ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗΣ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΟΡΥΚΤΩΝ ΠΟΡΩΝ

ΚΑΤΕΥΘΥΝΣΗ ΜΗΧΑΝΙΚΩΝ ΓΕΩΤΕΧΝΟΛΟΓΙΑΣ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΤΕ

Αυτόνομα Συστήματα και Λειτουργική Ασφάλεια στη Μεταλλευτική

Πτυχιακή Εργασία

του

Χαρίλαου Γραμμένου με Α.Μ. GE05779

που υποβάλλεται στο Τμήμα Μηχανικών Ορυκτών Πόρων
του Πανεπιστημίου Δυτικής Μακεδονίας
για τη μερική εκπλήρωση των υποχρεώσεων απόκτησης
του Πτυχίου Μηχανικού Γεωτεχνολογίας Περιβάλλοντος ΤΕ

Κοζάνη, Σεπτέμβριος 2021

Ευχαριστίες

Σε αυτό σημείο θα ήθελα να ευχαριστήσω την οικογένεια μου που με στήριξε σε αυτό το νέο μου ταξίδι των σπουδών. Ακόμα, θα ήθελα να ευχαριστήσω τον καθηγητή του Τμήματος, Δρ. Ιωάννη Καπαγερίδη.

Περιεχόμενα

ΠΕΡΙΛΗΨΗ

Σε αυτό το θέμα θα εξετάσουμε για την κατευθυντήρια γραμμή για την εφαρμογή λειτουργικής ασφάλειας σε αυτόνομων συστημάτων ασφάλειας. Πιο συγκεκριμένα, μια ομάδα που ειδικεύεται πάνω σε αυτό το θέμα είναι η Global Mining Guidelines (GMG) η οποία έδωσε σε δημοσίευση ένα έγγραφο το οποίο αναλύει τα θέματα γύρω από την ασφάλεια των αυτόνομων συστημάτων. Αναφέρεται στην αυτόνομη εξόρυξη η οποία γίνεται ένα συγκεκριμένο κώδικα ασφάλειας ο οποίος θα είναι ασφαλείς για τον χειριστή και για να μην δημιουργήσει πρόβλημα στα μηχανήματα εξόρυξης. Στο έγγραφο ακόμα η ομάδα της GMG αναφέρει για αυτόνομα συστήματα που το προσωπικό θα πρέπει να περάσει μια εκπαίδευση η οποία θα τους δείχνει στην πράξη μια ασφαλή αυτοματοποίηση και θα κατανοήσουν τους κινδύνους του αυτοματισμού. Στον έγγραφο ακόμα αναγράφεται για την OPS που είναι υπεύθυνη για να παρέχει στους χειριστές του ορυχείου όλες τις απαραίτητες πληροφορίες για την λειτουργική ασφάλεια για την ανάπτυξη του προϊόντος. Αρμόδιος μετά την ανάπτυξη του προϊόντος είναι η επιχείρηση όμως η OPS εξακολουθεί να υπεύθυνη για τις αλλαγές όσον αφορά για την αναβάθμιση του λογισμικού. Ο κύκλος ζωής του προϊόντος αντιστοιχεί με τον κύκλο ζωής της λειτουργικής ασφάλειας η οποία δείχνει το εύρος ζωής ενός προϊόντος. Στο έγγραφο αυτό επίσης αναφέρεται στην διαχείριση κινδύνου ενός αυτόματου συστήματος το οποίο μπορεί να έχει ένα λειτουργικό πρόβλημα είτε λογισμικού είτε κακής λειτουργικής χρήσης του χειριστή. Κλείνοντας, στο έγγραφο της GMG αναφέρονται συγκεκριμένα ISO που είναι απαραίτητα για την λειτουργική ασφάλεια των μηχανημάτων και πρωτόκολλα που θα πρέπει να ακολουθήσει η εταιρία αλλά και ο χειριστής των αυτόνομων μηχανημάτων έτσι ώστε να υπάρξει μια ομαλή λειτουργία ανάμεσα στα μηχανήματα και στους χειριστές αυτών.

ABSTRACT

In this subject we will look at the guideline for implementing functional safety in standalone safety systems. More specifically, a group that specializes on this topic is the Global Mining Guidelines (GMG) which has published a paper that discusses the issues surrounding security in autonomous systems. It refers to autonomous mining which becomes a specific safety code which will be safe for the operator and not to create a problem for the mining machines. In the paper still the GMG team mentions about autonomous systems that the staff should go through a training which will show them in practice a safe automation and understand the risks of automation. The document even mentions about OPS being responsible for providing mine operators with all the necessary operational safety information for product development. Responsible after the product development is the company however the OPS is still responsible for the changes in terms of upgrading the software. The product life cycle corresponds to the functional safety life cycle which indicates the life span of a product. This document also refers to the risk management of an automated system which may have a functional problem either software or operator misuse. In conclusion, GMG's document mentions specific ISOs that are necessary for the operational safety of the machines and protocols that the company and the operator of the autonomous machines should follow so that there is a smooth operation between the machines and their operators.

