οποιουδήποτε από αυτά τα Διεθνή Πρότυπα, σύμφωνα με το πεδίο εφαρμογής τους μπορεί να θεωρηθεί ότι πληροί τις σχετικές βασικές απαιτήσεις ασφάλειας. Το ISO/TR 23849 παρέχει καθοδήγηση σχετικά με την εφαρμογή αυτού του μέρους του ISO 13849 και του IEC 62061 στο σχεδιασμό της ασφάλειας. [1]

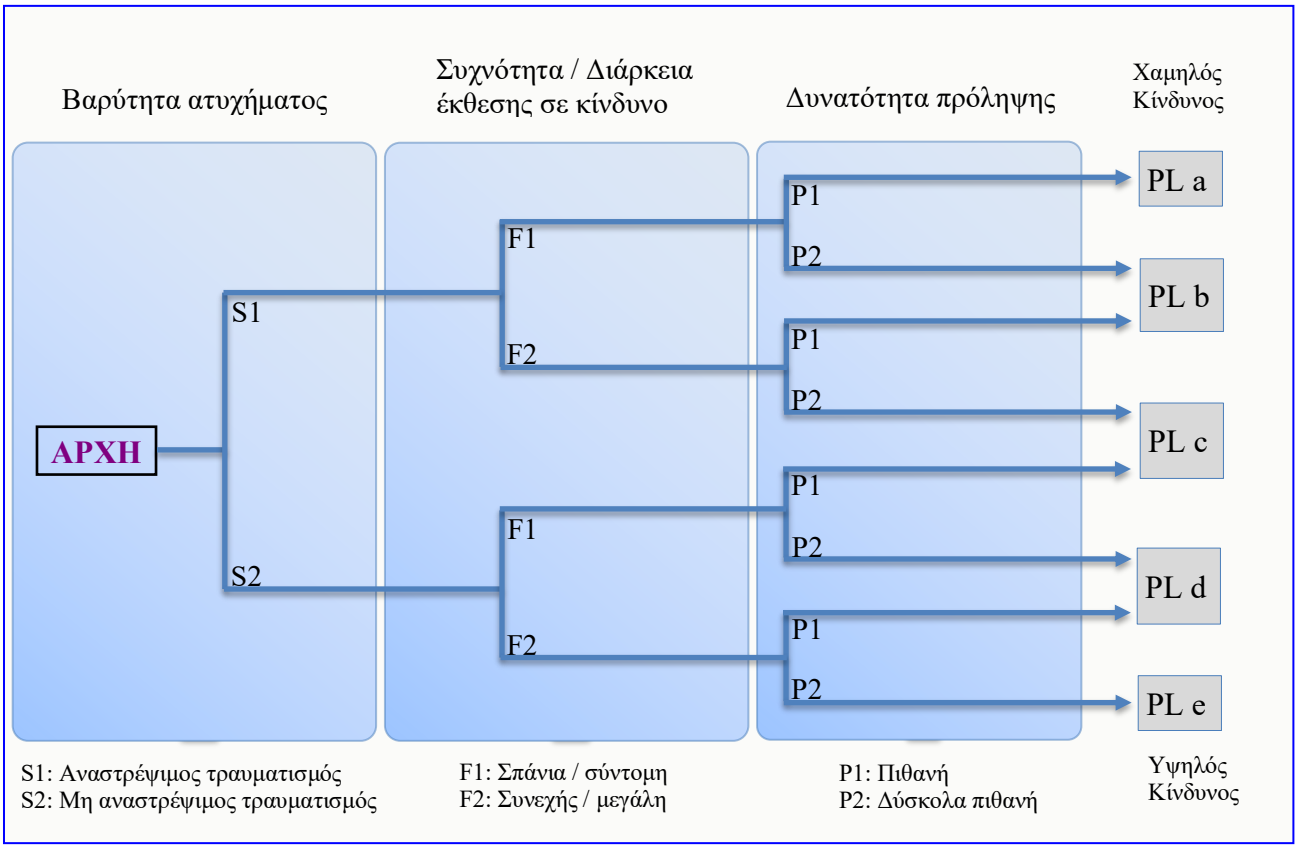
Το ISO 13849 παρέχει απαιτήσεις ασφαλείας και καθοδήγηση σχετικά με τις αρχές για το σχεδιασμό και την ενοποίηση εξαρτημάτων συστημάτων ελέγχου που σχετίζονται με την

ασφάλεια (SRP/CS), συμπεριλαμβανομένου του σχεδιασμού λογισμικού. Για αυτά τα μέρη του SRP/CS, καθορίζει χαρακτηριστικά που περιλαμβάνουν το επίπεδο απόδοσης που απαιτείται για την εκτέλεση λειτουργιών ασφαλείας. Ισχύει για SRP/CS για υψηλή ζήτηση και συνεχή λειτουργία, ανεξάρτητα από τον τύπο τεχνολογίας και ενέργειας που χρησιμοποιείται (ηλεκτρική, υδραυλική, πνευματική, μηχανική κ.λπ.), για όλα τα είδη μηχανημάτων. Δεν προσδιορίζει τις λειτουργίες ασφαλείας ή τα επίπεδα απόδοσης που πρόκειται να χρησιμοποιηθούν σε μια συγκεκριμένη περίπτωση.

Το ISO 13849 παρέχει συγκεκριμένες απαιτήσεις για SRP/CS χρησιμοποιώντας προγραμματιζόμενα ηλεκτρονικά συστήματα. Δεν παρέχει συγκεκριμένες απαιτήσεις για το σχεδιασμό προϊόντων που αποτελούν μέρη του SRP/CS. Ωστόσο, μπορούν να χρησιμοποιηθούν οι αρχές που δίνονται όπως κατηγορίες ή επίπεδα απόδοσης. Παραδείγματα προϊόντων που αποτελούν μέρη του SRP/CS είναι: ρελέ, ηλεκτρομαγνητικές βαλβίδες, διακόπτες θέσης, PLC, μονάδες ελέγχου κινητήρα, συσκευές ελέγχου με τα δύο χέρια, εξοπλισμός ευαίσθητος στην πίεση. Για το σχεδιασμό τέτοιων προϊόντων, είναι σημαντικό να γίνεται αναφορά στα ειδικά ισχύοντα Διεθνή Πρότυπα, π.χ. ISO 13851, ISO 13856-1 και ISO 13856-2.

Οι απαιτήσεις που παρέχονται στο ISO 13849 για προγραμματιζόμενα ηλεκτρονικά συστήματα είναι συμβατές με τη μεθοδολογία για το σχεδιασμό και την ανάπτυξη ηλεκτρικών, ηλεκτρονικών και προγραμματιζόμενων ηλεκτρονικών συστημάτων ελέγχου για μηχανήματα που σχετίζονται με την ασφάλεια που δίνεται στο IEC 62061.

Στην παρακάτω Εικόνα 10 δίνεται η μεθοδολογία για την αξιολόγηση των κινδύνων με το πρότυπο EN ISO 13849-1.



Εικόνα 10. Μεθοδολογία αξιολόγησης κινδύνων με το EN ISO 13849-1

Τα επίπεδα του EN ISO 13849-1 καθορίζονται και από τη μέση πιθανότητα μιας επικίνδυνης βλάβης ανά ώρα όπως φαίνεται παρακάτω στον Πίνακα 15:

Πίνακας 15. Πιθανότητα επικίνδυνης βλάβης /ώρα

Performance level (PL)	Μέση πιθανότητα μιας επικίνδυνης βλάβης ανά ώρα (1/h)
a	$\geq 10^{-5}$ έως $< 10^{-4}$
b	$\geq 3x10^{-6}$ έως $< 10^{-5}$
c	$\geq 10^{-6}$ έως $3x10^{-6}$
d	$\geq 10^{-7}$ έως 10^{-6}
e	$\geq 10^{-8}$ έως 10^{-7}

2.2.2 IEC 62061 Safety Integrity Levels SIL 1- 3

Σε αυτό το πρότυπο η βαρύτητα της πιθανής βλάβης εκτιμάται σε 1-4 επίπεδα, και στη συνέχεια αξιολογείται η πιθανότητα εμφάνισης του επικίνδυνου συμβάντος εξετάζοντας 3 επιπλέον παραμέτρους όπου το άθροισμά τους μας δίνουν την κλάση. Στους παρακάτω πίνακες δίνονται τα επίπεδα καθώς και οι παράμετροι που μας ορίζουν τα Levels SIL 1-3.

Πίνακας 16. Επίπεδα SIL 1-3

Βαρύτητα τραυματισμού (Severity of injury)	**S**
Μη αναστρέψιμη: Θάνατος, απώλεια ματιών ή μπράτσου	4
Μη αναστρέψιμη: Μόνιμη απώλεια άκρων	3
Αναστρέψιμη: Απαραίτητη ιατρική περίθαλψη	2
Αναστρέψιμη: Απαραίτητες πρώτες βοήθειες	1

Συχνότητα / Διάρκεια έκθεσης (Frequency / Duration of exposure)	**F**
≥ 1 per h	5
< 1 per h to ≥ per day	5
< 1 per day to ≥ per 14 days	4
< 1 per 14 days to ≥ per year	3
< 1 per year	2

Πιθανότητα εμφάνισης (Probability of occurrence)	**W**
Συχνά	5
Πολύ Πιθανά	4
Πιθανά	3
Σπάνια	2
Μηδαμινά	1

Δυνατότητα πρόληψης (Possibility of prevention)	**P**
Αδύνατη	5
Δυνατή	3
Πιθανή	1

Βαρύτητα τραυματισμού (Severity of injury)	**Class = F + W + P**				
	S	**4**	**5-7**	**8-10**	**11-13**	**14-15**
Μη αναστρέψιμη: Θάνατος, απώλεια ματιών ή μπράτσου	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Μη αναστρέψιμη: Μόνιμη απώλεια άκρων	3			SIL 1	SIL 2	SIL 3
Αναστρέψιμη: Απαραίτητη ιατρική περίθαλψη	2				SIL 1	SIL 2
Αναστρέψιμη: Απαραίτητες πρώτες βοήθειες	1					SIL 1

Η επιβεβαίωση μίας κλάσης SIL ή PL εξαρτάται από πολλούς παράγοντες που είναι οι παρακάτω:

- T1 = διάστημα δοκιμών ή διάρκεια ζωής (όποιο είναι μικρότερο)
- T2 = διάστημα διαγνωστικών δοκιμών
- MTTF = μέσος χρόνος μέχρι το σφάλμα
- MTTFd = μέσος χρόνος μέχρι το επικίνδυνο σφάλμα

- DC = διαγνωστική κάλυψη
- β = ευαισθησία σε κοινές αιτίες αστοχίας
- βD = υπολογισμός της ευαισθησίας σε κοινές αιτίες αστοχίας
- λ = ποσοστό αποτυχίας (ανά ώρα)
- λD = επικίνδυνο ποσοστό αποτυχίας
- λDD = ανιχνεύσιμο ποσοστό επικίνδυνης αποτυχίας
- λDU = μη ανιχνεύσιμο ποσοστό επικίνδυνης αποτυχίας
- λSD = ανιχνεύσιμο ποσοστό ασφαλούς αποτυχίας
- λSU = μη ανιχνεύσιμο ποσοστό ασφαλούς αποτυχίας

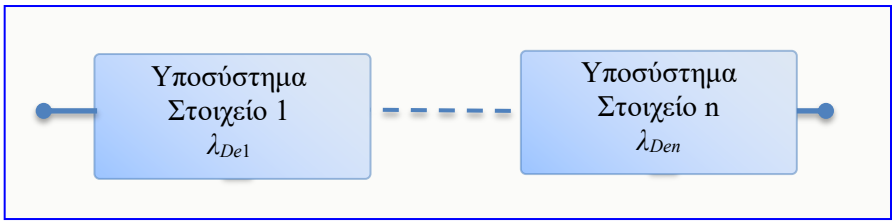
Ο έλεγχος επιβεβαίωσης των προτύπων εξαρτάται από τα υποσυστήματα και την αρχιτεκτονική αυτών [16]

2.2.3 Πρότυπο EN 62061

Το πρότυπο EN 62061 καθορίζει μέσα από την αρχιτεκτονική υποσυστημάτων την πιθανότητα επικίνδυνων σφαλμάτων του εξοπλισμού (Hardware), παρακάτω δίνονται οι αρχιτεκτονικές αυτών των υποσυστημάτων.

Υποσύστημα Α (σειριακή διάταξη)

Τα στοιχεία του υποσυστήματος Α είναι σε σειριακή διάταξη, σε αυτή τη διάταξη οι πιθανότητες των επικίνδυνων αποτυχιών των στοιχείων προστίθενται.

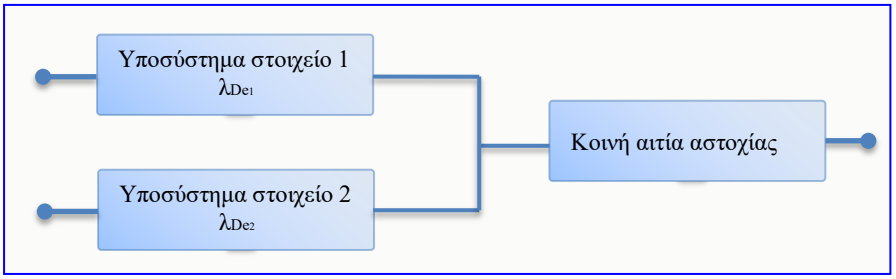


$$\lambda_D = \lambda_{De1} + \cdots\cdots + \lambda_{Den}$$
$$PFH_D = \lambda_D \times 1h$$

Εξίσωση 1

Υποσύστημα Β (παράλληλη διάταξη (redundant) χωρίς διαγνωστική λειτουργία)

Τα στοιχεία του υποσυστήματος Β είναι σε παράλληλη διάταξη χωρίς διαγνωστική λειτουργία και η πιθανότητα επικίνδυνου σφάλματος δίνεται με τους παρακάτω τύπους. Όταν η αρχιτεκτονική περιλαμβάνει ενιαία ανοχή σφάλματος, υπάρχει το ενδεχόμενο κοινής αιτίας βλάβης και πρέπει να ληφθεί υπόψη. Σε μία τέτοια διάταξη μπορούν να υπάρχουν ενεργοποιητές (Actuators).



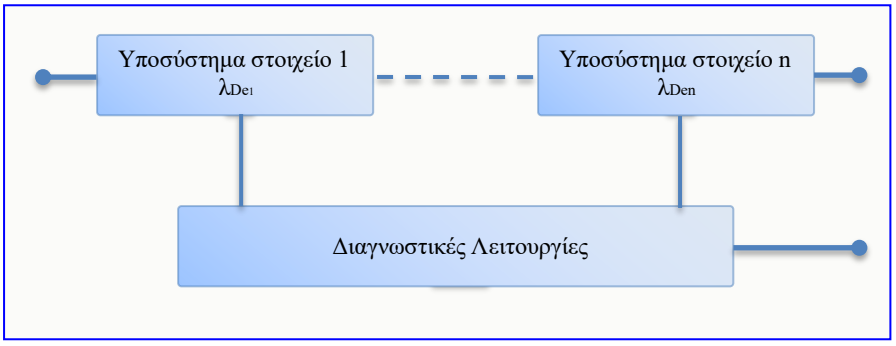
$$\lambda_D = (1-\beta)^2 \times \lambda_{De1} + \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_D = \lambda_D \times 1h$$

Εξίσωση 2

Υποσύστημα C (διάταξη με διαγνωστική λειτουργία)

Το επόμενο διάγραμμα δείχνει τη λειτουργική αναπαράσταση ενός συστήματος μηδενικής ανοχής σφάλματος με διαγνωστική λειτουργία. Η διαγνωστική κάλυψη χρησιμοποιείται για τη μείωση της πιθανότητας των επικίνδυνων υλικών βλαβών του υλικού. Ο ορισμός της διαγνωστικής κάλυψης είναι η αναλογία του ποσοστού ανιχνευόμενων επικίνδυνων αποτυχιών σε σύγκριση με το ποσοστό όλων των επικίνδυνων αποτυχιών. Σε μία τέτοια διάταξη μπορούν να υπάρχουν αισθητήρια-όργανα (Sensors).



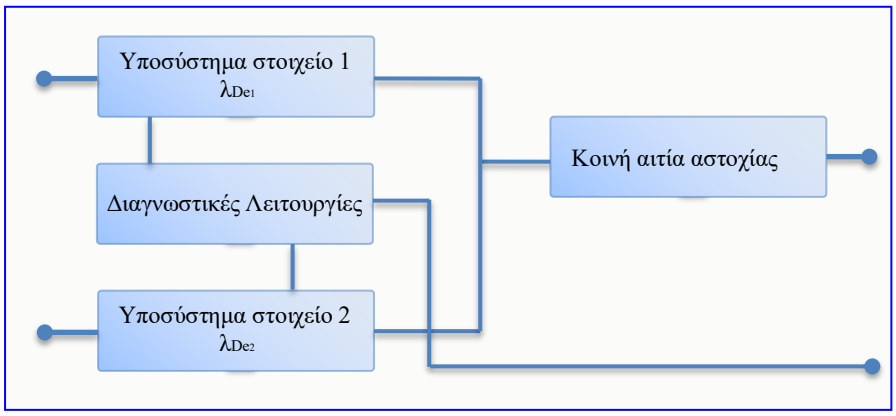
$$\lambda_D = \lambda_{De1}(1-DC_1) + \ \ldots\ldots + \lambda_{Den}(1-DC_n)$$

$$PFH_D = \lambda_D \times 1h$$

Εξίσωση 3

Υποσύστημα D (διάταξη με διαγνωστική λειτουργία)

Το υποσύστημα D είναι ενιαίο με αντοχή σφάλματος στις λειτουργίες διάγνωσης, το σύνολο των επικίνδυνων βλαβών του συστήματος επηρεάζεται από το σχεδιασμό των στοιχείων του υποσυστήματος. Σε μία τέτοια διάταξη μπορούν να υπάρχουν Ελεγκτές (Controllers).



Η πιθανότητα επικίνδυνων σφαλμάτων σε συστήματα με όμοια στοιχεία υπολογίζεται ως εξής:

$$\lambda_D = (1-\beta)^2\left\{\left[\lambda_{De}{}^2 \times 2 \times DC\right]\times {T_2}/{2} + \left[\lambda_{De}{}^2 \times (1-DC)\right]\times T_1\right\} + \beta \times \lambda_{De}$$

Εξίσωση 4

Η πιθανότητα επικίνδυνων σφαλμάτων σε συστήματα με ανόμοια στοιχεία υπολογίζεται ως εξής:

$$PFH_D = \lambda_D \times 1h$$

$$\lambda_D = (1-\beta)^2\left\{\left[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2\right]\times {T_2}/{2} + \left[\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2)\right]\times {T_1}/{2}\right\} + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$

Εξίσωση 5

Ασφαλές κλάσμα αποτυχίας (Safe failure fraction)

Το κλάσμα ασφαλούς αποτυχίας είναι παρόμοιο με τη διαγνωστική κάλυψη, αλλά λαμβάνει επίσης υπόψη τυχόν εγγενή τάση αποτυχίας προς μια ασφαλή κατάσταση. Για παράδειγμα, όταν μια ασφάλεια καεί, υπάρχει αποτυχία, αλλά είναι πολύ πιθανό ότι η αποτυχία θα είναι σε ένα ανοιχτό κύκλωμα το οποίο, στις περισσότερες περιπτώσεις, θα ήταν «ασφαλής» αποτυχία. Το SFF είναι το άθροισμα του ποσοστού των "ασφαλών" βλαβών συν το ποσοστό των ανιχνευόμενων επικίνδυνων αποτυχιών διαιρούμενο με το άθροισμα του ποσοστού των "ασφαλών" βλαβών συν το ποσοστό ανιχνευόμενων και μη εντοπισμένων επικίνδυνων βλαβών. Είναι σημαντικό να συνειδητοποιηθεί ότι οι μόνοι τύποι προβλημάτων που πρέπει να ληφθούν υπόψη είναι εκείνοι που θα μπορούσαν να έχουν κάποια επίδραση στη λειτουργία ασφαλείας.

$$SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{TOTAL}}$$

Εξίσωση 6

Πίνακας 17. Safe failure fraction (SFF)

Safe failure fraction (SFF)	Hardware Fault Tolerance		
	0	1	2
<60%	Μη επιτρεπτό	SIL 1	SIL 2
60%<90%	SIL 1	SIL 2	SIL 3
90%<99%	SIL 2	SIL 3	SIL 3
≥99%	SIL 3	SIL 3	SIL 3

2.2.4 Πρότυπο EN ISO 13849-1

Σε αυτό το σημείο θα αναλυθεί ένας απλουστευμένος αλλά πρακτικός οδηγός για τον τρόπο εφαρμογής των συστημάτων ελέγχου ανά κατηγορίες που είναι αναπόσπαστο μέρος του (EN) ISO13849-1 ως καθορισμένη αρχιτεκτονική.

Κατηγορία B (Category B)

Η κατηγορία B πρέπει να θεωρείται ως το βασικό θεμέλιο πάνω στο οποίο κατασκευάζονται όλες οι άλλες κατηγορίες. Δεν έχει ειδικές διατάξεις ή δομές ασφάλειας πέραν των Βασικών Αρχών Ασφαλείας όπως αναφέρονται στο ISO 13849-2. Αυτές αντιπροσωπεύουν γενικές καλές πρακτικές στο σχεδιασμό και την επιλογή υλικών.

Κατηγορία 1 (Category 1)

Η κατηγορία 1 απαιτεί τη χρήση σωστά δοκιμασμένων εξαρτημάτων και αρχών καλής ασφάλειας. Η χρήση των καλά δοκιμασμένων εξαρτημάτων αποσκοπούν στην ελαχιστοποίηση της πιθανότητας απώλειας της ασφαλής λειτουργίας, αλλά σημειώστε ότι ένα μόνο σφάλμα μπορεί να οδηγήσει ακόμα σε απώλεια της ασφαλής λειτουργίας.

Κατηγορία 2 (Category 2)

Η κατηγορία 2 εκτός από την τήρηση των απαιτήσεων της κατηγορίας B και τη χρήση σωστά δοκιμασμένων αρχών ασφαλείας το σύστημα ασφαλείας πρέπει να υποβληθεί σε δοκιμές για την κάλυψη της κατηγορίας 2. Οι δοκιμές πρέπει να σχεδιάζονται για την ανίχνευση σφαλμάτων στα τμήματα του συστήματος ελέγχου που σχετίζονται με την ασφάλεια. Εάν δεν εντοπιστούν σφάλματα επιτρέπεται στο μηχάνημα να λειτουργεί. Εάν εντοπιστούν σφάλματα η λειτουργία αντίδρασης σφάλματος πρέπει να εξασφαλίσει ότι το μηχάνημα θα παραμείνει σε ασφαλή κατάσταση.

Κατηγορία 3 (Category 3)

Η κατηγορία 3 εκτός από την τήρηση των απαιτήσεων της κατηγορίας Β και των καλά δοκιμασμένων αρχών ασφάλειας, η κατηγορία 3 απαιτεί την επιτυχή εκτέλεση της ασφαλούς λειτουργίας με την παρουσία ενός μόνο σφάλματος. Μερικά ελαττώματα, όπως διασταυρούμενα σφάλματα τα οποία δεν προκαλούν άμεση απώλεια της ασφαλούς ασφαλείας μπορεί να μην εντοπιστούν. Αυτό σημαίνει ότι για την κατηγορία 3 μια συσσώρευση μη ανιχνευόμενων βλαβών μπορεί να οδηγήσει σε απώλεια της ασφαλής λειτουργίας.

Κατηγορία 4 (Category 4)

Η κατηγορία 4 εκτός από την τήρηση των απαιτήσεων της κατηγορίας Β και των καλά δοκιμασμένων αρχών ασφάλειας, σε αντίθεση με την κατηγορία 3, όπου η συσσώρευση σφαλμάτων μπορεί να οδηγήσει σε απώλεια της ασφαλούς λειτουργίας η κατηγορία 4 απαιτεί την εκτέλεση της ασφαλούς λειτουργίας σε περίπτωση συσσώρευσης βλαβών. Στην πράξη αυτό επιτυγχάνεται συνήθως με την ύπαρξη υψηλού επιπέδου διάγνωσης για να εξασφαλιστεί ότι όλα τα σχετικά σφάλματα εντοπίζονται πριν από οποιαδήποτε συσσώρευση.

2.2.5 Επαλήθευση του Performance Level (Verification of Performance Level, PL)

Το EN ISO 13849-1 περιγράφει μια μέθοδο προσδιορισμού του PL που επιτυγχάνεται με συνδυασμό των παρακάτω:

- την αξιοπιστία των στοιχείων ως Mean Time To dangerous (MTTFd).
- την διαγνωστική κάλυψη (Diagnostic Coverage).
- Common Cause Factors (CCF).
- την κατηγορία (Category).

MTTFd

Το MTTFd όπως φαίνεται στον παρακάτω Πίνακα 18 διακρίνεται σε τρία επίπεδα:

Πίνακας 18. MTTFd

Level	Range
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd < 100 years

Για πνευματικά, μηχανικά και ηλεκτρομηχανικά εξαρτήματα (πνευματικές βαλβίδες, ρελέ, διακόπτες, διακόπτες θέσης, κλπ.). Μπορεί να είναι δύσκολο να υπολογιστεί ο μέσος χρόνος για επικίνδυνη βλάβη (MTTFd). Οι περισσότεροι από τους κατασκευαστές αυτών των εξαρτημάτων δίνουν μόνο τον μέσο αριθμό κύκλων έως ότου το 10% των εξαρτημάτων

αποτύχουν επικίνδυνα (B10d). Ο μέσος αριθμός κύκλων έως ότου το 10% των εξαρτημάτων αποτύχει επικίνδυνα (B10d) πρέπει να καθοριστεί από τον κατασκευαστή του κατασκευαστικού στοιχείου σύμφωνα με τα σχετικά πρότυπα προϊόντων για τις μεθόδους δοκιμής (π.χ. IEC 60957-5-1, ISO 19973, IEC 61810). Πρέπει να οριστούν οι επικίνδυνες λειτουργίες αστοχίας του εξαρτήματος, π.χ. να κολλήσει σε τελική θέση ή να αλλάξει τους χρόνους μεταγωγής. Ο χρόνος λειτουργίας του εξαρτήματος (T10d) είναι ο μέσος χρόνος έως ότου αποτύχει το 10% των εξαρτημάτων. Ο υπολογισμός του MTTFd γίνεται ως εξής:

$$MTTF_d = \frac{T_{10d}}{0,1}$$

$$T_{10d} = \frac{B_{10d}}{n_{op}} \qquad n_{op} = \frac{d_{op} \times h_{op} \times 3600 s/h}{t_{cycle}}$$

Εξίσωση 7

Όπου
d_{op} = η μέση λειτουργία σε ημέρες ανά έτος
h_{op} = η μέση λειτουργία σε ώρες ανά ημέρα
t_{cycle} = είναι ο μέσος χρόνος μεταξύ της έναρξης δύο διαδοχικών κύκλων του στοιχείου. (π.χ. μεταγωγή μιας βαλβίδας) σε δευτερόλεπτα ανά κύκλο.

Παράδειγμα
Εάν έχουμε ένα transistor με τα παρακάτω στοιχεία:
d_{op} = 180 ημέρες ανά έτος
h_{op} = 12 ώρες ανά ημέρα
t_{cycle} =8 δευτερόλεπτα ανά κύκλο.
B_{10d} = 50 εκατομμύρια κύκλοι.

$$n_{op} = \frac{180 \times 12 \times 3600}{8} = 9,72 \times 10^5 \, κύκλοι/έτος$$

$$T_{10d} = \frac{50 \times 10^6}{9,72 \times 10^5} = 51,4 έτη$$

$$MTTF_d = \frac{115,7}{0,1} = 514 έτη$$

Εξίσωση 8

Diagnostic Coverage

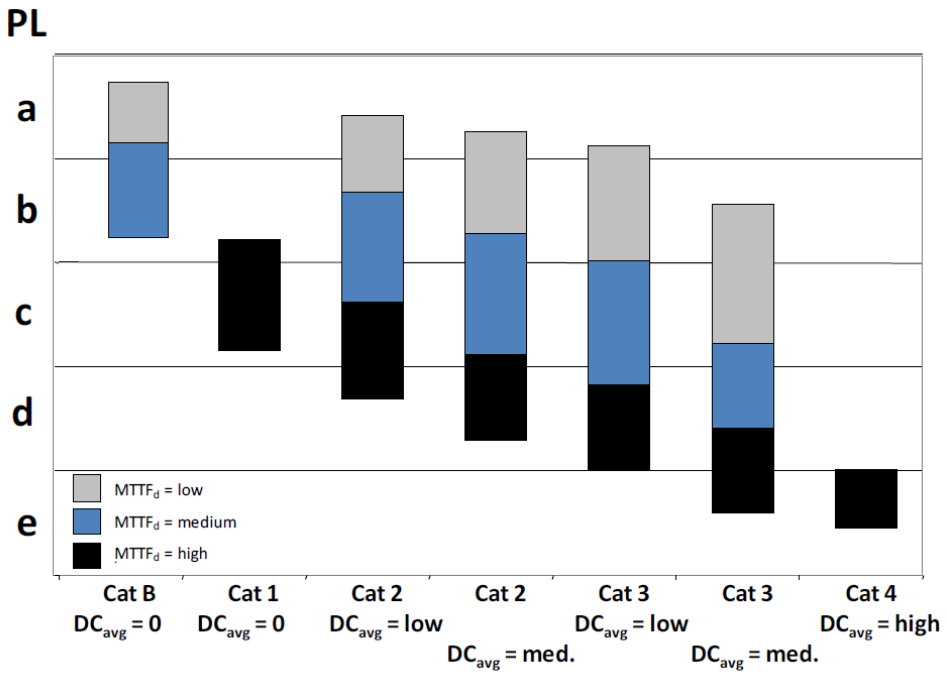
Και τα δύο πρότυπα απαιτούν από τον χρήστη να ποσοτικοποιήσει το ποσό της διαγνωστικής κάλυψης των συναφών λειτουργιών ελέγχου ασφάλειας, αυτό ορίζεται ως η μείωση της πιθανότητας των επικίνδυνων υλικών βλαβών που προκύπτουν από τη λειτουργία των αυτόματων διαγνωστικών δοκιμών.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DTOTAL}}$$

Εξίσωση 9

Όταν εντοπιστεί σφάλμα, οι μηχανισμοί παρακολούθησης χειρίζονται το σφάλμα ξεκινώντας μια κατάλληλη ενέργεια που εξαρτάται από την εφαρμογή. Για πολλές εφαρμογές στον τομέα των μηχανημάτων μια τέτοια κατάλληλη ενέργεια είναι να ξεκινήσει μια επονομαζόμενη ασφαλής κατάσταση (δηλ. η λειτουργία ασφαλείας πραγματοποιείται). Ο όρος ασφαλής κατάσταση υποδηλώνει ότι το σύστημα ελέγχου απομακρύνει άμεσα τον κίνδυνο (π.χ. διακόπτοντας / εμποδίζοντας αμέσως την επικίνδυνη κίνηση ενός τμήματος μιας μηχανής, αφαιρώντας την ισχύ σε έναν κινητήρα). Για άλλες μηχανές ή εφαρμογές, άλλες ενέργειες μπορεί να είναι πιο κατάλληλες, όπως η ενεργοποίηση ενός συναγερμού.

Για να επιβεβαιωθεί ότι έχει επιτευχθεί ένα απαιτούμενο επίπεδο απόδοσης, είναι απαραίτητο να συγκριθεί η αρχιτεκτονική και η διαγνωστική κάλυψη με το MTTFd.



Εικόνα 11. Σύγκριση αρχιτεκτονική και διαγνωστική κάλυψη με το MTTFd

Κοινή αιτία αποτυχίας, (Common cause failures, CCF)

CCF ονομάζεται η βλάβη η οποία είναι το αποτέλεσμα ενός ή περισσοτέρων συμβάντων και η οποία προκαλεί ταυτόχρονες αστοχίες δύο ή περισσοτέρων ξεχωριστών εξαρτημάτων σε ένα σύστημα πολλαπλών εξαρτημάτων και οδηγεί στην αποτυχία μιας λειτουργίας ελέγχου σχετιζόμενη με την ασφάλεια.

Το πρότυπο EN ISO 13849-1 απαιτεί να προσδιορίζεται το επίπεδο απόδοσης του συστήματος ελέγχου με εκτίμηση του CCF ως μία σημαντική πτυχή. Μια αξιολόγηση του CCF είναι απαραίτητη για κάθε επικύρωση της ασφάλειας αλλά μπορεί να πραγματοποιηθεί με διαφορετικούς τρόπους.

Το πρότυπο παρέχει μια (ποιοτική) διαδικασία για την εκτίμηση των μέτρων CCF που εφαρμόστηκαν σε δομές κατηγορίας 2, 3 ή 4. Η διαδικασία παρουσιάζεται με τον ακόλουθο Πίνακα 19 βαθμολόγησης.

Προκειμένου να πληρούνται οι απαιτήσεις, απαιτείται βαθμολογία τουλάχιστον 65 βαθμών ή μεγαλύτερη. Για κάθε καταχωρημένο μέτρο, μόνο το πλήρες σκορ ή τίποτα δεν μπορεί να διεκδικηθεί. Εάν ένα μέτρο ικανοποιείται μόνο εν μέρει, η βαθμολογία σύμφωνα με αυτό το μέτρο είναι μηδέν. Το μέγιστο σκορ είναι 100 πόντοι.

Πίνακας 19. Βαθμολογίας CCF

No	Measure against CCF	Max Score	Achieved Score
1	Separation/segregation	15	15
2	Diversity	20	15
3.1	Design: Protection against overvoltage, current, etc	15	15
3.2	Design: Components are well tried	5	5
4	Assessment/analysis	5	0
5	Competence/training	5	0
6.1	Environmental: EMC	25	25
6.2	Environmental: Other influencers	10	0
Total		100	75

ΚΕΦΑΛΑΙΟ 3

Ασφαλής λειτουργία συστημάτων (Safety Function)

Οι ολοένα αυξανόμενες απαιτήσεις αυτοματοποίησης της παραγωγής κάνουν τα συστήματα αυτοματισμού πιο σύνθετα και ευάλωτα σε αστοχίες. Για το λόγο αυτό έχουν δημιουργηθεί οδηγίες (π.χ. SIL) που πρέπει να τηρούνται, ώστε να εξασφαλίζεται η ασφαλής λειτουργία τους σε περίπτωση αστοχίας τόσο του υλικού όσο και του λογισμικού. Για την αξιόπιστη λειτουργία ενός Fail Safety συστήματος καθώς και για να μπορεί ένα σύστημα να λειτουργεί σε SIL2 ή SIL3 θα πρέπει να έχει Safety Hardware και Software. Στο παρόν κεφάλαιο αναλύεται η απόκριση του Hardware ενός Basic PLC και του εξοπλισμού ενός συστήματος αυτοματισμού. Επίσης παρουσιάζεται περιγραφική ανάλυση του πειράματος που υλοποιήθηκε για να καταγραφούν οι μετρήσεις, ανάλυση και αξιολόγηση των μετρήσεων ώστε να διαπιστωθεί εάν σε αυτά τα συστήματα μπορεί να γίνει χρήση βασικού εξοπλισμού και ταυτόχρονα να είναι εξασφαλισμένη η ασφαλή λειτουργία. Με την πιστοποίηση πως με ένα Basic εξοπλισμό PLC αλλά με διαφορετική διαχείριση αυτού ότι μπορεί να αναβαθμισθεί η ασφάλεια των συστημάτων αυτοματισμού, τότε με πολύ μικρό κόστος σε χρόνο και σε χρήμα ειδικά σε υφιστάμενα συστήματα αυτοματισμού θα μπορεί να υπάρχει ασφαλή λειτουργία.

Η ασφαλής λειτουργία ορίζει μια κατάσταση στην οποία ο κίνδυνος ζημιάς μειώνεται σε ένα ανεκτό επίπεδο ή να μπορεί να θεωρηθεί ως ακίνδυνος. Ο στόχος των συστημάτων ασφαλείας είναι να μειώσουν τον κίνδυνο για τους ανθρώπους και τις μηχανές σε ένα αποδεκτό επίπεδο. Το πρώτο βήμα είναι επομένως να προσδιοριστεί ο κίνδυνος να αναλυθεί και στη συνέχεια να μειωθεί.

Η ευθύνη για το σχεδιασμό και τη σωστή λειτουργία ενός συστήματος είναι αποκλειστικά του κατασκευαστή του συστήματος. Τα επιμέρους προϊόντα που χρησιμοποιούνται μπορεί να έχουν αναπτυχθεί για να εκτελούν λειτουργίες που σχετίζονται με την ασφάλεια είναι όμως μέρος μιας συνολικής εγκατάστασης ή μηχανής και από μόνα τους δεν εξασφαλίζουν την ασφαλή λειτουργία μίας μηχανής. Ένα πλήρες σύστημα που σχετίζεται με την ασφάλεια είναι γενικά εξοπλισμένο με αισθητήρες, μονάδες αξιολόγησης και μονάδες σηματοδότησης. Παρακάτω περιγράφονται συστήματα έχουν αναπτυχθεί για να εκτελούν λειτουργίες που σχετίζονται με την ασφάλεια.

3.1 Ασφαλή Συστήματα

Μια ασφαλής λειτουργία περιγράφει την αντίδραση μιας μηχανής/εγκατάστασης στην εμφάνιση ενός συγκεκριμένου γεγονότος-σφάλματος (π.χ. άνοιγμα προστατευτικής πόρτας). Η εκτέλεση της λειτουργίας ασφαλείας πραγματοποιείται από ένα σύστημα ελέγχου που σχετίζεται με την ασφάλεια. Αυτό συνήθως περιλαμβάνει τρία υποσυστήματα, ανίχνευση, αξιολόγηση και αντίδραση.

Ανίχνευση (Sensors):

Ανίχνευση απαίτησης ασφάλειας π.χ.: Στάση Έκτακτης Ανάγκης ή ενεργοποίηση αισθητήρα για την παρακολούθηση μιας επικίνδυνης περιοχής (συστοιχία φωτός, λέιζερ σαρωτή, κ.λπ.).

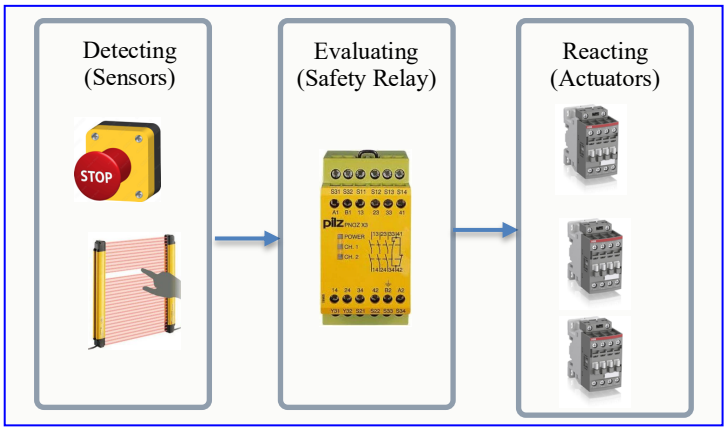
Αξιολόγηση (Safety Relay):

- Ανίχνευση απαίτησης ασφαλείας και ασφαλής έναρξη της αντίδρασης (π.χ. απενεργοποίηση των κυκλωμάτων ενεργοποίησης).
- Παρακολούθηση της σωστής λειτουργίας αισθητήρων και ενεργοποιητών
- Έναρξη αντίδρασης κατά τον εντοπισμό σφαλμάτων

Αντίδραση (actuators):

Απενεργοποίηση του κινδύνου μέσω ενεργοποιητών.

Στο παρακάτω σχήμα φαίνεται η διάταξή τους.



Εικόνα 12. Σχηματική διάταξη Συστήματος ελέγχου ασφαλής λειτουργίας

Για την καλύτερη κατανόηση ενός συστήματος ασφαλούς λειτουργίας θα πρέπει να είναι γνωστά τα παρακάτω:

Redundancy

Με την Redundancy δυνατότητα για την ίδια λειτουργία χρησιμοποιούνται περισσότερα από ένα στοιχεία, οπότε μία ελαττωματική λειτουργία ενός στοιχείου εκτελείται αντ' αυτού από τα άλλα στοιχεία. Μια Redundancy διαμόρφωση μειώνει την πιθανότητα αποτυχίας μιας λειτουργίας λόγω ενός ελαττωματικού στοιχείου. Αυτή η απαίτηση είναι απαραίτητη για την επίτευξη του SIL 3 σύμφωνα με το IEC 62061, SIL 3 σύμφωνα με το IEC 61508 και PL e (Κατ. 4) σύμφωνα με ISO 13849-1 (απαραίτητο επίσης για SIL 2 / PL d υπό ορισμένες συνθήκες). Η απλούστερη μορφή Redundancy είναι η χρήση δύο καναλιών (two-channel redundancy). Εάν ένα κύκλωμα αποτύχει η χρήση δύο καναλιών διασφαλίζει τη διατήρηση της λειτουργίας ασφαλείας.

Ανίχνευση διασταυρούμενων κυκλωμάτων (Cross-circuit detection)

Η ανίχνευση διασταυρούμενου κυκλώματος είναι μια διαγνωστική λειτουργία ενός ρελέ ασφαλείας (Safaty Relay) που ανιχνεύει βραχυκυκλώματα μεταξύ των καναλιών εισόδου (κυκλώματα αισθητήρων). Ένα βραχυκύκλωμα μπορεί να προκληθεί π.χ. από συμπίεση ενός

περιβλήματος καλωδίου. Σε συσκευές χωρίς ανίχνευση βραχυκυκλώματος μπορεί να σημαίνει ότι σε ένα Stop Emergency δύο καναλιών η λειτουργία δεν διακόπτεται ακόμη και αν μόνο μία επαφή NC είναι ελαττωματική (δευτερεύον σφάλμα).

Στα Safety Relays η ανίχνευση βραχυκυκλώματος υλοποιείται στα κυκλώματα αισθητήρων μέσω σημάτων με διαφορετικούς παλμούς ρολογιού. Εάν τα χρονισμένα σήματα επικαλύπτονται το Safety Relay η συσκευή ανιχνεύει βραχυκύκλωμα. Σε μερικά Safety Relay η ανίχνευση βραχυκυκλώματος μπορεί να απενεργοποιηθεί για να επιτραπεί η χρήση ηλεκτρονικών αισθητήρων.

Κύκλωμα ενεργοποίησης (Enabling Circuit)

Ένα κύκλωμα ενεργοποίησης παρέχει ένα σήμα εξόδου που σχετίζεται με την ασφάλεια. Από εξωτερική άποψης τα κυκλώματα ενεργοποίησης συνήθως λειτουργούν ως επαφές NO (Normally Open). Ένα μεμονωμένο κύκλωμα ενεργοποίησης που έχει ρυθμιστεί σε Redundancy λειτουργία σε ένα Safety Relay μπορεί να χρησιμοποιηθεί για SIL 3 / PL e.

Τα Safety Relays είναι εξοπλισμένα μόνο με κυκλώματα ενεργοποίησης με NO (Normally Open) λειτουργία. Αυτό σημαίνει ότι όταν ενεργοποιείται η λειτουργία ασφαλείας ή ανιχνεύεται σφάλμα, τα κυκλώματα ενεργοποίησης θα μεταφέρονται πάντα στην ασφαλή κατάσταση.

Κύκλωμα σηματοδότησης (Signaling Circuit)

Μια τρέχουσα διαδρομή σηματοδότησης παρέχει ένα σήμα εξόδου που σχετίζεται με την ασφάλεια. Τα κυκλώματα σηματοδότησης μπορούν να υλοποιούνται με λειτουργία επαφής NC ή NO. Στα Safety Relay τα κυκλώματα σηματοδότησης υλοποιούνται πάντα ως κυκλώματα NC (Normally Close). Αυτό σημαίνει ότι όταν ενεργοποιηθεί η λειτουργία ασφαλείας ή αν εντοπιστεί σφάλμα, τα κυκλώματα σηματοδότησης θα είναι πάντα κλειστά.