1. ΠΡΟΛΟΓΟΣ

Το Global Mining Guidelines Group (GMG) είναι ένα δίκτυο εκπροσώπων από εταιρείες εξόρυξης, εξοπλισμός και προμηθευτές τεχνολογίας, ερευνητικοί οργανισμοί, ακαδημαϊκοί, ρυθμιστικούς οργανισμούς, συμβούλους και ενώσεις του κλάδου που συνεργάζονται για την αντιμετώπιση των προκλήσεων που αντιμετωπίζει ο κλάδος μας. Η GMG στοχεύει να επιταχύνει τη βελτίωση των επιδόσεων εξόρυξης, της ασφάλειας και της βιωσιμότητας και δημιουργεί κατευθυντήριες γραμμές, όπως αυτή, που αντιμετωπίζουν κοινές προκλήσεις του κλάδου. Οι κατευθυντήριες γραμμές της GMG είναι έγγραφα με αξιολόγηση από ομότιμους που προσφέρουν βέλτιστες πρακτικές, συμβουλές για την εφαρμογή νέων τεχνολογιών, ανάπτυξη ευθυγράμμισης της βιομηχανίας ή εκπαίδευση σε ευρεία κλίμακα. Αναπτύσσονται μέσω συνεργασίας σε ολόκληρο τον κλάδο για να βοηθήσουν την παγκόσμια εξορυκτική κοινότητα στην εφαρμογή πρακτικών για τη βελτίωση των λειτουργιών ή / και την εφαρμογή νέων τεχνολογιών. Λάβετε υπόψη ότι οι οδηγίες GMG δεν είναι βιομηχανικά πρότυπα. Τα σχέδια εγγράφων ελέγχονται και εγκρίνονται από τα μέλη της ομάδας εργασίας πριν από την έγκριση από το Εκτελεστικό Συμβούλιο της GMG.

2. ΟΡΙΣΜΟΙ ΟΡΩΝ ΚΑΙ ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Αυτόνομη μηχανή: Αναφέρεται σε αυτόνομες και ημιαυτόνομες μηχανές (ASAM), όπως αυτές ορίζονται στο ISO 17757 (2019a, 3.1.3.1 και 3.1.3.2). Στην παρούσα κατευθυντήρια γραμμή, αναφέρεται συγκεκριμένα σε μηχανήματα εξόρυξης.

Αυτόνομο σύστημα: Αναφέρεται σε αυτόνομα και ημιαυτόνομα συστήματα (ASAMS), όπως αυτά ορίζονται στο ISO 17757 (2019a, 3.1.2). Στην παρούσα κατευθυντήρια γραμμή, αναφέρεται συγκεκριμένα σε συστήματα εξόρυξης.

Ικανότητα: Η ύπαρξη ατόμων με τις απαραίτητες γνώσεις, δεξιότητες και εμπειρία για την εφαρμογή της λειτουργικής ασφάλειας σε αυτόνομα συστήματα.

Ντετερμινιστικό σύστημα: Ένα σύστημα όπου τα αποτελέσματα καθορίζονται με βάση γνωστούς και κατανοητούς τρόπους και συνθήκες.

Λειτουργική ασφάλεια: Αναφέρεται στο "μέρος της συνολικής ασφάλειας που εξαρτάται από τη σωστή λειτουργία ενός συστήματος ή εξοπλισμού σε απόκριση στις εισόδους του". Ορίζεται ως "η ανίχνευση ενός δυνητικά επικίνδυνης κατάστασης που έχει ως αποτέλεσμα την ενεργοποίηση ενός προστατευτικής ή διορθωτικής διάταξης ή μηχανισμού για την αποτροπή της εμφάνισης επικίνδυνων συμβάντων ή την παροχή μετριασμού για τη μείωση της συνέπεια του επικίνδυνου συμβάντος" (Πηγή: www.iec.ch).* **Κύκλος ζωής λειτουργικής ασφάλειας**: Η διαδικασία διαχείρισης της λειτουργικής ασφάλειας κατά τη διάρκεια της ζωής ενός προϊόντος.

Ανεξάρτητος: Σε ένα πλαίσιο επανεξέτασης ή διερεύνησης, αναφέρεται σε έναν διαχωρισμό αρμοδιοτήτων για τη διατήρηση της αντικειμενικότητας.

Επίπεδο ακεραιότητας / επίπεδο απόδοσης: Προσδιορισμός του κινδύνου μείωση του κινδύνου που απαιτείται να παρέχεται από κάθε λειτουργία ασφάλειας. Παραδείγματα περιλαμβάνουν το επίπεδο επιδόσεων μηχανής (MPL), το επίπεδο επιδόσεων (PL) και το επίπεδο ακεραιότητας ασφάλειας (SIL).

Χειριστής ορυχείου: Η επιχείρηση εξόρυξης που εφαρμόζει τη λειτουργική ασφάλειας στα αυτόνομα συστήματα στα ορυχεία ποιος είναι υπεύθυνος για τον κύκλο ζωής της λειτουργικής ασφάλειας της εφαρμογής.

Μη ντετερμινιστικό σύστημα: (π.χ. συστήματα επέμβασης σε περίπτωση έκτακτης ανάγκης, προηγμένα συστήματα υποβοήθησης οδηγού και σχεδιασμός διαδρομής με τεχνητή νοημοσύνη). Ενδέχεται να μην είναι δυνατόν να καθοριστεί ένα επίπεδο ακεραιότητας/βαθμολογία επιπέδου επιδόσεων (π.χ. MPL / PL / SIL) κατά τη χρήση αυτών των συστημάτων.

Αρχικός προμηθευτής προϊόντος (OPS): που είναι υπεύθυνος για μέρος ή για το σύνολο του εξοπλισμού κύκλου ζωής της λειτουργικής ασφάλειας του προϊόντος.

Λειτουργία ασφάλειας: Οι λειτουργίες του μηχανήματος που απαιτούνται για την επίτευξη ή τη διατήρηση μιας ασφαλούς κατάστασης και των οποίων η αποτυχία ή η δυσλειτουργία θα μπορούσαν να αυξήσουν τον κίνδυνο τραυματισμού ή βλάβης στα εμπλεκόμενα άτομα ή το περιβάλλον.

Διαχειριστής συστήματος: Το άτομο που έχει τον έλεγχο ενός συστήματος.

Ασφάλεια συστήματος: Μέτρα που λαμβάνονται για να επιβεβαιωθεί ότι το ο συνολικός σχεδιασμός ενός συστήματος είναι ασφαλής για λειτουργία. Η λειτουργική ασφάλεια αποτελεί μέρος της ασφάλειας του συστήματος.

* Ο επίσημος ορισμός της λειτουργικής ασφάλειας σύμφωνα με το διεθνές πρότυπο IEC 61508 είναι: "Το μέρος της συνολικής ασφάλειας που αφορά το EUC (Equipment Under Control) και το σύστημα ελέγχου του EUC που εξαρτάται από την ορθή λειτουργία των συστημάτων που σχετίζονται με την ασφάλεια E/E/ΠΕ (ηλεκτρικά/ηλεκτρονικά/προγραμματιζόμενα ηλεκτρονικά) και άλλων μέτρων μείωσης του κινδύνου."

3. ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Αυτόνομη εξόρυξη, αυτόνομα συστήματα, λειτουργική ασφάλεια, κύκλος ζωής, κινητές αυτόνομες μηχανές, διαχείριση κινδύνου, ασφάλεια

4. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Αυτό το έγγραφο παρέχει καθοδήγηση σχετικά με την εφαρμογή της λειτουργικής ασφάλειας σε νέες εφαρμογές αυτόνομων συστημάτων στην εξόρυξη σε επιφανειακές και υπόγειες λειτουργίες. Προορίζεται ως αφετηρία για να βοηθήσει τους αναγνώστες που εφαρμόζουν αυτόνομα συστήματα να πλοηγηθούν στην επικοινωνία με άλλους βασικούς φορείς, αλλά δεν είναι μια ακριβής διαδικασία που πρέπει να ακολουθηθεί και δεν χρησιμεύει ως πρότυπο ή σύνολο κανόνων. Καλύπτει υλικό επί τόπου - την εξόρυξη και συναφείς δραστηριότητες υποστήριξης που συμβάλλουν στην εξόρυξη υλικού, όπως γεώτρηση, ανατίναξη, φόρτωση, μεταφορά, ντάμπινγκ.

Τα μη ντετερμινιστικά συστήματα είναι εκτός του πεδίου εφαρμογής του της παρούσας κατευθυντήριας γραμμής. Ωστόσο, ορισμένες πληροφορίες υψηλού επιπέδου για τα μη ντετερμινιστικά συστήματα παρέχονται στην ενότητα 13.

Ενώ η λειτουργική ασφάλεια εντάσσεται στο ευρύτερο πεδίο της ασφάλειας του συστήματος, η καθοδήγηση σχετικά με τη συνολική ασφάλεια του συστήματος δεν εμπίπτει στο πεδίο εφαρμογής της παρούσας κατευθυντήριας γραμμής. Ωστόσο, η ενότητα 6 περιγράφει κάποιο πλαίσιο σχετικά με την εφαρμογή αυτόνομων συστημάτων και τη συνολική ασφάλεια και το προσάρτημα Α περιγράφει τον τρόπο με τον οποίο η λειτουργική ασφάλεια εντάσσεται στη διαχείριση της συνολικής ασφάλειας. Ένα ξεχωριστό έγγραφο της GMG για τη συνολική ασφάλεια των αυτόνομων συστημάτων βρίσκεται επί του παρόντος υπό ανάπτυξη.

Τα τέσσερα βασικά κοινά της παρούσας κατευθυντήριας γραμμής είναι:

- Όσοι σχεδιάζουν και προμηθεύουν αυτόνομα συστήματα (δηλ. OPS)
- Οι ομάδες παράδοσης και ολοκλήρωσης επιχειρήσεων
- Οι ομάδες τεχνολογίας, λειτουργίας και συντήρησης των εταιρειών εξόρυξης
- Ρυθμιστικές αρχές

Οι ομάδες αυτές έχουν διαφορετικές προοπτικές και ανάγκες, οπότε το πεδίο εφαρμογής διατηρήθηκε αρκετά ευρύ ώστε να καλύπτει όλες.