Κύκλωμα ανάδρασης (Feedback Circuit)

Ένα κύκλωμα ανάδρασης χρησιμοποιείται για την παρακολούθηση ελεγχόμενων ενεργοποιητών (π.χ. ρελέ ή επαφές φορτίου). Τα κυκλώματα ενεργοποίησης μπορούν να ενεργοποιηθούν μόνο όταν το κύκλωμα ανάδρασης κλείσει.

Κατηγορίες Στάσης (Stop Categories)

- Κατηγορία Στάσης 0
  Μη ελεγχόμενη απενεργοποίηση με άμεση απενεργοποίηση της τροφοδοσίας στη μονάδα ελέγχου των στοιχείων του μηχανήματος.
- Κατηγορία Στάσης 1
  Ελεγχόμενη στάση όπου η τροφοδοσία στη μονάδα ελέγχου διακόπτεται με χρονική καθυστέρηση ή διακόπτεται μόλις επιτευχθεί στάση.

Ο τερματισμός με χρονική καθυστέρηση των κυκλωμάτων ελέγχου σύμφωνα με την κατηγορία 1 δεν είναι εγγυημένη σε όλες τις καταστάσεις λειτουργίας. Στην περίπτωση ορισμένων εσωτερικών σφαλμάτων της συσκευής και κατά την αποσύνδεση της τάσης τροφοδοσίας τα κυκλώματα ελέγχου απενεργοποιούνται ακαριαία.

Αυτόματη εκκίνηση (Automatic Start)

Στην αυτόματη εκκίνηση, η συσκευή ξεκινά χωρίς χειροκίνητη επιβεβαίωση αλλά μόνο μετά από τον έλεγχο της σωστής λειτουργία του Safety Realy. Αυτή η λειτουργία είναι επίσης γνωστή ως δυναμική λειτουργία και δεν επιτρέπεται για συσκευές Stop Emergency. Συσκευές ασφαλείας για επικίνδυνες ζώνες (π.χ. διακόπτες θέσης, φως συστοιχίες, χαλάκια απενεργοποίησης ασφαλείας) μπορούν να χρησιμοποιήσουν τη λειτουργία αυτόματης εκκίνησης εάν δεν υπάρχει κίνδυνος.

Χειροκίνητη εκκίνηση (Manual Start)

Στη χειροκίνητη εκκίνηση η συσκευή εκκινείται πατώντας το κουμπί START αλλά μόνο μετά από τον έλεγχο της σωστής λειτουργία του Safety Relay. Σε μια χειροκίνητη εκκίνηση το κουμπί START δεν ελέγχεται για τη σωστή λειτουργία του και ενεργοποίησή του είναι αρκετή για την εκκίνηση. Αυτή η λειτουργία δεν επιτρέπεται για συσκευές Stop Emergency.

Παρακολούθηση εκκίνησης (Monitored Start)

Στην παρακολουθούμενη εκκίνηση, η συσκευή εκκινείται πατώντας το μπουτόν START αλλά μόνο μετά από τον έλεγχο της σωστής λειτουργία του Safety Relay. Σε αντίθεση με τη χειροκίνητη εκκίνηση η παρακολουθούμενη εκκίνηση ελέγχει για αλλαγή σήματος του μπουτόν START. Αυτό σημαίνει ότι το μπουτόν START δεν μπορεί να παρακαμφθεί (π.χ. βραχυκυκλωμένο). Για PL e (ISO 13849-1) καθώς και το SIL 3 (IEC 62061), η παρακολουθούμενη εκκίνηση πρέπει να χρησιμοποιείται στην περίπτωση του Stop Emergency. Για άλλους αισθητήρες/λειτουργίες ασφαλείας η ανάγκη παρακολούθησης της εκκίνησης εξαρτάται από την εκτίμηση του ενδεχόμενου κινδύνου. Εάν το μπουτόν START πατηθεί για περισσότερα από μερικά δευτερόλεπτα π.χ. 2-3 το Safety Relay θεωρεί το μπουτόν START είναι βραχυκυκλωμένο και μεταβαίνει στην κατάσταση σφάλματος

Λειτουργία με δύο χέρια/συγχρονισμός (Two-hand operation/synchronism)

Η λειτουργία με δύο χέρια είναι μία περίπτωση ελέγχου για την ταυτόχρονη λειτουργία π.χ. αισθητηρίων, μπουτόν κλπ. Σε αυτήν την περίπτωση δηλαδή δεν αρκεί οι δύο επαφές ενός μπουτόν να τεθούν σε κλειστή κατάσταση αλλά πρέπει να κλείσουν με διαφορά μικρότερη του 0,5 δευτερολέπτου. Αυτό διασφαλίζει για παράδειγμα ότι οι πρέσες ενεργοποιούνται μόνο όταν οι αισθητήρες ενεργοποιούνται ταυτόχρονα και με τα δύο χέρια, ελαχιστοποιόντας τον κίνδυνο τραυματισμού ενός χειριστή.

Αλληλουχία (Cascading)

Η αλληλουχία των Safety Relays χρησιμοποιείται για την ενεργοποίηση των Safety Relays σε σειρά. Πολλές λειτουργίες ασφαλείας μπορούν να συνδεθούν με μία λογική κοινού τερματισμού. Έτσι μπορούν να δημιουργηθούν κυκλώματα για επιλεκτική απενεργοποίηση στοιχείων κίνησης.

Η σύνδεση μεταξύ των μονάδων ασφαλείας πρέπει να συνδέονται μόνο σε σειρά και να μη συνδέεται η τελευταία μονάδα με την πρώτη γιατί έτσι θα δημιουργούταν ένας βρόχος που

θα εμπόδιζε εκκίνηση. Η αλληλουχία υλοποιείται μέσα σε έναν πίνακα ελέγχου με διαμόρφωση ενός καναλιού, αυτό επιτρέπεται ακόμη και με το SIL3 / PLe επειδή η δρομολόγηση καλωδίων εντός του πίνακα ελέγχου προστατεύεται από βραχυκυκλώματα.

Δοκιμή εκκίνησης (Startup testing)

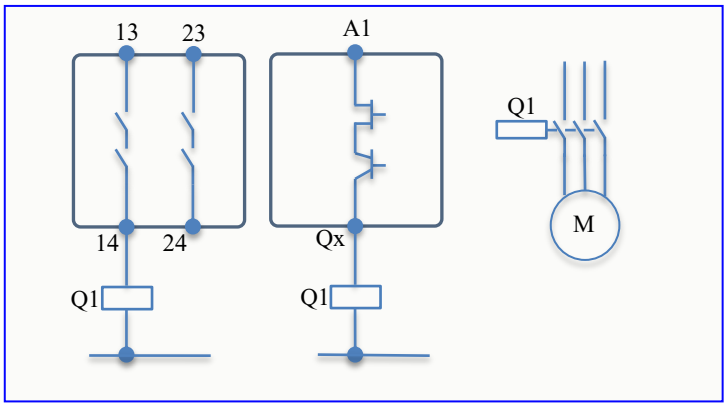
Το αισθητήριο ή ο εξοπλισμός προστασίας πρέπει να ανοίξει και να κλείσει ξανά μετά την τροφοδοσία. Η τάση αποκαθίσταται προτού μπορέσουν να περάσουν οι ενεργοποιήσεις Safety Realy. Η δοκιμή εκκίνησης διασφαλίζει για τυχόν σφάλματα στα αισθητήρια. Τα Safety Relays δεν αποθηκεύουν στη μνήμη τους τα σφάλματα εάν διακοπή η τροφοδοσία τους. Ο μη εξουσιοδοτημένος χειρισμός του εξοπλισμού προστασίας μπορεί επίσης να εντοπιστεί κατά την δοκιμή εκκίνησης. Ο διαχειριστής της μονάδας ασφαλείας κρίνει εάν πρέπει να πραγματοποιηθεί δοκιμή εκκίνησης (εκτίμηση κινδύνου).

Σύνδεση ενεργοποιητών (Connection of actuators)

Για την επίτευξη Επιπέδου Απόδοσης / Ακεραιότητας (PL/SIL) Ασφαλείας οι ενεργοποιητές πρέπει να παρακολουθούνται με κύκλωμα ανάδρασης. Για χωρητικά και επαγωγικά φορτία συνιστάται ένα κατάλληλο προστατευτικό κύκλωμα ώστε να μπορεί να κατασταλεί ή να μειωθεί η ηλεκτρομαγνητική παρεμβολή και να αυξηθεί η διάρκεια ζωής.

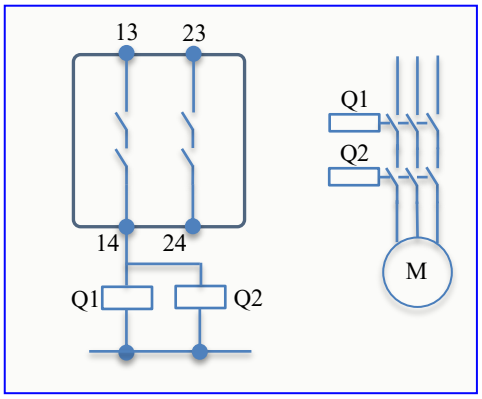
3.1.1 Καλωδίωση Ενεργοποιητών (Actuator Connections)

Καλωδίωση ενεργοποιητών έως PLc / Cat.2 για το ISO 13849-1 ή SIL 1 για το IEC 62061.



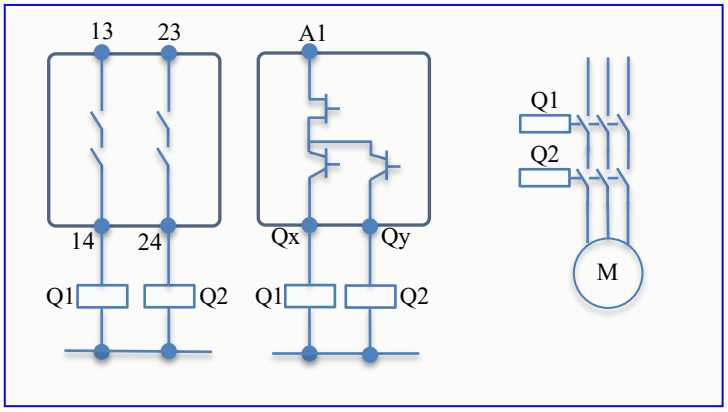
Εικόνα 13. Καλωδίωση Ενεργοποιητών PLc / Cat.2

Καλωδίωση ενεργοποιητών έως PLe / Cat.4 για το ISO 13849-1 ή SIL 3 για το IEC 62061.



Εικόνα 14. Καλωδίωση ενεργοποιητών έως PLe / Cat.4

Καλωδίωση ενεργοποιητών έως PLe / Cat.4 για το ISO 13849-1 ή SIL 3 για το IEC 62061.

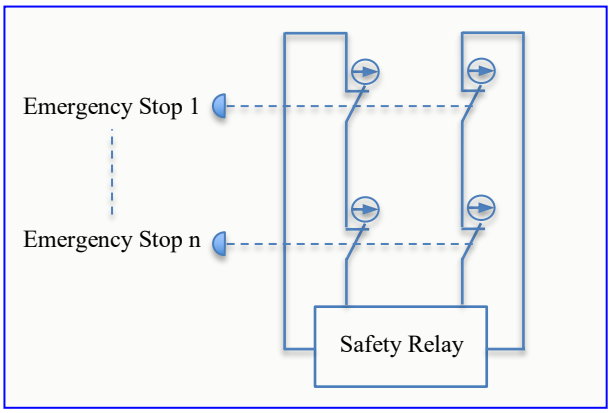


Εικόνα 15. Καλωδίωση ενεργοποιητών έως PLe / Cat.4

3.1.2 Σειριακή καλωδίωση αισθητηρίων (Series connection of sensors)

Σύνδεση EMERGENCY STOP σε σειρά (Series connection of EMERGENCY STOP)

Η σύνδεση στοιχείων EMERGENCY STOP σε σειρά προσφέρει το υψηλότερο επίπεδο ασφαλείας (SIL 3 σύμφωνα με το IEC 62061, SIL 3 σύμφωνα με το IEC 61508 και PLe (Κατ. 4) σύμφωνα με το ISO 13849-1). Αυτό γίνεται γιατί έστω και ένα EMERGENCY STOP να λειτουργεί διασφαλίζεται η ασφαλής λειτουργία. Στο παρακάτω σχέδιο φαίνεται η απαιτούμενη μορφή της καλωδίωσης.

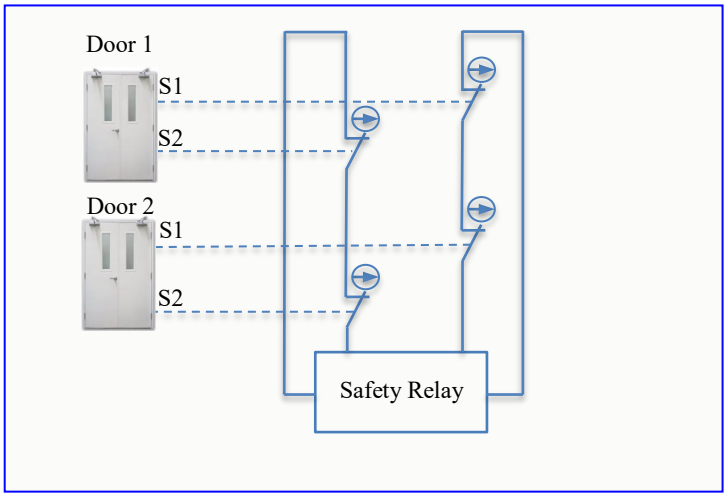


Εικόνα 16. Σειριακή Σύνδεση EMERGENCY STOP

Σύνδεση διακοπτών θέσης σε σειρά (Series connection of position switches)

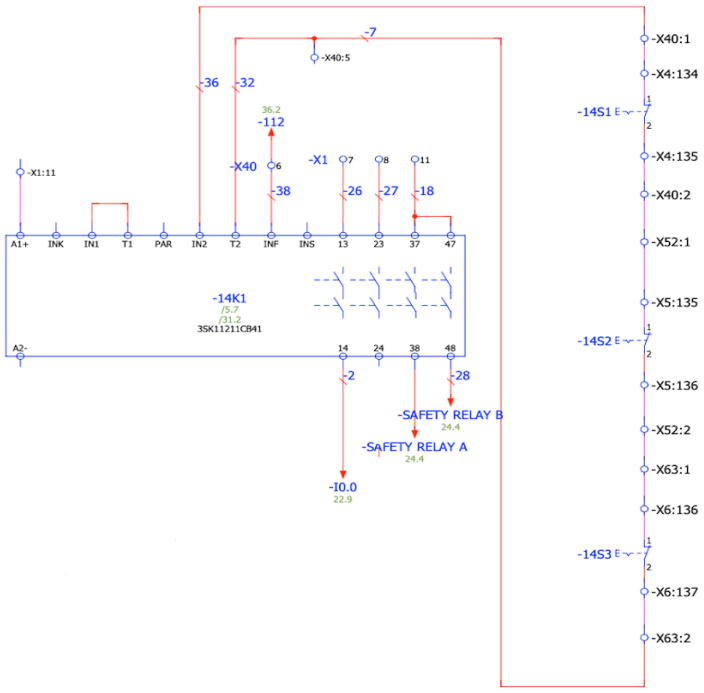
Γενικά, οι διακόπτες θέσης μπορούν να συνδεθούν σε σειρά εάν διασφαλίζεται ότι π.χ. οι προστατευτικές πόρτες δεν ανοίγουν τακτικά και ταυτόχρονα (διαφορετικά δεν θα μπορεί να εντοπιστεί τυχόν σφάλμα αυτών).

Για το επίπεδο ασφάλειας SIL3 σύμφωνα με το IEC 62061, το SIL3 σύμφωνα με το IEC 61508, και το PLe (Κατ. 4) σύμφωνα με το ISO 13849-1 δεν πρέπει ποτέ να συνδέονται σε σειρά, επειδή κάθε επικίνδυνο σφάλμα πρέπει να ανιχνεύεται και από που προέρχεται.



Εικόνα 17. Σειριακή Σύνδεση διακοπτών θέσης

Τα Safety Relay χρησιμοποιούνται ακόμη και σήμερα σε απλά συστήματα αυτοματισμού παρέχοντας επιπλέον δυνατότητες όπως ένα ή και περισσότερα κανάλια ελέγχου, χρονικές καθυστερήσεις, δυνατότητες επικοινωνίας κλπ. Στην παρακάτω Εικόνα 18 περιγράφεται μία τυπική χρήση ενός Safety Relay.



Εικόνα 18. Τυπική χρήση ενός Safety Relay

Όπως φαίνεται στην Εικόνα 18 υπάρχουν τρία μπουτόν «Stop Emergency». Το πρώτο παίρνει τάση από το Safety Relay και είναι καλωδιωμένο σε σειρά με τα υπόλοιπα δύο. Έτσι, όταν πατηθεί ένα από τα τρία μπουτόν ανοίγει το κύκλωμα και δεν υπάρχει επιστροφή τάσης στο Safety Relay. Χάνοντας την τάση το Safety Relay ανοίγει τις επαφές Safety Relay A και B με αποτέλεσμα να γίνεται και παύση της λειτουργίας της μηχανής.

3.2 Programmable Logical Controllers (PLC)

Τις τελευταίες δεκαετίες η υλοποίηση των συστημάτων αυτοματισμού και κυρίως σε βιομηχανικά περιβάλλοντα υλοποιούνται από PLC. Τα πλεονεκτήματά τους και η συνεχής αναβάθμισή τους τα έχουν εδραίωση στο χώρο αυτό. Στα συστήματα προγραμματιζόμενης λογικής, η κατασκευή και συρμάτωση του πίνακα είναι ανεξάρτητη από τη λειτουργία που πρόκειται να εκτελέσει ο αυτοματισμός. Πάνω στις κλέμες του ελεγκτή συνδέονται όλα τα στοιχεία, που δίνουν εντολές (τερματικοί διακόπτες, μπουτόν κ.λπ.), καθώς και όλα τα στοιχεία που δέχονται εντολές (πηνία, ρελέ ισχύος κινητήρων, βαλβίδες, λυχνίες κ.λπ.).

Η λειτουργία του αυτοματισμού προγραμματίζεται στην μνήμη του ελεγκτή, ακόμα και την τελευταία στιγμή, πριν από τη θέση σε λειτουργία. Επομένως η μελέτη (πρόγραμμα) μπορεί να γίνεται παράλληλα με την επιλογή του υλικού και την κατασκευή του πίνακα.

Αν στην συνέχεια χρειαστεί να γίνουν αλλαγές στη λειτουργία, γεγονός σύνηθες στον αυτοματισμό, τότε αυτές γίνονται πολύ απλά «διορθώνοντας» το πρόγραμμα, χωρίς να χρειαστεί να επέμβουμε τη συρμάτωση του πίνακα. Για την κάλυψη των απαιτήσεων της κάθε εφαρμογής υπάρχουν τα Βασικά PLC και PLC βασιζόμενα στα Βασικά αλλά εμπλουτιζόμενα με επιπλέον λειτουργίες και δυνατότητες, έτσι θα μπορούσανε να κατηγοριοποιηθούν ως εξής:

- Βασικά PLC
- Redundancy PLC
- Safety PLC

3.2.1 Βασικά PLC

Η επιλογή ενός PLC (τύπος - μέγεθος - κόστος) εξαρτάται κυρίως από:

- το πλήθος των στοιχείων που δίνουν εντολή σε αυτό (είσοδοι)
- το πλήθος των στοιχείων που δέχονται εντολή από αυτό (έξοδοι)
- το πλήθος των λειτουργιών που απαιτείται να κάνει ο αυτοματισμός (μέγεθος προγράμματος, απαιτούμενη μνήμη και δυνατότητες της κεντρικής μονάδας)

Ανεξάρτητα όμως από τον τύπο και το μέγεθος ενός PLC θα περιέχει τουλάχιστον τα παρακάτω στοιχεία:

- Μονάδα τροφοδοσίας
- Κεντρική μονάδα (CPU) με τον μικροεπεξεργαστή και την μνήμη για το πρόγραμμα
- Μονάδες Εισόδων-Εξόδων
- Μονάδες Επικοινωνίας

Μονάδα τροφοδοσίας

Η μονάδα τροφοδοσίας χρησιμεύει για να δημιουργηθούν από την τάση του δικτύου οι απαραίτητες εσωτερικές τάσεις για την τροφοδοσία αποκλειστικά των ηλεκτρικών στοιχείων, που υπάρχουν μέσα στον ελεγκτή (τρανζίστορ, ολοκληρωμένα κ.λπ.). Επίσης για να διατηρηθεί το περιεχόμενο της μνήμης RAM σε μια διακοπή τάσης με τη βοήθεια μπαταρίας, που ενσωματώνεται σ' αυτή.

Τα σπουδαιότερα τεχνικά χαρακτηριστικά μιας μονάδας τροφοδοσίας είναι τα εξής:

Είσοδος: Ονομαστική τάση, ανοχές τάσης, συχνότητα, απορροφούμενο ρεύμα, προστασία.

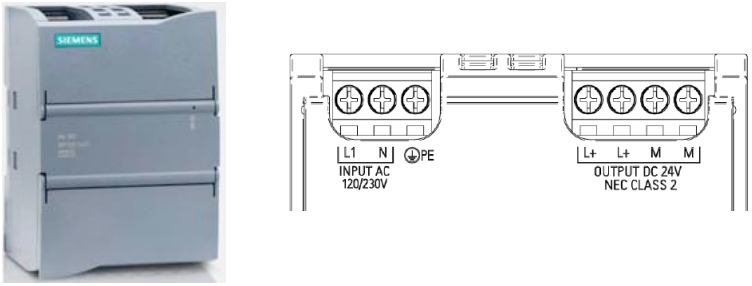
Έξοδος: Ονομαστική τάση, ονομαστικό ρεύμα, προστασία βραχυκυκλώματος.

Διάφορα: Μπαταρία για διατήρηση μνήμης RAM.

Αν το πρόγραμμα ενός ελεγκτή πρόκειται να αποθηκευτεί σε μνήμη RAM, τότε απαραίτητα πρέπει να υπάρχει στο σύστημα και μια μπαταρία για τη διατήρηση του περιεχομένου της μνήμης σε μια διακοπή τάσης του δικτύου. Αυτή η μπαταρία που είναι συνήθως λιθίου τοποθετείται στη μονάδα τροφοδοσίας και μπορεί να κρατήσει το πρόγραμμα της μνήμης RAM για πολύ μεγάλο χρονικό διάστημα.

Πρέπει, όμως, να προσεχτούν τα εξής σημεία:

- Η μπαταρία θα πρέπει να αλλάζεται με την συχνότητα που ορίζει ο κατασκευαστής.
- Το SOFTWARE του ελεγκτή πρέπει να παρέχει στο χρήστη τη δυνατότητα να αξιολογήσει το γεγονός, ότι η μπαταρία έχει πέσει κάτω από το όριο ασφαλείας.
- Η αντικατάσταση της μπαταρίας πρέπει πάντοτε να γίνεται με τον ελεγκτή υπό τάση για να μην χαθεί το πρόγραμμα.



Εικόνα 19. Μονάδα τροφοδοσίας

Κεντρική μονάδα επεξεργασίας (CPU)

Η CPU έχει τα εξής χαρακτηριστικά:

- Ενσωματωμένη μνήμη εργασίας (Working Memory)
- Ενσωματωμένη μνήμη φορτώματος (Load memory)
- Εξωτερική Flash EPROM φορτώματος (Load memory) που επεκτείνει την ενσωματωμένη.

Η Load μνήμη περιλαμβάνει όλα τα Block Λογικής (συμπεριλαμβανομένων και Block που δεν απαιτούνται για την εκτέλεση του προγράμματος πχ. Block Header), μπλοκ Δεδομένων και Δεδομένων παραμετροποίησης που δεν χάνονται ούτε με το Reset της μνήμης ούτε με την απώλεια μπαταρίας του τροφοδοτικού.

Με την Μεταγωγή της CPU από την κατάσταση Stop στην κατάσταση εκτέλεσης του προγράμματος μεταφέρονται από την Load μνήμη στην Working μνήμη τα μπλοκ λογικής και δεδομένων που είναι απαραίτητα για την εκτέλεση του προγράμματος. Η working μνήμη είναι γρηγορότερη από την Load μνήμη και σβήνει με Reset memory της CPU ή αν πέσει η μπαταρία του τροφοδοτικού.

Η CPU εμπεριέχει Status Leds και Leds σφαλμάτων ενώ ο τρόπος λειτουργίας επιλέγεται με κλειδί (KEY). Όταν το κλειδί μετακινηθεί ο τρόπος λειτουργίας της CPU δεν μπορεί να αλλάξει. Αυτή η δυνατότητα προστατεύει το πρόγραμμα της εφαρμογής από μη εξουσιοδοτημένη αλλαγή ή διαγραφή του.

Η CPU περιλαμβάνει διαγνωστική μνήμη μήκους συνήθως 100-500 μηνυμάτων που δεν σβήνεται ούτε με την πτώση τάσης ούτε με το Reset της μνήμης και καταγράφονται με ώρα και ημερομηνία γεγονότα που συνδέονται με:

- Σφάλματα της CPU.
- Σφάλματα συστήματος της CPU.
- Σφάλματα περιφερειακών modules.
- Μεταγωγή από κατάσταση Stop-Εκτέλεση προγράμματος (RUN) -Stop.
- Προγραμματιστικά λάθη στο πρόγραμμα εφαρμογής.

Η διαγνωστική μνήμη μπορεί να διαβασθεί ON-LINE τοπικά με έναν φορητό ηλεκτρονικό υπολογιστή.

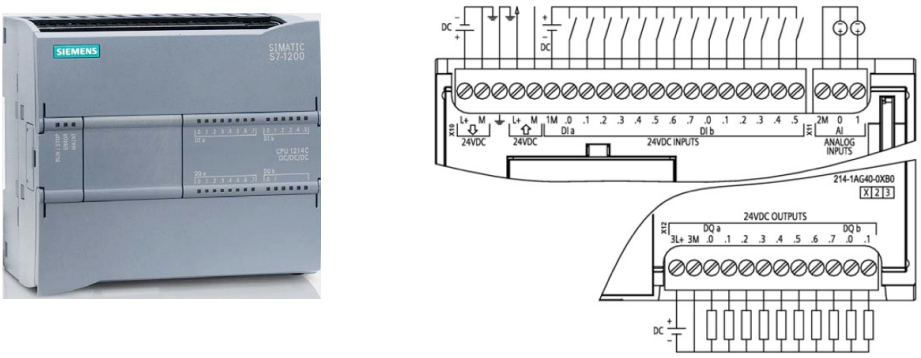
Επίσης η CPU περιλαμβάνει Διαγνωστικό Alarm μπλοκ στο οποίο προγραμματίζοντας την Διεύθυνση μιας οποιασδήποτε κάρτας εισόδου / εξόδου λαμβάνονται διαγνωστικά bit για την κάρτα όπως:

- Βλάβη κάρτας
- Εσωτερικό εξωτερικό σφάλμα
- Πρόβλημα σε κάποιο κανάλι της κάρτας
- Έλλειψη εξωτερικής τάσης
- Έλλειψη φίσσας καλωδίων, ειδικά στις κάρτες αναλογικών εισόδων αν στο στάδιο αρχικής παραμετροποίησης της κάρτας ενεργοποιήσει ο χρήστης την ανίχνευση κομμένου καλωδίου τότε είτε με την ενεργοποίηση του διαγνωστικού Alarm μπλοκ είτε με την μη ενεργοποίηση του αλλά οπτικά σε εξωτερικό LED της κάρτας (System Fault) ειδοποιείται τοπικά ή remote το σύστημα για το κομμένο καλώδιο οποιοδήποτε αναλογικού οργάνου(4..20mA)
- Ο μέσος κύκλος εκτέλεσης για 1000 εντολές είναι συνήθως 0.3msec - 0.6msec
- Έχει εσωτερικά βοηθητικά ρελαί (Flags) από τα οποία μπορούν να είναι μόνιμα (διατήρηση περιεχομένου τους σε περίπτωση διακοπής τάσης ή μεταγωγής της CPU από RUN-Stop- RUN).

- Έχει χρονικά και οι απαριθμητές που είναι ενσωματωμένα στην CPU είναι τα οποία όλα μπορούν να είναι μόνιμα.
- Υπάρχει ενσωματωμένο ρολόι πραγματικού χρόνου
- Υποστηρίζονται Γλώσσες προγραμματισμού όπως LAD (LADDER) FBD (Πύλες) STL (λίστα εντολών) σύμφωνα με τα διεθνή Standards IEC 1131-3 Part 3 αλλά και επιπλέον γλώσσες προγραμματισμού με την χρήση Optional Software πακέτων
- Υποστηρίζεται δομημένος προγραμματισμός με την ύπαρξη ειδικών μπλοκ οργάνωσης (OB) Block δεδομένων (DB, Block λειτουργία (FC, FB), Block Λειτουργιών συστήματος (SFC, SFB) και Block δεδομένων συστήματος (SDB).
- Υποστηρίζονται οι παρακάτω εντολές
  - Λογικής bit BOOLEAN (AND, OR)
  - Λογικής Word boolean (AND, OR) με 16 bit-Σταθερές.
  - Λογικής Double Boolean (AND,OR) με 32 bit- Σταθερές
  - Εντολές παλμού.
  - Set / Reset bit (πχ. Inputs, Outputs, Memorys)
  - Εντολές ολίσθησης Δεξιά, αριστερά και κυκλικής ολίσθησης.
  - Set /Reset bit (π.χ. Inputs, Outputs, Memorys)
  - Εντολές ολίσθησης δεξιά, αριστερά και κυκλικής ολίσθησης
  - Εντολές χρονικών και απαριθμητών
  - Αποθήκευσης και μεταφοράς τιμών από και προς καταχωρητές byte, Word, Doubleword.
  - Εντολές σύγκρισης (16bit, 32 bit ακέραιων αριθμών, 32 bit δεκαδικών αριθμών).
  - Αριθμητικές πράξεις όπως α) Πρόσθεση/πολλαπλασιαμό 16bit ακέραια
    β) Πρόσθεση/πολλαπλασιαμό 32 bit ακέραια
    γ) Πρόσθεση/πολλαπλασιαμό 32 bit δεκαδικών
  - Εύρεση τετραγωνικής ρίζας, Λογαριθμικές πράξεις, τριγωνομετρικές λειτουργίες.
  - Εντολές αλλαγής ελέγχου του προγράμματος από μπλόκ σε μπλοκ και από εντολή σε εντολή μέσα στο ίδιο μπλοκ.
  - Εντολές μετατροπής κώδικα (πχ BCD σε 16 bit Ακέραια).
  - Διάφοροι τρόποι εκτέλεσης του προγράμματος όπως κυκλικός, ελεγχόμενος από γεγονός ή από χρόνο.
  - Ένδειξη μεγίστου - ελαχίστου- μέσου κύκλου εκτέλεσης προγράμματος
  - Υποστήριξη αναλογικό - ολοκληρωτικό- διαφορικού ελεγκτή κλειστού βρόχου (PID Controller) με την βοήθεια επιπλέον πακέτου παραμετροποίησης και πακέτου Block Λειτουργίας.

Στην κεντρική μονάδα (CPU) ο μικροεπεξεργαστής προσπελαύνει συνεχώς (κυκλικά) το πρόγραμμα, που είναι γραμμένο στην μνήμη. Ρωτάει συνεχώς, αν οι διάφορες είσοδοι έχουν ή δεν έχουν τάση (επαφές κλειστές ή ανοιχτές), επεξεργάζεται τις εντολές του προγράμματος και βάσει αυτών εξαναγκάζει τις εξόδους να διεγερθούν ή όχι (δηλ. να αποκτήσουν ή όχι τάση, οπότε διεγείρονται ή όχι τα συνδεδεμένα σ' αυτές ρελέ, βαλβίδες κ.λπ.).

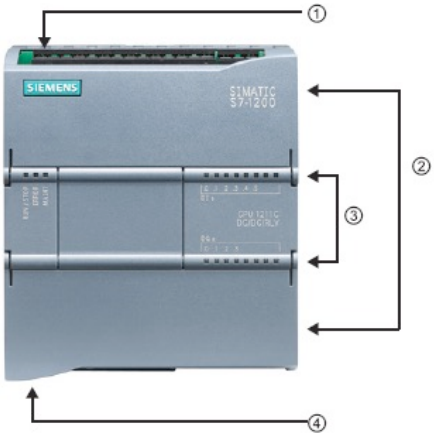
Το πρόγραμμα γράφεται στη μνήμη με τη βοήθεια μιας συσκευής προγραμματισμού (προγραμματιστής). Αυτή συνδέεται στην κεντρική μονάδα μόνο όταν πρόκειται να γραφτεί ή να μεταφερθεί το πρόγραμμα στην μνήμη, ή αν πρόκειται να γίνουν αλλαγές. Επίσης, χρησιμοποιείται για τον έλεγχο των διαφόρων σημάτων κατά την εξέλιξη του προγράμματος και για την ανεύρεση σφαλμάτων.



Εικόνα 20. Κεντρική Μονάδα Επεξεργασίας (CPU)

Στοιχεία ελέγχου και απεικόνισης μίας Compact CPU

Μία Compact CPU έχει ενσωματωμένη τροφοδοσία (σύνδεση 24 V) και ενσωματωμένες εισόδους και εξόδους, διαθέτει μια ενσωματωμένη σύνδεση TCP/IP για επικοινωνία με μια συσκευή προγραμματισμού. Η CPU μπορεί έτσι να επικοινωνεί με συσκευές HMI ή άλλες CPU μέσω δικτύου Ethernet.



Εικόνα 21. Compact CPU

1. Σύνδεση 24 VDC.
2. Block βύσματα ακροδεκτών για την καλωδίωση των σημάτων (κάτω από τα καπάκια).

3. LED κατάστασης για τις καταστάσεις των Εισόδων/Εξόδων και την κατάσταση της CPU.
4. Σύνδεση TCP/IP (στην κάτω πλευρά της CPU).

Μπορεί να έχει προαιρετικά κάρτα μνήμης για να αποθηκεύει ένα πρόγραμμα καθώς και δεδομένα, δεδομένα συστήματος, αρχεία και έργα. Μπορεί να χρησιμοποιηθεί για:

- Μεταφορά προγράμματος σε πολλαπλές CPU
- Ενημέρωση υλικολογισμικού για CPU, μονάδες σήματος (SM) και μονάδες επικοινωνίας (CMs)
- Εύκολη αντικατάσταση της CPU

Εικόνα 22. Κάρτα Μνήμης

Λειτουργικές Καταστάσεις της CPU

Η CPU μπορεί να έχει τις ακόλουθες τρεις λειτουργικές καταστάσεις:

- Στην κατάσταση λειτουργίας STOP → η CPU δεν εκτελεί το πρόγραμμα.
- Στην κατάσταση λειτουργίας STARTUP → η CPU ξεκινά.
- Στην κατάσταση λειτουργίας RUN → το πρόγραμμα εκτελείται κυκλικά.

Status and error displays

Η λυχνία κατάστασης RUN / STOP στην μπροστινή πλευρά της CPU υποδεικνύει την τρέχουσα κατάσταση λειτουργίας της CPU ανάλογα με το χρώμα του LED.
Κίτρινο LED δείχνει την κατάσταση λειτουργίας STOP.
Πράσινο LED δείχνει την κατάσταση λειτουργίας RUN.
LED που αναβοσβήνει δείχνει κατάσταση λειτουργίας STARTUP.
Σφάλμα LED για την ένδειξη σφαλμάτων
Maint LED για ένδειξη ότι απαιτείται συντήρηση.

Εικόνα 23. Status and error displays

Μονάδες Εισόδων - Εξόδων

Τα καλώδια που έρχονται από τα αισθητήρια της παραγωγικής διαδικασίας (τερματικοί, μπουτόν, διακόπτες), συνδέονται στις κλέμες των μονάδων εισόδων (είσοδοι του PLC).

Αντίστοιχα, τα καλώδια που πηγαίνουν προς τα ρελέ ισχύος, βαλβίδες, λυχνίες κ.λπ. συνδέονται στις κλέμες των μονάδων εξόδου (έξοδοι του PLC).

Μονάδες ψηφιακών εισόδων

Ένας ελεγκτής αντιλαμβάνεται ότι μια εξωτερική επαφή (π.χ. τερματικός) έκλεισε όταν στην αντίστοιχη κλέμα εισόδου εμφανίζεται τάση. Η τάση αυτή ονομάζεται τάση εισόδων.

Η τάση για την τροφοδοσία των εισόδων δεν δημιουργείται από τη μονάδα τροφοδοσίας του ελεγκτή, αλλά πρέπει να τη δημιουργήσουμε εμείς με κατάλληλο τροφοδοτικό (για DC) ή μετασχηματιστή τάσης χειρισμού (για AC). Εξαίρεση αποτελούν συνήθως οι πολύ μικροί ελεγκτές, στους οποίους ο κατασκευαστής μπορεί να έχει ενσωματώσει ένα μικρό τροφοδοτικό.

Μία κάρτα ψηφιακών εισόδων ικανοποιεί π.χ. τα παρακάτω χαρακτηριστικά:

- Τάση εισόδου: Ονομαστική τιμή 24 VDC.
- Επιτρεπτή περιοχή 20.4 - 28.8 VDC.
- Γαλβανική απομόνωση.
- Περιοχή τάσης για το σήμα ‘’1’’ 15-30VDC, περιοχή τάσης για το σήμα ‘’0’’ 0-5VDC.
- Ένδειξη της κατάστασης του σήματος της κάθε ψηφιακής εισόδου με LED.
- Επιπρόσθετη φίσσα καλωδίωσης που μετακινείται απλά και χωρίς κίνδυνο να τοποθετηθεί σε λάθος τύπο κάρτας (περιλαμβάνει Key πολικότητας)
- Μέγιστος χρόνος ανταπόκρισης στην ονομαστική τάση εισόδου :1.2 -4.8 ms
- Ρεύμα εισόδου για σήμα ‘’1’’ μέγιστο 7.5 mA
- Δυνατότητα συλλογής ψηφιακής πληροφορίας μέχρι 1000m με μπλενταρισμένο καλώδιο 600 m χωρίς μπλενταρισμένο καλώδιο.

Τα σπουδαιότερα τεχνικά χαρακτηριστικά μίας μονάδας εισόδων είναι: το πλήθος εισόδων, η γαλβανική απομόνωση, η ονομαστική τάση, οι ανοχές τάσης για σήμα «1», οι ανοχές τάσης για σήμα «0», η μέγιστη συνολική διαδρομή καλωδίων, το ρεύμα που απορροφά

κάθε είσοδος σε σήμα «1», το ρεύμα που απορροφά η μονάδα συνολικά από τα εσωτερικά DC 5V, η απαιτούμενη πρίζα καλωδίων (τύπος).

Μονάδες ψηφιακών εξόδων

Οι μονάδες ψηφιακών εξόδων χρησιμεύουν για τη διέγερση των εξωτερικών στοιχείων της εγκατάστασης όπως ρελέ κινητήρων, βαλβίδες, ενδεικτικές λυχνίες κλπ. Όταν από το πρόγραμμα δοθεί εντολή για τη διέγερση ενός π.χ. εξωτερικού ρελέ, τότε κλείνει ο αντίστοιχος «διακόπτης» της εξόδου. Η τάση εμφανίζεται στην κλέμα εξόδου και το ρελέ οπλίζει. Η τάση αυτή ονομάζεται τάση εξόδων. Ο «διακόπτης» εξόδου είναι συνήθως ηλεκτρονικός (τρανζίστορ, triac), αλλά μπορεί να είναι και μηχανική επαφή μικρορελέ.

Η τάση για την τροφοδοσία των μονάδων εξόδων δεν δημιουργείται από τη μονάδα τροφοδοσίας του ελεγκτή, αλλά με κατάλληλο τροφοδοτικό (για DC) ή μετασχηματιστή τάσης χειρισμού (για AC).

Τα κυκλώματα και οι τάσεις των εισόδων είναι τελείως ανεξάρτητα από τα κυκλώματα και τις τάσης των εξόδων. Επομένως η τάση για τις εισόδους μπορεί να είναι διαφορετική από την τάση για τις εξόδους. Επιπλέον υπάρχει η δυνατότητα και ξεχωριστής τάσης ανά μονάδα εισόδων ή εξόδων. Συνήθως μια μονάδα εξόδων περιλαμβάνει 4 ή 8 ή 16 ή 32 εξόδους, ανάλογα με τον τύπο του ελεγκτή και την τάση.

Τα σπουδαιότερα τεχνικά χαρακτηριστικά μίας μονάδας εξόδων είναι: το πλήθος των εξόδων, η γαλβανική απομόνωση, η ονομαστική τάση, οι ανοχές τάσης, το ονομαστικό ρεύμα κάθε εξόδου, το ελάχιστο ρεύμα φορτίου, η ταυτόχρονη φόρτιση εξόδων μιας ομάδας, η προστασία εξόδων, η μέγιστη συνολική διαδρομή καλωδίων, η συχνότητα ζεύξεων, το ρεύμα που απορροφά η μονάδα συνολικά από τα εσωτερικά 5V, η απαιτούμενη πρίζα καλωδίων (τύπος).

Αν γίνει κάποιο βραχυκύκλωμα στο εξωτερικό κύκλωμα μιας εξόδου, τότε χρειάζεται η «επέμβαση» της προστασίας που υπάρχει μέσα στη μονάδα. Στην απλούστερη περίπτωση, η προστασία αυτή είναι μια ασφάλεια υπερταχείας τήξης και μάλιστα μία ανά μονάδα εξόδων. Αντίθετα, στις μονάδες DC 24V, είναι συνηθισμένη η «ηλεκτρονική» προστασία. Σ' αυτή την περίπτωση, όταν συμβεί ένα εξωτερικό βραχυκύκλωμα, η προστασία μειώνει ή και μηδενίζει ακόμα την τάση εξόδου της μονάδας, ώστε το ρεύμα εξόδου να μην υπερβεί το μέγιστο επιτρεπόμενο.

Μία τυπική κάρτα ψηφιακών εξόδων έχει:

- Τάση τροφοδοσίας 24VDC.
- Γαλβανική απομόνωση.
- Επιτρεπτή περιοχή τάσης 20.4...28.8 VDC.
- Τάση εξόδου για ''σήμα''1'' 24VDC ±0.8V.
- Ρεύμα εξόδου για ''1'' σε 60C°, 0.5^{A}.
- Ελάχιστο ρεύμα για ''1'' σε 60C°, 5mA.
- Συνολικό ρεύμα εξόδου (ανά ομάδα εξόδων) 2^{A}.
- Φορτίο Λαμπτήρα 5W.

- Συχνότητα ζεύξεων επαφών.
  Ωμικών 100HZ.
  Επαγωγικών 0.5HZ.
  Φορτία ενδείξεως 100HZ.
- Ένδειξη κατάστασης του σήματος της κάθε ψηφιακής εξόδου με LED.
- Επιπρόσθετη φίσσα καλωδίων.
- Ηλεκτρονική προστασία από βραχυκύκλωμα.

Μονάδες αναλογικών εισόδων

Μία αναλογική κάρτα εισόδων μπορεί να επεξεργασθεί αισθητήρια με δυνατότητα μετρήσεων βασικών περιοχών τάσης, ρεύματος και ωμικής αντίστασης όπως:

- ± 1V /200 ΚΩ Αντίσταση εισόδου.
- 1..5V/200 ΚΩ Αντίσταση εισόδου και περιοχών ρεύματος.
- 4...20mA/80Ω Αντίσταση εισόδου.
- ±20mA/ 80Ω Αντίσταση εισόδου.
- Θερμοστοιχεία N, E, J, K.
- PT100 Standard /10 Mohms.

Μία τυπική κάρτα αναλογικών εισόδων έχει:

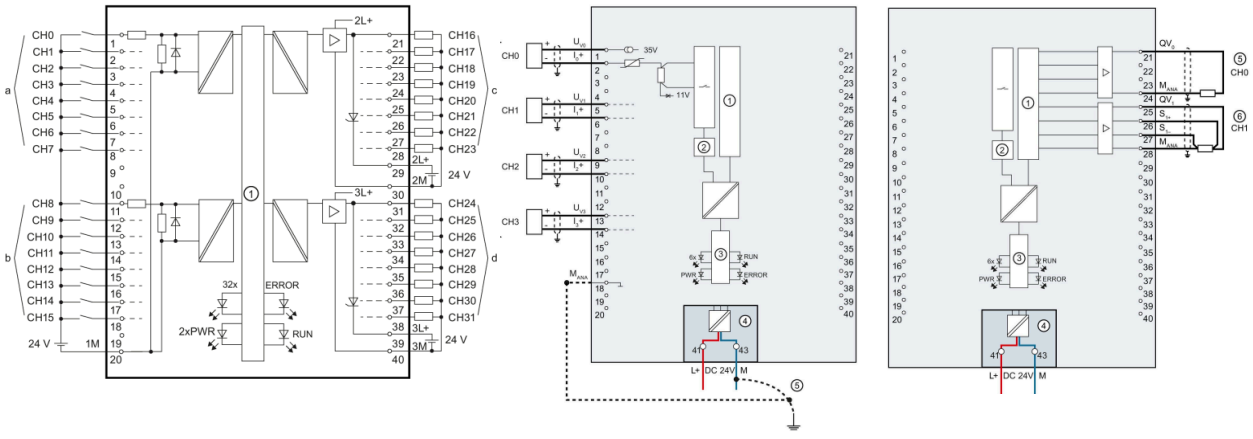
- Η ανάλυση του A/D μετατροπέα της κάρτας είναι 13bits.
- Ο κύκλος ολοκλήρωσης / μετατροπής για κάθε κανάλι 2.5/100msec.
- Το μήκος καλωδίου μέχρι το αισθητήριο θα είναι τουλάχιστον 200m με μπλενταρισμένο καλώδιο.
- Έχει γαλβανική απομόνωση.
- Προστασία έναντι ανάστροφου πολικότητας.
- Επιτρεπτή τάση εισόδου για κανάλι τάσης 20V.
- Επιτρεπτό ρεύμα εισόδου για κανάλι ρεύματος 40mA.
- Αντιστάθμιση Θερμοκρασίας: εσωτερική ή εξωτερικό με Module αντιστάθμισης.
- Όριο σφάλματος λειτουργίας (πάνω από την περιοχή θερμοκρασίας πού αναφέρεται στην περιοχή εισόδου) max ±1%.
- Όριο Βασικού σφάλματος (Όριο σφάλματος λειτουργίας στα 25° πού αναφέρεται στην περιοχή εισόδου) max ± 0.6 %
- Δυνατότητα διάγνωσης μέσω κόκκινου Led για σφάλματα καναλιών
- Φίσσα καλωδίων με στοιχείο κωδικοποίησης. Όταν η φίσσα τοποθετείται για πρώτη φορά στην κάρτα τότε το στοιχείο κωδικοποίησης επιδρά στο να μπορεί να τοποθετηθεί η φίσσα σε κάρτες της ιδίας περιοχής τάσης ή ρεύματος.

Μονάδες αναλογικών εξόδων

Μία αναλογική κάρτα εξόδων μπορεί να εντολοδοτήσει ηλεκτρονικά στοιχεία μέσω βασικών περιοχών τάσης και ρεύματος.

Μία τυπική κάρτα αναλογικών εξόδων έχει:

- Τάση τροφοδοσίας 24VDC.
- Γαλβανικά απομονωμένη.
- Περιοχές εξόδου τάσης ±10V, 0-10V 1-5V και περιοχές εξόδου ρεύματος 4..20mA, ±20mA, 0-20mA πού μπορούν να αλλαχθούν με μηχανικά Jumbers πάνω στην κάρτα ενώ διάφορες ρυθμίσεις μπορούν να γίνουν από το Software.
- Αντίσταση φορτίου για τα κανάλια τάσης min 1ΚΩ.
- Αντίσταση φορτίου για τα κανάλια ρεύματος max 0.5 ΚΩ.
- Χωρητικά φορτία max 1μF.
- Επαγωγικά φορτία max 1 mH.
- Προστασία από βραχυκύκλωμα με ρεύμα βραχυκύκλωσης 25mA για εξόδους τάσης.
- Ισχύς εξόδου με τάση ανοικτού κυκλώματος 18V.
- Η ανάλυση του D/A Converter είναι 11 bits+Πρόσημο (±10V, 4..20mA, ±20mA, 1-5V) , 12 Bits (0-10V, 0-20mA).
- Ο κύκλος μετατροπής για κάθε κανάλι είναι max 0.8 msec και ειδικά για Ωμικά φορτία 0.1ms για χωρητικά φορτία 3.3 m για επαγωγικά φορτία 0.5.ms.
- Όρια λειτουργίας (0..60°C στην περιοχή εξόδου) Τάση ± 0,5% Ρεύμα ± 0.6%.
- Βασικό σφάλμα (0-25°C στην περιοχή εξόδου) Τάση ±0,2% Ρεύμα ±0,3%.
- Το μήκος καλωδίου μέχρι το στοιχείο ενεργοποίησης είναι 200m με μπλενταρισμένο καλώδιο.
- Φίσσα καλωδίου με την ίδια λογική όπως της αναλογικής κάρτας εισόδου.
- Δυνατότητα διάγνωσης μέσω κόκκινου Led για σφάλματα καναλιών



Εικόνα 24. Κάρτες Εισόδων και Εξόδων

Κάρτες επικοινωνίας

Το PLC για την επικοινωνία με άλλα στοιχεία του συστήματος αυτοματισμού εκτός από σήματα εισόδων και εξόδων μπορεί να διαθέτει και κάρτες που να υποστηρίζουν διάφορα πρωτόκολλα επικοινωνίας όπως RS232, RS422, RS485, TCP/IP, κλπ για ανταλλαγή δεδομένων π.χ με ένα άλλο PLC, με ένα Scanner, με έναν εκτυπωτή.

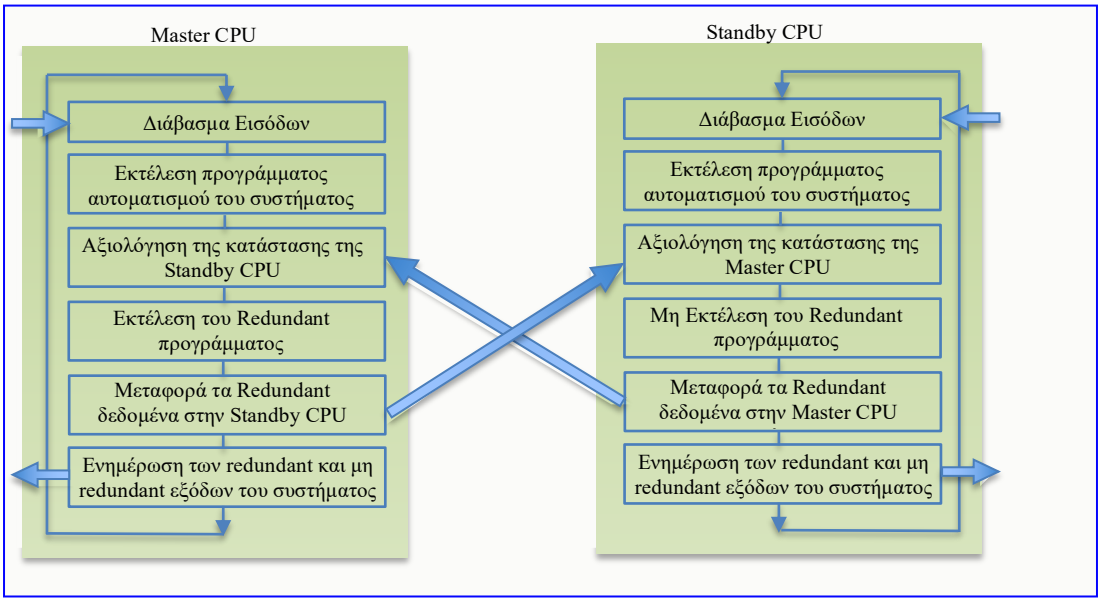
3.2.2 Redundant PLC

Ο σκοπός της χρήσης συστημάτων αυτοματισμού με ανοχή σε σφάλματα είναι να μειωθούν οι χρόνοι διακοπής της παραγωγής, ανεξάρτητα από το αν οι βλάβες οφείλονται σε σφάλμα/βλάβη ή οφείλονται σε συντήρηση. Όσο υψηλότερο είναι το κόστος παύσης της παραγωγής τόσο μεγαλύτερη είναι η ανάγκη χρήσης ενός συστήματος με ανοχή σε σφάλματα. Το γενικά υψηλότερο κόστος των συστημάτων ανοχής σε σφάλματα ανακτάται σύντομα από την αποφυγή παύσεων της παραγωγής.

Σε πολύ κρίσιμες εφαρμογές όπως στα διυλιστήρια, αεροδρόμια, πυρηνικά εργοστάσια απαιτούνται τέτοια συστήματα όχι μόνο για το κόστος παύσης της παραγωγής αλλά και για την πρόκληση ατυχημάτων.

Software Redundancy

Σε πολλές εφαρμογές οι απαιτήσεις για την ανοχή σε σφάλματα δεν μπορούν να καλύψουν το κόστος ειδικών συστημάτων ανοχής σε σφάλματα. Έτσι συχνά απλοί μηχανισμοί λογισμικού είναι επαρκείς για να επιτρέψουν τη συνέχιση μιας αποτυχημένης εργασίας ελέγχου σε ένα υποκατάστατο σύστημα εάν παρουσιαστεί ένα σφάλμα. Οι μηχανισμοί αυτοί μπορούν να εφαρμοστούν για τον έλεγχο διαδικασιών που ανέχονται καθυστερήσεις μετάβασης σε ένα υποκατάστατο σύστημα σε εύρος μερικών δευτερολέπτων, π.χ. σε έργα νερού, εγκαταστάσεις επεξεργασίας νερού ή ροές κυκλοφορίας.
Το παρακάτω διάγραμμα ροής δείχνει την αρχή λειτουργίας ενός Software Redundancy συστήματος.



Εικόνα 25. Software Redundancy

Το ανεκτικό σε σφάλματα (fault-tolerant) λογισμικό είναι φορτωμένο και στην κύρια (Master) και στην σε αναμονή (Standby) CPU. Το πρόγραμμα επεξεργάζεται μόνο στην κύρια CPU και όχι στην σε αναμονή CPU. Η μη επεξεργασία του προγράμματος της CPU σε κατάσταση αναμονής αποτρέπει προβλήματα όπως λάθη συναγερμών, διαφορετικό κύκλο επεξεργασίας κ.λπ. Το πρόγραμμα στην CPU αναμονής είναι φυσικά πάντα έτοιμο να αναλάβει την επεξεργασία. Αυτός ο τύπος της λειτουργίας αναμονής περιγράφεται ως ζεστή αναμονή (Hot Standby). Σε συστήματα με Hardware Redundancy στην κατάσταση Hot Standby οι δύο CPU είναι συνέχεια συντονισμένες, κάνοντας έτσι τη διαδικασία της μεταγωγής από τη μία στην άλλη ποιο γρήγορη.

Η κύρια CPU μεταφέρει συνεχώς τα πραγματικά δεδομένα της διεργασίας στον σταθμό αναμονής, έτσι σε περίπτωση σφάλματος η CPU που είναι σε αναμονή να έχει όλα τα απαραίτητα δεδομένα και να συνεχίσει τη λειτουργία του συστήματος. Ωστόσο, η μεταφορά τέτοιων δεδομένων μπορεί να διαρκέσει αρκετούς κύκλους επεξεργασίας ανάλογα με τη μέθοδο επικοινωνίας και τον όγκο των δεδομένων, δηλαδή η επεξεργασία στον σταθμό αναμονής καθυστερεί πάντα για συγκεκριμένο αριθμό κύκλων σε σύγκριση με τον κύριο, ανάλογα με την απόδοση της επικοινωνίας και τον όγκο των δεδομένων. Αλλαγή σταθμού από master σε standby ενεργοποιείται αμέσως μετά τον εντοπισμό ενός σφάλματος στην κύρια CPU ή σε μια μονάδα της κύρια CPU π.χ. μίας κάρτας επικοινωνίας. Μετά την αλλαγή ο σταθμός αναμονής αναλαμβάνει τη κύρια λειτουργία.

Το Redundant Software ελέγχει και συντονίζει τις περιοχές μνήμης των δύο CPU όπως Χρονικά, Μετρητές, Μνήμες κ.λπ. και μόνο αυτό έχει πρόσβαση εγγραφής σε αυτές τις περιοχές.

Εκτός από τα στοιχεία του Redundant Software μία CPU μπορεί να έχει πρόγραμμα που να ελέγχει συσκευές που αφορούν μόνο αυτή τη CPU και όχι και τη δεύτερη CPU, το Redundant Software λογισμικού δεν έχει καμία επιρροή σε αυτές τις συσκευές. Οι συσκευές αυτές δηλαδή υποδηλώνουν μονάδες I/O που έχουν εκχωρηθεί μόνο σε μία CPU. Τέτοιες μονάδες μπορούν να συνδεθούν ως κεντρικές ή κατανεμημένες συσκευές στο δικό τους κύριο σύστημα επικοινωνίας, ή μπορεί να συνδεθούν ως κατανεμημένες συσκευές σε ένα από τα δύο κύρια συστήματα επικοινωνίας που περιέχουν τις Redundant μονάδες επικοινωνίας.

Το μη Redundant στοιχείο του προγράμματος μπορεί να ανταλλάξει τα δεδομένα του με το Redundant λογισμικό μέσω κατάλληλων ρουτινών. Τα δεδομένα αυτών των ρουτινών ανταλλάσσονται μέσω του Redundant λογισμικού και επομένως διατίθενται στην συνεργαζόμενη CPU. Οι είσοδοι γράφονται στην μνήμη στην αρχή της κύριας ρουτίνας (OB 1). Το Redundant λογισμικό υποβάλλεται σε επεξεργασία πριν οποιαδήποτε δεδομένα του (είσοδοι, έξοδοι, μνήμες, χρονικά, μετρητές, κλπ) μεταφερθούν στο σύστημα αναμονής. Ο σταθμός αναμονής πρέπει να λάβει τα δεδομένα από τον ενεργό σταθμό αφού έχει ολοκληρώση την εκκίνησή του. Στο τέλος της κύριας ρουτίνας (OB 1) οι έξοδοι του Redundant μεταφέρονται στις μνήμες των εξόδων της κύριας και της αναμονής CPU και από εκεί μεταφέρεται στις συσκευές εξόδων στο τέλος του κυκλικής επεξεργασίας.

Για την αποφυγή καθυστερήσεων της εκκίνησης του σταθμού αναμονής μετά από αστοχία της κύριας το πρόγραμμα με ανοχή σε σφάλματα μεταφέρεται πλήρες στον σταθμό αναμονής για την κάλυψη καταστάσεων έκτακτης ανάγκης/μετάβασης.

Ο χρόνος που απαιτείται για τη μεταφορά των δεδομένων μπορεί να διαρκέσει περισσότερο από έναν κύκλο επεξεργασίας της CPU, αυτό εξαρτάται από τον τρόπο επικοινωνίας και τον όγκο των δεδομένων που θα μεταφερθούν. Κατά την κανονική λειτουργία η CPU αναμονής μεταφέρει μέσω επικοινωνίας το τελευταίο PIO (Process Image) σε όλες τις κάρτες επικοινωνίας του συστήματος, αυτά όμως τα δεδομένα αγνοούνται από τις κάρτες επικοινωνίας επειδή όλα δεδομένα αξιοποιούνται από την κύρια CPU. Κατά τη διάρκεια ενός σφάλματος-αποτυχίας master-standby, οι πιο πρόσφατες τιμές PIO των καρτών επικοινωνίας παγώνουν και ακόμα και εάν δεν έχει ολοκληρωθεί η ανακατεύθυνση από την κύρια CPU στην CPU αναμονής το τελευταίο PIO που μεταφέρθηκε πλήρως στην CPU αναμονής εξέρχεται από τις μονάδες επικοινωνίας στις κάρτες σημάτων. Η αλλαγή της κύριας σε κατάσταση αναμονής μπορεί να διαρκέσει αρκετούς κύκλους, ανάλογα με το φύση του σφάλματος.

Για την αντικατάσταση μίας χαλασμένης CPU όλα τα δεδομένα διαμόρφωσης και ολόκληρο το πρόγραμμα πρέπει να φορτωθεί από συσκευή προγραμματισμού ή την κάρτα μνήμης στη νέα, δεν μεταφέρεται δηλαδή αυτόματα από τη σε λειτουργία CPU στη νέα CPU αυτόματα όπως γίνεται στο Hardware Redundancy.

Εάν μία CPU βρεθεί σε κατάσταση λειτουργίας STOP, η δεύτερη CPU θα λειτουργήσει αυτόματη ως κύρια σε λειτουργία Master. Η επικοινωνία της CPU που είναι στο STOP είναι ενεργή αλλά δεν μεταφέρει το PIO στις κάρτες επικοινωνίας, όταν η CPU αλλάξει από κατάσταση STOP σε κατάσταση RUN, τότε μεταφέρει το PIO στις κάρτες επικοινωνίας ως CPU αναμονής.

Hardware Redundancy

Το Hardware Redundancy αποτελείται από δύο υποσυστήματα που συγχρονίζονται μέσω καλωδίων οπτικών ινών.

Και τα δύο υποσυστήματα δημιουργούν ένα ανεκτικό σε σφάλματα σύστημα αυτοματισμού (fault-tolerance automation system) που λειτουργεί με δύο κανάλια και βασίζεται στην αρχή του ενεργού πλεονασμού (active redundancy). Ενεργός πλεονασμός σημαίνει ότι όλοι οι περιττοί πόροι (redundant resources) βρίσκονται συνεχώς σε λειτουργία και συμμετέχουν ταυτόχρονα στην εκτέλεση της εργασίας ελέγχου, αυτό σημαίνει ότι τα προγράμματα και στις δύο CPU είναι πανομοιότυπα και εκτελούνται συγχρονισμένα από τις CPU.

Για τον διαχωρισμό των δύο υποσυστημάτων χρησιμοποιούνται οι παραδοσιακές εκφράσεις “master” και “reserve” για συστήματα ανοχής σφαλμάτων δύο καναλιών. Το reserve πάντα επεξεργάζεται συμβάντα σε συγχρονισμό με το master και δεν περιμένει για τυχόν σφάλματα από το master για να αρχίσει την επεξεργασία του. Η διάκριση που γίνεται μεταξύ της master και της reserve CPU είναι πολύ σημαντική για εξασφάλιση των αντιδράσεων σε περίπτωση σφαλμάτων. Για παράδειγμα, η reserve CPU μπορεί να μπει σε STOP όταν ο εφεδρικός σύνδεσμος έχει κάποιο σφάλμα, ενώ η κύρια CPU παραμένει σε RUN.

Ανάθεση Master/Reserve

Όταν το σύστημα ενεργοποιείται η CPU που ξεκίνησε πρώτη αναλαμβάνει κύρια (master) λειτουργία και η συνεργαζόμενη CPU αναλαμβάνει το ρόλο της εφεδρικής λειτουργίας (reserve).

Η προκαθορισμένη επιλογή κύριας/εφεδρικής διατηρείται όταν ενεργοποιηθούν και οι δύο CPU ταυτόχρονα.

Η ανάθεση κύριας/εφεδρικής αλλάζει όταν:

- Η εφεδρική CPU ξεκινά πριν από την κύρια CPU (διάστημα τουλάχιστον 3 δευτερολέπτων)
- Η κύρια CPU αποτυγχάνει ή μπαίνει σε STOP

Συγχρονισμός των υποσυστημάτων

Η κύρια και η εφεδρική CPU συνδέονται με καλώδια οπτικών ινών εκτελούν συγχρονισμένα το πρόγραμμα μέσω αυτής της σύνδεσης. Ο συγχρονισμός εκτελείται αυτόματα από το λειτουργικό σύστημα και δεν έχει καμία επίδραση στο πρόγραμμα του χρήστη.

Διαδικασία συγχρονισμού βάσει συμβάντων

Ο συγχρονισμός βάσει συμβάντων σημαίνει ότι η κύρια και η εφεδρική CPU συγχρονίζουν πάντα τα δεδομένα τους όταν συμβαίνει ένα γεγονός που μπορεί να οδηγήσει σε διαφορετικές εσωτερικές καταστάσεις των υποσυστημάτων.

Η κύρια και η εφεδρική CPU συγχρονίζονται όταν:

- Υπάρχει άμεση πρόσβαση στα I/O.
- Παρουσιάζονται διακοπές λειτουργίας.

- Τα χρονικά του χρήστη ενεργοποιούνται ή απενεργοποιούνται.
- Τα δεδομένα τροποποιούνται από άλλες συσκευές μέσω επικοινωνίας.

Η μέθοδος συγχρονισμού βάσει συμβάντων διασφαλίζει την απρόσκοπτη συνέχιση της λειτουργίας από την εφεδρική CPU όταν η κύρια CPU έχει κάποιο σφάλμα.

Αυτοέλεγχος

Οι δυσλειτουργίες ή τα σφάλματα πρέπει να εντοπίζονται και να αναφέρονται το συντομότερο δυνατό. Κατά συνέπεια εφαρμόζονται εκτενείς λειτουργίες αυτοδιαγνωστικού ελέγχου που εκτελούνται αυτόματα και εξ ολοκλήρου στο παρασκήνιο.

Τα στοιχεία και οι λειτουργίες που ελέγχονται είναι:

- Σύζευξη των κεντρικών rack.
- Επεξεργαστής.
- Εσωτερική μνήμη της CPU.
- Δίαυλος I/O.

Εάν ο αυτοέλεγχος εντοπίσει ένα σφάλμα το σύστημα προσπαθεί να το εξαλείψει.

Καταστάσεις ενός Redundant συστήματος

Οι καταστάσεις ενός redundant συστήματος προκύπτουν από τις καταστάσεις λειτουργίας των δύο CPU. Ο όρος "κατάσταση συστήματος" χρησιμοποιείται ως απλοποιημένος όρος που προσδιορίζει την κατάσταση της κάθε CPU στην ταυτόχρονη λειτουργία τους. Οι καταστάσεις λειτουργίας περιγράφουν τη συμπεριφορά των CPU σε οποιαδήποτε δεδομένη χρονική στιγμή και είναι χρήσιμες για τον προγραμματισμό της εκκίνησης, της δοκιμής και της διάγνωσης των σφαλμάτων.

Πίνακας 20. Καταστάσεις Redundant Συστήματος

Κατάσταση Συστήματος	Κατάσταση των δύο CPU	
	Master	Reserve
Stop	Stop	Stop, Power Off, Defective
Start-up	Start-up	Stop, Power Off, Defective, no Synchronization
Single mode	Run	Stop, Power Off, Error-Search, Defective, no Synchronization
Link-up	Run	Start-up, Link-up
Update	Run	Update
Redundant	Run	Run
Hold	Hold	Stop, Power Off, Error-Search, Defective, no Synchronization

Σε γενικές γραμμές οι δύο CPU έχουν ίσα δικαιώματα είτε είναι master είτε reserve. Για λόγους αναγνωσιμότητας η κύρια CPU (CPU 0) ξεκινάει πριν ενεργοποιηθεί η εφεδρική CPU (CPU 1).

Το παρακάτω σχήμα δείχνει τις καταστάσεις λειτουργίας των δύο CPU, από το Power On έως την redundant λειτουργία του συστήματος.

Πίνακας 21. Βήματα έναρξης Redundant Συστήματος

Steps	Master CPU		Reserve CPU
1 → Stop	Stop		Stop
2→ Start-up	Start-up		Stop
3→Single Mode	Run		Stop
4→ Link-up	Run →	Updating the user program →	Start-up /Link-up
5→ Update	Run →	Updating dynamic data →	Update
6→Redundant Mode	Run		Run

Για την καλύτερη κατανόηση παρακάτω δίνεται η επεξήγηση των καταστάσεων.

Stop: Οι CPU δεν εκτελούν καμία ρουτίνα.

Start-up: Η κύρια CPU συγκρίνει την υπάρχουσα διαμόρφωση I/O με την δηλωμένη διαμόρφωση.

Link-up και Update: Η κύρια CPU ελέγχει και ενημερώνει το περιεχόμενο μνήμης της εφεδρικής CPU πριν αναλάβει τη λειτουργία συστήματος. Αυτό υλοποιείται σε δύο διαδοχικές φάσεις: σύνδεση και ενημέρωση. Η κύρια CPU είναι πάντα σε λειτουργία RUN και η εφεδρική CPU είναι σε Link-up ή Update κατά τη διάρκεια των φάσεων σύνδεσης και ενημέρωσης. Εκτός από τις λειτουργίες σύνδεσης και ενημέρωσης το σύστημα υποστηρίζει επίσης την σύνδεση και ενημέρωση σε συνδυασμό με την μεταγωγή κύριας και εφεδρικής CPU.

Run: Η CPU εκτελεί το πρόγραμμα του χρήστη.

Single: Η CPU εκτελεί το πρόγραμμα του χρήστη χωρίς να είναι διαθέσιμη η δεύτερη CPU.

Redundant: Η κύρια CPU και η εφεδρική CPU είναι πάντα σε λειτουργία RUN και οι δύο CPU εκτελούν το πρόγραμμα χρήστη σε συγχρονισμό και εκτελούν αμοιβαίους ελέγχους.

Επικοινωνίες (Communications)

Οι αυξημένες απαιτήσεις για τη διαθεσιμότητα ενός συνολικού συστήματος απαιτούν και αυξημένη αξιοπιστία του συστήματος επικοινωνίας που σημαίνει εφαρμογή διπλής επικοινωνίας.

Παρακάτω δίνεται μια επισκόπηση των βασικών εννοιών για χρήση επικοινωνιών με ανοχή σφαλμάτων (fault-tolerant).

Η διαθεσιμότητα του συστήματος επικοινωνίας μπορεί να βελτιωθεί με τον πλεονασμό των μέσων, διπλών μονάδων ή διπλών όλων των στοιχείων διαύλου. Σε περίπτωση βλάβης κατά τη διάρκεια της λειτουργίας μίας μονάδας διασφαλίζεται από τους μηχανισμούς παρακολούθησης και συγχρονισμού ότι οι λειτουργίες επικοινωνίας αναλαμβάνονται από τα εφεδρικά στοιχεία.

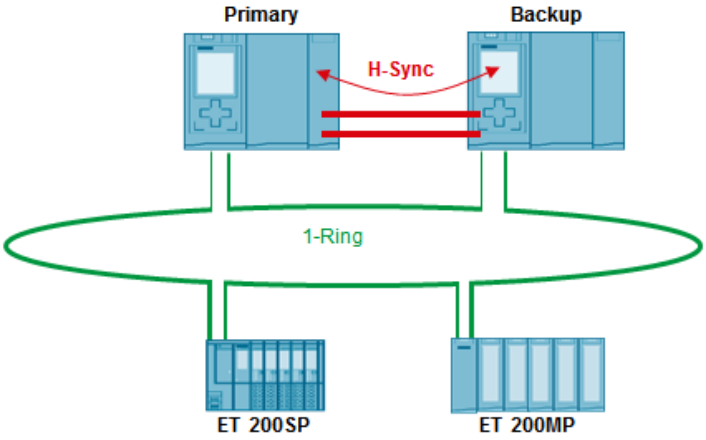
Οι κόμβοι πλεονασμού (Redundancy nodes) διαθέτουν μία εξαιρετική αξιοπιστία για την επικοινωνία μεταξύ δύο συστημάτων. Ένα σύστημα με στοιχεία πολλαπλών καναλιών

αντιπροσωπεύεται από κόμβους πλεονασμού. Οι κόμβοι πλεονασμού είναι ανεξάρτητοι, όταν δηλαδή έχουμε αποτυχία ενός στοιχείου εντός του κόμβου δεν επηρεάζει την αξιοπιστία στους άλλους κόμβους.

Η απαίτηση για μεγαλύτερη διαθεσιμότητα με στοιχεία επικοινωνίας σημαίνει ότι είναι απαραίτητες διπλές συνδέσεις επικοινωνίας μεταξύ των εμπλεκομένων συστημάτων. Σε αντίθεση με μια απλή επικοινωνία, μια διπλή με ανοχή σε σφάλματα αποτελείται από τουλάχιστον δύο υποσυνδέσεις. Ανάλογα από τις απαιτήσεις του συστήματος μπορούμε να έχουμε έως και τέσσερις υποσυνδέσεις, εκ των οποίων οι δύο να είναι πάντα εγκατεστημένοι (ενεργοί) για τη διατήρηση της επικοινωνίας σε περίπτωση σφάλματος. Ο αριθμός των υποσυνδέσεων εξαρτώνται από τις πιθανές εναλλακτικές διαθέσιμες διαδρομές.

Ο ευκολότερος τρόπος για την βελτίωση της διαθεσιμότητας μεταξύ συνδεδεμένων συστημάτων είναι να εφαρμογή διπλού δίαυλου επικοινωνίας χρησιμοποιώντας σύστημα διπλού δακτυλίου οπτικών ινών ή χάλκινων καλωδίων. Οι συνδεδεμένοι κόμβοι μπορεί να αποτελούνται από απλά τυπικά στοιχεία. Η τοπολογία δακτυλίου περιέχει βασικά δύο διπλά στοιχεία και σχηματίζει αυτόματα ένα 1-από-2 κόμβους πλεονασμού. Ένα δίκτυο οπτικών ινών μπορεί να δημιουργηθεί ως τοπολογία γραμμής ή αστέρα.

Στην Εικόνα 26 φαίνεται ένα τέτοιο σύστημα [17], [18]. Οι δύο CPU είναι η Primary (master) και η Backup (reserve), ενώ το ET200SP και ET200MP είναι οι κάρτες σημάτων για τον έλεγχο του συστήματος αυτοματισμού και κάθε φορά ελέγχονται από τη CPU που είναι Master. Η δικτύωση μεταξύ τους είναι σε τοπολογία Ring, έτσι ώστε εάν κοπεί το καλώδιο σε ένα σημείο το σύστημα να συνεχίσει να λειτουργεί κανονικά.



Εικόνα 26. Σύστημα Redundant PLC

3.2.3 Safety PLC

Όταν οι απαιτήσεις της διεργασίας για Safety λειτουργία του αυτοματισμού είναι μεγάλες και σύνθετες τότε δεν το καλύπτουν τα Safety Relay οπότε γίνεται χρήση των Safety PLC. Για παράδειγμα σε μία τέτοια διεργασία δεν υπάρχει απλά ένα Stop Emergency αλλά χρησιμοποιείται και μία Laser Curtain. Αυτό π.χ. σημαίνει ότι εάν περάσει από τον χώρο που βρίσκεται η μηχανή κάποιος εργάτης θα πρέπει η λειτουργία της μηχανής να σταματήσει και να ξεκινήσει ξανά όταν βγει ο εργάτης. Μάλιστα αυτό θα πρέπει να γίνει μετά από ορισμένο χρόνο και κάποιο Reset.

Οι περισσότεροι κατασκευαστές PLC παράγουν πλέον Safety PLC με επιπλέον λειτουργίες, τόσο σε Hardware όσο και σε Software (από ότι στα Basic PLC). Υπάρχουν PLC που είναι μόνο για τη Safety λειτουργία αλλά και PLC που εκτελούν ταυτόχρονα και την αυτόματη και την Safety λειτουργία.

Σε σύνθετα συστήματα αυτοματισμού η επικίνδυνη λειτουργία της μηχανής ελέγχεται από ένα Safety PLC (και όχι από ένα Safety Relay) θέτοντας πολλές φορές διαφορετικό τρόπο ασφαλούς σταματήματος της παραγωγής, ανάλογα με το πρόβλημα που υπάρχει κάθε φορά. Στο Safety PLC υπάρχει πρόγραμμα ασφαλείας και οι ειδικές Safety μονάδες Εισόδων και Εξόδων. Μόλις παρουσιαστεί κάποιο σφάλμα καλωδίωσης ή πιεσθεί το μπουτόν Emergency

ή ανοίξει η Safety Door ανιχνεύεται αυτόματα και η μηχανή μεταβαίνει σε Safety κατάσταση. Η παρακολούθηση της καλωδίωσης των ενεργοποιητών και των αισθητήρων που σχετίζονται με την ασφάλεια γίνεται από τις ειδικές μονάδες Εισόδων και Εξόδων του PLC.

Η καλωδίωση και η αρχιτεκτονική των λειτουργιών προστασίας σύμφωνα με το SIL 3 (EN 62061) Cat.4 (EN 954) είναι η ίδια με αυτή του Safety Realy. Το Stop Emergency και οι Safety Doors συνδέονται μέσω δύο καναλιών στις ειδικές κάρτες του PLC.

Η Safety Integrated Technology είναι η πλήρως ενσωματωμένη έννοια ασφάλειας για αυτοματισμούς και μονάδες κίνησης με αποδεδειγμένες τεχνολογίες και συστήματα αυτοματισμού που χρησιμοποιούνται για την ασφαλή λειτουργία της παραγωγής. Επίσης καλύπτει ολόκληρη την αλυσίδα ασφάλειας από αισθητήρες και ενεργοποιητές έως τον ελεγκτή, συμπεριλαμβανομένης της επικοινωνίας που σχετίζεται με την ασφάλεια πάνω από τα τυπικά δίκτυα.

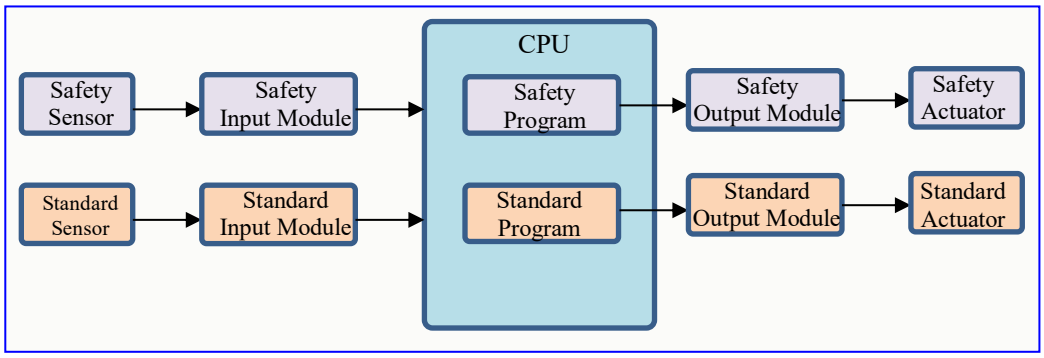
Το PLC δηλαδή εκτός από την αυτόματη λειτουργία της παραγωγής αναλαμβάνει και την ασφαλή λειτουργία αυτής. Ένα ιδιαίτερο χαρακτηριστικό του Safety Integrated Technology είναι ότι εξασφαλίζει όχι μόνο αξιόπιστη ασφάλεια, αλλά και υψηλό επίπεδο ευελιξίας και παραγωγικότητας. Η ενσωμάτωση της ασφαλής και της αυτόματης λειτουργίας σε ένα PLC έχει τα ακόλουθα σημαντικά πλεονεκτήματα:

- Μεγαλύτερη ευελιξία από τις ηλεκτρομηχανικές λύσεις.
- Μείωση των καλωδιώσεων.
- Απαιτείται μόνο μία CPU λόγω της συνύπαρξης του τυπικού προγράμματος και του προγράμματος ασφαλείας.
- Απλή επικοινωνία μεταξύ του τυπικού προγράμματος και του προγράμματος ασφάλειας.
- Λιγότερος χρόνος υλοποίησης της εφαρμογής.

Για την διπλή λειτουργία (Safety και αυτόματη) του συστήματος το PLC διαθέτει CPU όπου ταυτόχρονα εκτελεί το πρόγραμμα για την αυτόματη λειτουργία αλλά και για τη Safety. Διαθέτει τυπικές κάρτες Εισόδων και Εξόδων για την αυτόματη λειτουργία και ειδικές κάρτες για τη Safety. Η κύρια διαφορά μεταξύ των Safety καρτών και των τυπικών είναι ότι οι Safety κάρτες έχουν σχεδιαστεί με δύο κανάλια εσωτερικά, δύο ενσωματωμένοι επεξεργαστές παρακολουθούν ο ένας τον άλλον και ελέγχουν αυτόματα τα κυκλώματα εισόδου και εξόδου. Σε περίπτωση σφάλματος, θέτουν τη Safety κάρτα σε ασφαλή κατάσταση.

Οι ψηφιακές Safety κάρτες εισόδων αποκτούν (ανιχνεύοντας) τις καταστάσεις σημάτων των αισθητήρων που σχετίζονται με την ασφάλεια (π.χ. Stop Emergency), εκτελούν δοκιμές βραχυκυκλώματος και διασταυρούμενου κυκλώματος, καθώς και αναλύσεις ασυμφωνίας και στέλνουν τα αντίστοιχα μηνύματα στη CPU.

Οι ψηφιακές Safety κάρτες εξόδων είναι κατάλληλες για εργασίες απενεργοποίησης με παρακολούθηση βραχυκυκλώματος μέχρι τον ενεργοποιητή.



Εικόνα 27. Standard και Safety λειτουργία σε ένα PLC

Το Standard και το Safety πρόγραμμα αναπτύσσονται στο ίδιο περιβάλλον προγραμματισμού και επειδή υφίστανται στην ίδια CPU μπορούν να επικοινωνούν μεταξύ τους μέσω μεταβλητών χωρίς όμως το ένα να επηρεάζει το άλλο σε περίπτωση προβλήματος.

Τηρώντας τους κανόνες του ανοιχτού προτύπου IEC 61784 για την επικοινωνία που σχετίζεται με την ασφάλεια υπάρχει η δυνατότητα της Standatrd επικοινωνίας με τη Safety μέσω της ίδιας σύνδεσης (καλωδιακή ή ασύρματη μέσω WLAN). Με τον τρόπο αυτό η υπάρχουσα υποδομή του δικτύου της τυπικής επικοινωνίας μπορεί επίσης να χρησιμοποιηθεί ταυτόχρονα για επικοινωνία που σχετίζεται με την ασφάλεια. Τα δεδομένα που σχετίζονται με την ασφάλεια και τα τυπικά δεδομένα μεταδίδονται μέσω του ίδιου διαύλου. Χρησιμοποιούνται τα υπάρχοντα τυπικά πρωτόκολλα διαύλου το λεγόμενο "Black Channel" στα οποία τα δεδομένα που σχετίζονται με την ασφάλεια μεταφέρονται ως πρόσθετα δεδομένα. Αυτό σημαίνει ότι η επικοινωνία που σχετίζεται με την ασφάλεια είναι ανεξάρτητη από το σύστημα διαύλου και τα στοιχεία του κατώτερου επιπέδου δικτύου.

Ένα μήνυμα που ανταλλάσσεται μεταξύ δύο Safety μονάδων μεταφέρεται στο ωφέλιμο φορτίο ενός τυπικού μηνύματος. Στην περίπτωση επικοινωνίας μιας αρθρωτής Safety συσκευής με πολλές Safety μονάδες το ωφέλιμο φορτίο αποτελείται από πολλά μηνύματα. Ξεκινά με τα Safety δεδομένα εισόδου/εξόδου λαμβάνοντας υπόψη το αναφερόμενο υποσύνολο δεδομένων. Η δομή δεδομένων μιας συγκεκριμένης Safety συσκευής ορίζεται σε σχετικό αρχείο από τον κάθε κατασκευαστή της Safety μονάδας (GSD File). Ο αυτοματισμός της παραγωγής και ο αυτοματισμός των διεργασιών θέτουν διαφορετικές απαιτήσεις σε ένα Safety σύστημα. Ο πρώτος λειτουργεί με σύντομα σήματα συνήθως "bits" τα οποία πρέπει να υποβληθούν σε επεξεργασία πολύ γρήγορα, ενώ ο δεύτερος λειτουργεί με μεγαλύτερες τιμές διεργασίας συνήθως "floating point" που μπορεί να είναι κάπως πιο αργές.

Επομένως η επικοινωνία προσφέρει δύο διαφορετικά μήκη για δομές δεδομένων. Το ένα περιορίζεται σε 12 byte με CRC 3byte ενώ το άλλο περιορίζεται σε 123 byte με CRC 4byte. Ένα μήνυμα τελειώνει με μια υπογραφή CRC που εξαρτάται από το μήκος των δεδομένων εισόδου/εξόδου. Ο αποστολέας και ο παραλήπτης έχουν ο καθένας τους δικούς τους μετρητές που συγχρονίζονται με τη βοήθεια του byte ελέγχου και του byte κατάστασης. Ο σωστός συγχρονισμός παρακολουθείται μέσω της τιμής του μετρητή στον υπολογισμό της υπογραφής

CRC. Χρησιμοποιώντας τον CRC ένας Παραλήπτης μπορεί να δει εάν έλαβε ή όχι τα μηνύματα πλήρως και με τη σωστή σειρά. Με την επιβεβαίωση ο CRC απαντά στον Αποστολέα για επαλήθευση.

Στην Safety τεχνολογία δεν είναι υποχρεωτική μόνο η μετάδοση των σωστών σημάτων της διεργασίας και τιμών της διεργασίας, αλλά και ενημέρωσης τους εντός ενός χρόνου ανοχής σφαλμάτων της διεργασίας. Αυτό σημαίνει ότι μια Safety συσκευή μπορεί ανεξάρτητα να ενεργοποιήσει τα προκαθορισμένα μέτρα ασφαλείας όταν ξεπεραστεί ο χρόνος, για παράδειγμα, σταματώντας μια κίνηση. Για αυτό, η συσκευή χρησιμοποιεί ένα χρονόμετρο Watchdog που επανεκκινείται όταν φθάνει ένα Safety μήνυμα με νέο CRC.

Το πρόγραμμα ασφαλείας (Safety program) για τον έλεγχο των λειτουργιών που σχετίζονται με την ασφάλεια του συστήματος αποτελείται από μια ενότητα που δημιουργείται από τον χρήστη και μια ενότητα που δημιουργείται από το λειτουργικό του Safety PLC και περιέχει μεταξύ άλλων μία διαφοροποιημένη λογική για την ενότητα χρήστη. Το τυπικό πρόγραμμα και το πρόγραμμα ασφάλειας δημιουργούνται στο ίδιο περιβάλλον προγραμματισμού. Τα μπλοκ λειτουργιών με πιστοποίηση TÜV για όλες τις κοινές λειτουργίες ασφαλείας απλοποιούν περαιτέρω τον προγραμματισμό.

Το τυπικό πρόγραμμα και το πρόγραμμα ασφαλείας εκτελούνται ανεξάρτητα το ένα από το άλλο από την CPU. Λόγω της ενσωμάτωσης των δύο προγραμμάτων σε μία CPU, η επικοινωνία μεταξύ των δύο προγραμμάτων μπορεί να υλοποιηθεί χρησιμοποιώντας καθολικές μεταβλητές (Global Tags). Οι αλλαγές στο τυπικό πρόγραμμα δεν έχουν καμία επίδραση στο πρόγραμμα ασφάλειας, έτσι ώστε η ακεραιότητά του να παραμένει ανέπαφη.

Οι βασικές διαφορές των Safety PLC από των Basic PLC είναι:

…σε Hardware:

Ένα Safety PLC είναι ένας ειδικά σχεδιασμένος ελεγκτής για χρήση ασφαλείας (υπάρχουν PLC όπου μπορούν να λειτουργούν και ως ελεγκτές ασφαλείας αλλά και ως ελεγκτές αυτοματισμού). Το Safety PLC διαθέτει λειτουργίες αυτοδιάγνωσης. Έχει υψηλή αξιοπιστία και καλύπτει τα απαιτούμενα πρότυπα ασφαλείας όπως SIL3 / IEC61508 και Category 4 / ISO 13849.

Το Safety PLC επικοινωνεί με το Automation PLC μέσω δικτύου ή σημάτων Input/Output, διαχειρίζεται το σύστημα έκτακτης ανάγκης και όταν τηρούνται οι προϋποθέσεις επιτρέπει στο Automation PLC να λειτουργεί. Στο Safety PLC συνδέονται όλα τα αισθητήρια ασφαλείας με διπλές καλωδιώσεις και επαφές για διπλούς ελέγχους. Τέλος και οι actuators ενεργοποιούνται με διπλές εντολές.