5. ΕΙΣΑΓΩΓΗ

Η παγκόσμια εξορυκτική βιομηχανία αγκαλιάζει την αυτοματοποίηση. Ωστόσο, οι απαιτήσεις για τη διαχείριση της λειτουργικής ασφάλειας είναι ασαφείς. Υπάρχουν διάφοροι λόγοι για αυτή την έλλειψη σαφήνειας:

Η χρήση αυτόνομων συστημάτων επιταχύνεται, αλλά η υιοθέτηση είναι ανομοιογενής σε ολόκληρη τη βιομηχανία.

- Τα σημερινά OPS βρίσκονται σε διαφορετικά στάδια ωριμότητας σε όσον αφορά τη διαχείριση της λειτουργικής ασφάλειας.
- Αρκετά διεθνή και εθνικά συστήματα λειτουργικής ασφάλειας πρότυπα υπάρχουν ή βρίσκονται υπό ανάπτυξη, αλλά υπάρχει ένα έλλειψη σαφήνειας σχετικά με το τι ισχύει για τις αυτόνομες συστήματα στα ορυχεία.

Η παρούσα κατευθυντήρια γραμμή παρέχει μια κοινή προσέγγιση για την εφαρμογή λειτουργικής ασφάλειας σε αυτόνομα συστήματα και παραπομπές διεθνή πρότυπα στο πλαίσιο της εξορυκτικής βιομηχανίας και της τρέχουσας ωριμότητάς της. Η παρούσα κατευθυντήρια γραμμή επίσης περιγράφει σαφείς προσδοκίες για τις απαιτήσεις επικοινωνίας για την υποστήριξη της διαχείρισης αλλαγών και της αποτελεσματικής εφαρμογής. Για το σκοπό αυτό, η παρούσα κατευθυντήρια γραμμή:

- Προσδιορίζει σημαντικό υλικό αναφοράς και παραθέτει τα πρότυπα που είναι σχετικά με την εφαρμογή της λειτουργικής ασφάλειας σε διάφορες πτυχές των αυτόνομων συστημάτων (ενότητα 7)
- περιγράφει ένα παράδειγμα κύκλου ζωής λειτουργικής ασφάλειας για την εφαρμογή αυτόνομων συστημάτων στην εξόρυξη και προσδιορίζει ορισμένες βασικές προσδοκίες και ευθύνες για την παροχή πληροφοριών, τεκμηρίωσης και υποστήριξης σε κάθε στάδιο (ενότητα 8)
- Προσφέρει καθοδήγηση υψηλού επιπέδου για την ανάπτυξη λογισμικού, επαλήθευση και επικύρωση (ενότητα 9)- διαχείριση ικανοτήτων (ενότητα 10), την ασφάλεια στον κυβερνοχώρο (ενότητα 11), και τεκμηρίωση διασφάλισης (ενότητα 12)

6. ΙΣΤΟΡΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΥΛΟΠΟΙΗΣΗ ΑΥΤΟΝΟΜΩΝ ΚΑΙ ΗΜΙΑΥΤΟΝΟΜΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η εστίαση στη λειτουργική ασφάλεια είναι σημαντική για τα αυτόνομα συστήματα λόγω της εξάρτησής τους από την τεχνολογία (π.χ. hardware and software) για τη διαχείριση των λειτουργιών ασφαλείας. Ισχυρή εστίαση στην στους διοικητικούς ελέγχους που είναι κρίσιμοι για την ασφάλεια του συστήματος είναι επίσης σημαντικός.

6.1 Διαχείριση των ανθρώπων και της αλλαγής

Η διαχείριση αλλαγών θα πρέπει να είναι ολοκληρωμένη διότι, για παράδειγμα, οι αλλαγές λογισμικού μπορούν να επηρεάσουν τη λειτουργία του συστήματος και οι ενέργειες του χειριστή συστήματος μπορεί να επηρεάσουν την ασφάλεια. Θα πρέπει επίσης να υπάρχει κατάλληλη επικοινωνία με όλους τους ενδιαφερόμενους φορείς και όλες οι απαραίτητες ενημερώσεις στην τεκμηρίωση των χρηστών - όπως οδηγίες και εγχειρίδια εκπαίδευσης - για να επιβεβαιωθεί ότι το προσωπικό επιχειρήσεων είναι έτοιμο να προσαρμοστεί στην αλλαγή.

6.2 Λειτουργία

Συγκρούσεις μεταξύ των διαδικασιών για την επανδρωμένη λειτουργία και εκείνων για την αυτόνομη λειτουργία πρέπει να αντιμετωπιστούν.

Οι επιχειρησιακές διαδικασίες πρέπει να είναι σαφώς καθορισμένες. Τα αυτόνομα συστήματα απαιτούν τυποποιημένες λειτουργικές διαδικασίες σε κώδικα που είναι εκτελέσιμος, διότι μια μηχανή δεν μπορεί να να κατανοήσει την πρόθεση των τυποποιημένων λειτουργικών διαδικασιών όπως ο άνθρωπος.

Διαφορετικά επίπεδα αυτόνομης ωριμότητας απαιτούν διαφορετικά πρακτικές ασφάλειας. Για παράδειγμα, μια τρέχουσα πρακτική είναι ο καθορισμός μιας ζώνης αυτόνομης λειτουργίας που περιορίζει την μη εξουσιοδοτημένη πρόσβαση. Ωστόσο, καθώς η κινητή αυτόνομη μηχανή εξελίσσεται, αυτή η πρακτική δεν θα είναι πάντα η πιο αποδοτική επιλογή. Προκειμένου να αντιμετωπιστούν τα διαφορετικά επίπεδα ωριμότητας, θα πρέπει να αναπτυχθούν ή να επικαιροποιηθούν πρότυπα ασφαλείας.

Οι μετρήσεις για τα αυτόνομα συστήματα πρέπει να είναι πολλές ακριβέστερη όσον αφορά τη λειτουργική ασφάλεια.

- Οι μετρήσεις κατάστασης υποδομής / συστήματος πρέπει να είναι ακριβείς. Για παράδειγμα, εάν μια συσκευή GPS κινείται μισό μέτρο, μπορεί να επηρεάσει σημαντικά τον τρόπο με τον οποίο το αυτόνομο σύστημα λειτουργεί.
- Οι μετρήσεις υγείας του αυτόνομου συστήματος εξόρυξης είναι κρίσιμες στην επικύρωση της απόδοσης που διαμορφώνει τις παραδοχές στις εκτιμήσεις κινδύνου.

6.3 Σχέση προμηθευτή γνήσιου προϊόντος και χειριστή ορυχείου

Η επιχειρησιακή πρόθεση καθορίζει την έννοια των επιχειρήσεων και τις παραδοχές σχετικά με τον τρόπο λειτουργίας του συστήματος. Η επιχειρησιακή πρόθεση αποτελεί σύμπραξη μεταξύ του χειριστή του ορυχείου και του OPS όταν χρησιμοποιούνται αυτόνομα συστήματα, ενώ είναι υπό τον έλεγχο του χειριστή του ορυχείου όταν χρησιμοποιούνται επανδρωμένα συστήματα.

Απαιτούνται αποτελεσματικοί δίαυλοι επικοινωνίας μεταξύ του OPS και του χειριστή του ορυχείου για την αντιμετώπιση πτυχών όπως ο υπολειπόμενος κίνδυνος και οι απαιτήσεις λειτουργίας και συντήρησης. Ενδέχεται να απαιτείται μεγαλύτερη αλληλεπίδραση λόγω της πολυπλοκότητας των συστημάτων αυτών. Για περισσότερες πληροφορίες, ανατρέξτε στον Κώδικα Πρακτικής της Δυτικής Αυστραλίας για την ασφαλή αυτόνομη εξόρυξη (Τμήμα Κυβέρνησης της Δυτικής Αυστραλίας της Ορυχεία, βιομηχανικός κανονισμός και ασφάλεια, 2015).

6.4 Αξιολόγηση κινδύνων και διαχείριση έκτακτης ανάγκης

Οι εκτιμήσεις κινδύνου απαιτούν:

- Επειδή τα αυτόνομα συστήματα είναι συνήθως πιο πολύπλοκα από τα επανδρωμένα συστήματα.
- Ισχυρή εστίαση στους διοικητικούς ελέγχους στους οποίους εξαρτάται το αυτόνομο σύστημα. Θα πρέπει επίσης να εξετάζουν τον τρόπο με τον οποίο

αλλάζει η ανθρώπινη συμπεριφορά καθώς οι πτυχές του λειτουργίας αντικαθίστανται από το αυτόνομο συστήματα.

- Περισσότερη εστίαση σε σενάρια ακραίων περιπτώσεων, τα οποία είναι τα σενάρια που δοκιμάζουν το σχεδιασμό του συστήματος σε απροσδόκητες και συχνά μη δοκιμασμένους τρόπους. Ενώ ο χειριστής του συστήματος μπορεί να προσαρμοστεί στην αβεβαιότητα και την αλλαγή όταν χρησιμοποιεί ένα επανδρωμένο σύστημα, ένα αυτόνομο σύστημα λειτουργεί εντός του όρια σχεδιασμού.

Οι διαδικασίες έκτακτης ανάγκης πρέπει να αναθεωρηθούν για να συμπεριλάβουν αυτόνομες επιχειρήσεις. Οι ακόλουθες ερωτήσεις πρέπει να ληφθούν υπόψη κατά την αναθεώρηση και την ενημέρωση των υφιστάμενων διαδικασιών και ως μέρος της τρέχουσας διαχείρισης αλλαγών:

- Πώς να σταματήσετε μια αυτόνομη λειτουργία
- Πώς να προσεγγίσετε την αυτόνομη ζώνη λειτουργίας
- Πώς να αφαιρέσετε το αυτόνομο μηχάνημα αν χαλάσει
- Απαιτήσεις κατάρτισης για τους ανταποκριτές έκτακτης ανάγκης