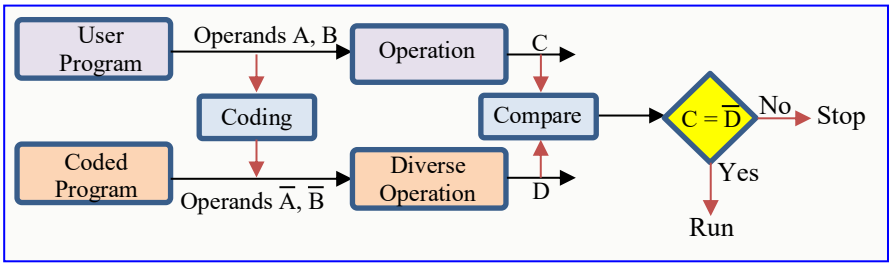
..σε Software

Τα πρότυπα ασφαλείας απαιτούν αυστηρούς περιορισμούς στις γλώσσες προγραμματισμού ενός Safety PLC. Για το λόγο αυτό οι περισσότεροι κατασκευαστές Safety PLC παρέχουν ειδικές γλώσσες προγραμματισμού όπου πιστοποιημένα καλύπτουν αυτούς τους περιορισμούς. Στο λειτουργικό ενός Safety PLC δε λειτουργούν μόνο ρουτίνες για τον έλεγχο των σημάτων αλλά τρέχουν και ρουτίνες για τη διασφάλιση της σωστής λειτουργίας της CPU.

Την λειτουργία ενός Safety PLC μπορεί εξ ορισμού να την τροποποιήσει μόνο ένας πιστοποιημένος μηχανικός. Η τροποποίηση μπορεί να γίνει μέσα από τις ρυθμίσεις επιπέδων ασφαλείας καταγράφοντας αυτόματα τις αλλαγές (signature).

Λειτουργία του Safety Program

Ο χρήστης προγραμματίζει τη λογική για τη Safety λειτουργία της μηχανής π.χ. όταν πιεσθεί το Stop Emeregency να σταματήσει η παραγωγή. Με την ολοκλήρωση της Safety λογικής αυτόματα παράγεται επιπλέον κώδικας με “Diversified” λογική, μέσα από πιστοποιημένους μηχανισμούς που έχει παράγει ο κατασκευαστής της CPU χωρίς τη δυνατότητα επέμβασης από τον χρήστη. Η Safety και Diversified λογικές εκτελούνται διαδοχικά συγκρίνονται τα αποτελέσματά τους και εάν είναι διαφορετικά τότε η CPU μεταβαίνει σε Safety κατάσταση. Στην Εικόνα 28 φαίνεται η λειτουργία του Safety προγράμματος.



Εικόνα 28. Safety λειτουργία

Οι CPU που σχετίζονται με την ασφάλεια λειτουργούν σύμφωνα με τις αρχές του πλεονασμού (Redundancy) και της διαφοροποίησης (Diversification), οι οποίες επιτρέπουν την υλοποίηση Safety συστημάτων με μόνο μία CPU και έναν επεξεργαστή. Με το πρόγραμμα ασφαλείας ο χρήστης προγραμματίζει τη λογική της ασφαλής λειτουργίας του συστήματος και αυτόματα το λειτουργικό δημιουργεί πρόσθετα μπλοκ που βασίζονται σε "διαφοροποιημένη" λογική σε σχέση με το πρόγραμμα του χρήστη και χρησιμοποιεί "διαφοροποιημένους" τελεστές και λειτουργίες.

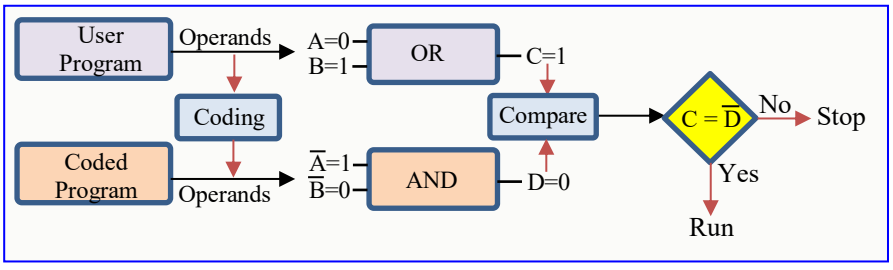
Τα δύο μέρη του προγράμματος ασφαλείας εκτελούνται διαδοχικά και τα αποτελέσματα συγκρίνονται. Εάν παρουσιαστεί σφάλμα, η CPU αντιδρά και θέτει το σύστημα σε ασφαλή κατάσταση. Το λειτουργικό δημιουργεί επίσης μπλοκ συστήματος που μπορούν να χρησιμοποιηθούν για παράδειγμα για τη διαχείριση της Safety επικοινωνίας.

Ο έλεγχος σφαλμάτων αφορά:

- Τα παλιά μηνύματα που δεν έχουν ενημερωθεί αποστέλλονται ξανά σε λάθος χρονική στιγμή.
- Ένα μήνυμα δεν λαμβάνεται ή δεν αναγνωρίζεται.
- Εισάγεται ένα μήνυμα που αναφέρεται σε μια άγνωστη πηγή.
- Η καθορισμένη ακολουθία (π.χ. CRC, χρονικές αναφορές) των μηνυμάτων μιας συγκεκριμένης πηγής είναι εσφαλμένη.

- Τα μηνύματα μπορεί να καταστραφούν λόγω σφαλμάτων σε έναν κόμβο διαύλου, δηλαδή σφαλμάτων στο μέσο μετάδοσης ή λόγω αμοιβαίας παρεμβολής μηνυμάτων.
- Τα μηνύματα μπορούν να καθυστερήσουν πέρα από το επιτρεπόμενο χρόνο άφιξης, π.χ. ως αποτέλεσμα σφαλμάτων στο μέσο μετάδοσης, υπερφορτωμένων καλωδίων σύνδεσης, αμοιβαίων παρεμβολών ή κόμβων διαύλου (συσκευές) που στέλνουν μηνύματα με τέτοιο τρόπο ώστε οι υπηρεσίες να καθυστερούν ή να μην αναγνωρίζονται.
- Ένα μήνυμα που προέρχεται από μια φαινομενικά έγκυρη πηγή εισάγεται επιπλέον. Έτσι, ένα μήνυμα που δεν σχετίζεται με την ασφάλεια μπορεί να ληφθεί από μια συσκευή που σχετίζεται με την ασφάλεια, η οποία στη συνέχεια το ταξινομεί ως σχετικό με την ασφάλεια.
- FIFO (First-In-First-Out) σφάλμα, δεν τηρείται η σωστή σειρά δεδομένων.

Στο ακόλουθο παράδειγμα περιγράφεται πώς μπορεί να επαληθευτεί η έξοδος μίας λογικής πύλης OR χρησιμοποιώντας μια αντίστροφη λειτουργία της πύλης AND. Συγκρίνοντας την έξοδο δύο ξεχωριστών υπολογιστικών αποτελεσμάτων αναβαθμίζεται το επίπεδο αξιοπιστίας των αποτελεσμάτων της CPU. Κατά συνέπεια, η CPU είναι σε θέση να ανιχνεύσει αν έχει δυσλειτουργήσει και μπορεί να απενεργοποιηθεί λαμβάνοντας υπόψη ότι είναι ασφαλέστερο να σταματήσει μια διαδικασία παρά να συνεχίσει να την εκτελεί με ελαττωματικό εξοπλισμό. Εάν υποτεθεί ότι στην περίπτωση που το πρόγραμμα του χρήστη σκοπεύει να εκτελέσει μια εντολή OR και ότι το A και το B έχουν τιμές 1001 και 1010 (σε δυαδική αναπαράσταση) αντίστοιχα. Η αναμενόμενη έξοδος C της λειτουργίας OR θα πρέπει να είναι 1011. Σε αυτό το σενάριο, η αντίστροφη πράξη που χρησιμοποιείται είναι μια πύλη AND. Το πρώτο βήμα είναι να υπολογισθεί το αντίστροφο των A και B ($\overline{A}$, $\overline{B}$), που είναι 0110 και 0101 αντίστοιχα. Το δεύτερο βήμα είναι να υπολογισθεί η έξοδο της πύλης AND D, η οποία είναι 0100. Τέλος, πρέπει να υπολογίσθεί το αντίστροφο της εξόδου ($\overline{D}$) που αποδεικνύεται ότι είναι 1011. Σε αυτήν την περίπτωση C = $\overline{D}$ άρα η CPU θα έπαιρνε την απόφαση να συνεχίσει να λειτουργεί. Σε κάθε άλλη περίπτωση θα έμπαινε σε λειτουργία διακοπής.



Εικόνα 29. Παράδειγμα Safety λειτουργίας

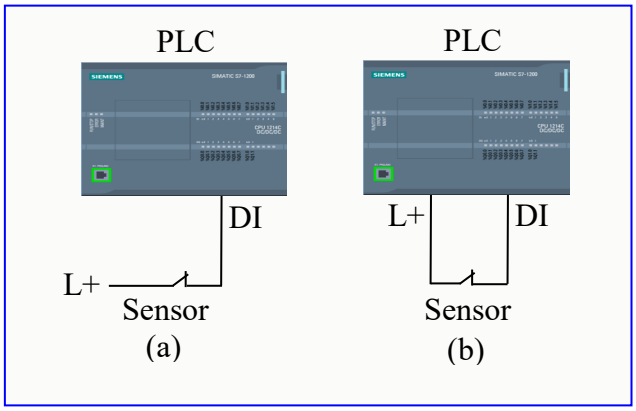
3.3 Καλωδίωση σημάτων Safety PLC

Παρακάτω απεικονίζονται και αναλύονται οι συνδεσμολογίες και οι μέθοδοι διαχείρισης του Hardware των σημάτων (Είσοδοι-Έξοδοι) ενός Safety PLC.

3.3.1 Καλωδίωση αισθητηρίων (sensors) στις κάρτες Εισόδων του Safety PLC

Η σύνδεση των αισθητηρίων με τις κάρτες εισόδων μπορεί να γίνει με ένα μονό κανάλι ή με ένα διπλό κανάλι. Οι Safety κάρτες Εισόδων έχουν δύο ανεξάρτητα γαλβανικά απομονωμένα κανάλια. [2] Παρακάτω δίνονται οι δυνατότητες καλωδίωσης των αισθητηρίων.

3.3.1.1 Καλωδίωση αισθητηρίου με ένα κανάλι (1oo1)



Εικόνα 30. Καλωδίωση αισθητηρίου με ένα κανάλι (1oo1)

Στην Εικόνα 30 υπάρχει καλωδίωση μίας επαφής (Normally Closed για safety λόγους) του αισθητηρίου σε μία κάρτα εισόδου ενός PLC. Η τροφοδοσία του αισθητηρίου μπορεί να γίνεται από εξωτερικό τροφοδοτικό (a) ή από το PLC (b). Η συγκεκριμένη καλωδίωση παρόλο που συνδέεται σε Fail Safe κάρτα εισόδου στο PLC μπορεί να παρέχει ασφάλεια Cat.2/ PLc/SIL1.

Για τον εντοπισμό μίας αλλαγής σε μία είσοδο πάντοτε έχουμε μία καθυστέρηση που τις περισσότερες φορές είναι ρυθμιζόμενη και αφορά τον χρόνο από την αλλαγή του σήματος εισόδου στη μονάδα μέχρι να εντοπιστεί και να κωδικοποιηθεί ως νέο σήμα. Η καθυστέρηση εισόδου χρησιμεύει για την καταστολή "debounce" σύντομων παλμών παρεμβολής. Για την καταστολή του θορύβου μπορεί να ορισθεί ένας χρόνος καθυστέρησης εισόδου για ένα κανάλι ή ένα ζεύγος καναλιών.

Οι παλμοί παρεμβολής των οποίων ο χρόνος είναι μικρότερος από τον καθορισμένο χρόνο καθυστέρησης εισόδου (σε ms) καταστέλλονται. Οι παλμοί κατασταλμένων παρεμβολών δεν είναι ορατοί στο PII. Μια υψηλή καθυστέρηση εισόδου καταστέλλει μεγαλύτερους παλμούς παρεμβολής αλλά έχει ως αποτέλεσμα μεγαλύτερο χρόνο αντίδρασης.

Οι τιμές για την καθυστέρηση εισόδου εξαρτώνται από τον χρόνο εκκίνησης του αισθητήρα μετά τη δοκιμή βραχυκυκλώματος και τον χρόνο για δοκιμή βραχυκυκλώματός της.

Κατά την λειτουργία ελέγχου της διαδικασίας των ψηφιακών σημάτων εισόδου υπάρχει ένας συνεχείς έλεγχος αξιολόγησης 1oo1, όπου ανιχνεύει και σηματοδοτεί ασυνήθιστα χαρακτηριστικά σήματος που σχετίζονται με τη διαδικασία, όπως η πολύ συχνή διακύμανση του σήματος εισόδου μεταξύ "0" και "1". Εάν προκύψουν χαρακτηριστικά σήματος όπως αυτά είναι σημάδι ότι οι αισθητήρες είναι ελαττωματικοί ή υπάρχουν αστάθειες που σχετίζονται με τη διαδικασία. Κάθε κανάλι εισόδου έχει ένα παραμετροποιημένο χρονικό παράθυρο ελέγχου. Το παράθυρο ελέγχου ξεκινά την πρώτη φορά που αλλάζει το σήμα εισόδου. Εάν το σήμα εισόδου αλλάζει μέσα στο παράθυρο ελέγχου τουλάχιστον τόσο συχνά όσο ο επιτρεπόμενος αριθμός αλλαγών σήματος ανιχνεύεται σφάλμα. Εάν δεν εντοπιστεί σφάλμα στο παράθυρο ελέγχου η επόμενη αλλαγή σήματος επανεκκινεί το χρονικό παράθυρο ελέγχου. Εάν εντοπιστεί σφάλμα σηματοδοτείται ένα διαγνωστικό. Εάν το σφάλμα δεν παρουσιαστεί για χρονικό διάστημα ίσο με το τριπλάσιο του χρόνου παραθύρου ελέγχου το διαγνωστικό επαναφέρεται στην κανονική λειτουργία. Η ρύθμιση του χρόνου του παραθύρου ελέγχου συνήθως είναι από 1 έως 100 δευτερόλεπτα.

3.3.1.2 Καλωδίωση αισθητηρίου με δύο κανάλια (1oo2)

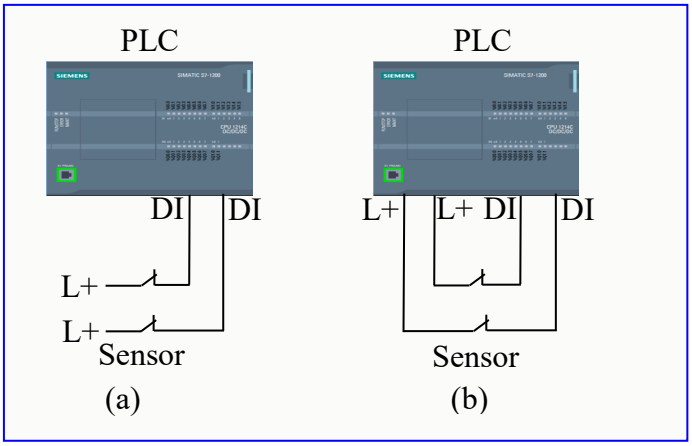
Για ισοδύναμη/μη ισοδύναμη αξιολόγηση 1oo2 τα δύο κανάλια εισόδου καταλαμβάνονται από:

- Ένα αισθητήρα δύο καναλιών.
- Δύο μονοκάναλους αισθητήρες.
- Έναν μη ισοδύναμο αισθητήρα.

Τα σήματα εισόδου συγκρίνονται εσωτερικά για ισοδυναμία ή μη ισοδυναμία. Για την αξιολόγηση 1oo2, δύο κανάλια συνδυάζονται σε ένα ζεύγος καναλιών.

Όταν χρησιμοποιείται ένας αισθητήρας δύο καναλιών ή δύο αισθητήρες μονού καναλιού που μετρούν την ίδια μεταβλητή της διαδικασίας τα κανάλια θα ανταποκρίνονται ελαφρώς με καθυστέρηση μεταξύ τους λόγω της ακρίβειας των διατάξεών τους. Για την ισοδυναμία/μη ισοδυναμία στην περίπτωση εισόδων λόγω αστοχίας χρησιμοποιείται η ανάλυση της ασυμφωνίας προκειμένου να εντοπισθεί η παρουσία σφαλμάτων από την διαφορά χρόνου των δύο σημάτων με την ίδια λειτουργικότητα. Η ανάλυση ασυμφωνίας ξεκινά εάν ανιχνευθεί διαφορετικός χρόνος για δύο συσχετισμένα σήματα εισόδου. Διενεργείται μια δοκιμή για να προσδιοριστεί εάν η διαφορά έχει εξαφανιστεί μετά την εκπνοή ενός καθορισμένου χρόνου - του λεγόμενου χρόνου ασυμφωνίας, εάν όχι τότε υπάρχει σφάλμα ασυμφωνίας. Ενώ ο εκχωρημένος χρόνος ασυμφωνίας εκτελείται εσωτερικά στη μονάδα, είτε η «τελευταία έγκυρη τιμή» ή το «0» παρέχεται στο πρόγραμμα ασφαλείας στη F-CPU από τα εμπλεκόμενα κανάλια εισόδου, ανάλογα με τον τρόπο παραμετροποίησης της συμπεριφοράς ασυμφωνίας.

Έλεγχος ισοδυναμίας: Εάν, μετά τη λήξη του εκχωρημένου χρόνου ασυμφωνίας, τα σήματα εισόδου δεν συμφωνούν, για παράδειγμα λόγω διακοπής καλωδίου σε γραμμή αισθητήρα, ανιχνεύεται σφάλμα ασυμφωνίας και δημιουργείται το διαγνωστικό μήνυμα "Σφάλμα ασυμφωνίας" με πληροφορίες των ελαττωματικών καναλιών.



Εικόνα 31. Καλωδίωση αισθητηρίου με δύο κανάλια (1oo2)

Στην Εικόνα 31 υπάρχει καλωδίωση δύο επαφών (Normally Closed για safety λόγους) ενός αισθητηρίου σε δύο εισόδους του PLC ή από δύο ανεξάρτητα αισθητήρια καλωδίωση από μία επαφή (Normally Closed για safety λόγους) σε δύο εισόδους στο PLC. Οι Fail Safe κάρτες εισόδων του PLC ελέγχουν τις δύο εισόδους και τις μεταφέρουν στη CPU ως μία είσοδο εάν είναι ενεργοποιημένες ή όχι ή εάν υπάρχει κάποια δυσλειτουργία (π.χ. έχουν σήμα στην μία είσοδο αλλά δεν έχουν στην άλλη). Η τροφοδοσία του αισθητηρίου μπορεί να γίνει από εξωτερικό τροφοδοτικό (a) έχοντας έτσι ασφάλεια μέχρι Cat. 3/PLd/SIL2 ή από το PLC (b) έχοντας έτσι ασφάλεια μέχρι Cat. 4/PLe/SIL3.

Οι παραπάνω συνδεσμολογίες αναφέρονται σε κάρτες Εισόδων Fail Safe, όπου έχουν ενσωματωμένες έξτρα λειτουργίες, όπως έλεγχο κομμένου καλωδίου, μη συγχρονισμό των εισόδων, κλπ. Γι' αυτό το λόγο μπορούμε να έχουμε πιστοποιημένα από τους κατασκευαστές μέχρι και SIL3.

3.3.1.3 Έλεγχος Βραχυκλώματος (Short-circuit test)

Η δοκιμή βραχυκυκλώματος είναι χρήσιμη μόνο όταν γίνεται χρήση απλών διακοπτών που δεν έχουν δικό τους τροφοδοτικό. Για διακόπτες με τροφοδοτικό δεν είναι δυνατή η δοκιμή βραχυκυκλώματος. Η ανίχνευση βραχυκυκλώματος απενεργοποιεί προσωρινά την τροφοδοσία του αισθητήρα. Εάν εντοπιστεί βραχυκύκλωμα, η Safety μονάδα ενεργοποιεί μια διαγνωστική διακοπή και η είσοδος απενεργοποιείται.

Τα βραχυκυκλώματα που μπορούν να εντοπισθούν είναι:

- Βραχυκύκλωμα εισόδου στο L+.
- Βραχυκύκλωμα της εισόδου άλλου καναλιού εάν αυτό έχει σήμα "1".
- Βραχυκύκλωμα εισόδου με τροφοδοσία αισθητήρα άλλου καναλιού.
- Βραχυκύκλωμα τροφοδοσίας αισθητήρα με τροφοδοσία αισθητήρα άλλου καναλιού.

Η τιμή της εισόδου που ελέγχεται για βραχυκύκλωμα παγώνει κατά τη διάρκεια του χρόνου εκτέλεσης της δοκιμής βραχυκυκλώματος (χρόνος δοκιμής βραχυκυκλώματος + χρόνος εκκίνησης του αισθητήρα μετά τη δοκιμή βραχυκυκλώματος). Η δοκιμή βραχυκυκλώματος προφανώς επηρεάζει τον χρόνο απόκρισης του αντίστοιχου καναλιού ή ζεύγους καναλιών.

Όταν ενεργοποιηθεί η δοκιμή βραχυκυκλώματος, η αντίστοιχη τροφοδοσία του αισθητήρα απενεργοποιείται για προκαθορισμένο χρόνο. Εάν η μονάδα δεν ανιχνεύσει σήμα "0" στην είσοδο εντός του καθορισμένου χρόνου, δημιουργείται ένα διαγνωστικό μήνυμα.

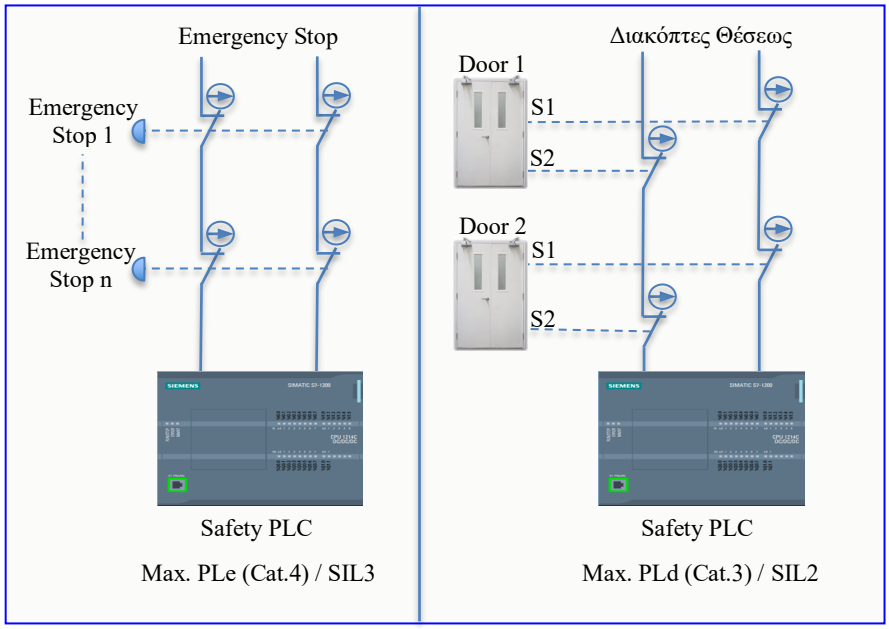
Εκτός από το χρόνο απενεργοποίησης για την δοκιμή βραχυκυκλώματος, πρέπει επίσης να καθοριστεί και ο χρόνος εκκίνησης για την υλοποίηση της δοκιμής βραχυκυκλώματος. Μέσω αυτής της παραμέτρου κοινοποιείται στη μονάδα ο χρόνος που χρειάζεται ο χρησιμοποιούμενος αισθητήρας για την εκκίνηση μετά την ενεργοποίηση της τροφοδοσίας του.

Κατά την παραμετροποίηση των καρτών πρέπει να δίνεται προσοχή στα παρακάτω:

- Εάν το κανάλι είναι παθητικοποιημένο (passivated), μπορεί να οφείλεται σε πολύ υψηλή χωρητικότητα μεταξύ της τροφοδοσίας και της εισόδου του αισθητήρα. Δηλαδή από τη χωρητικότητα ανά μονάδα μήκους του καλωδίου και τη χωρητικότητα του χρησιμοποιούμενου αισθητήρα.
- Οι διαθέσιμες τιμές για την καθυστέρηση της εισόδου εξαρτώνται από τον χρόνο εκκίνησης του αισθητήρα μετά τη δοκιμή βραχυκυκλώματος και τον χρόνο για δοκιμή βραχυκυκλώματος της παραμετροποιημένης τροφοδοσίας του αισθητήρα.
- Ο χρόνος επανεκκίνησης πρέπει να είναι μεγαλύτερος από τον χρόνο σβησίματος του χρησιμοποιούμενου αισθητήρα.
- Επειδή ο χρόνος επανεκκίνησης επηρεάζει τον χρόνο απόκρισης της μονάδας, συνιστάται να ρυθμίζεται όσο το δυνατόν μικρότερος, αλλά αρκετά μεγάλος ώστε ο αισθητήρας να ρυθμιστεί αξιόπιστα.
- Οι τιμές για την καθυστέρηση της εισόδου εξαρτώνται από τον χρόνο εκκίνησης του αισθητήρα μετά τη δοκιμή βραχυκυκλώματος και τον χρόνο για τη δοκιμή του βραχυκυκλώματος.

Σειριακή Σύνδεση αισθητηρίων

Στην παρακάτω Εικόνα 32 φαίνονται δύο βασικές συνδεσμολογίες αισθητηρίων σε σειρά:

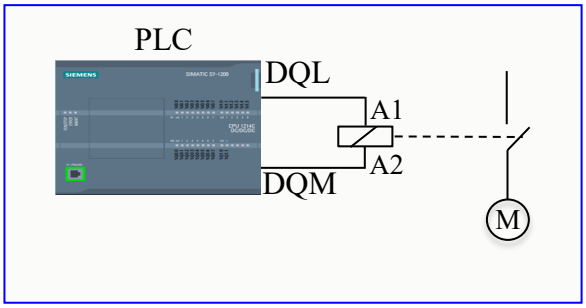


Εικόνα 32. Σειριακή σύνδεση αισθητηρίων

3.3.2 Καλωδίωση ενεργοποιητές (actuators) στις κάρτες Εξόδων του Safety PLC

Παρακάτω δίνονται οι δυνατότητες καλωδίωσης των ενεργοποιητών με ένα Relay ανά έξοδο και με δύο Relay ανά έξοδο.

Καλωδίωση ενός Relay ανά έξοδο

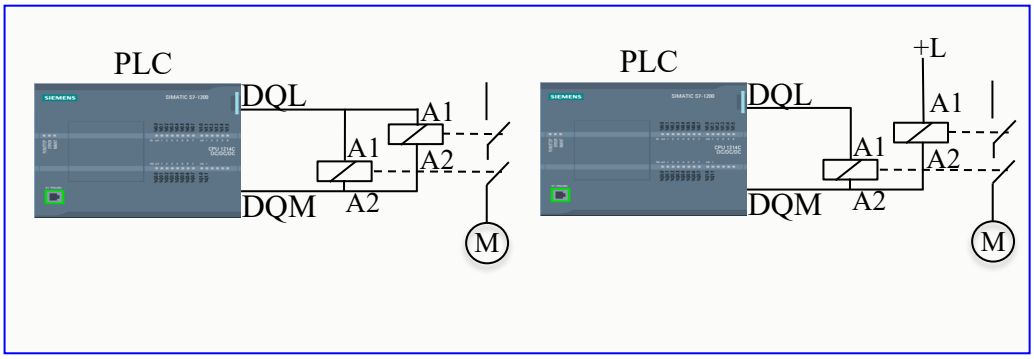


Εικόνα 33. Καλωδίωση ενεργοποιητή με ένα Relay

Στην Εικόνα 33 έχουμε την καλωδίωση ενός Relay με έξοδο από Fail Safe κάρτα. Στις Fail Safe κάρτες εξόδων η κάθε έξοδος δε μας δίνει μόνο π.χ. 24VDC για την ενεργοποίηση του Relay αλλά και 0VDC. Δηλαδή όταν δεν υπάρχει εντολή εξόδου από το PLC στο Relay το κύκλωμα και στο A1 και στο A2 είναι ανοικτό. Οι Fail Safe κάρτες εξόδων έχουν επιπλέον

διαγνωστικές ρουτίνες για πρόσθετους ελέγχους π.χ. κομμένο καλώδιο, έλεγχο ικανότητας εντολοδότησης όταν αυτό απαιτηθεί κλπ.

Καλωδίωση δύο Relay ανά έξοδο



Εικόνα 34. Καλωδίωση ενεργοποιητή με δύο Relays

Στην Εικόνα 34 έχουμε την καλωδίωση δύο Relays με μία έξοδο από Fail Safe κάρτα. Με αυτή τη συνδεσμολογία μπορούμε να έχουμε ασφάλεια μέχρι Cat.4/PLe/SIL3. Ένα από τα δύο Relays θα μπορούσε να έχει μόνιμα τάση στο A1 και να οπλίζει όταν μέσω της Q του PLC κλείσει κύκλωμα από το A2. Συνήθως συστήνεται να είναι καλωδιωμένα στη κάρτα του PLC και τα δύο Relays. Σε αυτή τη λειτουργία μέσα από το πρόγραμμα του χρήστη εντολοδοτείται μία ψηφιακή έξοδος, η πληροφορία αυτή μεταφέρεται στη κάρτα εξόδου και στη συνέχεια οπλίζουν δύο Relays. Κάνοντας χρήση δύο Relays εξασφαλίζεται πως το στοιχείο που εντολοδοτείται (π.χ. ένας κινητήρας) δε θα μπει σε λειτουργία εάν για κάποιο λόγο οπλίσει μόνο ένα Relay ή δεν απενεργοποιηθεί ένα Relay.

Για την αξιόπιστη λειτουργία των εξόδων πραγματοποιούνται δοκιμές ελέγχου αυτών. Οι δοκιμές επαναλαμβάνονται συνήθως κάθε 1.000sec όταν δεν θέλουμε να έχουμε γρήγορη φθορά των ενεργοποιητών, ενώ κάθε 100sec για γρήγορο εντοπισμό σφάλματος.

Ο χρόνος επανάληψης είναι ο μέγιστος χρόνος μετά την απενεργοποίηση της εξόδου ώστε να μπορεί να ανιχνευθεί ένα σήμα ανάδρασης προτού δηλωθεί ως σφάλμα βραχυκυκλώματος. Ο χρόνος επανάληψης πρέπει να ρυθμιστεί αρκετά μεγάλος, ειδικά όταν γίνεται εναλλαγή χωρητικών φορτίων, ώστε να επιτρέπεται η εκ φόρτιση της χωρητικότητας μεταγωγής εντός του χρόνου επανάληψης.

Για τον έλεγχο της καλωδίωσης του ενεργοποιητή, αλλάζουν σε 0 τα σήματα στην έξοδο ενώ η έξοδος είναι ενεργή. Ένας αρκετά αργός ενεργοποιητής δεν ανταποκρίνεται στην προσωρινή απενεργοποίηση της εξόδου και παραμένει ενεργοποιημένος (Light Test).

Η υπερφόρτωση και η διακοπή του καλωδίου ανιχνεύονται από ένα σήμα 0 στην έξοδο. Κατά τη διάρκεια της δοκιμής ένα δοκιμαστικό σήμα μεταβαίνει στο κανάλι εξόδου ενώ το κανάλι εξόδου είναι ανενεργό (σήμα εξόδου "0"). Στη συνέχεια, το κανάλι εξόδου

ενεργοποιείται για λίγο και διαβάζεται ξανά. Ένας αρκετά αργός ενεργοποιητής δεν ανταποκρίνεται σε αυτό και παραμένει απενεργοποιημένος (Dark Test).

Όπως και για τις τυπικές μονάδες, οι διευθύνσεις των μονάδων εισόδου και εξόδου που είναι ασφαλείς για σφάλματα μπορούν να οριστούν ελεύθερα από τον χρήστη. Εκτός από τις διευθύνσεις εισόδου και εξόδου που ελέγχει ο χρήστης, οι μονάδες εισόδου ή εξόδου ασφαλούς αστοχίας καταλαμβάνουν επιπλέον bytes για τις εισόδους και τις εξόδους για την επεξεργασία της επικοινωνίας που σχετίζεται με την ασφάλεια (αυτά τα επιπλέον bytes δεν μπορεί να τα χρησιμοποιήσει ο χρήστης) καταλαμβάνονται από τις μονάδες ασφαλείας εκχωρούνται μεταξύ άλλων για επικοινωνία που σχετίζεται με την ασφάλεια μεταξύ των μονάδων ασφαλείας και της F-CPU σύμφωνα με το πρωτόκολλο επικοινωνίας.

ΚΕΦΑΛΑΙΟ 4

Πείραμα ελέγχου απόκρισης διπλών επαφών σε ένα Basic PLC

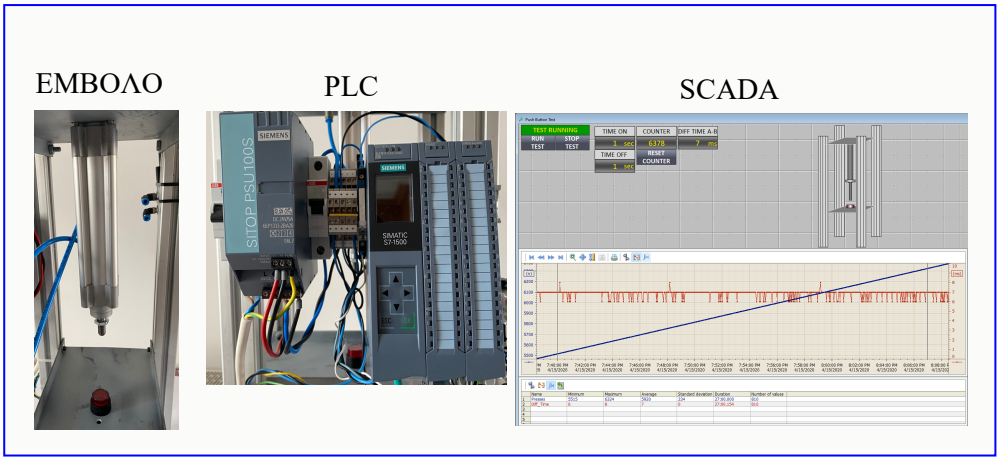
Στο παρακάτω πείραμα γίνεται έλεγχος της απόκρισης διπλών επαφών ενός στοιχείου (π.χ. μπουτόν). Μέσα από τα αποτελέσματα του πειράματος θα μπορέσουν να εξαχθούν αποτελέσματα για το εάν με συμβατικές κάρτες σε ένα PLC είναι δυνατόν να υπάρξει λειτουργία SIL 2 και όχι SIL 1.

Αυτό που πρέπει να ερευνηθεί με το παρακάτω πείραμα είναι η απόκριση των διπλών επαφών ενός στοιχείου (όπως ενός μπουτόν) τόσο στην αρχή της λειτουργίας του όσο και όταν αυτό έχει χρησιμοποιηθεί μερικές χιλιάδες φορές και να εξαχθούν έτσι ασφαλή συμπεράσματα.

Εάν είναι γνωστή την αναμενόμενη απόκριση ενός στοιχείου ελέγχου θα μπορεί μέσα από λειτουργίες που υποστηρίζουν τα Basic PLC και όχι τα Safety να ελεγχθεί ασφαλέστερα και να παράγει Safety λειτουργία. Γίνεται κατανοητό πως εάν αυτό είναι εφικτό να υλοποιηθεί (με τις όποιες ενδεχόμενες παραδοχές απαιτηθούν) θα σήμαινε πως θα μπορούσε να αυξηθεί η αξιοπιστία των υπαρχόντων συστημάτων αυτοματισμού χωρίς επιπρόσθετο δαπανηρό εξοπλισμό αλλά και εξειδικευμένες εργασίες εγκατάστασης και προγραμματισμού. Σε αυτή τη περίπτωση θα υλοποιείται Safety λειτουργία του στοιχείου (π.χ. μπουτόν) και όχι Safety λειτουργία της CPU του PLC.

4.1 Overview του πειράματος

Για την υλοποίηση του πειράματος χρησιμοποιήθηκε βιομηχανικός εξοπλισμός που χρησιμοποιείται για τον έλεγχο συστημάτων αυτοματισμού και συνοπτικά φαίνεται στην Εικόνα 35.



Εικόνα 35. Εξοπλισμός πειράματος

Έμβολο - Μπουτόν

Για την εξομοίωση του πατήματος του μπουτόν εγκαταστάθηκε ένα έμβολο αέρα. Όταν το έμβολο παίρνει εντολή από το PLC θα κατεβαίνει και πιέζει το μπουτόν. Η εντολή του PLC (δηλαδή μία ψηφιακή έξοδος) δίνει 24VDC σε μία βαλβίδα και αυτή διοχετεύει αέρα στο έμβολο με αποτέλεσμα αυτό να κατεβαίνει προς τα κάτω. Απενεργοποιώντας την εντολή η βαλβίδα αλλάζει την παροχή του αέρα στο έμβολο και έτσι το έμβολο ανεβαίνει προς τα επάνω. Με αυτή τη διαδικασία ελέγχεται το έμβολο και κατά συνέπεια και το πάτημα του μπουτόν. Ρυθμίζοντας την πίεση του αέρα που διοχετεύεται στο έμβολο δίνεται η δυνατότητα να πιέζεται το μπουτόν με χαμηλή ή γρήγορη ταχύτητα, κάτι που δίνει επιπλέον πληροφορίες για την απόκριση των επαφών του μπουτόν. Στο μπουτόν υπάρχει μία λυχνία 24VDC και δύο Normally Closed επαφές. Όταν το μπουτόν πιέζεται η λυχνία ανάβει και οι επαφές ανοίγουν. Για το πείραμα χρησιμοποιήθηκαν μπουτόν από δύο διαφορετικούς κατασκευαστές. Αυτό έγινε με σκοπό να διαπιστωθεί εάν τα δύο μπουτόν θα είχαν την ίδια συμπεριφορά και όχι ποιας εταιρείας είναι καλύτερο. Επίσης χρησιμοποιήθηκε μπουτόν που έχουν αυτόματη επαναφορά και όχι αυτά που κουμπώνουν και χρειάζονται τράβηγμα ή περιστροφή για να ξεκουμπώσουν. Έτσι με την αυτόματη επαναφορά του μπουτόν υπάρχει η δυνατότητα να ξανά πατηθεί άμεσα, με τον τρόπο αυτό επιτεύχθηκαν πάρα πολλά πατήματα σε ελάχιστο χρόνο.

PLC

Για την εντολοδότηση του εμβόλου αλλά και για το διάβασμα των επαφών του μπουτόν χρησιμοποιήθηκε ένα PLC της SIEMENS της σειράς S7-1500.

Συγκεκριμένα χρησιμοποιήθηκε η CPU 511C. Αυτή είναι από τις μικρότερες σε δυνατότητες CPU της μεσαίας σειράς που διαθέτει η εταιρεία SIEMENS στα PLC. Έχει ενσωματωμένα σήματα εισόδων και εξόδων. Έτσι χρησιμοποιήθηκε μία ψηφιακή έξοδο για την εντολοδότηση του εμβόλου και δύο ψηφιακές εισόδους για το διάβασμα των επαφών του μπουτόν.

Η συγκεκριμένη CPU (όπως πλέον και οι περισσότερες CPU) διαθέτει δυνατότητα διαβάσματος των Εισόδων σε χρόνους μικρότερους των 0,05ms αλλά και ρουτίνες Interrupt για πιο άμεσο διάβασμα και επεξεργασία των Εισόδων.

Εικόνα 36. PLC

SCADA

Για SCADA χρησιμοποιήθηκε το WinCC V7.5 της SIEMENS. Το WinCC V7.5 διαθέτει το interface της επικοινωνίας με το PLC (στο πείραμα χρησιμοποιήθηκε το Profinet), δυνατότητες Visualization, Control αλλά και Tag logging που απαιτούνταν για διεξαγωγή του πειράματος.

4.2 PLC - Piston Control

Για τον έλεγχο του αυτοματισμού του πειράματος μέσου του προγράμματος TIA V16 προγραμματίστηκε η ρουτίνα FB1 (Function Block) σε γλώσσα SCL για τον έλεγχο του Εμβόλου. Με την ρουτίνα FB1 ελέγχεται μέσω του SCADA η λειτουργία του εμβόλου δηλαδή πότε και για πόσο θα ενεργοποιείται για να πιέζει το μπουτόν.

```
REGION Pulse Generator
    #TIME_OFF := "CLOCK_DATA".TIME_OFF * 1000;
    #TIME_ON := "CLOCK_DATA".TIME_ON * 1000;
    #IEC_Timer_0_Instance(IN := NOT "Tag_1",
                          PT := #TIME_OFF,
                          Q => "PULSE_ON_OFF");
    #IEC_Timer_0_Instance_1(IN := "PULSE_ON_OFF",
                            PT := #TIME_ON,
                            Q => "Tag_1");
END_REGION

REGION Piston Control
    "OUT_EMBOLO" := "ENABLE" & "PULSE_ON_OFF";
END_REGION

REGION Piston Position
    #IEC_Timer_0_Instance_3(IN:="OUT_EMBOLO",
                            PT:=T#6S,
                            ET=>#TIME_OUTPUT);
    "PISTON_POSITION" := #TIME_OUTPUT / 14;
    #IEC_Timer_0_Instance_4(IN:=NOT "OUT_EMBOLO",
                            PT:=T#6S,
                            ET=>#TIME_OUTPUT_1);
    IF ("OUT_EMBOLO" = 0)  THEN
        "PISTON_POSITION" := (1000-#TIME_OUTPUT_1)/14;
    END_IF;
    IF ("CONTACT_A"=0)OR("CONTACT_B"=0) THEN
    "PISTON_POSITION" := 80;
END_IF;
IF ("PISTON_POSITION" < 0) THEN
    "PISTON_POSITION" :=0;
END_IF;

END_REGION

REGION Lamp ON-OFF
    IF ("CONTACT_A" = 0) OR ("CONTACT_B" = 0) THEN
        "LAMP_ON" := 1;
    ELSE
        "LAMP_ON" := 0;
    END_IF;
END_REGION
```

Εικόνα 37. FB1

Pulse Generator: Με τη χρήση δύο IEC TON Timers υλοποιήθηκε μία παλμογεννήτρια όπου γίνεται ON και OFF με ρυθιζόμενη η διάρκειά της από το SCADA.

Piston Control: Όταν δοθεί 'ENABLE' από το SCADA και ON από την παλμογεννήτρια δίνεται εντολή στο έμβολο να πάει προς τα κάτω. Αυτό έχει σαν συνέπεια όταν υπάρξει 'ENABLE' από το SCADA το έμβολο να υλοποιεί μία παλινδρομική κίνηση κάθε π.χ τρία δευτερόλεπτα.

Piston Position: Ανάλογα με το πόσο χρόνο είναι ενεργοποιημένη η εντολή για το έμβολο, παράγεται η ανάλογη τιμή στην μεταβλητή 'PISTON POSITION' για να φαίνεται και στο SCADA η θέση του εμβόλου.

Lamp ON-OFF: Όταν απενεργοποιηθεί μία από τις εισόδους των επαφών του μπουτόν ενεργοποιείται η μεταβλητή 'LAMP_ON' για να απεικονίζεται και στο SCADA πως έχει πατηθεί το μπουτόν.

4.3 PLC - Inputs Control

Για τον έλεγχο των εισόδων στο PLC υλοποιήθηκαν οι παρακάτω διαδικασίες:

Απενεργοποίηση φίλτρο Delay

Για την αποφυγή παρεμβολών από την εγκατάσταση σε ένα σύστημα αυτοματισμού οι είσοδοι στα PLC έχουν τη δυνατότητα εισαγωγής μίας καθυστέρησης ενεργοποίησης σε ένα κανάλι ή ζεύγος καναλιών.

Οι παλμοί παρεμβολών των οποίων ο παλμός είναι μικρότερος από την καθορισμένη καθυστέρηση εισόδου (σε ms) αγνοούνται και έτσι δεν είναι ορατοί στο PII του PLC.