6.5 Διαμόρφωση

Θα πρέπει να εφαρμοστεί μια προσέγγιση **διαχείρισης ρυθμίσεων** για την καθιέρωση και τη διατήρηση της βέλτιστης απόδοσης του αυτόνομου συστήματος. Η διαδικασία αυτή πρέπει να καταγράφει όλα τα στοιχεία υλικού και λογισμικού που θα μπορούσαν να επηρεάσουν την ασφάλεια (π.χ., ο ορισμός της διαμόρφωσης πρέπει να περιλαμβάνει τα μηχανικά στοιχεία του οχήματος που χρησιμοποιούνται στην επανδρωμένη λειτουργία, καθώς και την ανίχνευση, τους υπολογισμούς και τον συντονισμό που υλοποιούνται στο λογισμικό). Η διαδικασία αυτή πρέπει επίσης να καταγράφει τις πτυχές της παράδοσης, της ολοκλήρωσης και της συντήρησης που θα μπορούσαν να επηρεάσουν την ασφάλεια.

Για περαιτέρω οδηγίες ανατρέξτε στο ISO 10007, Διαχείριση ποιότητας-Κατευθυντήριες γραμμές για τη διαχείριση διαμόρφωσης (2017c).

Οι ενημερώσεις μπορεί να γίνονται συχνά λόγω του γρήγορου ρυθμού της καινοτομίας.

7. ΣΥΝΙΣΤΩΜΕΝΟ ΥΛΙΚΟ ΑΝΑΦΟΡΑΣ

Θα πρέπει να ληφθούν υπόψη τα ακόλουθα έγγραφα κατά τη διαδικασία σχεδιασμού και υλοποίησης:

- Τοπικά και διεθνή πρότυπα
- Οδηγίες του κλάδου
- Κανονισμοί και νομοθεσία δικαιοδοσίας
- Εταιρικά πρότυπα
- Πληροφορίες για τα προϊόντα OPS και πωλητών

Στον πίνακα 1 παρατίθενται τα πρότυπα που σχετίζονται με την εφαρμογή της λειτουργικής ασφάλειας σε διάφορες πτυχές των αυτόνομων συστημάτων. Μια περίληψη καθενός από αυτά τα πρότυπα, καθώς και άλλα πρότυπα που δεν είναι βασικά, αλλά εξακολουθούν να είναι χρήσιμες αναφορές, μπορούν να βρεθούν στο Παράρτημα Β. Οι μετέπειτα αναφορές στα πρότυπα αυτά γίνονται με βάση τον αριθμό του προτύπου. Πλήρεις παραπομπές, συμπεριλαμβανομένων των επιμέρους δημοσιευμένων τμημάτων, υπάρχουν στην ενότητα 15.

Table 1. Key Standards (in numerical order)

Standard	Citation(s)
ISO 12100 Safety of machinery – General Principles for design – Risk assessment and risk reduction	International Organization for Standardization, 2010
ISO 13849 Safety of machinery – Safety-related parts of control systems	International Organization for Standardization, 2015b, 2012b
ISO 17757 Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety	International Organization for Standardization, 2019a
ISO 19014 Earth-moving machinery – Functional safety (Parts 1 and 3 are published, Parts 2, 4, and 5 are currently in development)	International Organization for Standardization, 2018c, 2018d
ISO 31000 Risk management	International Organization for Standardization, 2018e
IEC 31010 Risk management – Risk assessment techniques	International Electrotechnical Commission, 2019b
IEC 61508 Functional safety of electrical / electronic / programmable electronic safety-related systems	International Electrotechnical Commission, 2010a–2010g
IEC 62061 Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems	International Electrotechnical Commission, 2015b

8. ΚΥΚΛΟΣ ΖΩΗΣ ΛΕΙΤΟΥΡΓΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Ο κύκλος ζωής της λειτουργικής ασφάλειας είναι μια διαδικασία για τη διαχείριση της λειτουργικής ασφάλειας κατά τη διάρκεια της ζωής ενός προϊόντος. Η παρούσα ενότητα αποτελεί ένα παράδειγμα κύκλου ζωής λειτουργικής ασφάλειας για εφαρμογές αυτόνομων συστημάτων που περιγράφει τη σχέση μεταξύ του κύκλου ζωής του προϊόντος του OPS και του κύκλου ζωής της εφαρμογής του χειριστή του ορυχείου. Επίσης, συνοψίζει ορισμένες συστάσεις για τις πληροφορίες που πρέπει να κοινοποιούνται μεταξύ των βασικών συμμετεχόντων. Τα OPS μπορεί να διαφέρουν ως προς τον τρόπο με τον οποίο διαχειρίζονται την προσέγγιση του κύκλου ζωής των προϊόντων τους, οπότε οι συστάσεις αυτές μπορεί επίσης να διαφέρουν ανάλογα με την προσέγγιση. Αυτό το παράδειγμα κύκλου ζωής εξετάζει επίσης τόσο τα νέα όσο και τα υφιστάμενα συστήματα και τον τρόπο με τον οποίο η διαδικασία μπορεί να προσαρμοστεί για το καθένα.