Για τις ανάγκες του πειράματος απενεργοποιήθηκε πλήρως αυτό το delay έτσι ώστε να υπάρχει όσο ποιο άμεση ανταπόκριση της εισόδου στο PII του PLC γίνεται. Αυτό δε δημιουργεί κάποιο πρόβλημα από τυχόν παρεμβολές γιατί το πείραμα υλοποιήθηκε στο εργαστήριο όπου δεν υπάρχει ηλεκτρομαγνητικός θόρυβος όπως σε ένα βιομηχανικό περιβάλλον.

Εικόνα 38. Απενεργοποίηση φίλτρο Delay

Απενεργοποιώντας το Input Delay έχουμε τη δυνατότητα να διαβάσουμε την απόκριση μίας εισόδου σε χρόνο μικρότερο του 1ms.

Ενεργοποίηση διαδικασίας Interrupt

Επειδή χρειάζεται να αναγνωσθεί η απόκριση μίας εισόδου μέσα στη CPU του PLC όσο πιο άμεσα γίνεται, ενεργοποιήθηκε η διαδικασία Hardware Interrupt. Με τη διαδικασία Hardware Interrupt η είσοδος δε διαβάζεται σε μια ρουτίνα του PLC, όπου αυτή καλείται μέσα

από την Main ρουτίνα του κύκλου της, γιατί αυτό θα σήμαινε επιπλέον καθυστέρηση και σε μη σταθερά χρονικά διαστήματα αλλά άμεσα όταν αλλάξει η κατάσταση της εισόδου. [3]

Εικόνα 39. Ενεργοποίηση Interrupt διαδικασία

Στην παραπάνω Εικόνα 39 φαίνεται η ενεργοποίηση του Hardware Interrupt στο Falling Edge, δηλαδή μετάβαση στη ρουτίνα του Interrupt τη στιγμή που έχουμε μετάβαση της Εισόδου από 1 σε 0. Οι επαφές που χρησιμοποιήθηκαν στο μπουτόν είναι Normally Closed. Για κάθε Είσοδο εκτελείται διαφορετική ρουτίνα Interrupt. Σε κάθε Interrupt ρουτίνα τρέχει ο παρακάτω κώδικας:

```
1
2 REGION Read CPU Clock
3     "CLOCK_DATA".CLOCK_TIME_OB_A := #DATE_TIME;
4 END_REGION
5
6 REGION Time A
7     "CLOCK_DATA".CLOCK_TIME_A := #DATE_TIME;
8 END_REGION
9
```

Read CPU Clock: Διαβάζουμε το Real Time Clock της CPU.

Time A: Γράφουμε το Real Time Clock της CPU στην μεταβλητή: "CLOCK_DATA". CLOCK_TIME_A. Αυτή η εντολή εκτελείται όταν ενεργοποιείται η ρουτίνα Interrupt, δηλαδή όταν απενεργοποιείται η Είσοδος. Με αυτή τη μέθοδο αποθηκεύεται το Real Time Clock της CPU στην παραπάνω μεταβλητή.

4.4 PLC - Difference Record

Για τον υπολογισμό και καταγραφή της διαφοράς χρόνου απενεργοποίησης των δύο Εισόδων υλοποιήθηκε η παρακάτω διαδικασία στη ρουτίνα FB2 (Function Block 2):

```
1
2 REGION Calculate Difference
3     "R_TRIG_DB"(CLK:=("CONTACT_A"=0)&("CONTACT_B"=0),
4                 Q=>"Tag_6");
5         IF "Tag_6" THEN
6             "CLOCK_DATA".CLOCK_TIME_DIFF := T_DIFF(IN1 := "CLOCK_DATA".CLOCK_TIME_B, IN2 := "CLOCK_DATA".CLOCK_TIME_A);
7         END_IF;
8
9     END_REGION
```

Εικόνα 40. FB2

Calculate Difference: Όταν και στις δύο Εισόδους υπάρχει κατάσταση 0 η διαφορά χρόνου απόκρισης μεταξύ των δύο Εισόδων υπολογίζεται (σε ms). Η ακρίβεια του υπολογισμού, με το συγκεκριμένο Configuration του πειράματος μπορεί να είναι ανά 1ms. Αυτή η ακρίβεια όπως θα αναλυθεί και παρακάτω είναι υπεραρκετή για τις ανάγκες του πειράματος.

4.5 PLC - Push Button Count

Η απόκριση των μπουτόν δεν είναι ίδια τόσο με το πέρασμα του χρόνου αλλά και μετά από τις πολλές χρήσεις του, έτσι για ποιο σωστά αποτελέσματα πρέπει να είναι γνωστή οι χρήσει του. Για να ελέγξουμε εάν η απόκριση των επαφών του μπουτόν είναι ίδια ή διαφορετική μετά από κάποιες εκατοντάδες πατήματα, υλοποιήθηκε η παρακάτω ρουτίνα FB3 (Function Block 3). Με την ρουτίνα FB3 γίνεται η καταμέτρηση των πατημάτων του μπουτόν.

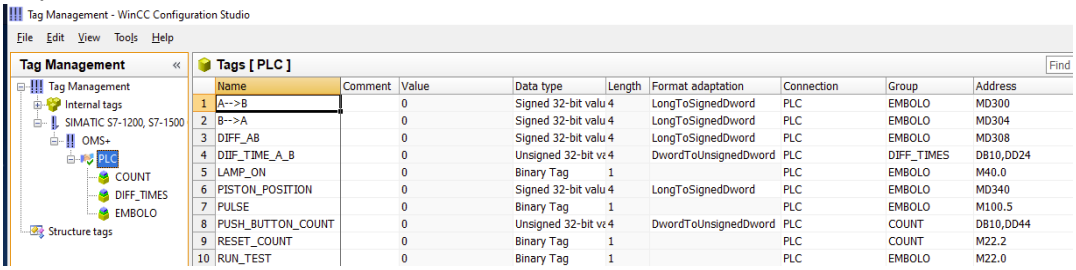
```
1  REGION Push Button Count
2      "IEC_Counter_0_DB".CTU(CU:=("CONTACT_A" = 0) OR ("CONTACT_B" = 0),
3                             R:="RESET_COUNT",
4                             PV:=1000000,
5                             Q=>#COUNT_TEMP,
6                             CV=>"CLOCK_DATA".COUNTER_PUSH_BUTTON);
7      IF ("RESET_COUNT") THEN
8          "RESET_COUNT":= 0;
9      END_IF;
10 END_REGION
```

Εικόνα 41. FB3

Push Button Count: Όταν υπάρξει 0 σε μία ή και στις δύο Εισόδους ανεβαίνει η τιμή του μετρητή μας. Εάν υπάρξει 1 στη μεταβλητή "RESET_COUNT" μηδενίζεται ο μετρητή - αυτή η μεταβλητή ενεργοποιείται από το SCADA όταν για παράδειγμα τοποθετηθεί ένα νέο μπουτόν και ξεκινά ξανά από την αρχή το πείραμα.

4.6 SCADA- Configuration

Για τον έλεγχο του πειράματος μέσα από το WinCC υλοποιήθηκαν (συνοπτικά) τα παρακάτω:

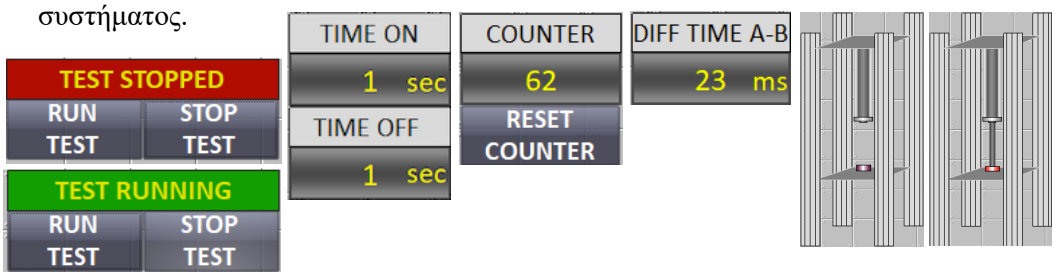


	Name	Comment	Value	Data type	Length	Format adaptation	Connection	Group	Address
1	A-->B		0	Signed 32-bit valu	4	LongToSignedDword	PLC	EMBOLO	MD300
2	B-->A		0	Signed 32-bit valu	4	LongToSignedDword	PLC	EMBOLO	MD304
3	DIFF_AB		0	Signed 32-bit valu	4	LongToSignedDword	PLC	EMBOLO	MD308
4	DIF_TIME_A_B		0	Unsigned 32-bit va	4	DwordToUnsignedDword	PLC	DIFF_TIMES	DB10,DD24
5	LAMP_ON		0	Binary Tag	1		PLC	EMBOLO	M40.0
6	PISTON_POSITION		0	Signed 32-bit valu	4	LongToSignedDword	PLC	EMBOLO	MD340
7	PULSE		0	Binary Tag	1		PLC	EMBOLO	M100.5
8	PUSH_BUTTON_COUNT		0	Unsigned 32-bit va	4	DwordToUnsignedDword	PLC	COUNT	DB10,DD44
9	RESET_COUNT		0	Binary Tag	1		PLC	COUNT	M22.2
10	RUN_TEST		0	Binary Tag	1		PLC	EMBOLO	M22.0

Εικόνα 42. Μεταβλητές SCADA

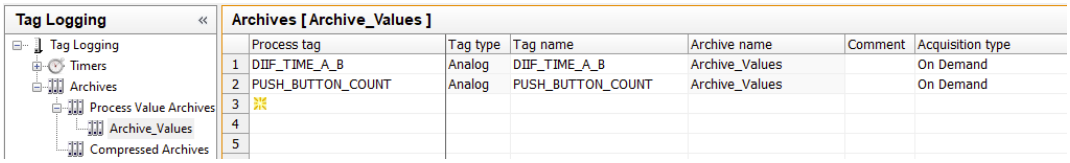
- Δημιουργία επικοινωνίας WinCC-PLC και ορισμός των απαραίτητων μεταβλητών (Tag).

- Ανάπτυξη του γραφικού περιβάλλοντος στοιχεία για την απεικόνιση και το χειρισμό του συστήματος.



Εικόνα 43. Στοιχεία απεικόνισης και χειρισμού του SCADA

- Δημιουργία καταγραφών σε SQL, ανάπτυξη στο γραφικό περιβάλλον στοιχεία για την απεικόνιση και το χειρισμό του συστήματος.



Εικόνα 44. Δημιουργία βάσης δεδομένων στο SCADA

Η καταγραφή της διαφοράς του χρόνου των δύο Εισόδων δεν υλοποιείται σε κάποια χρονική διάρκεια αλλά τη στιγμή που χάνονται και οι δύο Είσοδοι από το PLC.

4.7 Πείραμα απόκρισης Εισόδων

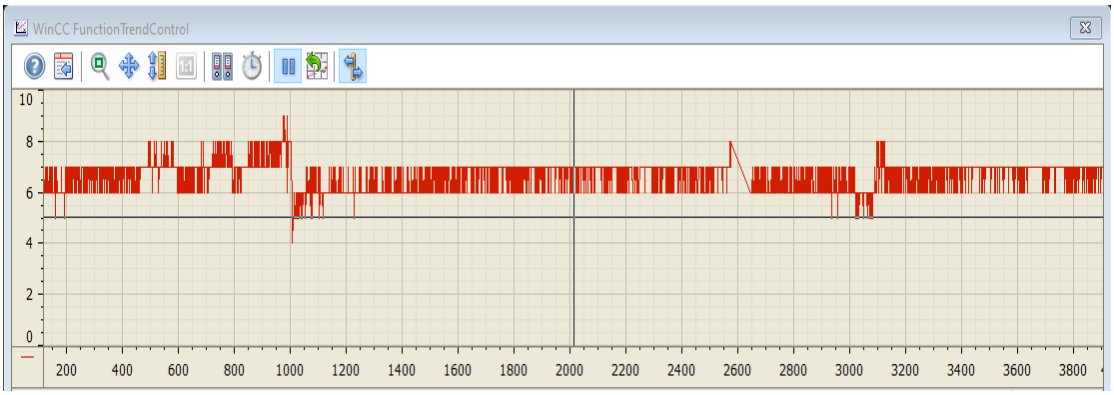
Για την εξαγωγή καλύτερων συμπερασμάτων με το πείραμα υλοποιήθηκαν δοκιμές με διαφορετικούς παράγοντες κάθε φορά. Παρακάτω αναλύεται η κάθε δοκιμή που υλοποιήθηκε.

Δοκιμή 1

Για αυτή την δοκιμή:

- Τοποθετήθηκε ένα καινούργιο μπουτόν με δύο Normally Closed επαφές.
- Η ταχύτητα πατήματος του εμβόλου ρυθμίστηκε σε 10cm/sec,
- Το έμβολο τοποθετήθηκε έτσι ώστε να μην πατάει στην μέση του μπουτόν αλλά προς την άκρη
- Καταγράφτηκαν 3.800 δείγματα.

Στο παρακάτω γράφημα φαίνεται ποια ήταν διαφορά της απόκρισης των δύο επαφών του μπουτόν.



Εικόνα 45. Δοκιμή 1

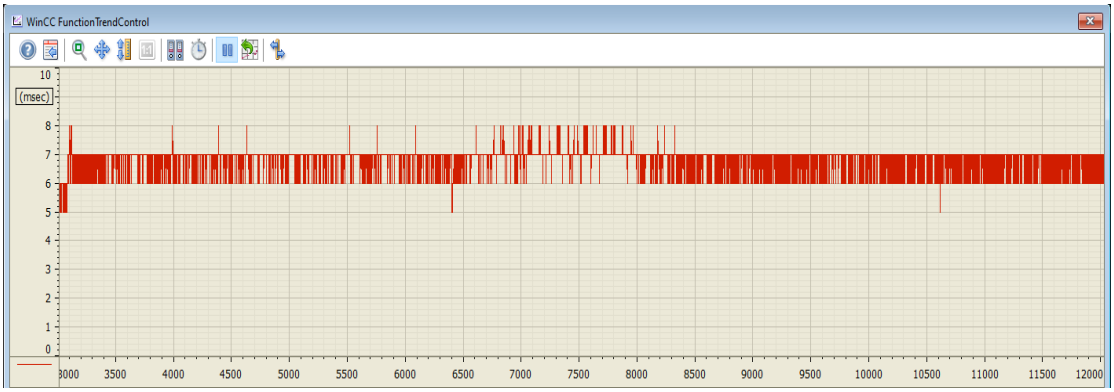
Μελετώντας το παραπάνω γράφημα παρατηρήθηκε πως η διαφορά χρόνου της απόκρισης των δύο επαφών ήταν 4-9 msec, με μέση τιμή περίπου 6,8msec.

Δοκιμή 2

Σε αυτή την δοκιμή:

- Χρησιμοποιήθηκε το ίδιο μπουτόν (δύο Normally Closed επαφές)
- Η ταχύτητα πατήματος του εμβόλου παρέμεινε σταθερή (10cm/sec)
- Το έμβολο τοποθετήθηκε έτσι ώστε να πατάει στην μέση του μπουτόν
- Καταγράφτηκαν 9.000 δείγματα.

Στο παρακάτω γράφημα φαίνεται ποια ήταν διαφορά της απόκρισης των δύο επαφών του μπουτόν.



Εικόνα 46. Δοκιμή 2

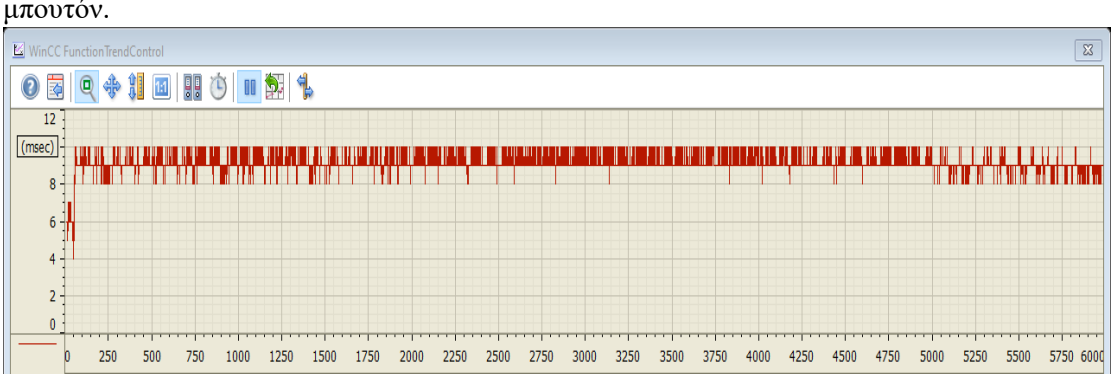
Από το παραπάνω γράφημα παρατηρήθηκε πως η διαφορά χρόνου της απόκρισης των δύο επαφών ήταν 5-8msec, με μέση τιμή περίπου 6,5msec.

Δοκιμή 3

Για την τρίτη δοκιμή:

- Τοποθετήθηκε ένα καινούργιο μπουτόν με δύο Normally Closed επαφές
- Η ταχύτητα πατήματος του εμβόλου ρυθμίστηκε σε 5cm/sec
- Το έμβολο τοποθετήθηκε έτσι ώστε να πατάει στην μέση του μπουτόν
- Καταγράφτηκαν 6.000 δείγματα.

Στο παρακάτω γράφημα φαίνεται ποια ήταν διαφορά της απόκρισης των δύο επαφών του μπουτόν.



Εικόνα 47. Δοκιμή 3

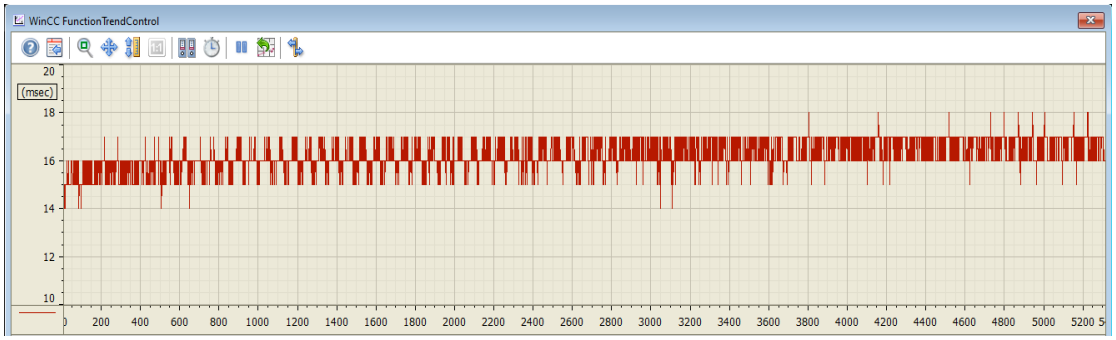
Από το παραπάνω γράφημα παρατηρήθηκε πως η διαφορά χρόνου της απόκρισης των δύο επαφών ήταν 8-10msec (εκτός από τα πρώτα 100 περίπου δείγματα που είχαμε γρήγορο πάτημα του εμβόλου), με μέση τιμή περίπου 9,2 msec.

Δοκιμή 4

Στην τέταρτη δοκιμή:

- Τοποθετήθηκε ένα καινούργιο μπουτόν με δύο Normally Closed επαφές
- Η ταχύτητα πατήματος του εμβόλου ρυθμίστηκε σε 3cm/sec
- Το έμβολο τοποθετήθηκε έτσι ώστε να πατάει στην μέση του μπουτόν
- Καταγράφτηκαν 5.500 δείγματα.

Στο παρακάτω γράφημα φαίνεται ποια ήταν διαφορά της απόκρισης των δύο επαφών του μπουτόν.



Εικόνα 48. Δοκιμή 4

Μελετώντας το παραπάνω γράφημα παρατηρήθηκε πως η διαφορά χρόνου της απόκρισης των δύο επαφών ήταν 14-18msec με μέση τιμή περίπου 16,3msec.

Από τις παραπάνω δοκιμές που υλοποιήθηκαν διαπιστώθηκαν τα εξής:

- Η διαφορά του χρόνου απόκρισης των επαφών σε μπουτόν με γρήγορο πάτημα δεν ξεπερνά τα 10msec και με αργό πάτημα δεν ξεπερνά 20 msec.
- Ακόμη και μετά από 13000 πατήματα οι επαφές έχουν την ίδια συμπεριφορά απόκρισης.
- Ο χρόνος απόκρισης των επαφών δε διαφέρει πολύ όταν το πάτημα γίνεται στη μέση ή στην άκρη.
- Ο χρόνος απόκρισης των επαφών δε διαφέρει όταν το πάτημα γίνεται ανά μικρό χρονικό διάστημα π.χ. ανά 2 sec ή ανά 1 min.

Από τις διαφορετικές δοκιμές που υλοποιήθηκαν παρατηρήθηκε πως η διαφορά του χρόνου απόκρισης των επαφών είναι γενικά σταθερή ακόμη και μετά από αρκετές χιλιάδες πατήματα. Δεν πρέπει να φυσικά να αγνοείται πως η χρήση αυτών των στοιχείων, όπως το Stop Emergency, είναι στοιχεία που δεν ενεργοποιούνται συχνά μέσα στη παραγωγική διαδικασία αλλά μόνο όταν υπάρξει πρόβλημα. Έχει παρατηρηθεί ότι θα μπορούσε να περάσουν ακόμη και ημέρες και να μην έχουν χρησιμοποιηθεί καθόλου. Αυτό σημαίνει πως εάν μία μηχανή έχει κύκλο ζωής περίπου 10-15 χρόνια ένα Stop Emergency πιθανό να ενεργοποιηθεί συνολικά ακόμη και λιγότερο από 5.000 φορές. Φυσικά για την αξιοπιστία του στοιχείου (π.χ. Stop Emergency) πολύ σημαντικό ρόλο παίζουν τα υλικά κατασκευής του. Ένα στοιχείο με καλά υλικά αντέχει στο χρόνο, σε υψηλές θερμοκρασίες, υγρασίες, κραδασμούς κλπ, κάτι που οι περισσότεροι κατασκευαστές πλέον λαμβάνουν υπόψη τους.

4.8 Συμπεράσματα

Μετά από τις παραπάνω δοκιμές καταρχήν μπορεί να βγει το συμπέρασμα πως μέσα από ένα Basic PLC μπορεί να ανιχνευθεί - ελεγχθεί η απόκριση δύο διαφορετικών επαφών ενός μπουτόν χωρίς επιπλέον ειδικό hardware. Η διαφορά χρόνου απόκρισης είναι μικρή με μία μέση τιμή στα 10msec. Εάν αυξηθεί αυτή η διαφορά κατά πολύ π.χ. στα 300msec αυτόματα

δημιουργείται πρόβλημα. Βέβαια το πρόβλημα αυτό είναι ανιχνεύσιμο οπότε η παραγωγή μπορεί να σταματήσει με ασφάλεια. Στις περισσότερες Safety κάρτες η διαφορά χρόνου απόκρισης μεταξύ των δύο επαφών ρυθμίζεται στα 500msec και αυτές με δικό τους μηχανισμό ελέγχουν αυτή τη διαφορά για να βγάλουν ενδεχόμενο πρόβλημα. Υπάρχουν πολλά παλαιά συστήματα αυτοματισμού με αργές διεργασίες που είναι σε λειτουργία και λόγο της παραγωγής ή της δομής που έχουν είναι σχεδόν απαγορευτική η αναβάθμισή της Safety λειτουργία τους, αυτή τη στιγμή στις περισσότερες περιπτώσεις αντικαθίστανται πλήρης με νέα συστήματα.

Το τελικό συμπέρασμα που βγαίνει από το πείραμα που διεξήχθη είναι πως κάνοντας χρήση Basic PLC και με χρήση συγκεκριμένων ρουτινών μπορεί να αυξηθεί η αξιοπιστία της λειτουργίας του αυτοματισμού χωρίς επιπρόσθετο εξοπλισμό. Αυτό σημαίνει πως χωρίς μεγάλο κόστος είτε σε χρήματα είτε σε χρόνο υλοποίησης ακόμα και υπάρχοντα συστήματα αυτοματισμού μπορούν να έχουν μία ποιο αξιόπιστη ασφαλή λειτουργία χωρίς την αντικατάστασή τους με νέα συστήματα όπως προτείνουν οι κατασκευαστές PLC.

ΚΕΦΑΛΑΙΟ 5

Ανάπτυξη αλγορίθμων για Fail Safety λειτουργία σε Basic PLC

Ο στόχος της λειτουργίας μίας μηχανής παραγωγής είναι να διατηρηθούν οι πιθανοί κίνδυνοι τόσο για τον άνθρωπο όσο και για το περιβάλλον το δυνατό χαμηλότεροι χωρίς όμως να περιορίσουν (όσο αυτό είναι εφικτό) την παραγωγή. Στο παρόν κεφάλαιο αναλύονται οι μηχανισμοί που έχουν αναπτυχθεί για την μείωση των πιθανόν κινδύνων σε περιπτώσεις αστοχίας τόσο του Hardware όσο και του Software σε ένα σύστημα αυτοματισμού. Μέσα από την ανάλυση των υπαρχόντων ειδικών αυτών συστημάτων θα αναπτυχθούν αλγόριθμοι που θα μπορούν να τρέχουν σε Basic PLC ανεβάζοντας την αξιοπιστία κατά τη λειτουργία τους, έτσι ώστε να μειωθούν οι πιθανοί κίνδυνοι σε περιπτώσεις αστοχίας του Hardware και του Software. Εάν αποδειχθεί πως με Basic εξοπλισμό PLC αλλά με διαφορετικό προγραμματισμό αυτού μπορεί να αναβαθμισθεί η ασφάλεια των συστημάτων αυτοματισμού, τότε χωρίς κόστος για επιπλέον ειδικό εξοπλισμό σε υφιστάμενα συστήματα αυτοματισμού θα μπορεί να υπάρχει Fail Safety λειτουργία.

Οι νομικές έννοιες και οι απαιτήσεις που διέπουν την απόδειξη επαρκούς ασφάλειας (πότε και πώς πρέπει να παρέχονται αποδείξεις) δεν πρέπει να είναι διαφορετικές. Για παράδειγμα όμως στην ΕΕ υπάρχουν απαιτήσεις τόσο για τον κατασκευαστή όσο και για τον χειριστή της εγκατάστασης, οι οποίες καθορίζονται από οδηγίες, νόμους και πρότυπα.

Στις ΗΠΑ υπάρχουν διαφορετικές απαιτήσεις ανάλογα με την περιοχή ή ακόμη και τις τοπικές ρυθμίσεις. Σε όλες όμως τις ΗΠΑ υπάρχει μια βασική αρχή ότι ο εργοδότης πρέπει να εγγυηθεί έναν ασφαλή χώρο εργασίας. Η νομοθεσία περί ευθύνης του προϊόντος θεωρεί τον κατασκευαστή υπεύθυνο για ζημίες που προκαλούνται από το προϊόν του.

Το σημαντικό για τους κατασκευαστές μηχανημάτων είναι ότι ισχύουν πάντα οι νόμοι και οι κανονισμοί στη χώρα όπου λειτουργεί το μηχάνημα ή το εργοστάσιο. Για παράδειγμα το μηχάνημα που πρόκειται να χρησιμοποιηθεί στην ΕΕ πρέπει να πληροί τις απαιτήσεις της ΕΕ ακόμη και αν ο κατασκευαστής του μηχανήματος έχει την έδρα του στις ΗΠΑ. Παρακάτω αναλύονται τα συστήματα ελέγχου που έχουν αναπτυχθεί για να καλύψουν τις παραπάνω ανάγκες εναρμονισμένα σχεδόν στο σύνολο των οδηγιών διεθνώς.

5.1 Redundant Systems

Τα redundant συστήματα αυτοματισμού χρησιμοποιούνται για την επίτευξη μεγαλύτερης διαθεσιμότητας. Ο Σκοπός αυτών των συστημάτων είναι να μειωθεί η πιθανότητα διακοπής της παραγωγής, η προστασία των ατόμων, του περιβάλλοντος και ο ασφαλής τερματισμός λειτουργίας της παραγωγής. Όσο υψηλότεροι είναι οι κίνδυνοι και το κόστος διακοπής της παραγωγής τόσο πιο χρήσιμη είναι η χρήση ενός Redundant συστήματος.

Η αξιολόγηση των Redundant συστημάτων βασίζεται συνήθως στις παραμέτρους αξιοπιστίας και διαθεσιμότητας. Ένα συνήθως χρησιμοποιούμενο μέτρο αξιοπιστίας είναι το MTBF (Μέσος χρόνος μεταξύ αποτυχίας). Αυτό μπορεί να αναλυθεί στατιστικά με βάση τις

παραμέτρους των εν λειτουργία συστημάτων ή με υπολογισμό των ποσοστών αστοχίας των χρησιμοποιούμενων εξαρτημάτων.

Το MTBF ενός Redundant συστήματος καθορίζεται από το MDT (Mean Down Time) ενός στοιχείου του συστήματος. Αυτός ο χρόνος προέρχεται ουσιαστικά από τον χρόνο εντοπισμού των σφαλμάτων και τον χρόνο που απαιτείται για την επισκευή τους.

Το MDT ενός συστήματος καθορίζεται από τους χρόνους:

- Απαιτούμενος χρόνος ανίχνευσης του σφάλματος.
- Απαιτούμενος χρόνος εύρεσης της αιτίας του σφάλματος.
- Απαιτούμενος χρόνος για την αντιμετώπιση των προβλημάτων και την επανεκκίνηση του συστήματος.

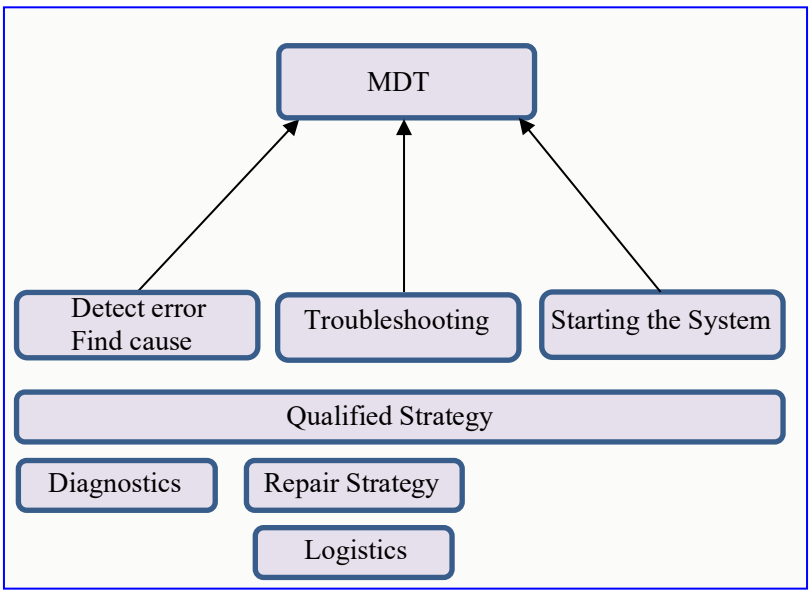
Το σύστημα MDT υπολογίζεται με βάση το MDT των επιμέρους στοιχείων του συστήματος. Η δομή στην οποία τα στοιχεία αποτελούν το σύστημα αποτελεί επίσης μέρος του υπολογισμού.

Συσχέτιση μεταξύ MDT και MTBF:

Η τιμή MDT έχει την υψηλότερη σημασία για την ποιότητα της συντήρησης του συστήματος και οι πιο σημαντικοί παράγοντες είναι:

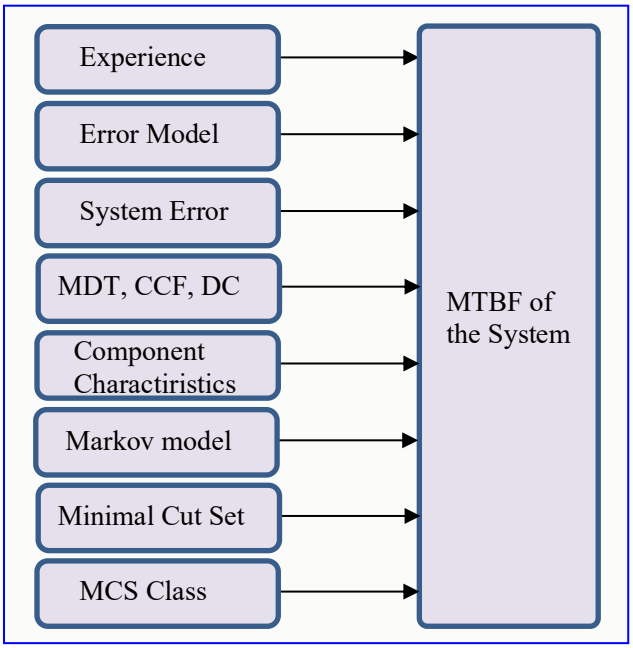
- Ειδικευμένο προσωπικό.
- Αποτελεσματική εφοδιαστική αλυσίδα.
- Εργαλεία υψηλής απόδοσης για διάγνωση και αναγνώριση σφαλμάτων.
- Μια καλή στρατηγική επισκευής.

Στην παρακάτω Εικόνα 49 φαίνεται η εξάρτηση του MDT από τους χρόνους και τους παράγοντες που αναφέρονται πιο πάνω.



Εικόνα 49. MDT

Στην παρακάτω Εικόνα 50 φαίνονται οι παράμετροι που περιλαμβάνονται στον υπολογισμό του MTBF ενός συστήματος.



Εικόνα 50. MTBF

Η παραπάνω ανάλυση προϋποθέτει τα παρακάτω:

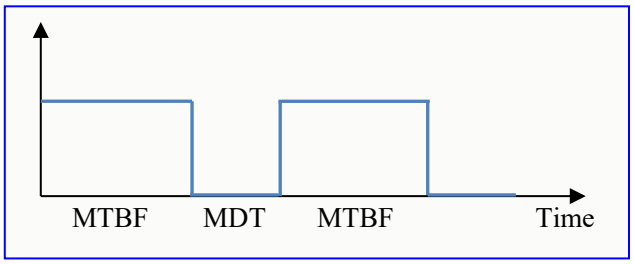
- Το ποσοστό αποτυχίας όλων των στοιχείων και όλων των υπολογισμών βασίζεται σε έναν μέσο όρο θερμοκρασίας 40 ° C.
- Η εγκατάσταση και η διαμόρφωση του συστήματος δεν περιέχουν σφάλματα.
- Όλα τα ανταλλακτικά είναι διαθέσιμα τοπικά, προκειμένου να αποφευχθούν εκτεταμένοι χρόνοι επισκευής λόγο έλλειψης ανταλλακτικών (αυτό διατηρεί το στοιχείο MDT στο ελάχιστο).
- Το MDT μεμονωμένων εξαρτημάτων είναι 4 ώρες. Το MDT του συστήματος υπολογίζεται με βάση το MDT των επιμέρους στοιχείων συν τη δομή του συστήματος.
- Το MTBF των εξαρτημάτων να πληροί τα πρότυπα:
  - SN 29500 (Αυτό το πρότυπο είναι συμβατό με MIL – HDBK 217 – F).
  - IEC 60050.
  - IEC 61709.
- Οι υπολογισμοί γίνονται χρησιμοποιώντας τη διαγνωστική κάλυψη κάθε στοιχείου.
- Ανάλογα με τη διαμόρφωση του συστήματος ο συντελεστής CCF είναι μεταξύ 0,2% και 2%.

Η χρήση Redundant μονάδων αυξάνει σε μεγάλο βαθμό MTBF. Ο υψηλής ποιότητας αυτοέλεγχος επιτρέπει τον εντοπισμό σχεδόν όλων των σφαλμάτων, έτσι η υπολογιζόμενη διαγνωστική κάλυψη είναι περίπου 90%. Η αξιοπιστία σε αυτόνομη λειτουργία περιγράφεται από τον αντίστοιχο ρυθμό αστοχίας. Η αξιοπιστία σε Redundant λειτουργία περιγράφεται από το ποσοστό αστοχίας των σχετικών εξαρτημάτων και ονομάζεται "MTBF". Οι συνδυασμοί αποτυχημένων στοιχείων που προκαλούν μία αστοχία του συστήματος περιγράφεται και υπολογίζεται χρησιμοποιώντας μοντέλα Markov.

Η διαθεσιμότητα είναι η πιθανότητα ενός συστήματος να λειτουργεί σε μια δεδομένη χρονική στιγμή. Αυτή μπορεί να είναι ενισχυμένη με τη χρήση Redundant μονάδων I/O. Τα Redundant στοιχεία είναι διατεταγμένα έτσι ώστε η λειτουργικότητα του συστήματος να μην επηρεάζεται από την αποτυχία ενός μεμονωμένου στοιχείου. Η διαθεσιμότητα ενός συστήματος εκφράζεται ως ποσοστό και ορίζεται από το μέσο χρόνο μεταξύ αστοχίας (MTBF) και του μέσου χρόνου επισκευής MDT. Η διαθεσιμότητα ενός δύο καναλιών συστήματος ανοχής σφαλμάτων (1-από-2) μπορεί να υπολογιστεί χρησιμοποιώντας τον ακόλουθο τύπο:

$$\mathbf{V} = \frac{\mathbf{MTBF_{1v2}}}{\mathbf{MTBF_{1v2}} + \mathbf{MDT}} * \mathbf{100\%}$$

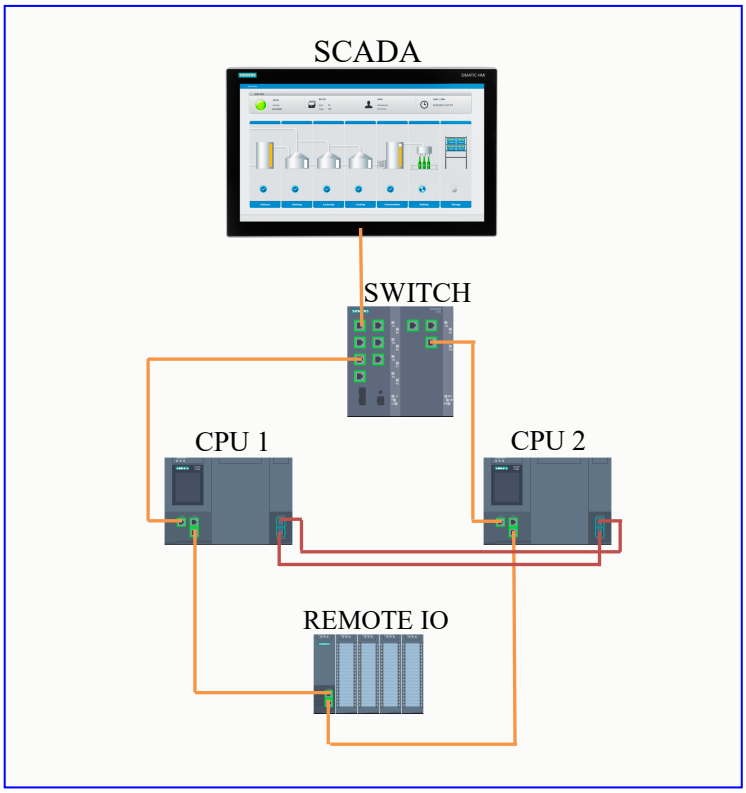
Εξίσωση 10



Εικόνα 51 Availability

Σε ένα σύστημα ελέγχου μπορούμε να έχουμε CPU Redundancy, Network Redundancy, I/O Redundancy, Sensor Redundancy και Switchover Bump less. Σε ένα Redundant σύστημα υπάρχουν δύο όμοιες CPU όπου εκτελούν τον ίδιο κώδικα παράλληλα. Οι δύο CPU συγχρονίζονται μέσω επικοινωνίας συνήθως με διπλές συνδέσεις. Το σύστημα έχει μονάδες συγχρονισμού που υποστηρίζουν το Hot-Swapping έτσι ώστε εάν μία CPU αποτύχει η άλλη CPU διατηρεί τον έλεγχο της διαδικασίας και η παραγωγική διαδικασία συνεχίζεται χωρίς κάποια ανωμαλία. Για λόγους ασφάλειας και λειτουργικότητας μία CPU μπορεί να είναι σε απόσταση μέχρι 10m όταν έχουμε μονάδες συγχρονισμού που επικοινωνούν με χαλκό και μέχρι 10km όταν επικοινωνούν με οπτικές ίνες.

Στην παρακάτω Εικόνα 52 φαίνεται μία τυπική διαμόρφωση ενός Redundant σύστημα.



Εικόνα 52. Σύστημα Redundant PLC

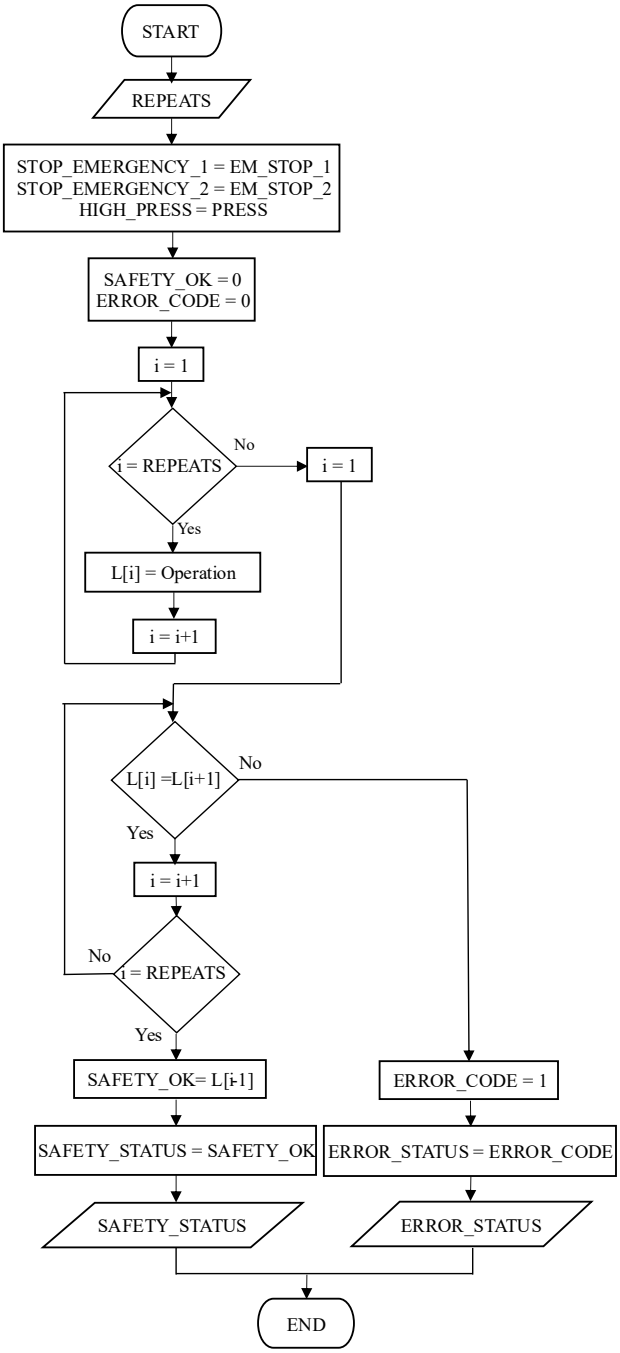
Το σύστημα αποτελείται από ένα SCADA που είναι το interface του χειριστή με τη μηχανή, δύο CPU με Redundant λειτουργία, ένα σύστημα καρτών (συνήθως Inputs και Outputs) για τη λειτουργία της μηχανής και οι απαιτούμενες κάρτες επικοινωνίας. Ο έλεγχος-λειτουργία της μηχανής υλοποιείται ως εξής:

Οι δύο CPU επικοινωνούν μεταξύ τους με διπλή σύνδεση (για λόγους Redundant) μέσω οπτικών ινών. Οι επικοινωνία απαιτείται για να ελέγχει η μία CPU την κατάσταση της άλλης και για το συγχρονισμό τους. Δηλαδή η εκτέλεση του κώδικα ελέγχου της μηχανής είναι πάντα συγχρονισμένη. Πάντα η μία CPU τίθεται και λειτουργεί ως Master και η άλλη ως Standby. Η CPU που λειτουργεί ως Master είναι αυτή που εντολοδοτεί μέσω καρτών εξόδων τα στοιχεία της μηχανής. Και οι δύο CPU διαβάζουν τις κάρτες εισόδων, τις επεξεργάζονται ανεξάρτητα και γνωρίζουν σε τι βήμα λειτουργίας βρίσκεται η μηχανή. Όταν η Standby CPU διαπιστώσει πρόβλημα στη Master CPU τότε αυτόματα αυτή μπαίνει σε λειτουργία Master και θέτει την άλλη σε Standby. Ο χρόνος μεταγωγής ελέγχου από τη μία CPU στην άλλη είναι μικρότερος των 5ms. Το SCADA επικοινωνεί ‘φυσικά’ και με τις δύο CPU αλλά η ενημέρωση και οι χειρισμοί υλοποιούνται από τη Master CPU.