Αυτό το παράδειγμα κύκλου ζωής καλύπτει ένα συνολικό περιβάλλον αυτόνομου συστήματος που σχετίζεται με τον ιστότοπο με πολλά επίπεδα αυτοματισμού. Αυτά τα στρώματα περιλαμβάνουν διάφορους τύπους κύκλων ζωής προϊόντων που πρέπει να ενσωματωθούν στον κύκλο ζωής της εφαρμογής (Εικόνα 1).

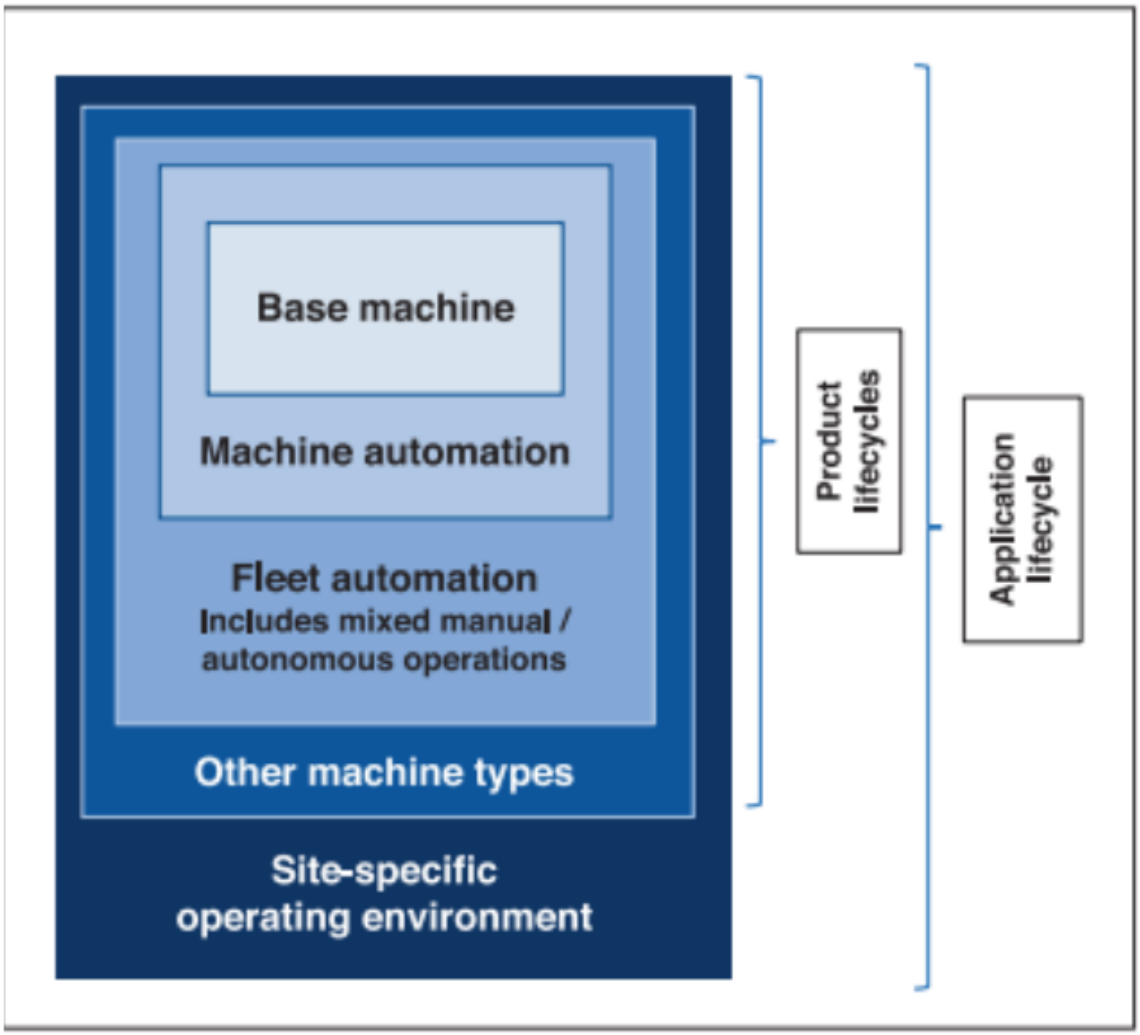

Figure 1. Layers of the Overall Autonomous System Environment

Το Σχήμα 2 συνοψίζει αυτό το παράδειγμα κύκλου ζωής. Πίνακες 2-12 περιγράφουν τις προσδοκίες και τις σχετικές πληροφορίες, την τεκμηρίωση ή την υποστήριξη που ο φορέας εκμετάλλευσης του ορυχείου και το OPS μπορούν να είναι υπεύθυνοι για την παροχή σε κάθε σχετικό στάδιο. Το Σχήμα 2 και οι Πίνακες 2-12 περιγράφουν τα βασικά στάδια τόσο του κύκλου ζωής του προϊόντος όσο και του κύκλου ζωής της εφαρμογής, από την ιδέα και το πεδίο εφαρμογής έως τη λειτουργία και τη συντήρηση, καθώς και ορισμένες βασικές πτυχές (άλλοι έλεγχοι κινδύνου, επιχειρησιακή ετοιμότητα και διαχείριση αλλαγών) που πρέπει να λαμβάνονται υπόψη στο πλαίσιο της διαχείρισης του κύκλου ζωής της λειτουργικής ασφάλειας. Στο Σχήμα 2, τα διακεκομμένα βέλη υποδεικνύουν πού εντάσσονται αυτές οι άλλες πτυχές στο συνολικό παράδειγμα του

κύκλου ζωής. Τα βέλη μεταξύ των δύο κύκλων ζωής αντιπροσωπεύουν ορισμένες βασικές επικοινωνίες.