5.2 Ανάπτυξη αλγορίθμων για Fail Safety λειτουργία σε Basic PLC

Αναλύοντας τα δύο παραπάνω συστήματα φαίνεται πως με τη χρήση αυτών σε ένα σύστημα αυτοματισμού αυξάνεται τόσο η διαθεσιμότητα όσο και η αξιόπιστη λειτουργία του. Οι απαιτήσεις όμως σε κόστος αλλά και σε ιδιαίτερη τεχνογνωσία είναι τόσο υψηλές όπου σε πολλές περιπτώσεις και κυρίως σε μικρές εφαρμογές τα κάνουν απαγορευτικά για χρήση. Έχοντας εις γνώση όλα τα παραπάνω και με γνώμονα τη χρήση Basic PLC σχεδιάσθηκε και αναπτύχθηκε ένας αλγόριθμος που μπορεί να χρησιμοποιηθεί εύκολα και χωρίς κάποια ιδιαίτερη τεχνογνωσία, ανεβάζοντας την αξιοπιστία ενός συστήματος αυτοματισμού.

Η βασική ιδέα αυτού του αλγορίθμου είναι πως τα PLC είναι μικροελεγκτές ειδικά κατασκευασμένοι για χρήση σε βιομηχανικό περιβάλλον και που πολύ δύσκολα αποτυγχάνουν. Όταν όμως αποτυγχάνουν οι συνέπειες τόσο για την παραγωγή όσο και για την πρόκληση ατυχήματος μπορεί να είναι καταστροφικές. Για τους λόγους αυτούς η ιδέα είναι το PLC να μην επεξεργάζεται μόνο μία φορά τον κώδικα του αυτοματισμού αλλά ‘n’ φορές πριν βγάλει τις εντολές προς τα στοιχεία της μηχανής. Στο τέλος των ‘n’ φορών της επεξεργασίας του κώδικα συγκρίνονται τα αποτελέσματα της κάθε επεξεργασίας και εάν είναι ίδια τότε βγαίνουν και οι εντολές προς τα στοιχεία της μηχανής, σε αντίθετη περίπτωση η μηχανή μεταβαίνει σε κατάσταση ασφαλής λειτουργίας. Στην παρακάτω Εικόνα 50 φαίνεται η διαδικασία λειτουργίας του αλγορίθμου.



Εικόνα 53. Λειτουργία Αλγορίθμου

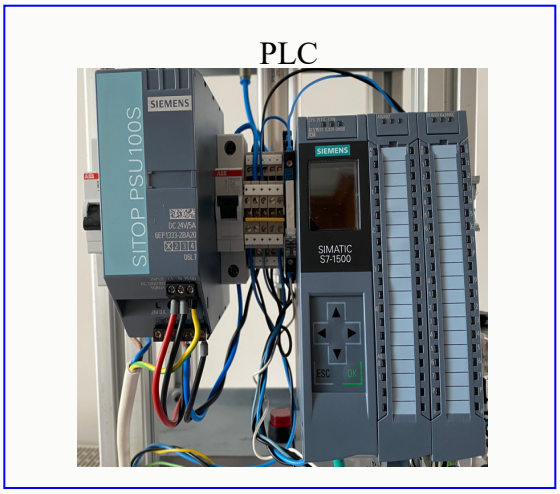
Περιγραφή Αλγορίθμου

Η λειτουργία του αλγόριθμου είναι η εξής:

1. Γίνεται εισαγωγή των επιθυμητών επαναλήψεων εκτέλεσης του κώδικα (n).
2. Γίνεται εισαγωγή των μεταβλητών (εισόδων και εξόδων) του κώδικα (IN1, IN2, OUT1, OUT2, κ.τ.λ.).
3. Εκτελείται ο κώδικας 'n' φορές και σε κάθε εκτέλεση τα αποτελέσματα του κώδικα (Έξοδοι) αποθηκεύονται σε ένα πίνακα.
4. Μετά την εκτέλεση του κώδικα ελέγχονται τα αποτελέσματα που βρίσκονται στον πίνακα και εάν είναι ίδια τότε βγαίνουν στις αντίστοιχες εξόδους σε διαφορετική περίπτωση βγαίνει μήνυμα σφάλματος και το σύστημα μεταβαίνει σε κατάσταση ασφαλής λειτουργίας.

5.2.1 Overview του πειράματος

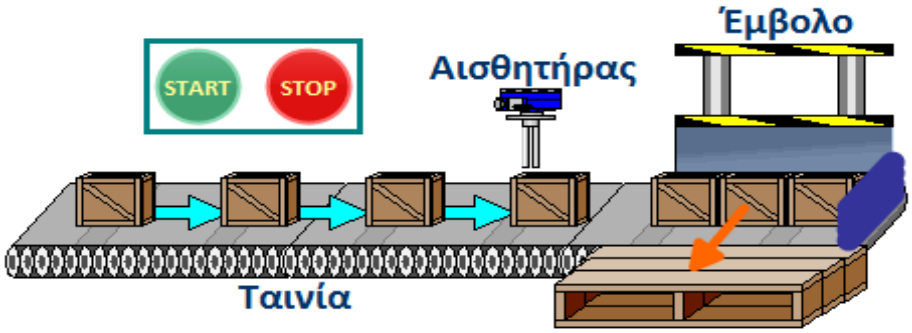
Για την υλοποίηση του πειράματος χρησιμοποιήθηκε βιομηχανικός εξοπλισμός που χρησιμοποιείται για τον έλεγχο συστημάτων αυτοματισμού και συνοπτικά φαίνεται στην παρακάτω Εικόνα 54.



Εικόνα 54. Εξοπλισμός πειράματος

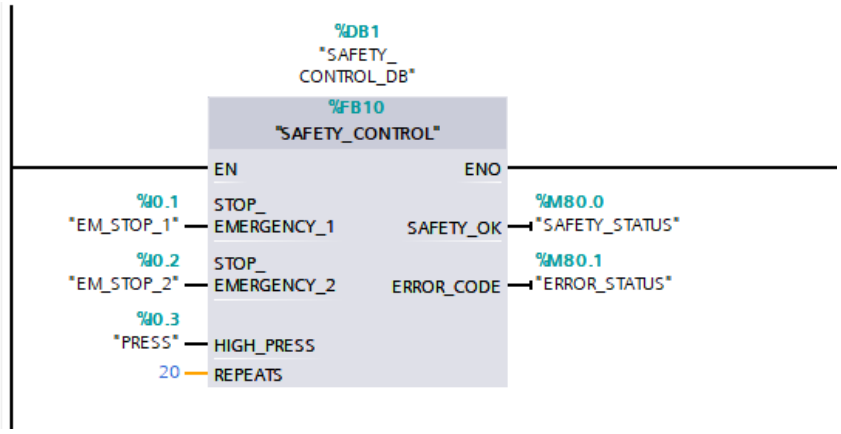
Για το πείραμα χρησιμοποιήθηκε η CPU 511C της SIEMENS αυτή είναι από τις μικρότερες σε δυνατότητες CPU της μεσαίας σειράς που διαθέτει η εταιρεία SIEMENS στα PLC και έχει ενσωματωμένα σήματα Εισόδων και Εξόδων. Η εφαρμογή της Safety λειτουργίας εφαρμόσθηκε σε ένα σύστημα αυτοματισμού όπου αφορά την πλήρωση παλετών με κιβώτια. Στο πείραμα ελέγχουμε την Safety λειτουργία και όχι τη διαδικασία της πλήρωσης των παλετών (αυτό αφορά άλλο τμήμα του κώδικα του PLC). Για τη Safety λειτουργία του συστήματος έχουμε δύο μπουτόν Stop Emergency (Normally Closed) και έλεγχο πίεσης του εμβόλου (από πρεσσοστάτη) όπου όταν ανεβεί πάνω από ένα όριο (από κάποιο πιθανό εμπόδιο) δίνει μία ψηφιακή είσοδο (Normally Closed). Όσο δεν υπάρχει πάτημα μπουτόν Stop

Emergency και δεν έχουμε υψηλή πίεση στο έμβολο ο κώδικας της Safety λειτουργίας μας δίνει μία έξοδο. Η έξοδος αυτή χρησιμοποιείται για την τροφοδοσία των εξόδων του συστήματος οπότε εάν χαθεί ότι και να δίνει το πρόγραμμα του αυτοματισμού οι έξοδοι του συστήματος αδρανοποιούνται και η λειτουργία της μηχανής σταματά. Στην παρακάτω Εικόνα 55 φαίνεται η διάταξη της μηχανής.



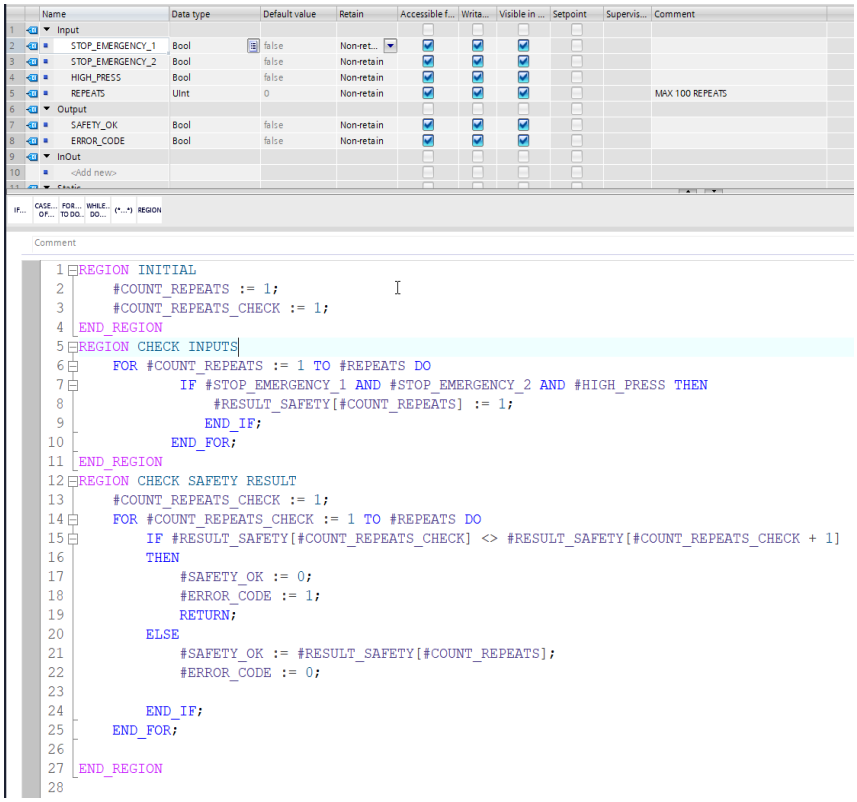
Εικόνα 55. Διάταξη μηχανής

Για την εφαρμογή του πειράματος χρησιμοποιήθηκε το πρόγραμμα TIA V16 και εκεί αναπτύχθηκε η ρουτίνα FB10 (Function Block 10) σε γλώσσα SCL. Παρακάτω δίνεται ο κώδικας της ρουτίνας και η επεξήγηση αυτού.



Εικόνα 56. OB1

OB1: Το OB1 είναι το Main Block που εκτελεί η CPU όταν είναι η στιγμή της επεξεργασίας του κώδικα που έχει γράψει ο χρήστης. Για αυτό εκεί καλείται και η ρουτίνα FB10 δηλώνοντας σε μορφή παραμέτρων τα απαιτούμενα δεδομένα ως Είσοδοι και Έξοδοι ανάλογα τη χρήση τους.



	Name	Data type	Default value	Retain	Accessible f...	Write...	Visible in ...	Setpoint	Supervis...	Comment
1	Input									
2	STOP_EMERGENCY_1	Bool	false	Non-ret...	☑	☑	☑	☐		
3	STOP_EMERGENCY_2	Bool	false	Non-retain	☑	☑	☑	☐		
4	HIGH_PRESS	Bool	false	Non-retain	☑	☑	☑	☐		
5	REPEATS	UInt	0	Non-retain	☑	☑	☑	☐		MAX 100 REPEATS
6	Output									
7	SAFETY_OK	Bool	false	Non-retain	☑	☑	☑	☐		
8	ERROR_CODE	Bool	false	Non-retain	☑	☑	☑	☐		
9	InOut									
10	<Add new>									

```
1  REGION INITIAL
2      #COUNT_REPEATS := 1;
3      #COUNT_REPEATS_CHECK := 1;
4  END_REGION
5  REGION CHECK INPUTS
6      FOR #COUNT_REPEATS := 1 TO #REPEATS DO
7              IF #STOP_EMERGENCY_1 AND #STOP_EMERGENCY_2 AND #HIGH_PRESS THEN
8                  #RESULT_SAFETY[#COUNT_REPEATS] := 1;
9              END_IF;
10         END_FOR;
11 END_REGION
12 REGION CHECK SAFETY RESULT
13     #COUNT_REPEATS_CHECK := 1;
14     FOR #COUNT_REPEATS_CHECK := 1 TO #REPEATS DO
15         IF #RESULT_SAFETY[#COUNT_REPEATS_CHECK] <> #RESULT_SAFETY[#COUNT_REPEATS_CHECK + 1]
16         THEN
17             #SAFETY_OK := 0;
18             #ERROR_CODE := 1;
19             RETURN;
20         ELSE
21             #SAFETY_OK := #RESULT_SAFETY[#COUNT_REPEATS];
22             #ERROR_CODE := 0;
23
24         END_IF;
25     END_FOR;
26
27 END_REGION
28
```

Εικόνα 57. FB10

Πίνακας Παραμέτρων: Εδώ δηλώνονται οι παράμετροι της ρουτίνας.
Initial: Εδώ γίνεται η αρχικοποίηση των μεταβλητών επανάληψης.
Check Inputs: Εδώ γίνεται ο έλεγχος εάν η λειτουργία της παραγωγής είναι Safety ή όχι.
Check Safety Result: Εδώ γίνεται ο έλεγχος εάν η επεξεργασία του ελέγχου της Safety κατάστασης υλοποιήθηκε σωστά.

5.3 Συμπεράσματα

Το τελικό συμπέρασμα που βγαίνει από το παραπάνω πείραμα που διεξήχθη είναι πως κάνοντας χρήση Basic PLC και με χρήση συγκεκριμένων ρουτινών ελέγχου μπορεί να αυξηθεί η αξιοπιστία της λειτουργίας του αυτοματισμού χωρίς επιπρόσθετο εξοπλισμό. Αυτό σημαίνει πως χωρίς μεγάλο κόστος είτε σε χρήματα είτε σε χρόνο υλοποίησης ακόμα και υπάρχοντα συστήματα αυτοματισμού μπορούν να έχουν μία ποιο αξιόπιστη ασφαλή λειτουργία χωρίς την αντικατάστασή τους με νέα συστήματα όπως προτείνουν οι κατασκευαστές PLC.

ΚΕΦΑΛΑΙΟ 6

Ορισμοί Συντομεύσεων

Παρακάτω δίνονται οι ορισμοί των συντομεύσεων που χρησιμοποιούνται μέσα στο παρόν κείμενο.

Safety–Related Part of a Control System: SRP/CS
Μέρος ενός συστήματος ελέγχου που ανταποκρίνεται σε σήματα εισόδου που σχετίζονται με την ασφάλεια και παράγει σήματα εξόδου που σχετίζονται με την ασφάλεια. Τα συνδυασμένα μέρη ενός συστήματος ελέγχου που σχετίζονται με την ασφάλεια ξεκινούν από το σημείο όπου αρχίζουν τα σήματα εισόδου που σχετίζονται με την ασφάλεια (συμπεριλαμβανομένου, π.χ. του έκκεντρου ενεργοποίησης και του κυλίνδρου του διακόπτη θέσης) και τελειώνουν στην έξοδο των στοιχείων ελέγχου ισχύος (συμπεριλαμβανομένων, π.χ. των κύριων επαφών ενός relay). Εάν χρησιμοποιούνται συστήματα παρακολούθησης για διαγνωστικά, θεωρούνται επίσης ως SRP/CS.

Category (Κατηγορία)
Ταξινόμηση των εξαρτημάτων που σχετίζονται με την ασφάλεια ενός συστήματος ελέγχου ως προς την αντοχή τους σε σφάλματα και την επακόλουθη συμπεριφορά τους στην κατάσταση σφάλματος, και η οποία επιτυγχάνεται από τη δομική διάταξη των εξαρτημάτων, την ανίχνευση σφαλμάτων ή/και την αξιοπιστία τους

Fault (Σφάλμα)
Κατάσταση ενός αντικειμένου που χαρακτηρίζεται από αδυναμία εκτέλεσης μιας απαιτούμενης λειτουργίας, εξαιρουμένης της αδυναμίας κατά τη διάρκεια προληπτικής συντήρησης ή άλλων προγραμματισμένων ενεργειών ή λόγω έλλειψης εξωτερικών πόρων. Ένα σφάλμα είναι συχνά το αποτέλεσμα αστοχίας του ίδιου του στοιχείου. [19]

Failure (Αποτυχία)
Τερματισμός της ικανότητας ενός αντικειμένου να εκτελεί μια απαιτούμενη λειτουργία. Μετά από αποτυχία, το στοιχείο έχει σφάλμα. «Αποτυχία» είναι ένα συμβάν, όπως διακρίνεται από το «σφάλμα», που είναι μια κατάσταση. Η έννοια όπως ορίζεται δεν ισχύει για στοιχεία που αποτελούνται μόνο από λογισμικό. [19]

Dangerous Failure (Επικίνδυνη αποτυχία)
Αστοχία που έχει τη δυνατότητα να θέσει το SRP/CS σε επικίνδυνη κατάσταση ή κατάσταση αστοχίας. [20]

Common Cause Failure CCF (Κοινή αιτία αποτυχίας)

Αστοχίες διαφορετικών στοιχείων, που προκύπτουν από ένα μεμονωμένο συμβάν, όπου αυτές οι αστοχίες δεν είναι συνέπειες η μία της άλλης. [19]

Systematic Failure (Συστηματική Αποτυχία)
Αστοχία που σχετίζεται με ντετερμινιστικό τρόπο με μια συγκεκριμένη αιτία, η οποία μπορεί να εξαλειφθεί μόνο με τροποποίηση του σχεδιασμού ή της διαδικασίας κατασκευής, των λειτουργικών διαδικασιών, της τεκμηρίωσης ή άλλων σχετικών παραγόντων. Η διορθωτική συντήρηση χωρίς τροποποίηση συνήθως δεν θα εξαλείψει την αιτία της βλάβης. [19]

Muting (Σίγαση)
Προσωρινή αυτόματη αναστολή λειτουργίας(ών) ασφαλείας.

Manual Reset (Χειροκίνητη Επαναφορά)
Λειτουργία εντός του SRP/CS που χρησιμοποιείται για την χειροκίνητη αποκατάσταση μιας ή περισσότερων λειτουργιών ασφαλείας πριν από την επανεκκίνηση ενός μηχανήματος.

Harm (Κάνω κακό)
Σωματικός τραυματισμός ή βλάβη στην υγεία. [6]

Hazard (Κίνδυνος, πιθανή πηγή βλάβης)
Ένας κίνδυνος μπορεί να προσδιοριστεί η προέλευσή του (π.χ. μηχανικός κίνδυνος, ηλεκτρικός κίνδυνος) ή η φύση της πιθανής βλάβης (π.χ. κίνδυνος ηλεκτροπληξίας, κίνδυνος κοπής, τοξικός κίνδυνος, κίνδυνος πυρκαγιάς). Ο κίνδυνος που προβλέπεται σε αυτόν τον ορισμό: είτε υπάρχει μόνιμα κατά την προβλεπόμενη χρήση του μηχανήματος (π.χ. κίνηση επικίνδυνων κινούμενων στοιχείων, ηλεκτρικό τόξο κατά τη φάση συγκόλλησης, ανθυγιεινή στάση, εκπομπή θορύβου, υψηλή θερμοκρασία), είτε μπορεί να εμφανιστεί απροσδόκητα (π.χ. έκρηξη, κίνδυνος σύνθλιψης ως συνέπεια ακούσιας/απρόσμενης εκκίνησης, εκτίναξη ως συνέπεια θραύσης, πτώση ως συνέπεια επιτάχυνσης/επιβράδυνσης). [6]

Hazardous Situation (επικίνδυνη κατάσταση)
Περίπτωση κατά την οποία ένα άτομο εκτίθεται σε τουλάχιστον έναν κίνδυνο, η έκθεση αυτή μπορεί να προκαλέσει βλάβη αμέσως ή για κάποιο χρονικό διάστημα. [6]

Risk (κίνδυνος)
Συνδυασμός της πιθανότητας εμφάνισης της βλάβης και της σοβαρότητας αυτής της βλάβης. [6]

Residual Risk (υπολειπόμενος κίνδυνος)
Ο κίνδυνος που παραμένει μετά τη λήψη προστατευτικών μέτρων. [6]

Risk Assessment (εκτίμηση κινδύνου)

Συνολική διαδικασία που περιλαμβάνει ανάλυση κινδύνου και αξιολόγηση κινδύνου. [6]

Risk Analysis (ανάλυση κινδύνου)
Συνδυασμός των προδιαγραφών των ορίων του μηχανήματος, αναγνώρισης κινδύνου και εκτίμησης κινδύνου. [6]

Risk Evaluation (αξιολόγηση κινδύνου)
Αξιολόγηση του κινδύνου (με βάση την ανάλυση κινδύνου), εάν έχουν επιτευχθεί οι στόχοι μείωσης του κινδύνου. [6]

Intended Use of a Machine (προβλεπόμενη χρήση μιας μηχανής)
Χρήση του μηχανήματος σύμφωνα με τις πληροφορίες που παρέχονται στις οδηγίες χρήσης. [6]

Reasonably Foreseeable Misuse (Λογικά προβλέψιμη κακή χρήση)
Χρήση μιας μηχανής με τρόπο που δεν προορίζεται από τον σχεδιαστή, αλλά που μπορεί να προκύψει από άμεσα προβλέψιμη κακή ανθρώπινη συμπεριφορά. [6]

Safety Function (λειτουργία ασφαλείας)
Λειτουργία του μηχανήματος, η αστοχία του οποίου μπορεί να οδηγήσει σε άμεση αύξηση του(των) κινδύνου(ων). [6]

Monitoring (παρακολούθηση)
Λειτουργία ασφαλείας που διασφαλίζει ότι ένα προστατευτικό μέτρο ξεκινά εάν η ικανότητα ενός εξαρτήματος ή ενός στοιχείου να εκτελεί τη λειτουργία του μειώνεται ή εάν οι συνθήκες της διαδικασίας αλλάξουν κατά τέτοιο τρόπο ώστε να μειωθεί ο βαθμός μείωσης του κινδύνου**.**

Programmable Electronic System PES (Προγραμματιζόμενο ηλεκτρονικό σύστημα)
Σύστημα ελέγχου, προστασίας ή παρακολούθησης που εξαρτάται για τη λειτουργία του σε μία ή περισσότερες προγραμματιζόμενες ηλεκτρονικές συσκευές, συμπεριλαμβανομένων όλων των στοιχείων του συστήματος όπως τροφοδοτικά, αισθητήρες και άλλες συσκευές εισόδου, επαφές και άλλες συσκευές εξόδου. [20]

Performance Level, PL (Επίπεδο απόδοσης)
Διακριτό επίπεδο που χρησιμοποιείται για τον προσδιορισμό της ικανότητας των εξαρτημάτων των συστημάτων ελέγχου που σχετίζονται με την ασφάλεια να εκτελούν μια λειτουργία ασφαλείας υπό προβλέψιμες συνθήκες.

Required Performance Level PL_r (Απαιτούμενο επίπεδο απόδοσης)

Επίπεδο απόδοσης (PL) που εφαρμόζεται προκειμένου να επιτευχθεί η απαιτούμενη μείωση κινδύνου για κάθε λειτουργία ασφαλείας

Mean Time to Dangerous Failure MTTF$_D$ (Μέσος χρόνος για επικίνδυνη αποτυχία)
Προσδοκία του μέσου χρόνου μέχρι την επικίνδυνη αποτυχία.

Diagnostic Coverage DC (Διαγνωστική κάλυψη)

Μέτρο της αποτελεσματικότητας των διαγνωστικών, το οποίο μπορεί να προσδιοριστεί ως η αναλογία μεταξύ του ποσοστού αποτυχίας των ανιχνευόμενων επικίνδυνων αστοχιών και του ποσοστού αποτυχίας των συνολικών επικίνδυνων αστοχιών. Η διαγνωστική κάλυψη μπορεί να υπάρχει για το σύνολο ή μέρη ενός συστήματος που σχετίζεται με την ασφάλεια. Για παράδειγμα, θα μπορούσε να υπάρχει διαγνωστική κάλυψη για αισθητήρες ή/και λογικό σύστημα και/ή τελικά στοιχεία. [20]

Protective Measure (Προστατευτικό μέτρο)
Μέτρο που αποσκοπεί στη μείωση του κινδύνου, π.χ. εφαρμόζεται από τον σχεδιαστή: εγγενής σχεδιασμός, μέτρα προστασίας και συμπληρωματικά προστατευτικά μέτρα, πληροφορίες για χρήση. Εφαρμόζεται από τον χρήστη: οργάνωση (ασφαλείς διαδικασίες εργασίας, επίβλεψη, συστήματα άδειας για εργασία), παροχή και χρήση πρόσθετων διασφαλίσεων, ατομικός προστατευτικός εξοπλισμός, εκπαίδευση. [6]

Mission Time T_M (Ώρα αποστολής)
Χρονική περίοδο που καλύπτει την προβλεπόμενη χρήση ενός SRP/CS

Test Rate r_t (Ρυθμός δοκιμής)
Συχνότητα αυτόματων δοκιμών για τον εντοπισμό σφαλμάτων σε ένα SRP/CS.

Demand Rate r_D (Ποσοστό ζήτησης)
Συχνότητα των απαιτήσεων για δράση που σχετίζεται με την ασφάλεια του SRP/CS

Repair Rate r_r (Ποσοστό επισκευής)
Αμοιβαία τιμή του χρονικού διαστήματος μεταξύ της ανίχνευσης μιας επικίνδυνης βλάβης είτε μέσω διαδικτυακής δοκιμής, είτε προφανούς δυσλειτουργίας του συστήματος και της επανεκκίνησης της λειτουργίας μετά από επισκευή ή αντικατάσταση συστήματος/εξαρτήματος. Ο χρόνος επισκευής δεν περιλαμβάνει το χρονικό διάστημα που απαιτείται για τον εντοπισμό αστοχίας.

Machine Control System (Σύστημα ελέγχου μηχανής)
Σύστημα που ανταποκρίνεται σε σήματα εισόδου από μέρη στοιχείων μηχανής, χειριστές, εξοπλισμό εξωτερικού ελέγχου ή οποιονδήποτε συνδυασμό αυτών και παράγει σήματα εξόδου που κάνουν το μηχάνημα να συμπεριφέρεται με τον προβλεπόμενο τρόπο. Το σύστημα

ελέγχου μηχανής μπορεί να χρησιμοποιήσει οποιαδήποτε τεχνολογία ή οποιονδήποτε συνδυασμό διαφορετικών τεχνολογιών (π.χ. ηλεκτρική/ηλεκτρονική, υδραυλική, πνευματική, μηχανική).

Safety Integrity Level SIL (Επίπεδο ακεραιότητας ασφάλειας)
Διακριτό επίπεδο (ένα στα πιθανά τέσσερα) για τον καθορισμό των απαιτήσεων ακεραιότητας ασφάλειας των λειτουργιών ασφαλείας που θα εκχωρηθούν στα συστήματα που σχετίζονται με την ασφάλεια, όπου το επίπεδο ακεραιότητας ασφάλειας 4 έχει το υψηλότερο επίπεδο ακεραιότητας και ακεραιότητας ασφάλειας το επίπεδο 1 έχει το χαμηλότερο. [20]

Application Software (Λογισμικό εφαρμογής)
Ειδικό λογισμικό για την εφαρμογή που υλοποιείται από τον κατασκευαστή του μηχανήματος και γενικά περιέχει λογικές ακολουθίες, όρια και εκφράσεις που ελέγχουν τις κατάλληλες εισόδους, εξόδους, υπολογισμούς και αποφάσεις που είναι απαραίτητες για την ικανοποίηση των απαιτήσεων της SRP/CS

Embedded Software - Firmware System Software (Ενσωματωμένο λογισμικό – υλικό - λογισμικό)
Λογισμικό που αποτελεί μέρος του συστήματος που παρέχεται από τον κατασκευαστή ελέγχου και το οποίο δεν είναι προσβάσιμο για τροποποίηση από τον χρήστη του μηχανήματος

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ:

[1] International Organization for Standardization, ISO 13849-1, Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design, 2008.
[2] International Electrotechnical Commission, IEC 62061:2021, Safety of machinery - Functional safety of safety-related control systems, 2021.
[3] M. Medoff, R. Faller, Functional Safety - An IEC 61508 SIL 3 Compliant Development Process, Third Edition)" ISBN 9781934977088.
[4] Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης, ΟΔΗΓΙΑ 2012/18/ΕΕ, 2012.
[5] Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης, ΟΔΗΓΙΑ 2006/42/ΕΚ, 2006.
[6] International Organization for Standardization, ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction, 2022.

[7] International Electrotechnical Commission, IEC 60204-1 / EN 60204 Safety of machinery – Electrical equipment of machines, 2016.

[8] International Organization for Standardization, ISO 13850:2015 Safety of machinery — Emergency stop function — Principles for design, 2020.

[9] International Electrotechnical Commission, IEC 61439 The new standard for low-voltage switchgear and controlgear assEmblies, 2010.

[10] International Electrotechnical Commission, IEC 61000-6-3:2020 Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for equipment in residential environments, 2020.

[11] International Electrotechnical Commission, IEC 61800-1:2021 Adjustable speed electrical power drive systems, 2021.

[12] BSI Group, EN 55011:2016 Industrial, scientific and medical equipment–Radio-frequency disturbance characteristics Limits and methods of measurement, 2020.

[13] BSI Group, EN 61000-6-3:2007+A1:2011 Electromagnetic compatibility (EMC) Generic standards. Emission standard for residential, commercial and light-industrial environments, 2011.

[14] International Electrotechnical Commission, IEC 60947-1:2020 Low-voltage switchgear and controlgear, 2020.

[15] International Organization for Standardization, ISO 13849, Safety of machinery - Safety related parts of control systems, Part 2:Validation, Geneva: ISO ORG, 2012.

[16] M. Punch, Functional Safety for the Mining Industry – An Integrated Approach Using AS(IEC)61508, AS(IEC)62061 and AS4024.1, 1st Edition, ISBN 9780980766004.

[17] G. Gabor, D. Zmaranda, C. Gyorodi and S. Dale, "Redundancy method used in PLC related ap-plications," *3rd International Workshop on Soft Computing Applications ,* vol. DOI: 10.1109/SOFA.2009.5254867., pp. 119-126, 2009.

[18] Nguyen Tuan Hung and Truong Dinh Chau, "An Application Solution for PLC Redundancy in Distributed Control System," *International Symposium on Industrial Electronics,* 2011.

[19] International Electrotechnical Commission, IEC 60050-192:2015, International Electrotechnical Vocabulary (IEV), IEC, 2015.

[20] International Electrotechnical Commission, IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.

[21] Heidi Hartmann, Dr. Eric Scharpf and Hal Thomas, "Practical SIL Target Selection - Risk Analysis per the IEC 61511 Safety Lifecycle," ISBN:978-1-934977-03-3.

[22] D. Smith and K. Simpson, *The Safety Critical Systems Handbook", Elsevier Ltd,,* vol. ISBN: 9780128207000., 2011 .

[23] D. Darvas, I. Majzik and E. Blanco Viñuela, "Formal Verification of Safety PLC Based Control Software," *Integrated Formal Methods,* vol. 9681.

[24] K. Rástočný, J. Ždánsky, J. Balák and P. Holečko;, "Effects of diagnostic on the safety of a control system realised by safety PLC," vol. 7512118, 2016.

[25] Dániel Darvas, István Majzik and Enrique Blanco Viñuela, "Formal Verification of Safety PLC Based Control Software," *Springer,* vol. 9681, 2016.

[26] Hiroo Kanamaru, Tsuyoshi Mogi and Naoki Aoyama, "Functional safety application using safety PLC," *SICE Annual Conference,* vol. 4421408, pp. 2489-2492, 2007.

[27] Rástočný, J. Ždánsky and K., "Influence of safety PLC parameters to response time of safety functions," in *International Conference on Applied Electronics*, 2013.

[28] Attila Hilt, Gabor Jaro amd Ostvan Bakos, "Availability Prediction of Telecommunication Application Servers Deployed on Cloud P," *Periodica Polytechnica, Electrical Engineering, DOI: 60. 72-81. 10.3311/PPee.9051.,* 2016.

[29] D. J. Rankin and J. Jiang, "A Hardware-in-the-Loop Simulation Platform for the Verification and Validation of Safety Control Systems"," *IEEE Transactions on Nuclear Science ,* vol. 58, pp. 468-478, 2011.

[30] V.A. Gapanovich, E.N. Rozenberg and I.B. Shubinsky, "SOME CONCEPTS OF FAIL-SAFETY AND CYBER PROTECTION OF CONTROL SYSTEMS," Vols. DOI: 10.21683/1729-2646-2014-0-2-88-100., 2014.

[31] J. Ždánsky and J. Valigurský, "Application diagnostic of distributed control system with safety PLC," *ELEKTRO,* vol. DOI: 10.1109/ELEKTRO.2018.8398311, pp. 1-6, 2018.

[32] E. Theocharis, M. Papoutsidakis, A. Sort and C. Drosos, "Experimentation on the Electromechanical Behavior of Automation Safety Buttons Applied to an Industrial PLC," *WSEAS TRANSACTIONS ON SYSTEMS AND CONTROL ,* vol. DOI: 15. 10.37394/23203.2020.15.74, 2021.

[33] Feng Wang, Ou Yang, Ruibo Zhang and Lei Shi, "Method for assigning safety integrity level (SIL) during design of safety instrumented systems (SIS) from database",," *Loss Prevention in the Process Industries,* 2016.

[34] K. Rástočný, J. Ždánsky and J. Hrbček, "The Problems Related to Realization of Safety Function with SIL4 Using PLC," *Cybernetics & Informatics (K&I), ,* vol. DOI: 10.1109/KI48306.2020.9039878, pp. 1-5, 2020.

[35] J. Ždánsky and J. Valigurský, "Time response of safety function realised by decentralised SRCS with safety. PLC," *International Conference on Applied Electronics (AE) ,* vol. DOI: 10.23919/AE.2018.8501425, pp. 1-4, 2018.

[36] G. Buja and R. Menis, "Dependability and Functional Safety: Applications in Industrial Electronics Systems," *IEEE Industrial Electronics Magazine,* vol. 6, pp. 4-12, 2012.

[37] Abdullah Al Farooq Jessica Marquard, Kripa George and Thomas Moyer, "Detecting Safety and Security Faults in PLC Systems with Data Provenance," *IEEE International Symposium on Technologies for Homeland Security,* 2019.

[38] Younju Oh, Junbeom Yoo, Sungdeok Cha and Han Seong Son, "Software safety analysis of function block diagrams using fault trees, Reliability Engineering & System Safety," vol. 88, no. 3, pp. 215-228, 2005.

[39] M. M. a. J. Ždánsky, "Safety PLC Programming Based on UML Statechart," *ELEKTRO,* vol. DOI: 10.1109/ELEKTRO49696.2020.9130307, pp. 1-5, 2020.

[40] Tham M.T., Warwick K., Failsafe Control Systems: Applications and emergency management, Netherlands: Springer, 2011.

[41] D. Smith, K. Simpson, , Safety Critical Systems Handbook – A Straightforward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards, 3rd Edition, ISBN 9780080967813., 2010.

[42] SIEMENS, System overview of STEP 7 and WinCC, Programming and Operating Manual, 2019.

[43] SIEMENS, WinCC V7.5 Manual, WinCC: Working with WinCC, 2018.

[44] SIEMENS, "Learn-Training Document, TIA Portal Module 072-100," 2019. [Online]. Available: https://www.automation.siemens.com/sce-static/learning-training-documents/tia-portal/safety/sce-072-100-safety-pn-cpu1516f-et200sp-r2101-en.pdf. [Accessed 2023].

[45] H. Berger, Automating with SIMATIC: Hardware and Software, Configuration and Programming, Data Communication, Operator Control and Monitoring, 6th Edition, ISBN: 9783895789434, 2016.

Paper 1 Safety Standards in Industrial Applications: A Requirement for Fail-Safe Systems

International Journal of Computer Applications (0975 – 8887)
Volume 178 – No. 24, June 2019

Safety Standards in Industrial Applications: A Requirement for Fail-Safe Systems

E. Theocharis
Dept. of Industrial Design and Production Engineering
University of West Attica, Athens, Greece

M. Papoutsidakis
Dept. of Industrial Design and Production Engineering
University of West Attica, Athens, Greece

C. Drosos
Dept. of Industrial Design and Production Engineering,
University of West Attica, Athens, Greece

G. Chamilothoris
Dept. of Industrial Design and Production Engineering,
University of West Attica, Athens, Greece

ABSTRACT
This document considers the requirements of the safe operation of an industrial automation. It analyzes the detecting and reducing procedures of dangerous situations. It also describes the European legislations which need to be followed for designing, procurement, purchase or use of the industrial equipment in the European Union, but also in several other countries outside the European Union, to have an effective safe operation.

Keywords
Fail Safe Systems, Machinery Directives, Algorithms.

1. INTRODUCTION
The European Directives and the Legislation define the substantial safety and the requirements of industrial equipment. The safety requirements of the European Union under the Article 95 which states the free movement of products and under the Article 137 on the safe workplace are defined with the following instructions.

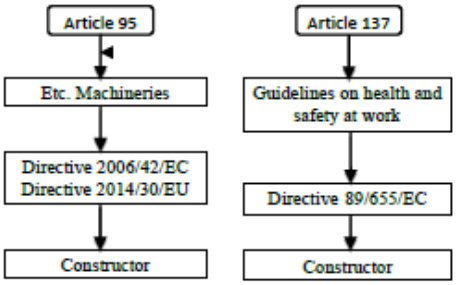


Fig 1: Instructions Article 95 / Article 137

The Safety Standards are distinguished hierarchically into three levels:

1. **Basic Safety Standards**
   They address basic engine design principles.
2. **Generic Safety Standards**
   They address general safety issues and special protection equipment.
3. **Machine Safety Standards**
   Special safety features of certain machinery categories, such as Low-Voltage, Pressers, etc.

2. APPLICATION OF MACHINERY DIRECTIVES ON A PRODUCTION LINE
The phases required for a safety production line are:

1. Risk Assessment
2. Risk Estimation
3. Verification

For a better understanding of the standards, we will design a machine following these standards. Figure 2 presents the machine we need to design.

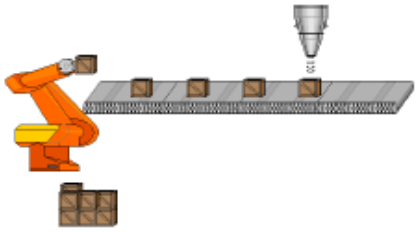


Fig 2: Line production

The use of the machine (line production) is for transporting the containers (through the robotic arm) from the pallet to the conveyor belt, then drive (through the conveyor belt) to the filling point, where at that point they fill up and then drive to the next machine (line production).

Our machine has the following technical features:

- Three-phase supply: 400VAC , 50Hz
- Operating temperature: from 0°C to 50°C
- Indoor usage: IP54
- Maximum box weight: 20 kilos
- Action radius of the robotic arm: 2,5m X 2,5m
- Use only by qualified personnel, skilled only with supervision and without visitor access
- Duration of operation: 200.000 hours

2.1 Risk Assessment
To analyze the Risk, we need to define, identify and estimate the limits of the machine. These estimations should be supported by qualitative or quantitative assessment of the risk, related to the risks posed by the machines. [1]

International Journal of Computer Applications (0975 – 8887)
Volume 178 – No. 24, June 2019

2.1.1 Determination of the Machine

The risk assessment begins with setting some machine limits, taking into account all the phases of the machine's life. That means determining the characteristics and performance of a machine or a series of machines in an integrated process and the related people in the surrounding area and products.

To wit, we should define the following:

- The limits of the machine: physical limits of the machine, the human / machine interfaces, the power supply,
- The time limits: life span, maintenance intervals, operating phases.
- And the user groups: education, experience, skills and visitors.

2.1.2 Risk Identification

Risk identification must be done for all the phases of the machine's life, which are assemblage, transportation, installation, commissioning and operation. The possible dangers we might face are squish, crashing, cutting, compressing, pulling, scrubbing, abrasion.

The possible dangers to the machine in our example are:

- ⇨ Robotic Arm: pushing and crashing
- ⇨ Conveyor Belt: pushing and crashing
- ⇨ Filling System: crashing and compression

2.1.3 Estimation of Risks

To estimate the risks, we need to know if there is a requirement to access the hazardous area, the duration of the exposure, the number of people, the frequency of access, if the probability of a dangerous occurrence is low, medium or high, if the machine's type of movement is sudden, fast or slow, what are the qualifications of the individuals, ability for updates and escape.

2.1.4 Evaluation of Risks

The machine's evaluation should initially be done per subsystem. In our example we have two subsystems which are:

Table 1. Robotic Arm

	Damage Severity	Possibility of occurrence			
		A	B	C	D
1	Necessary First Aid				
2	Necessary Treatment by a doctor				
3	Broken limbs or cut fingers				
4	Death, loss eyes or arms		4B		

A: Very Possible B: Possible C: Impossible D: Very Impossible

Table 2. Transportation and Filling

	Damage Severity	Possibility of occurrence			
		A	B	C	D
1	Necessary First Aid				
2	Necessary Treatment by a doctor				
3	Broken limbs or cut fingers		3B		
4	Death, loss eyes or arms				

A: Very Possible B: Possible C: Impossible D: Very Impossible

Overall, for our machine we have:

Table 3. Overall

	Damage Severity	Possibility of occurrence			
		A	B	C	D
1	Necessary First Aid				
2	Necessary Treatment by a doctor				
3	Broken limbs or cut fingers		3B		
4	Death, loss eyes or arms		4B		

A: Very Possible B: Possible C: Impossible D: Very Impossible

2.2 Risk Estimation

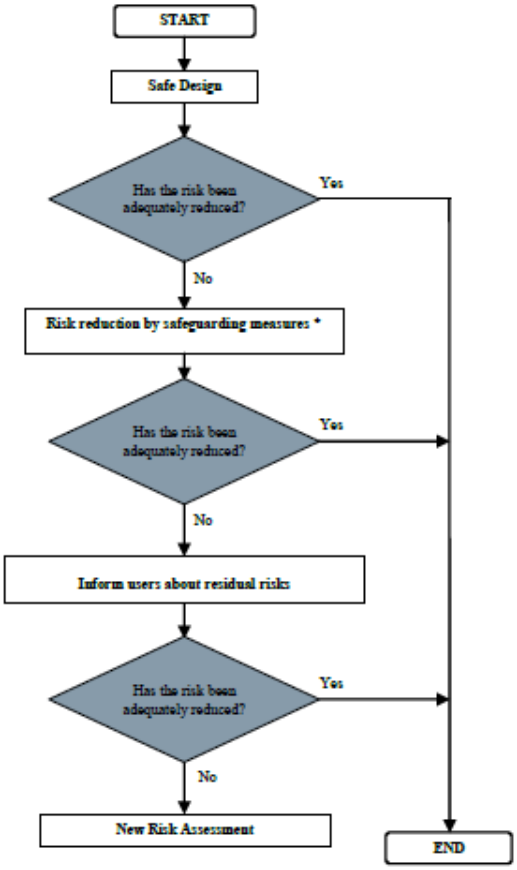


Fig 3: Methodology of Risk Estimation

After the Risk Estimation, we need to apply techniques with which we will reduce the risk. In the following Figure 3, the methodology we need to follow to detract the risk is given. [1]

*Technical measures in our example could be placing a protective fence for the arm and the filler.

International Journal of Computer Applications (0975 – 8887)
Volume 178 – No. 24, June 2019

2.3 Standard Based Verification

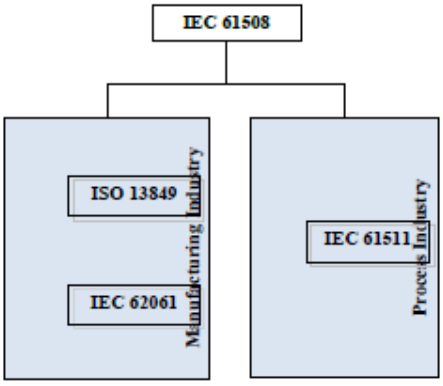


Fig 4: Safety standards on industry

For the operation safety of the machines, there are the following standards with different safety levels:

2.3.1 IEC 61508

The IEC 61508 template determines a general approach for all safe life cycle activities for systems consisting of electrical, electronically programmable electronic components and used to perform safety functions. This unified approach was adopted in order to develop a rational and consistent technical policy for all safety-related systems. The main objective is to facilitate the development of products and of international standards products based on the IEC 61508 series. It has been designed, while keeping in mind, that the framework must be strong and comprehensive enough to cover future developments.

Below the umbrella of the IEC 61508 templates are: [2], [16], [20]

- IEC 61511
- EN ISO 13849-1 Performance Levels PL a - e
- IEC 62061 Safety Integrity Levels SIL 1- 3

The use of IEC 61511 is selected for Process Industry, whilst the EN ISO 13849-1 and IEC 62061 are for Manufacturing Industry. The EN ISO 13849-1 is selected for low complexity Safety systems, whilst the IEC 62061 is selected for complex Safety systems which use Safety PLCs. All three templates follow the same steps: [3]

- Assess the Risks
- Allocate the safety measures
- Design Architecture
- Validate

2.3.2 IEC 61511

The Safety Instrumented Systems (SISs) have been used for many years to perform safety features to process industries. If the instruments are to be used for SIF, it is necessary to achieve certain minimum standards and performance levels. The IEC 61511 occupies with Safety Instrumented Systems (SISs) application and Safety Integrity Levels (SILs) for Process Industries. The typical levels of protection and risk mitigation are shown in the Figure 5 below. [4], [15]

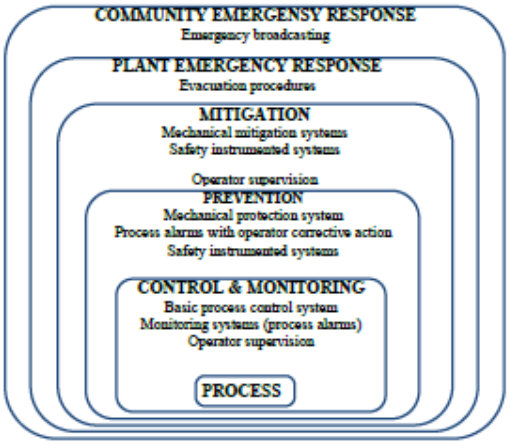


Fig 5: Levels of protection and risk mitigation

2.3.3 EN ISO 13849-1 Performance Levels PL a e

The following Figure 6 shows the methodology for Risk estimation with the EN ISO 13849-1 template. [5]

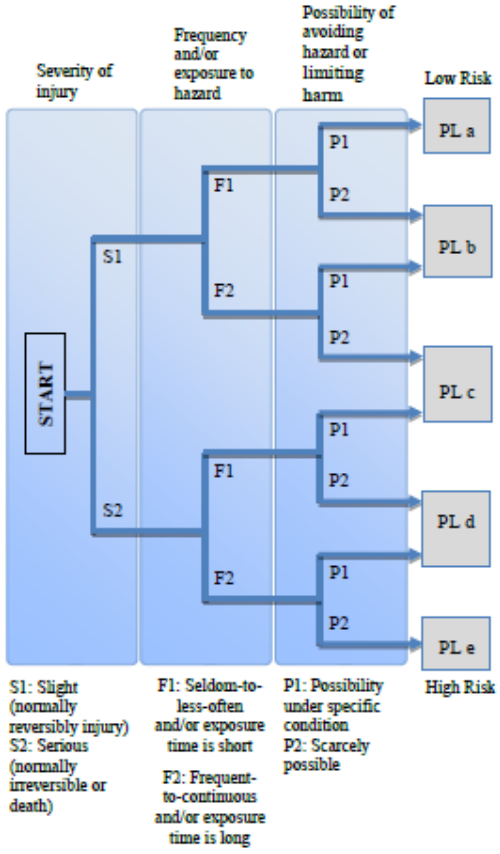


Fig 6: Performance Levels PL a – e

International Journal of Computer Applications (0975 – 8887)
Volume 178 – No. 24, June 2019

The levels of EN ISO 13849-1 are also defined from the average probability of a hazardous breakdown per hour as shown below:

Table 4. Performance Levels of ISO 13849-1

Performance level (PL)	Average probability of a hazardous breakdown per hour (1/h)
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3x10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $3x10^{-6}$
d	$\geq 10^{-7}$ to 10^{-6}
e	$\geq 10^{-8}$ to 10^{-7}

2.3.4 IEC 62061 Safety Integrity Levels SIL 1- 3

In this model, the severity of the potential damage is estimated at 1-4 levels, and then the probability of occurrence of the dangerous event is evaluated by looking at 3 additional parameters, where their summation gives us the class. The tables show us the levels and the parameters that define the Levels SIL 1-3. [6]

Table 5. Severity of injury

Severity of injury	S
Non-reversible: Death, eye or arm loss	4
Non-reversible: Permanent limb loss	3
Reversible: Necessary medical treatment	2
Reversible: Necessary first Aid	1

Table 6. Frequency / Duration of exposure

Frequency / Duration of exposure	F
≥ 1 per h	5
< 1 per h to ≥ per day	5
< 1 per day to ≥ per 14 days	4
< 1 per 14 days to ≥ per year	3
< 1 per year	2

Table 7. Probability of occurrence

Probability of occurrence	W
Very High	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Table 8. Possibility of prevention

Possibility of prevention	P
Weak	4
Strong	3
Possible	2

Table 9. Classes of SIL

Severity of injury	Class = F + W + P					
	S	4	5-7	8-10	11-13	14-15
Not Reversible: Death, loss eyes or arms	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Not Reversible: Broken limbs or cut fingers	3			SIL 1	SIL 2	SIL 3
Reversible: Necessary Treatment by a doctor	2				SIL 1	SIL 2
Reversible: Necessary First Aid	1					SIL 1

2.4 Use of Standards

The confirmation of a SIL or a PL class depends on many factors that are the following: [3, 5]

- T1 = interval test or life span (whichever is smaller)
- T2 = diagnostic test interval
- MTTF = average time until the error
- MTTFd = average time until the hazardous error
- DC = diagnostic coverage
- β = sensitivity to common causes of failure
- βD = calculating sensitivity to common causes of failure
- λ = failure percentage (per hour)
- λD = dangerous failure rate
- λDD = detectable rate of dangerous failure
- λDU = undetectable rate of dangerous failure
- λSD = detectable safe failure rate
- λSU = undetectable safe failure rate

The control of the verification of standards depends on their subsystems and their architecture.

2.4.1 EN 62061 Standard

The EN 62061 standard defines the possibility of dangerous equipment errors (Hardware), through the architecture of subsystems. The architectures of these subsystems are given below. [6], [14]

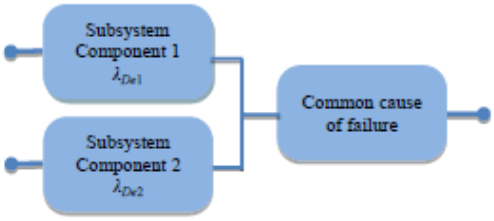
International Journal of Computer Applications (0975 – 8887)
Volume 178 – No. 24, June 2019

Subsystem A (serial order)
The components of subsystem A are in serial order, in this arrangement the probabilities of dangerous data failures are added.

$$\lambda_D = \lambda_{De1} + \Lambda\,\Lambda + \lambda_{Den}$$

$$PFH_D = \lambda_D \times 1h$$

Subsystem B (parallel arrangement (redundant) without diagnostic function)
The components of the subsystem B are in a parallel configuration without diagnostic function and the possibility of a hazardous error is given by the following formulas. When the architecture includes a single error tolerance, there is a possibility of a common cause of failure and must be taken into account. Such an arrangement can be made on actuators.

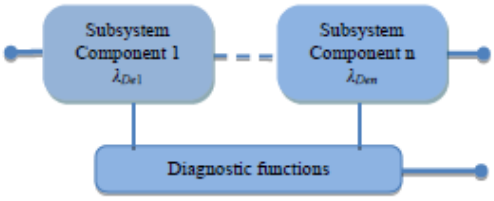


$$\lambda_D = (1-\beta)^2 \times \lambda_{De1} + \lambda_{De2} \times T_i + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_D = \lambda_D \times 1h$$

Subsystem C (arrangement with diagnostic function)
The following diagram shows the functional representation of a zero fault tolerance system with diagnostic function. Diagnostic coverage is used to reduce the likelihood of material damage to the material. The definition of diagnostic coverage is the ratio of the rate of detected dangerous failures as compared to the percentage of all dangerous failures.

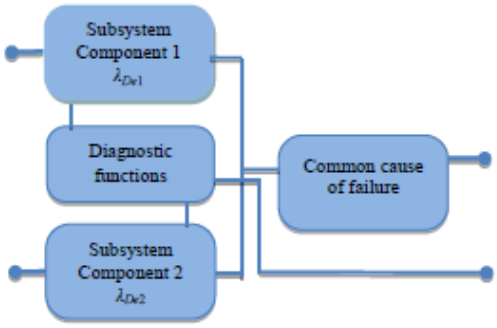
Such a device can be found in sensors.



$$\lambda_D = \lambda_{De1}(1-DC_1) + \ldots\ldots + \lambda_{Den}(1-DC_n)$$

$$PFH_D = \lambda_D \times 1h$$

Subsystem D (arrangement with diagnostic function)
Subsystem D is unitary with fault tolerance to diagnostic functions, all system failures are affected by design of subsystem elements. We can find such an arrangement through the Controllers.



The probability of dangerous errors in systems with similar elements is calculated as following:

$$\lambda_D = (1-\beta)^2\left\{\left[\lambda_{De}^2 \times 2 \times DC\right] \times T_2/2 + \left[\lambda_{De}^2 \times (1-DC)\right] \times T_1\right\} + \beta \times \lambda_{De}$$

The probability of dangerous errors in systems with dissimilar is calculated as following:

$$\lambda_D = (1-\beta)^2\left\{\left[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2\right] \times T_2/2\right\} +$$

$$\left\{+\left[\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2)\right] \times T_1/2\right\} + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$

Safe failure fraction $PFH_D = \lambda_D \times 1h$
The safe failure fraction is similar with the diagnostic coverage, but also takes into account any inherent tendency of failure to a safe situation. For example, when a fuse is burned, there is a failure, but it is very likely that the failure will be in an open circuit, which, in most cases, would be a "safe" failure. The SFF is (the sum of the "safe" damage rate plus the percentage of detected dangerous failures) divided by (the sum of the "safe" damage rate plus the percentage of detected and unidentified dangerous failures). It is important to realize that the only types of problems that need to be considered are those that could have an impact on a safe function.

$$SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{TOTAL}}$$

$$PFH_D = \lambda_D \times 1h$$

Table 10. Hardware Fault Tolerance

Safe failure fraction (SFF)	Hardware Fault Tolerance		
	0	1	2
<60%	Not Allowed	SIL 1	SIL 2
60%<90%	SIL 1	SIL 2	SIL 3
90%<99%	SIL 2	SIL 3	SIL 3
≥99%	SIL 3	SIL 3	SIL 3

2.4.2 EN ISO 13849-1 Standard
At this point, we will analyze a simplified but practical guide on how to implement the control systems, by category, that is an integral part of ISO13849-1 as defined architectures.

Category B
Category B should be considered as the basic foundation on which all other categories are built. It does not have any

International Journal of Computer Applications (0975 – 8887)
Volume 178 – No. 24, June 2019

further special arrangements or safety structures to the Basic Safety Principles as referenced in ISO 13849-2. These represent, generally, good tactics in designing and selecting materials.

$$PFH_D = \lambda_D \times 1h$$

Category 1
Category 1 requires the use of properly tested components and good safety principles. The use of properly tested components is designed to minimize the possibility of loss of a safe operation, but note that a single error can still lead to the loss of a safe operation.

Category 2
In addition to complying with Category B requirements and using properly tested safety principles, the safety system shall be tested to meet Category 2. The tests shall be designed to detect errors in the safety related parts of the control system. If there are no errors detected, the machine is allowed to operate. If errors are detected, the error response function must ensure that the machine remains in a safe state.

Category 3
In addition to complying with Category B requirements and properly tested safety principles, Category 3 requires the safe operation to be performed successfully in the presence of only one error. Some defects, such as cross-errors, which do not cause an immediate loss of safe security, may not be detected. This means that an accumulation of undetected damage can lead to loss of safe operation, for Category 3.

Category 4
In addition to complying with Category B requirements and properly tested safety principles, unlike Category 3, where the accumulation of errors can lead to a loss of safe operation, Category 4 requires safe operation to be performed in the event of accumulating faults. In practice, this is usually achieved by having a high-level diagnosis to ensure that all relevant errors are detected prior to any accumulation.

2.4.3 EN ISO 13849-1 Standard

The EN ISO 13849-1 describes a method determining PL, which is achieved by combining the following: [3], [5]

- Mean Time To dangerous (MTTFd)
- Diagnostic Coverage
- Common Cause Factors (CCF)
- Category

MTTFd
The MTTFd as shown in the table below, is divided into 3 levels:

Table 11. MTTFd Range

Level	Range
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd < 100 years

For pneumatic, mechanical and electromechanical components (pneumatic valves, relays, switches, position switches, etc.). It may be difficult to calculate the average time for dangerous damage (MTTFd). Most manufacturers of these components give only the average number of cycles until 10% of these components fails dangerously (B10d). The average number of cycles until 10% of these components fail dangerously (B10d) must be determined by the component manufacturer in accordance with the relevant product standards for the test methods (e.g. IEC 60957-5-1, ISO 19973, IEC 61810). Defective component failure functions must be defined, e.g. stick to the final position or change switching times. The operating time of the component (T10d) is the average time until 10% of the components fail. The MTTFd calculation is done as following:

Where $T_{10d} = \frac{B_{10d}}{n_{op}}$ $n_{op} = \frac{d_{op} \times h_{op} \times 3600s/h}{t_{cycle}}$

d_{op} = average function in days per year

h_{op} = average function in hours per day

t_{cycle} = average time between the beginning of two successive cycles of the element. (e.g. Switching a valve) in seconds per cycle.

Example
If we have a transistor with the following principles:

d_{op} = 180 days per year.

h_{op} = 12 hours per day.

t_{cycle} =8 seconds per cycle.

B_{10d} = 50 million cycles.

$$n_{op} = \frac{180 \times 12 \times 3600}{8} = 9{,}72 \times 10^5 cycle/year$$

$$T_{10d} = \frac{50 \times 10^6}{9{,}72 \times 10^5} = 51{,}4 year$$

$$MTTF_d = \frac{115{,}7}{0{,}1} = 514 year$$

Diagnostic Coverage
Both standards require the user to quantify the amount of diagnostic coverage of the associated security control functions. This is defined as the reduction in the probability of dangerous material damage, resulting from the operation of the automatic diagnostic tests

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DTOTAL}}$$

When a fault is detected, the monitoring mechanisms shall handle the fault by initiating an appropriate action which is application dependent. For many applications within the machinery sector such an appropriate action is to initiate a so called safe-state (i.e. the safety-function is performed). The term safe-state implies that the control system removes the hazard instantly (e.g. by immediately stopping/preventing hazardous movement of a part of a machine by remove the power to a motor). For other machines or applications other actions may be more appropriate, such as issuing an alarm.

In order to confirm that a required level of performance has been achieved, it is necessary to compare the architectural and diagnostic coverage with the MTTFd.

International Journal of Computer Applications (0975 – 8887)
Volume 178 – No. 24, June 2019

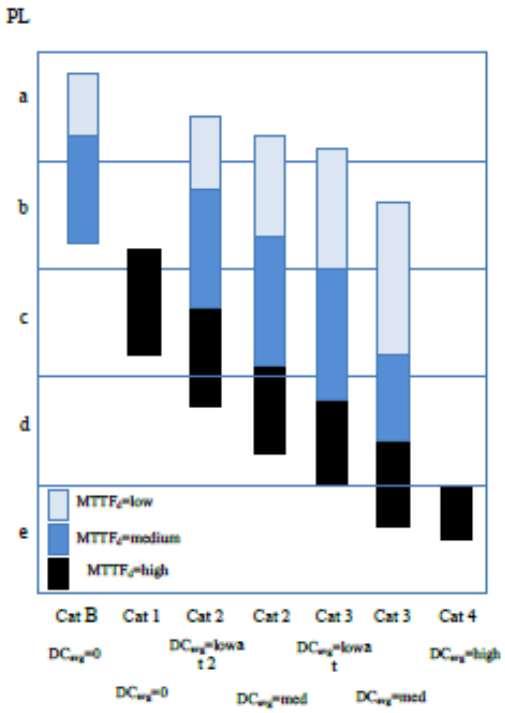


Fig 7: MTTFd - Diagnostic coverage

Common cause failures (CCF)

We call CCF the damage that is the result of one or more events and causes simultaneous failures of two or more separate components in a multi-component system and results in the failure of a safety-related control function.

The standard EN ISO 13849-1 requires the performance level of the control system to be determined with estimation of CCF as one important aspect. An assessment of CCF is necessary for every safety validation, but can be performed in different ways.

The standard provides a (qualitative) procedure for estimating the CCF measures implemented a category 2, 3 or 4 structures. The procedure is presented by following scoring table.

In order to fulfill the requirements a score of minimum 65 points or better is needed. For each listed measure, only the full score or nothing can be claimed. If a measure is only partly fulfilled, the score according to this measure is zero. The maximum score is 100 points.

Table 12. CCF Measures

No	Measure against CCF	Max Score	Achieved Score
1	Separation/segregation	15	15
2	Diversity	20	15
3.1	Design: Protection against overvoltage, current, etc	15	15
3.2	Design: Components are well tried	5	5
4	Assessment/analysis	5	0
5	Competence/training	5	0
6.1	Environmental: EMC	25	25
6.2	Environmental: Other influencers	10	0
Total		100	75

3. CONCLUSION

Based on the above analysis, we realize that we have all the necessary instructions and regulations so that the automation systems (simple or complex) can safely operate, even in cases of failure of their data. Every manufacturer of industrial automation can (with the existing technology) and must adhere to the safe operating regulations.

4. ACKNOWLEDGMENTS

All authors would like to thank the University of West Attica and specifically the Post Graduate Program of Studies (MSc) "New Technologies in Shipping and Transport", for the financial support provided to them to undertake this research project.

5. REFERENCES

[1] EN ISO 12100 (Safety of machinery - General principles for design - Risk assessment and Risk reduction).

[2] IEC 61508-3 (Functional Safety of Electrical/ Electronic/Programmable Electronic Safety – Related Systems).

[3] https://www.tuv-sud.co.uk/uploads/images/ 1397220180236544250395/sil-or-pl.pdf.

[4] IEC 61511 (Safety instrumented systems for the process industry sector).

[5] EN ISO 13849-1(Safety of machinery - Safety-related parts of control systems).

[6] IEC 62061 (Safety of machinery).

[7] https://www.itk.ntnu.no/sil/OLF-070-Rev2.pdf.

[8] https://www.festo.com/rep/en-us_us/assets/pdf/ FESTO_eGuide_final2.pdf.

[9] https://www.mts.com/cs/groups/public/documents/library /mts_4036317.pdf.

[10] https://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/safety-evaluation-tool/Pages/Default.aspx.

[11] https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp

[12] Tham M.T., Warwick K. "Fail-Safe Control Systems" ISBN 9789401066778.

[13] D. Smith, K. Simpson, "Safety Critical Systems Handbook – A Straightforward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards", 3rd Edition, ISBN 9780080967813.

[14] M. Punch, "Functional Safety for the Mining Industry – An Integrated Approach Using AS(IEC)61508, AS(IEC)62061 and AS4024.1." (1st Edition, ISBN 9780980766004.

[15] H. Hartmann, H. Thomas, E. Scharpf, "Practical SIL Target Selection - Risk Analysis per the IEC 61511 Safety Lifecycle", ISBN 9781934977033.

[16] M. Medoff, R. Faller, "Functional Safety - An IEC 61508 SIL 3 Compliant Development Process, (Third Edition)" ISBN 9781934977088.

[17] Dave Macdonald "Practical Industrial Safety, Risk Assessment and Shutdown Systems", ISBN 99780750658041.

[18] ALLEN-BRADLEY, SAFEBK-RM002C-EN-P, Safety related control systems for machinery.

[19] 2006/42/EC (Machinery Directive).

[20] IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety related systems).

[21] https://search-ext.abb.com/library/Download.aspx?DocumentID=2TLC172003M0204&LanguageCode=en&DocumentPartId=&Action=Launch.

[22] https://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/why-safety/Pages/default.aspx.

[23] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.

Paper 2 Experimentation on the Electromechanical Behavior of Automation Safety Buttons Applied to an Industrial PLC

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

Experimentation on the Electromechanical Behavior of Automation Safety Buttons Applied to an Industrial PLC.

E. THEOCHARIS
Dept. of Industrial Design and Production Engineering
University of West Attica
Thivon 250 & P. Ralli, Egaleo
GREECE

M. PAPOUTSIDAKIS
Dept. of Industrial Design and Production Engineering
University of West Attica
Thivon 250 & P. Ralli, Egaleo
GREECE

A. SORT
Dept. of Industrial Design and Production Engineering
University of West Attica
Thivon 250 & P. Ralli, Egaleo
GREECE

C. DROSOS
Dept. of Industrial Design and Production Engineering
University of West Attica
Thivon 250 & P. Ralli, Egaleo
GREECE

Abstract: - The growing automation demands of production make the automation systems more complex and vulnerable to failures. For this reason, some instructions have been created (CAT, SIL) that must be followed, in order to insure their safe operation in case of a failure of both the hardware and the software. For a credible operation of a Fail Safety system along with a system to work on SIL2 or SIL3, must have Safety Hardware and Software. This present paper analyses the response of the Hardware of a Basic PLC and the equipment of an automation system. It also presents a descriptive analysis of the experiment, which was conducted to record measurements in order to draw firm conclusions. In addition, the measurements are analysed and evaluated to verify if basic equipment could be used in these systems and insure the Safety function at the same time. The objective is to simply prove that if we manage an already existing Basic PLC equipment differently, it could upgrade the security of automation systems. Therefore, with a low cost in time and money, particularly in existing automation systems, there could be Fail Safety operations.

Key-Words: - Safety Relay, Safety PLC, Safety integrity level (SIL)

Received: September 1, 2020. Revised: December 15, 2020. Accepted: December 19, 2020.
Published: December 23, 2020.

1 Introduction

The reduction of risks in a production process depends on many factors. The main factors are:
a) The separation of the workers from the production machines in natural ways, like doors, bars, etc.
b) The electronic and mechanical equipment to be completely reliable, so that in case of a problem to deflect any accidents.[1,4]
In the first automation systems where Safety operation was needed, due to the process, Safety Relays were used. Safety Relays are specially designed Relays formally certified to constantly be armed. Thus, when wiring all the Normally Closed contacts of the protection elements in order (e.x. Stop Emergency) for the armament of the Relay, it automatically shuts down if any of these contacts turn on. For the operation of the automation system one Normally Open contact of Safety Relay is used, as a consequence by deactivating the Safety Relay it automatically pauses the operation of automation.
Safety Relays are still used today in simple automation systems providing additional capabilities, such as two or more control channels, time delays, communication abilities etc. In figure 1 below a typical Safety Relay use is being described.

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

E. Theocharis, M. Papoutsidakis,
A. Sort, C. Drosos

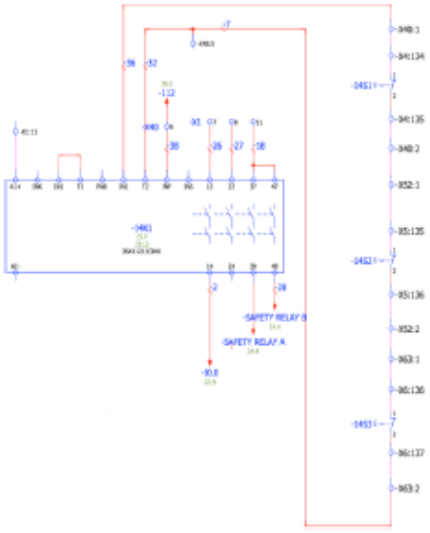


Fig. 1: Typical use of a Safety Relay

As shown in figure 1, there are three «Stop Emergency» buttons. The first button takes in current from the Safety Relay and it is wired up in series with the other two. So, if one of the three buttons is pressed the current turns on and there is no more voltage return in the Safety Relay. As a result of losing the voltage, the Safety Relay opens the contacts Safety Relay A and B and the automation system operation is then paused.

If the process requirements for Safety automation operations are large and complex then it is not covered only by Safety Relays, so Safety PLC is then used. For instance, there is not just a Stop emergency in such a process but there is also a Laser Curtain used. That means, if a worker walks through an area where machines are placed, then their operation must be stopped and start again once the worker has exited that area. In fact, the operation should resume after a certain time and after a Reset is performed.

Now, most PLC manufacturers produce Safety PLC with additional functions, both in Hardware and Software rather than in Basic PLC. There are PLCs that are only used for Safety operations and PLCs that perform both automatic and Safety operations at the same time.

In very critical facilities like refineries, airports, nuclear power plants, we use double Safety PLC, one is the Redundancy of the other. In a redundant system we have two CPUs which run the same program at the same time and are synchronized (usually with optical fibers) so that they are on the same processing step. If a CPU defects then the other CPU undertakes in order to resume controlling the system. The control of proper functioning and control transmission from one CPU to another is not programmed by the respective automation mechanic, but it has been implanted by the PLC manufacturer. That is to say, he has gone under extensive chek-ups and certifications, thus offering greater reliability. If both CPUs are available, only one of them has the control of the automation system, and so it is stated as Master. Primary and Backup are the two CPUs, while the ET200SP and ET200MP are signal cards for the automation system checkup and each time are being monitored from the Master CPU. The reticulation between them is in Ring topology, which means that if the cable is cut anywhere, the system will continue to operate normally. In most redundant systems, the channel switching time from one CPU to the other is less than 100 msec. This results in creating no malfunctions in the control system transitioning from one CPU to the other. In Figure 2 below, we can see this kind of system [7].

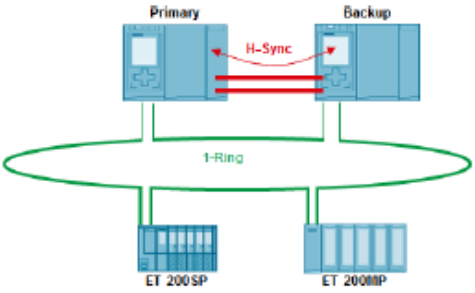


Fig. 2: Redundant PLC System

The basic Safety PLC properties are:

…in Hardware:

A Safety PLC is a specially designed controller for security use (there are PLCs that can operate both as security controllers and as automation controllers). The Safety PLC owns self-testing functions. It has high reliability and it meets the required security standards such as SIL3 / IEC61508 and Category 4 / ISO 13849. [2,5]

The Safety PLC interacts with the Automation PLC through Input/Output network or signals, it manages the emergency system and when the conditions are followed it then allows the Automation PLC to operate properly. In Safety PLC all the security sensors are connected with double wiring and double-checking contacts. Finally, by having double commands, the actuators are activated.

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

E. Theocharis, M. Papoutsidakis,
A. Sort, C. Drosos

...in Software:
The security standards require strict restrictions of the programming languages of a Safety PLC. For this reason, most Safety PLC manufacturers provide special programming languages which are formally certified to cover these restrictions. In the operation of a Safety PLC not only the signal check-up routines are operated, but also the routines to ensure proper operation as a CPU. Only a certified mechanical engineer can remotely modify the operation of a Safety PLC by default. The modification can occur through the security level settings by automatically recording the alterations (signature). [1].
The following units describe the use of Safety Input - Output PLC cards. The experiment checks how the Inputs of a Basic PLC respond so that they can be used to upgrade the security of automation systems

2 Signal Implementation of Safety PLC

The signals (Input - Output) of a Safety PLC are being described below. It will then be ascertained whether or not this connection and the additional internal security features of a Safety PLC signal card could be implemented using a Basic PLC.

2.1 Sensor wiring on safety PLC input cards

The connection of the sensors to the input cards can occur with a single channel or with a double channel. The Safety Input cards have two independently galvanic ally isolated channels. The sensor wiring capabilities are being given below. [2,4]

2.1.1 Sensor wiring with a single channel (1oo1)

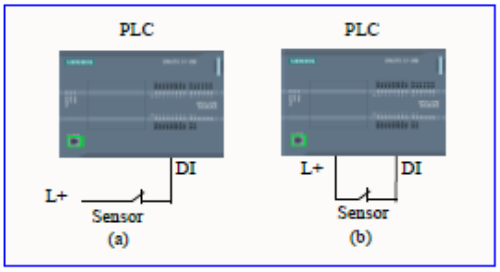


Fig. 3: Sensor wiring with a single channel (1oo1)

In figure 3 above, there is a contact wiring (Normally Closed for safety reasons) of a sensor in a PLC input. The sensor can be powered by an external power supply (a) or by the PLC (b). Although, if this wiring is connected to a Fail Safe input card in a PLC, it can provide security Cat.2/ PLc/SIL1.

2.1.2 Sensor wiring with double channels (1oo2)

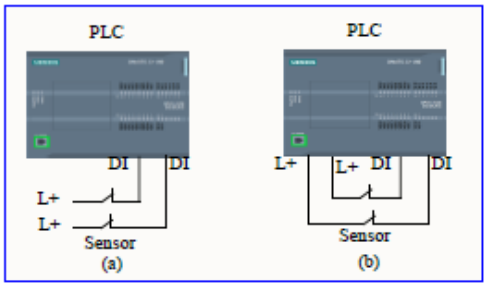


Fig. 4: Sensor wiring with double channels (1oo2)

In figure 4 above, there is wiring of two contacts (Normally Closed for safety reasons) of a sensor in two PLC inputs or of two independent sensor wirings from one contact (Normally Closed for safety reasons) in two PLC inputs. The Fail Safe input cards of the PLC check both inputs and they transfer the information in the CPU as a single input whether they are activated or not or if there is a malfunction (e.x. having a signal at one input but not having at the other). The power supply of a sensor can occur by an external power supply (a) thus, having security up to Cat. 3/PLd/SIL2 or from the (b) thus, having security up to Cat. 4/PLe/SIL3.
The above link assemblies refer to Input Fail Safe cards, where they have extra integrated features, like cut cable control, non-synchronization of inputs, etc. For this reason, these systems could be formally certified by the manufacturers even up to SIL3.

2.2 Wiring actuators in safety PLC output cards

The wiring capabilities of the sensors with one Relay per output and with two Relays per Output are given below.

2.2.1 Relay wiring per output

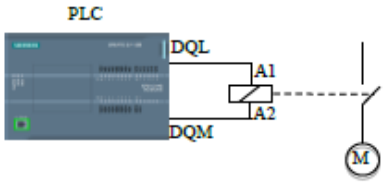


Fig. 5: Relay wiring per output

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

Figure 5 above displays the wiring of a Relay with one output from a Fail Safe card. In Fail Safe output cards, each output does not only give e.g. 24VDC for the activation of the Relay but also 0VDC. That is to say, when there is no output command from the PLC to the Relay, the circuit in both A1 and in A2 is open. The Fail Safe output cards have additional diagnostic routines for extra check-ups e.g. cut cabling, command capability check when it is required etc.

2.2.2 Two relay wiring per output

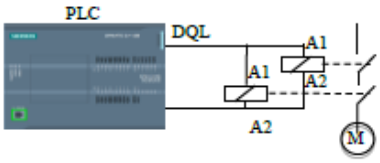


Fig. 6: Two relay wiring per output

Figure 6 above displays the wiring of two Relays with one output from a Fail Safe card. With this linkage we could have security up to Cat.4/PLe/SIL3. One of the two Relays could have a constant A1 voltage and load when through the Q of a PLC shuts down the circuit from the A2. It is usually recommended that both Relays are wired to the PLC card. In this function, a digital output is being commanded through the program. This information is then transferred to the output card and afterwards both relays are loaded. By using two relays, it ensures that the ordered component (e.g. an engine) will not start operating if for some reason only one relay is loaded or is not deactivated.

3 Double Contact Response of a Basic PLC Experiment

In the following experiment, the double contact response of a component is checked (e.g. button). Through the results of the experiment, we will draw conclusions whether it is possible to have not only SIL 1 function but also SIL 2, using concessional cards in a PLC.

With this experiment, the response of double contacts of a component (like that of a button) will be examined, both in the beginning of its operation and when it has been used a few thousand times. Knowing the expected response of the component, with the functions that support the Basic PLC, and not the Safety ones, the component can be examined and a Safety function can be produced. With this implementation as well as with many potential assumptions required, leads to the conclusion that the reliability of the already existing automation systems could be increased without any additional cost-effective equipment but also without any specialized installing and programming procedures. In this case of course, the Safety operation of the component (e.g. the button) will be achieved and not the PLC Safety operation of a CPU.

3.1 Overview of the Experiment

The implementation of this experiment required industrial equipment, which is used to monitor automation systems and is described in detail below.

3.1.1 Piston – Push button

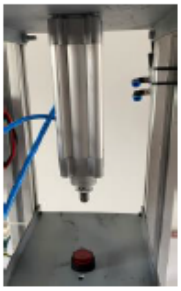


Fig. 7: Piston – Push Button

Ain air piston was installed to simulate the push of the button. When the piston takes an order from the PLC, it goes down and presses the button. The PLC command (i.e. a digital output) gives 24VDC to a valve which then channels air into the piston, causing it to go downward. By deactivating the command, the valve alters the air supply to the piston and this way the piston goes upward. This procedure checks the piston and therefore the push of the button. By adjusting the pressure of the air which channels into the piston, it is more possible to monitor the speed at which the button is pressed (slow or fast), something that will lead to additional information for the contact response of the button. To the button, a 24VDC lamp and two Normally Closed contacts are connected. When the button is pressed then the lamp switches on and the contacts

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

open up. The buttons were used from two different manufacturers, and this was done in order to monitor the behavior of each button and not which company button is better. Also, the buttons of the experiment have automatic reset so that they do not buckle and then need to be pulled or rotation to unbuckle. So, with the automatic reset there is a possibility of direct push of the button. In this way, many automatic presses are achieved in minimal time.

3.1.2 PLC

A Siemens series S7-1500 PLC was used to command the piston and also to read the contacts of the button.

Fig. 8: PLC

More specifically, a CPU 511 was used. That is one of the smallest in CPU capabilities in the mid-range PLC series which are owned by SIEMENS. It has input and output signals. This way, one digital output was used to command the piston and two digital inputs to read the contacts of the button.
That specific CPU (like most of the CPUs) has the ability to read Outputs in time less than 0,05m/s and Interrupt routines for a more immediate reading and processing of the Inputs.

3.1.3 Scada

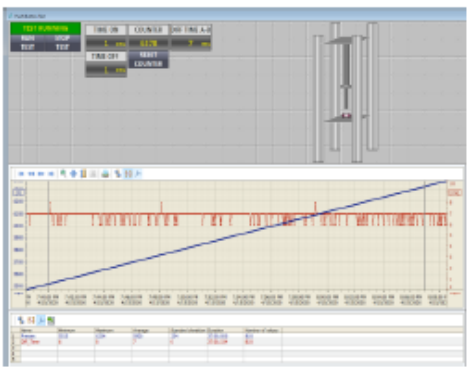


Fig. 9: Scada

The SCADA of the experiment was developed in WinCC V7.5 of SIEMENS. The WinCC V7.5 has the communication interface with the PLC (Profinet is used for the experiment), Visualization abilities, Control and Tag logging which are required for the conduct of the experiment.

3.2 PLC- Piston control

The automation check of the experiment was done through a TIA V16 program. An FB1 routine was developed (Function Block) in SCL language to control the Piston. With FB1 routine, the operation of the piston is controlled via SCADA, ie when and for how long it will be activated to push the button. [10]

```
REGION Pulse Generator
    #TIME_OFF := "CLOCK_DATA".TIME_OFF * 1000;
    #TIME_ON := "CLOCK_DATA".TIME_ON * 1000;
    #IEC_Timer_0_Instance(IN := NOT "Tag_1",
                          PT := #TIME_OFF,
                          Q => "PULSE_ON_OFF");
    #IEC_Timer_0_Instance_1(IN := "PULSE_ON_OFF",
                            PT := #TIME_ON,
                            Q => "Tag_1");
END_REGION

REGION Piston Control
    "OUT_EMBOLO" := "ENABLE" & "PULSE_ON_OFF";
END_REGION

REGION Piston Position
    #IEC_Timer_0_Instance_3(IN:="OUT_EMBOLO",
                            PT:=T#65,
                            ET=>#TIME_OUTPUT);
    "PISTON_POSITION" := #TIME_OUTPUT / 14;
    #IEC_Timer_0_Instance_4(IN:=NOT "OUT_EMBOLO",
                            PT:=T#65,
                            ET=>#TIME_OUTPUT_1);
    IF ("OUT_EMBOLO" = 0)  THEN
        "PISTON_POSITION" := (1000-#TIME_OUTPUT_1)/14;
    END_IF;
    IF ("CONTACT_A"=0)OR("CONTACT_B"=0) THEN
    "PISTON_POSITION" := 80;
END_IF;
IF ("PISTON_POSITION" < 0) THEN
    "PISTON_POSITION" :=0;
END_IF;

END_REGION

REGION Lamp ON-OFF
    IF ("CONTACT_A" = 0) OR ("CONTACT_B" = 0) THEN
        "LAMP_ON" := 1;
    ELSE
        "LAMP_ON" := 0;
    END_IF;
END_REGION
```

Fig. 10: FB1

Pulse Generator: A pulse generator was designed by using two IEC TON Timers. The ON / OFF interchange duration is regulated by the SCADA.
Piston Control: When SCADA gives the order 'ENABLE' and the pulse generator 'ON', the piston is ordered to go downward. As a result, when there

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

is 'ENABLE' signal from SCADA, the piston implements a back-and-forth motion.
Piston Position: Depending on how long the piston command is activated, the corresponding value in the 'PISTON POSITION' variable is generated in order to show the position of the piston in SCADA.
Lamp ON-OFF: If one of the input contacts of the button is lost, then it activates the 'LAMP ON' variable in order to show how the button was pressed in SCADA.

3.3 PLC - Inputs Control

The following procedures were implemented to monitor the inputs in PLCs.

3.3.1 Deactivation of delay filter

To avoid interference of installing to an automation system, the inputs in PLC have the ability to initiate an activation delay for one channel or for a pair of channels.
The interference pulses, of whose pulse is less than the specified input delay (ms), are ignored and thus are not visible in PII of the PLC.
For the purposes of this experiment, that delay was completely deactivated in order to achieve an immediate response as the one of the PII in PLC.
To be noted, that the experiment was carried out in the laboratory, where there is no electromagnetic noise as there is in an industrial environment.

Fig. 11: Input Parameters

When the Input Delay is deactivated, it is very possible to read the response of an input in time less than 1m/s.

3.3.2 Activation of interrupt procedure

Because the response of an input in the CPU of a PLC needs to be read as immediately as possible, the Hardware Interrupt procedure is then activated. With the Hardware Interrupt procedure the input in a PLC routine is read immediately when the input state changes. In this way, it was avoided to be carried through the Main routine of its cycle, because that would mean additional delay even for unstable time intervals. [3]

Fig. 12: Hardware Interrupts

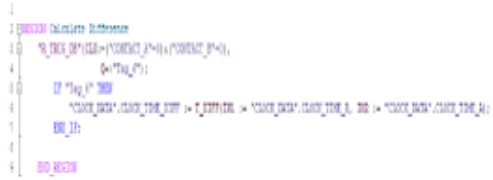
The figure above shows the activation of the Hardware Interrupt at Falling Edge, in other words a transition to the Interrupt routine the moment the Input transmission goes from 1 to 0. The contacts used to the button are Normally Closed. An alternative Interrupt routine is performed for each Input. The following code runs in each Interrupt routine:

```
1
2 REGION Read CPU Clock
3     "CLOCK_DATA".CLOCK_TIME_OB_A := #DATE_TIME;
4 END_REGION
5
6 REGION Time A
7     "CLOCK_DATA".CLOCK_TIME_A := #DATE_TIME;
8 END_REGION
9
```

Fig. 13: Read PLC Clock

Read CPU Clock: The Real Time Clock of a CPU is read.
Time A: The value is assigned by the Real Time Clock of the CPU to the variable: "CLOCK_DATA". CLOCK_TIME_A. That command is performed when the Interrupt routine is activated, in other words when the Input is deactivated. With this method, the Real Time Clock of the CPU is stored in the variable above.

3.4 PLC - Difference record



To calculate and record the deactivation time difference of two Inputs the following procedure was implemented in the pattern FB2 (Function Block):

Fig. 14: FB2

Calculate Difference: When in both of the Inputs there is 0 state, the time difference of the response between the two Inputs is calculated (in ms). The accuracy of the calculation, with the specific

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

Configuration in the experiment, can be per 1 ms. This accuracy, as will be ascertained below, is more than enough for the needs of the experiment.

3.5 PLC - Push button count

Button response does not remain the same, not only over time, but also after extreme usage, so that must be acknowledged by the user for more effective results.

To check the response of the button contacts whether it is similar or different after a few hundred clicks, the pattern FB3 was developed (Function Block). With an FB3 pattern, the pushes of the

```
REGION Push Button Count
    "IEC_Counter_0_DB".CTU(CU:=("CONTACT_A" = 0) OR ("CONTACT_B" = 0),
                           R:="RESET_COUNT",
                           PV:=1000000,
                           Q=>#COUNT_TEMP,
                           CV=>"CLOCK_DATA".COUNTER_PUSH_BUTTON);
    IF ("RESET_COUNT") THEN
        "RESET_COUNT":= 0;
    END_IF;
END_REGION
```

button are counted.

Fig. 15: FB3

Push Button Count: When one or both of the Inputs are zero (0) the value of the counter increases. If the "RESET_COUNT" variable has substance 1, then the counter is eliminated - this variable is then activated from the SCADA, when for example a new button is placed and the experiment starts again.

3.6 Scada - Configuration

The implementation of this experiment requires a reliable user interface, along with the equipment, as well as an automated recording procedure of the results. For this reason, WinCC was used, as it is one of the most reliable SCADA being used within the industrial environment. To monitor the experiment through WinCC, the following were (briefly) implemented:

- Creation of WinCC-PLC communication and definition of the necessary variables (Tag).

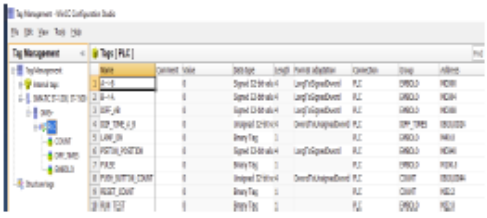


Fig. 16: Tag Management

- Graphical interface development data to display and operate the system.

Fig. 17: Screens

- Creation of records in SQL Development to the graphical interface data in order to display and operate the system.

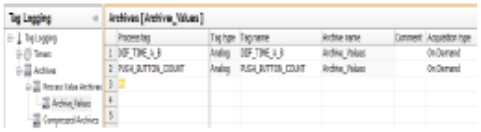


Fig. 18: Tag Logging

The recording of the time difference among the two Inputs is not implemented at a certain time but at the moment when both Inputs are lost from the PLC.

3.7 Input response experiment

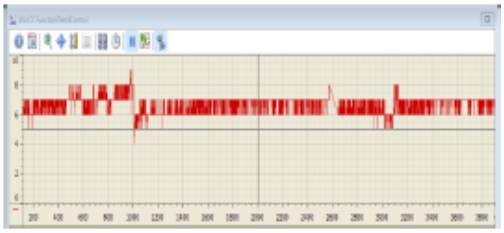
For more accurate conclusions, many different trials were tested with this experiment having different factors each time. Each trial tested is analyzed below.

Trial 1

For this trial:

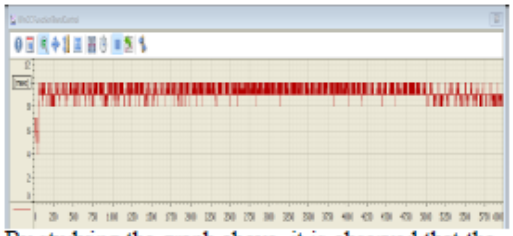
- A new button with two Normally Closed contacts was applied.
- The pressing speed of the piston was adjusted to 10cm/sec.
- The piston is positioned so that it does not push towards the center of the button but towards the edge.
- 3.800 samples were recorded.

The graph below illustrates the contact response of the button.



WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

Fig. 19: Trial 1 Report



By studying the graph above, it is observed that the response time is 4-9 msec, with an average value of approximately 6,8msec.

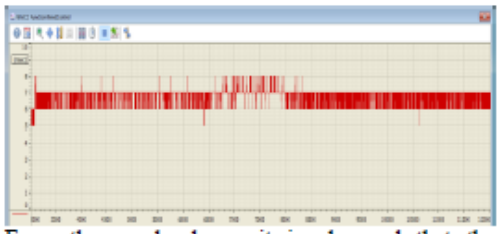
Trial 2

For this trial:

- The same button was used (two Normally Closed contacts).
- The pressing speed of the piston remained stable (10cm/sec).
- The piston was positioned in a way so that it pressed the middle of the button.
- 9.000 samples were recorded.

The graph below illustrates which was the contact response of the button.

Fig. 20: Trial 2 Report



From the graph above, it is observed that the response time is 5-8 msec, with an average value of approximately 6,5msec.

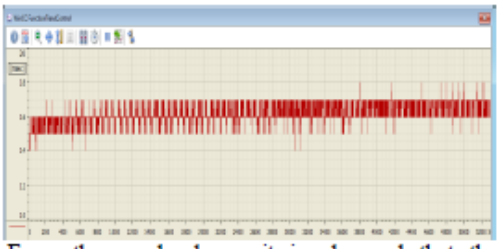
Trial 3

For the third trial:

- A new button was applied with two Normally Closed contacts.
- The pressing speed of the piston was adjusted to 5cm/sec.
- The piston was positioned in a way so that it pressed the center of the button.
- 6.000 samples were recorded.

The graph below illustrates what was the contact response of the button.

Fig. 21: Trial 3 Report



From the graph above, it is observed that the response time is 8-10 msec (except from the first almost 100 samples when the push of the piston was quick), with an average value of approximately 9,2msec.

Trial 4

For the fourth trial:

- A new button was placed with two Normally Closed contacts.
- The pressing speed of the piston was adjusted to 3cm/sec.
- The piston was positioned in a way so that it pressed the center of the button.
- 5.500 samples were recorded.

The graph below illustrates what was the contact response of the button.

Fig. 22: Trial 4 Report

By studying the graph above, it is observed that the response time is 14-18 msec with an average value of approximately 16,3msec.

The results of the trials above are the following:

- The difference in response time of the contacts on a button with a quick press, does not exceed the 10msec and with a slow press it does not exceed 20 msec.
- Even after 13.000 pushes, the contacts have the same bearing response.
- The response time of the contacts does not differ much when the push occurs in the canter or at the edge of the button.
- The response time of the contacts does not differ much when the push occurs for a short period of time e.g. per 2 sec or per 1 min.

From all the various tests which were performed, it is observed that the difference in response time of the contacts is generally stable, even after several thousand presses. It should be noted that by using these elements, like the Stop Emergency, are elements which are not often activated during the producing process but only when we have an issue. It has been observed that even days could pass and these elements would not have been used at all. This means, if a machine has approximately a 10-15 year old life cycle, a Stop Emergency is very likely to be

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

activated even less than 5.000 times. Of course, for the reliability of the item (e.g. Stop Emergency) its construction materials play a very important role. An item made with good materials endures time, high temperatures, humidity, vibrations etc, which is something that most manufacturers now consider.

4 Conclusion

After the tests were carried out, it is observed that the response of two different contacts of a button can be detected through a Basic PLC, without any additional, special hardware. The response time difference is low, with an average value of 10 msec. If this difference is greatly increased e.g. at 300 msec, it automatically means there is a problem in the contacts of the button. This problem is certainly easy to be detected, so the production can be stopped safely. In most Safety cards the response time difference between the two contacts is adjusted at 500 msec and these contacts monitor this difference with their own machinery in order to remove any possible problems. There are many old automation systems with slow processes that are still operating and due to their structure or their production rate are practically prohibited to upgrade their Safety operation. Today in most cases, those systems are completely replaced by new ones (with a high cost). According to everything mentioned above, it is concluded that by using specific CPU routines of a PLC in automation systems (especially existing ones) increases the reliability of the operation as well as the security, without any further costs, either in money or in implementation time. The final conclusion which emerges from the experiment is that by using Basic PLCs and particular routines, automation function reliability can be increased, without any additional equipment. This means, without extreme costs either in money or in implementation time, that even existing automation systems can have a more reliable and safe operation without being replaced by new systems, as PLC manufacturers recommend.

ACKNOWLEDGMENTS

All authors would like to thank the University of West Attica for the financial support provided to them to undertake this research project.

References:

[1] EN ISO 12100 (Safety of machinery - General principles for design - Risk assessment and Risk reduction).
[2] IEC 61508-3 (Functional Safety of Electrical/ Electronic/Programmable Electronic Safety – Related Systems).
[3] https://www.tuv-sud.co.uk/uploads/images/ 1397220180236544250395/sil-or-pl.pdf.
[4] IEC 61511 (Safety instrumented systems for the process industry sector).
[5] EN ISO 13849-1(Safety of machinery - Safety-related parts of control systems).
[6] IEC 62061 (Safety of machinery).
[7] S7-1500R/H redundant system, System Manual, 11/2019, A5E41814787-AB
[8] https://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/safety-evaluation-tool/Pages/Default.aspx.
[9] https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp
[10] Programming Guideline for S7-1200/1500, ID: 81318674, V1.6, 12/2018.
[11] Working with WinCC, System Manual, A5E45518672-AA, 09/2018.
[12] STEP 7 and WinCC Engineering V16, System Manual, 11/2019.
[13] Tham M.T., Warwick K. "Fail-Safe Control Systems" ISBN 9789401066778.
[14] D. Smith, K. Simpson, "Safety Critical Systems Handbook – A Straightforward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards", 3rd Edition, ISBN 9780080967813.
[15] M. Punch, "Functional Safety for the Mining Industry – An Integrated Approach Using AS(IEC)61508, AS(IEC)62061 and AS4024.1." (1st Edition, ISBN 9780980766004.
[16] H. Hartmann, H. Thomas, E. Scharpf, "Practical SIL Target Selection - Risk Analysis per the IEC 61511
[17] Safety Lifecycle", ISBN 9781934977033.
[18] https://download.beckhoff.com/download/document/automation/twinsafe/applicationguidetwinsafeen.pdf
[19] https://plcopen.org/system/files/downloads/plcopen_safety_part_1_version_2.01.pdf
[20] M. Medoff, R. Faller, "Functional Safety - An IEC 61508 SIL 3 Compliant Development Process, (Third Edition)" ISBN 9781934977088.

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2020.15.74

[21] Dave Macdonald "Practical Industrial Safety, Risk Assessment and Shutdown Systems", ISBN 99780750658041.
[22] https://www.leuze.com/media/assets/archive/UM_MSI-T_en_700948.pdf
[23] https://support.industry.siemens.com/cs/attachments/109444336/manual_safety_relays_3SK2_en-US.pdf?download=true
[24] https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=33003879_K01_000_07.pdf&p_Doc_Ref=33003879K01000.

Contribution of individual authors to the creation of a scientific article (ghostwriting policy)

E. Theocharis has construct the demo unit and implemented the PLC - SCADA code.
M. Papoutsidakis carried out the simulation and the optimization of the experiments.
A. Sort has organized and executed the experiments.
C. Drosos was responsible for the Reports and the requirement for their repetition.

Sources of funding for research presented in a scientific article or scientific article itself

All authors would like to thank the University of West Attica for the financial support provided to them to undertake this research project.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

Paper 3 Low-Cost Solution for Adding Safety Functions to Programmable Logic Controllers (PLCs)

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

Low-Cost Solution for Adding Safety Functions to Programmable Logic Controllers (PLCs)

EFSTATHIOS THEOCHARIS[1], MICHAIL PAPOUTSIDAKIS[1], ANDREW SHORT[1],
KONSTANTIA ZISIMOU[2]
[1]Deptartment of Industrial Design and Production Engineering,
University of West Attica,
Thivon 250 & P. Ralli, Egaleo,
GREECE

[2]Programming Teacher in a High School,
10th Gymnasio Nikaias, Artemidos 25,
Nikaia,
GREECE

Abstract: - Increasing requirements in automation and production make control systems more complex and vulnerable to failure. Breakdowns can cause delays in production, material damage, and above all, work-related accidents. For this reason, directives and legislation have been created at the country, European Union, and global levels that define the essential safety and requirements of industrial equipment. Guidelines must be observed by those involved in the design, supply, purchase, or use of industrial equipment in the European Union and several countries outside the European Union. Some guidelines (CAT, SIL) are created to ensure their safe operation in case of failure of both the hardware and the software. For a reliable operation of a fail safety system together with a system operating at SIL2 or SIL3, it must have Safety hardware and software.

Industrial equipment manufacturers are incorporating security features into a variety of devices. Depending on the Safety Integrity Level (SIL) requirements, these features can be used during the design phase to increase safety in the event of failures or malfunctions. With proper design, the process as well as its environment (including people) can be protected by entering a controlled safe state. Manufacturers have approached this problem in a number of ways, including adding redundant Central Processing Units (CPUs), using special hardware to interface input and output signals, and developing secure network protocols for communication. Unfortunately, these features cannot be added to existing machines, at least without upgrading some hardware. As the associated costs lead to slower adoption, manufacturers rely on previous work to support certain security features, notably CPU debugging. This is implemented in the form of software libraries that operate at a low level (logic gate), designed to run on older hardware (PLC) so that they can offer an increased level of security. This study analyzes the required guidelines and legislation that must be followed for the safe operation of a production unit. It describes the mechanisms that basic and specialized PLC systems utilize to ensure the safety of an automation system. The authors have developed algorithms to record behavior measurements of electronic equipment. By further analyzing the results, it is concluded that basic equipment can be reused in these systems to provide safety functions, at the same time conserving both cost and time.

Key-Words: - Mean Time Between Failure (MTBF), Safety Integrity Level (SIL), Safety Relay (SR)

Received: November 25, 2022. Revised: July 23, 2023. Accepted: August 20, 2023. Published: September 26, 2023.

1 Introduction

Machine manufacturers are increasingly focusing on improving the safety aspects of machinery and at the same time many countries strengthen the legislation and hold them accountable in case of injuries. For this reason, a plethora of ISO and IEC standards are available today. These standards simplify trade as they usually conform to the legislation of most countries.

In the field of industrial automation systems, Programmable Logic Controllers (PLCs) are commonly used to coordinate complex tasks and control machinery in an autonomous fashion. PLC manufacturers are building specialized products to allow their use in safety-critical applications or in industries where downtime is very expensive. These

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

new products increase their reliability by adding redundant systems to help self-diagnose a malfunction among others in a sensing device (e.g., a peripheral input device), an external safety component (such as an emergency stop button), or the CPU itself.

These technologies are still relatively new, novel, and expensive. For this reason, they are only adopted in newer, more expensive equipment. Older industrial machinery could have possibly been built with more relaxed safety standards. It is also a possibility that current owners of older but still expensive machinery are reluctant to upgrade their equipment with newer hardware due to the associated costs with the hardware, programming, design, and installation.

The authors believe that current PLCs used in older equipment (and do not currently conform to newer safety standards) can support at least a subset of the newer features such as diagnosing routines with no hardware modifications. This research is motivated by the fact that current owners of older machinery would be willing to improve their safety scores by only applying minor software updates.

As part of ongoing research in this area, the authors have already proposed a method that allows current non-fail-safe devices to detect external sensor failure by employing techniques in software and have shown that the advantages are comparable to those of the newer fail-safe devices. Extending this research, the paper proposes a software algorithm that will allow current legacy software to be able to detect hardware failure at the CPU level, for the executing program to be able to shut down in a safe manner, and to predict hardware faults of PLC itself.

Researchers are actively figuring out techniques that allow PLC-operated machinery to function in more safe and reliable ways. The authors of a paper have proposed a solution for formal verification that uses mathematical models of the specific application scenario to offer improvements in both fail and non-fail-safe PLCs, [1], [2].

Another approach discussed by researchers aims to detect safety violations (caused by faults or attacks) by comparing data sets of event sequences and the time of occurrence with data traces collected beforehand in Industrial Control Systems (ICS).

Furthermore, researchers are studying the advances of the new safety devices, in terms of the diagnostic capabilities, implementation strategies, and metrics such as response times of these routines, [3], [4].

Although the motivation of the research presented in this paper is in line with other work presented above (i.e., to study and improve upon the safety operation of devices), the approach discussed here differs in the following ways:

a) The solution extends previous work to directly port features of newer (fail-safe) PLCs to older legacy hardware.

b) The algorithm does not depend on each specific application scenario.

c) An application use case has been included to present the function of the algorithm.

The rest of this paper is organized as follows: Section (2) analyses current strategies for improving safety and downtime records in terms of relevant standards. Section 3 describes the approach that current PLC manufacturers are using to detect hardware failures in modern fail-safe equipment. Section 4 proposes a solution in the form of an algorithm that is able to run on legacy devices and present similar advantages as the newer more expensive products. The section also describes the experimentation setup. Finally, Section 5 summarizes the results of the presented approach.

2 Redundant Systems

The redundant automation systems are commonly used to offer greater availability. The objective of these systems is to reduce the possibility of production interruptions, the protection of individuals, the protection of the surrounding environment, and the safe termination of production. In very critical applications such as refineries, airports, and nuclear plants, such systems are required not only to avoid the cost associated with stopping production but also to prevent accidents.

Software Redundancy

In many applications, the requirements for fault-tolerant cannot be justified. Simple software mechanisms are sufficient to allow a failed process to continue on a substitute system if an error occurs. These mechanisms can be applied to control processes that can tolerate larger transition delays to a surrogate system, e.g., in waste-water plants, water treatment plants, or traffic streams.

Hardware Redundancy

Hardware Redundancy consists of two subsystems that are synchronized via fiber optic cables.

Both subsystems create a fault-tolerant automation system that works with two channels and is based on the principle of active redundancy. Active redundancy means that all redundant resources are continuously running and simultaneously participating in the execution of the control task. This means that the programs on both CPUs are

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

identical and are executed synchronously by the CPUs.

To separate the two subsystems, the traditional expressions "master" and "reserve" are used for two-channel fault-tolerant systems. The reserve always processes events in sync with the master and does not wait for any errors from the master to start processing. The distinction made between the master and the reserve CPU is very important to ensure reactions in case of errors. For example, the reserve CPU can go into STOP when the backup link has an error, while the primary CPU remains in RUN mode.

The higher the risks and the cost of abruptly terminating the production, the more beneficial it is to use such systems, [5].

The evaluation of the Redundant systems is usually based on reliability and availability parameters. A commonly used reliability measurement is the MTBF (Mean Time Between Failure). This can be statistically analyzed on the basis of the parameters of the ongoing operation systems or by calculating the failure rates of the individual components.

The Mean Detection Time (MDT) of a system is determined by the times below:

- Time required to detect the error.
- Time is required to find the cause of the error.
- Time is required to encounter the problems and restart the system.

The MDT system is calculated based on the MDT of the individual components in the system. The structure in which the components form the system is also a part of the calculation.

2.1 Correlation between MDT and MTBF

The MDT value is of high importance for maintaining the quality of the system. The most significant factors are:

- Qualified personnel
- Efficient logistics
- High-performance tools for debugging and recognizing identification
- A good repair strategy

Figure 1 shows how the MDT depends on the factors mentioned above.

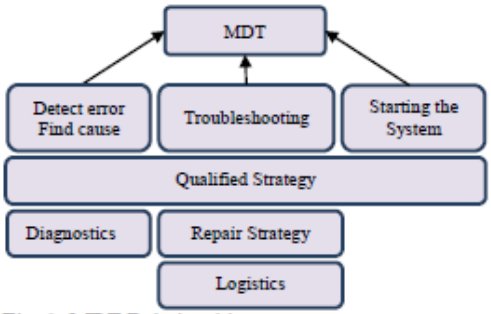


Fig. 1: MDT Relationships

The MTBF, or Mean Time Between Failures, is a critical metric used to assess the reliability of a system. It is calculated by dividing the total operational time by the number of failures that occur during that time period. Figure 2 shows the parameters included in the MTBF calculation of a system, [6].

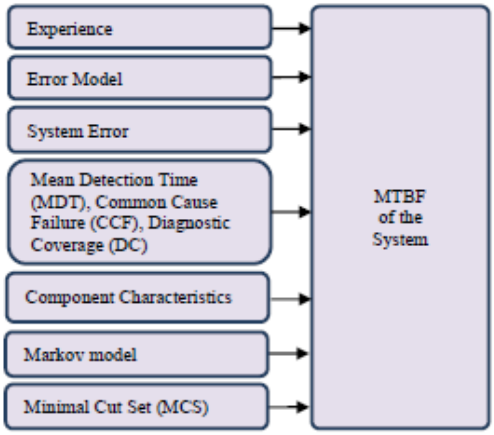


Fig. 2: MTBF

The analysis is based on the following assumptions:

- The failure rate of all the components and all the calculations is based on an average temperature of 40°C.
- All the spare parts are locally available, to prevent extensive repair times due to the lack of spare parts. This maintains the MDT element to its minimum.
- The MDT of individual spare parts is 4 hours. The MDT of the system is calculated based on the MDT of the individual components plus the structure of the system.
- The MTBF of the components meets the standards:

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

- SN 29500 (This prototype is compatible with MIL - HDBK 217 - F)
- IEC 60050, [7]
- IEC 61709, [8], (These calculations are made by using the diagnostic coverage of each component)

• Depending on the formulation of the system, the CCF coefficient ranges between 0,2% and 2%.

By using the Redundant units, the MTBF is greatly increased. They contain high-quality self-monitoring features that allow the identification of almost all errors with a reliability of at least 90%. Reliability in autonomous operation is defined by the corresponding failure rate. Reliability in Redundant operation is defined by the failure rate of the relevant components or otherwise "MTBF". The combinations of any failed components that cause a system failure are described and calculated using Markov models.

Availability is the probability that a system is operating at a given point in time. It can be improved by using Redundant I/O units. The Redundant components are arranged so that the functionality of the system is not affected by the failure of an individual component. The availability of a system is expressed as a percentage and is defined by the average time between failure (MTBF) and the average MDT repair time, [9]. The availability of a two-channel fault tolerance system (1 out of 2) can be calculated using the following formula as seen in Figure 3.

$$V = \frac{MTBF_{1v2}}{MTBF_{1v2} + MDT} * 100\%$$

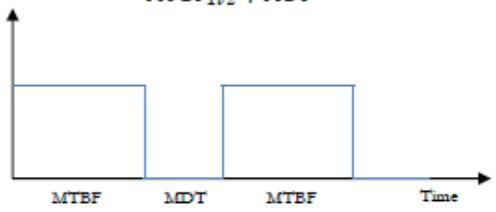


Fig. 3: Availability

A control system can have CPU Redundancy, Network Redundancy, I/O Redundancy, Sensor Redundancy, and PID bumpless Switchover capabilities. There are two similar CPUs in a Redundant system that execute the same code at the same time. These two CPUs synchronize through a special interface, often by means of a redundant connection. The system includes synchronization units that support Hot-Swapping, so in case one of the CPUs fails, the other CPU retains the procedure control and the production process can resume without any anomalies. For security and functionality purposes, a CPU can be up to 10 meters away when the synchronization units communicate through copper and up to 10km when they communicate through optical fiber cables. A standard configuration of a Redundant system is shown in Figure 4.

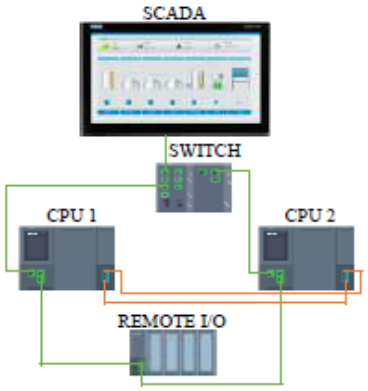


Fig. 4: Redundant Systems PLC, [10], [11]

The system consists of one Supervisory Control and Data Acquisition (SCADA), used as the interface for the machine operator, two CPUs with Redundant functions, an interface module (usually Inputs and Outputs) to operate the machine, and the required contact cards. The operation control of the machine is implemented as follows:

The two CPUs communicate with each other with a double connection (for Redundant purposes) through optical fibers. The communication is required so that one CPU can sense the state in which the other CPU is and also for their synchronization. That means that the execution of the machine's control code is always synchronized. One CPU is always set and operated as Master and the other one as Standby. The Master CPU is the one which controls the elements of the machine through output cards. Both CPUs scan the input cards, process them individually, and then determine what step of operation the machine is in. When the Standby CPU detects an error on the Master CPU, then it automatically goes into Master mode and assigns the other one into Standby mode. The control-switching time from one CPU to the other is usually less than 5ms. Although the SCADA communicates directly with both CPUs, any updates and operations are implemented by the Master CPU, [12], [13], [14].

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

Efstathios Theocharis, Michail Papoutsidakis,
Andrew Short, Konstantia Zisimou

3 Safety Technology

Safety Technologies have been developed for the safer operation of the machine, [15], [16], [17], as well as to avoid any accidents and deterioration, with the most basic ones being: (1) Contractual Safety Technology, and (2) Integrated Safety Technology.

3.1 Contractual Safety Technology

The safe operation of the machine is being monitored by a Safety Relay. Contacts of the Stop Emergency buttons, Safety Doors, etc., are wired to the Safety Relay and regardless of the commands given by the PLC automation system, the machine switches to Safety mode once a Stop Emergency has been pressed or a Safety Door has opened.
The wiring as well as the architecture of the protection functions are applied in accordance to EN 61508, [18], in SIL 3 or according to EN 954 in Cat. 4: The Stop Emergency button and the Safety Door positional switches are connected by two channels in the Safety Relay, [19], [20]. Two contacts are connected in series and are used to monitor the safe operation of the machine, [21].

3.2 Integrated Safety Technology

In complex automation systems, the safety functions of machinery are controlled by a Safety PLC (instead of a Safety Relay) that usually dictates an alternative way of safely stopping production, according to the issue arising each time, [22], [23], [24]. There is a separate safety program and special Safety Input and Output units in the Safety PLC, [1]. As soon as a wiring error occurs the emergency button is pressed or the safety door opens, the machine goes into Safety mode. The wiring of the actuators and the sensors related to safety are being monitored by these special input and output units of the PLC.

According to SIL 3 (EN 62061) Cat.4 (EN 954), the wiring as well as the architecture of the protection functions is similar to that of the Safety Relay. Stop emergency and safety doors are connected to the special PLC cards through two carriers, [24].

Safety Integrated Technology is the completely integrated security concept for automation and power units with proven technologies and automation systems used to safely operate the production. Additionally, it covers the entire security chain with sensors and actuators to the controller, including the security-related communication over the standard networks, [25]. Besides the automatic operation of the production, the PLC also undertakes its safe operation, [26]. In addition to ensuring reliable safety functions, Safety Integrated Technology also offers a high level of flexibility and productivity, [27].

The integration of a safe and automatic operation in a PLC has the following significant advantages:

- Greater flexibility than the electromechanical solutions
- Wiring reduction
- Only one CPU is required due to typical and safety program coexistence
- Simple communication between the typical and safety program
- Less implementation time of application

For dual operation (Safety and autonomous) of the system, the PLC utilizes a CPU that simultaneously executes the program for both the autonomous and safety operation (Figure 5). It provides standard Input and Output cards for the autonomous operation and special cards for the Safety functions. The main difference between Safety and standard cards is that the Safety cards have been constructed with two channels internally, two integrated processors monitor one another and automatically control the input and output circuit. In case of an error, they set the Safety card in safe mode. The digital Safety input cards acquire (by detecting) the signal status of sensors that are related to a safety status (e.g., emergency stop button pressed), perform short circuit and cross-circuit tests, as well as inconsistency analysis, and send the corresponding messages to the CPU. The digital Safety output cards are suitable for deactivation tasks and have additional capabilities to detect short-circuits of the actuator.

For the verification of the reliability of the outputs, tests are carried out at certain intervals. The tests are usually repeated every 1,000 sec when we don't want to have rapid wear of the actuators, and every 100 secs for fast fault detection. Retry time is the maximum time after the output is turned off that a feedback signal should be detected before it is declared as a short circuit fault. The repetition time must be set long enough, especially when switching capacitive loads, to allow the switching capacitance to discharge within the repetition time.

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

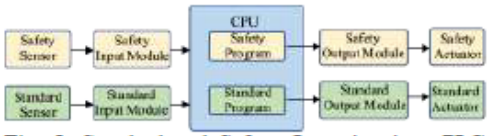


Fig. 5: Standard and Safety Operation in a PLC, [28]

The standard and safety programs are both developed in the same programming environment and because they co-exist in the same CPU, they can communicate with each other using variables without one affecting the other in case of an issue, [29].

3.3 Safety Program Operation

Safety-related CPUs work according to the principles of redundancy and diversification, which allow the implementation of safety systems with only one CPU and one processor. With the security program, the user programs the logic of the system's safe operation, and the operating system automatically creates additional blocks based on "differentiated" logic compared to the user's program as well as "differentiated" operators and functions.

The two parts of the security program are run sequentially and the results are compared. If an error occurs, the CPU reacts and puts the system into a safe state. The operating system also creates system blocks that can be used for example to manage Safety communication.

Error checking can help in the following circumstances:

- Old messages that have not been updated are sent again at the wrong time.
- A message is not received or recognized.
- A message referring to an unknown source is entered.
- The specified sequence (e.g. CRC, time references) of the messages of a particular source is incorrect.
- Messages can be corrupted due to errors at a bus node, i.e. errors in the transmission medium or due to mutual interference of messages.
- Messages can be delayed beyond the allowed arrival time, e.g. as a result of errors in the transmission medium, overloaded connection cables, mutual interference, or bus nodes (devices) sending messages in such a way that services are delayed or unrecognized.
- A message originating from a valid source is additionally inserted. Thus, a non-security-related message may be received by a security-related device, which then classifies it as security-related.
- FIFO (First-In-First-Out) error, the correct order of data is not observed.

In the following example, we will demonstrate the operation of a safety function while it is executing inside the CPU. The internals of the function are shown in Figure 6. A and B as used as the input signals. The objective is to run a logic operation on the inputs while at the same time detecting any CPU anomalies. If the result of the logic operation is (Boolean login) TRUE, and there are no faults detected, then the normal operation can resume. In any other case (i.e., the result of the logic operation is FALSE, or CPU malfunction is detected) the PLC should halt the execution of other instructions. In order to detect CPU faults, the logic operation is executed twice. First, the normal logic operation is carried out and its output is kept temporarily (variable C shown in Figure 6). Then, a suitable inverted logic operation is constructed which in turn results in output D. This inverted logic is implemented in safety by PLC manufacturers using certified mechanisms without the possibility of intervention by the user, [30]. The two intermediate outputs (C and D) are then compared and are expected to contain the same value. In the presence of a fault, it would be extremely unlikely that both functions would present the same erroneous response, therefore eradicating false negatives. In case the two outputs are different, the CPU enters safety mode status.

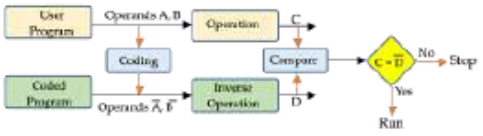


Fig. 6: Safety Operation

In the following example (Figure 7), we demonstrate how we can verify the output of a software OR gate using an inverse operation (AND gate). By comparing the output of two separate computation results, we add a layer of reliability and trustworthiness to the CPU results. Consequently, the CPU is able to detect whether it has malfunctioned and can disable itself considering that it is safer to stop a process rather than continue running it with faulty equipment. We assume that in this case, the user code intends to run an OR instruction and that A and B have values of 1001 and 1010 (in binary representation) respectively.

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

The expected output C of the OR operation should be 1011. In this scenario, the inverse operation used is an AND gate. The first step is to compute the inverse of A and B ($\overline{A}, \overline{B}$), which are 0110 and 0101 respectively. The second step is to compute the output of the AND gate D, which is 0100. Last, we need to compute the inverse of the output D ($\overline{D}$) which turns out to be 1011. In this case $C = \overline{D}$ so the CPU would decide to continue running. In any other case, it would enter a stopped mode.

Fig. 7: Safety Operation Example

4 Development of a Fail Safety Algorithm for use in basic PLC Hardware

The solutions demonstrated in the previous section require specialized hardware and expert knowledge, factors that prohibit their wide adoption, especially for smaller projects. For these reasons, an algorithm was designed and developed which can be used with ease and without any particular expertise, that leads to the increased reliability of an automation system.
The concept of the proposed solution is that by executing a logic operation multiple times may lead to the detection of a transient fault. Once the operation has finished executing multiple times, its output of each iteration is compared to the previous one. If the output of each iteration is not identical, the CPU would stop further code execution. Figure 8 illustrates the operation of the algorithm.

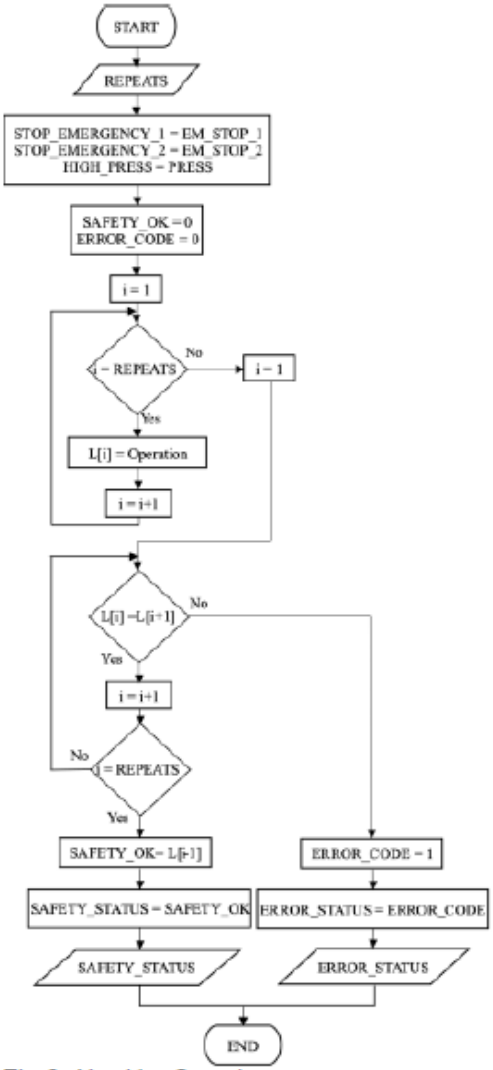


Fig. 8: Algorithm Operation

Algorithm Description
The operation of the algorithm is as follows:
1. The desired code execution iterations (n) is entered.
2. The variables (inputs and outputs) of the code are entered (IN1, IN2, OUT1, OUT2, etc.).
3. The code is executed 'n' times and in each execution the results of the code (Outputs) are stored in a table.
4. After the execution of the code, the results found in the table are checked and if they are the same then they are applied to the respective outputs. In

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

Efstathios Theocharis, Michail Papoutsidakis,
Andrew Short, Konstantia Zisimou

any other case, an error message is output and the system switches to safe mode.

4.1 Overview of the Experiment

For the evaluation of the algorithm, an experiment was carried out using industrial equipment as the automation (Figure 9).

PLC

Fig. 9: Experiment Equipment

The CPU consists of a SIEMENS CPU 511, one of the smallest (in terms of CPU capabilities) of the mid-range provided by SIEMENS, and has built-in input and output signals. The safety function was applied to an automation system used for pallets filled with boxes. The proposed algorithm in the previous section was incorporated into a pre-existing pallet stacking process. The safety functions of the system utilize two emergency stop buttons (Normally Closed) as well as the pressure feedback from the piston (by means of a pressure switch). In case of an obstacle in front of the piston area, the pressure will increase above a pre-set limit and will in turn activate a digital input (Normally Closed). As long as the emergency stop button is not pressed and the pressure switch has not been activated, the safety algorithm should allow the execution of the code responsible for pallet stacking and should energize the system's outputs responsible for actuators. In any other case, the actuators should become inactive and the machine operation would consequently stop. Figure 10 shows the machine's components.

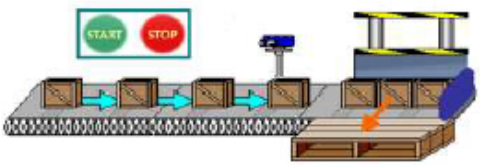


Fig. 10: Disposition of the Machine

For the implementation of the experiment, the TIA V16 program was used from which the FB10 routine (Function Block) was developed in SCL language. The code of the routine and its explanation are given below.

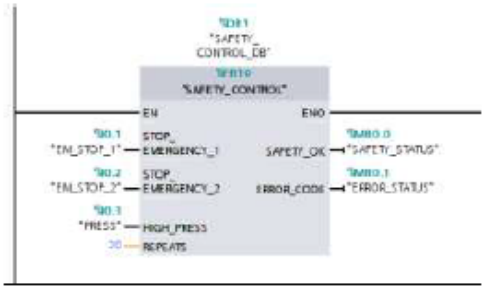


Fig. 11: OB1

OB1 is the Main Block which is executed by a CPU and contains the user code. The newly added function (FB10 shown in Figure 11) is declared along with the addresses of the actual Inputs and Outputs.

Please note that in the following algorithm, all variables other than the ones explicitly mentioned are temporary, have a start value of 0, and are released from system resources when the algorithm ends its operation. It is also worth mentioning that the algorithm is not able to determine the origin of the fault (either of the digital inputs or the CPU) but only the presence of the anomaly.

The number of repetitions can be configurable. A higher number of repetitions increases the reliability at the cost of processing overhead. In terms of the "Big O" notation, the algorithm executes in linear time O(n), where n relates directly to the number of repetitions.

Algorithm 1 – Checking for the existence of CPU faults or Input data mismatch.
Inputs – STOP_EMERGENCY_1, STOP_EMERGENCY_2 are inputs from the external safety switch (Boolean logic), HIGH_PRESS is the output of the pressure switch on the piston (Boolean logic), REPEATS configures the number of repetitions (configurable).
Outputs – SAFETY_OK = 1 when the safety checks are successful. Similarly, ERROR_STATUS = 1 under faulty scenario.

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

Fig. 12: FB10

The implemented source code in Structured Controled Language (SCL) is depicted in Figure 12. The routine parameters are initially stated in the parameter table. Additionally the code is categorized in the following logical sections:
Initial: This is where the iteration variables are initialized.
Check Inputs: This is where the operation of production is checked if it is safe or not.
Check Safety Result: This is where we check if the Safety status was implemented correctly.

5 Conclusion

The paper builds upon earlier research regarding methods for executing safety routines on legacy hardware and describes the operation of current fail-safe systems in the context of PLCs. More specifically, a high-level approach has been presented that allows monitoring the PLC itself while it is running safety critical routines inside the user program. The routines allow for the creation of PLC algorithms that replace low-level logic operations that in addition to the calculation output are also able to decide whether the CPU is faulty and consequently safely stop execution. The operation relies on an approach of calculation repetition and inverse operations, in effect sacrificing some CPU resources for the ability to be able to self-diagnose some types of CPU-related hardware failures. Furthermore, the proposed solution has been implemented in an actual pallet stacking machine to collect results and provide implementation information. The research concludes that legacy PLC hardware can make use of our proposed approach to offer advantages such as fault detection capabilities and consequently increased safety during the automation process without any additional hardware.

Most importantly, due to the minimum impact of changes involved, it is anticipated that the proposed solution can increase adoption and therefore the safe operation of existing machinery since it requires less costs and downtime. As further work, the authors of the paper will examine the impact of the execution of such routines in terms of CPU performance overhead as well as the feasibility of the execution of distributed systems (for systems requiring a higher level of redundancy).

Acknowledgments:
All authors would like to thank the University of West Attica and specifically the Post Graduate Program of Studies (MSc) "New Technologies in Shipping and Transport", for the support provided to them to undertake this research project.

References:

[1] K. Rástočný, J. Ždánsky, J. Balák and P. Holečko;, "Effects of diagnostic on the safety of a control system realised by safety PLC", vol. 7512118, 2016.

[2] Dániel Darvas, István Majzik and Enrique Blanco Viñuela, "Formal Verification of Safety PLC Based Control Software", *Springer*, vol. 9681, 2016.

[3] Hiroo Kanamaru, Tsuyoshi Mogi and Naoki Aoyama, "Functional safety application using safety PLC", *SICE Annual Conference*, vol. 4421408, pp.2489-2492, 2007.

[4] Rástočný, J. Ždánsky and K., "Influence of safety PLC parameters to response time of safety functions", in *International Conference on Applied Electronics*, 2013.

[5] Allen Bradley, "literature.rockwellautomation.com," [Online]. Available: https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um523_-en-p.pdf. [Accessed 12 2021].

[6] International Standardization Organization, "www.iso.org," Standardization, International Organization, 12 2015. [Online]. Available: https://www.iso.org/standard/69883.html. [Accessed 12 2021].

[7] International Electrotechnical Commission, "International Electrotechnical Commission (IEC) 60050-114:2014/AMD1," 2017.

[8] International Electric Components Standard, "webstore.iec.ch," 17 02 2017. [Online]. Available: https://webstore.iec.ch/publication/59985. [Accessed 12 2021].

[9] Attila Hilt, Gabor Jaro amd Ostvan Bakos, "Availability Prediction of Telecommunication Application Servers Deployed on Cloud P", *Periodica Polytechnica, Electrical Engineering*, DOI: 60.72-81.10.3311/PPee.9051., 2016.

[10] SIEMENS, "Siemens S7-1500 Technical Slides," SIEMENS, 2019. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:8ad3e246-011b-4206-aa85-1ec60aac51ac/version:1562856005/simatic-s7-1500-redundant-systems--techslides-2018-11-12-en.pdf. [Accessed 05 2022].

[11] Schneider-electric, "https://download.schneider-electric.com," Schneider-electric, 11 12 2018. [Online]. Available: Redundant Control and Communication for Power Control Systems (whitepaper) - https://download.schneider-electric.com/files?p_enDocType=White+Paper&p_File_Name=asc-pcm-wp-redundant-control.pdf&p_Doc_Ref=PCM-WP-REDCONT. [Accessed 6 2023].

[12] Nguyen Tuan Hung and Truong Dinh Chau, "An Application Solution for PLC Redundancy in Distributed Control System", *International Symposium on Industrial Electronics*, 2011.

[13] G. Gabor, D. Zmaranda, C. Gyorodi and S. Dale, "Redundancy method used in PLC related applications", *3rd International Workshop on Soft Computing Applications*, DOI: 10.1109/SOFA.2009.5254867., pp.119-126, 2009.

[14] D. J. Rankin and J. Jiang, "A Hardware-in-the-Loop Simulation Platform for the Verification and Validation of Safety Control Systems"," *IEEE Transactions on Nuclear Science* , vol. 58, pp.468-478, 2011.

[15] D. Darvas, I. Majzik and E. Blanco Viñuela, "Formal Verification of Safety PLC Based Control Software," *Integrated Formal Methods*, vol. 9681.

[16] V.A. Gapanovich, E.N. Rozenberg and I.B. Shubinsky, "Some Concepts of Fail-Safety and Cyber Protection of Control Systems", DOI: 10.21683/1729-2646-2014-0-2-88-100, 2014.

[17] J. Ždánsky and J. Valigurský, "Application diagnostic of distributed control system with safety PLC", *ELEKTRO*, DOI: 10.1109/ELEKTRO.2018.8398311, pp.1-6, 2018.

[18] IEC Standards, "webstore.iec.ch," 30 4 2010. [Online]. Available: https://webstore.iec.ch/publication/5517. [Accessed 3 2023].

[19] Heidi Hartmann, Dr. Eric Scharpf and Hal Thomas, "Practical SIL Target Selection - Risk Analysis per the IEC 61511 Safety Lifecycle", ISBN: 978-1-934977-03-3.

[20] E. Theocharis, M. Papoutsidakis, A. Sort and C. Drosos, "Experimentation on the Electromechanical Behavior of Automation Safety Buttons Applied to an Industrial PLC" WSEAS Transactions on Systems and Control, ISSN / E-ISSN: 1991-8763 / 2224-2856, Volume 15, 2020, Art. #74, DOI: 15. 10.37394/23203.2020.15.74, 2021.

[21] Mitsubishi Electric, 01 2008. [Online]. Available: http://dl.mitsubishielectric.com/dl/fa/document/catalog/plc/l08117eng/l08117enga.pdf. [Accessed 2023 07].

[22] Feng Wang, Ou Yang, Ruibo Zhang and Lei Shi, "Method for assigning safety integrity level (SIL) during design of safety instrumented systems (SIS) from database",", *Loss Prevention in the Process Industries*, 2016.

[23] D. Smith and K. Simpson, *The Safety Critical Systems Handbook", Elsevier Ltd*, ISBN: 9780128207000., 2011 .

[24] K. Rástočný, J. Ždánsky and J. Hrbček, "The Problems Related to Realization of Safety Function with SIL4 Using PLC", *Cybernetics & Informatics (K&I)*, DOI: 10.1109/KI48306.2020.9039878, pp.1-5, 2020.

[25] J. Ždánsky and J. Valigurský, "Time response of safety function realised by decentralised SRCS with safety. PLC", *International Conference on Applied Electronics (AE)*, DOI: 10.23919/AE.2018.8501425, pp.1-4, 2018.

[26] G. Buja and R. Menis, "Dependability and

WSEAS TRANSACTIONS on SYSTEMS and CONTROL
DOI: 10.37394/23203.2022.18.28

Functional Safety: Applications in Industrial Electronics Systems", *IEEE Industrial Electronics Magazine*, vol. 6, pp.4-12, 2012.

[27] Abdullah Al Farooq Jessica Marquard, Kripa George and Thomas Moyer, "Detecting Safety and Security Faults in PLC Systems with Data Provenance", *IEEE International Symposium on Technologies for Homeland Security*, 2019.

[28] plcopen.org, "https://plcopen.org," 2018. [Online]. Available: https://plcopen.org/system/files/downloads/__plcopen_safety_part_1_version_2.01.pdf (Accessed 12/2021). [Accessed 01 2022].

[29] M. M. a. J. Ždánsky, "Safety PLC Programming Based on UML Statechart," *ELEKTRO*, DOI: 10.1109/ELEKTRO49696.2020.9130307, pp.1-5, 2020.

[30] Younju Oh, Junbeom Yoo, Sungdeok Cha and Han Seong Son, "Software safety analysis of function block diagrams using fault trees, Reliability Engineering & System Safety", vol. 88, no. 3, pp.215-228, 2005.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

- Efstathios Theocharis has constructed the demo unit and implemented the PLC - SCADA code.
- Michail Papoutsidakis carried out the simulation and the optimization of the experiments.
- Andrew Short has organized and executed the experiments.
- Konstantia Zisimou was responsible for the Reports and the requirement for their repetition.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

All authors would like to thank the University of West Attica for the financial support provided to them to undertake this research project.

Conflict of Interest

The authors have no conflicts of interest to declare.