Ενώ τα στάδια του κύκλου ζωής του προϊόντος και της εφαρμογής μπορεί να είναι παρόμοια, δεν έχουν σχέση ένα προς ένα και δεν συμβαίνουν απαραίτητα ταυτόχρονα. Εάν το OPS και ο χειριστής ορυχείου αναπτύσσουν μια προσαρμοσμένη λύση, μπορεί να βρίσκονται σε παρόμοια χρονοδιαγράμματα. Ωστόσο, συχνά αναπτύσσεται πρώτα το προϊόν και, στη συνέχεια, ορισμένα στάδια του κύκλου ζωής του προϊόντος μπορεί να επανεξεταστούν με βάση την εφαρμογή. Για παράδειγμα, εάν ο φορέας εκμετάλλευσης ορυχείου κοινοποιεί πληροφορίες από οποιοδήποτε στάδιο του κύκλου ζωής της εφαρμογής πίσω στο OPS, τότε ένα προηγούμενο στάδιο του κύκλου ζωής του προϊόντος μπορεί να χρειαστεί να επαναληφθεί ή να επανεξεταστεί. Εάν εντοπιστούν τροποποιήσεις του σχεδιασμού κατά τη διάρκεια της εφαρμογής, ο προσδιορισμός των κινδύνων και η εκτίμηση κινδύνου μπορεί να χρειαστεί να επανεξεταστούν για το προϊόν. Περαιτέρω, η αλληλουχία δραστηριοτήτων που περιγράφεται στο σχήμα 2 είναι ένα από τα πολλά παραδείγματα του πώς μπορεί να μοιάζει η διαδικασία. Αυτό ισχύει ιδιαίτερα για τον κύκλο ζωής του προϊόντος, καθώς ορισμένα από τα στάδια μπορεί να πραγματοποιούνται με διαφορετική σειρά ή να μην ισχύουν σε κάθε περίπτωση ανάλογα με την προσέγγιση ανάπτυξης του προϊόντος.

Το OPS είναι υπεύθυνο για τη λειτουργική ασφάλεια κατά την ανάπτυξη ενός προϊόντος. Το OPS παρέχει στον χειριστή του ορυχείου όλες τις απαραίτητες πληροφορίες για να αποδείξει ότι πληρούνται οι προδιαγραφές της εφαρμογής και ότι το αυτόνομο σύστημα μπορεί να λειτουργήσει και να διατηρηθεί με την απαιτούμενη απόδοση ασφαλείας. Μόλις το προϊόν αναπτυχθεί σε μια επιχείρηση, ο φορέας εκμετάλλευσης ορυχείου είναι υπεύθυνος για τη συνολική ασφάλεια του αυτόνομου συστήματος. Ωστόσο, ο OPS εξακολουθεί να είναι υπεύθυνος για τις αλλαγές που πραγματοποιεί στο προϊόν του κατά τη διάρκεια του κύκλου αναβάθμισης του προϊόντος (π.χ. αναβάθμιση λογισμικού). Εάν η ολοκλήρωση πραγματοποιείται από τρίτο μέρος, τότε ο ολοκληρωτής του συστήματος θα είναι υπεύθυνος για την ανάπτυξη και την ανάλυση των λειτουργιών ασφαλείας εντός του αυτόνομου συστήματος, ενώ ο φορέας εκμετάλλευσης του ορυχείου θα εξακολουθεί να είναι υπεύθυνος για τη συνολική ασφάλεια του.

Η επικοινωνία και η διαφάνεια μεταξύ του φορέα εκμετάλλευσης ορυχείων που εφαρμόζει το αυτόνομο σύστημα και του OPS είναι απαραίτητη. Το OPS θα αναπτύξει τυπικά το αυτόνομο σύστημα για μια προοριζόμενη χρήση. με την πάροδο του χρόνου, ενδέχεται να υπάρξουν τροποποιήσεις τόσο στο σύστημα όσο και στις περιπτώσεις χρήσης στο πεδίο. Εάν γίνουν τέτοιες τροποποιήσεις, τότε είναι ζωτικής σημασίας οι χειριστές ορυχείων να εφαρμόζουν αρχές διαχείρισης αλλαγών και διαμόρφωσης. Ο χειριστής του ορυχείου πρέπει να καθορίσει τις απαιτήσεις των χρηστών του και τις προκύπτουσες απαιτήσεις συστήματος και ασφάλειας για την εφαρμογή τους. Στη συνέχεια, πρέπει να επικοινωνήσουν με το OPS για να επιβεβαιώσουν ότι το προϊόν πληροί αυτές τις απαιτήσεις.

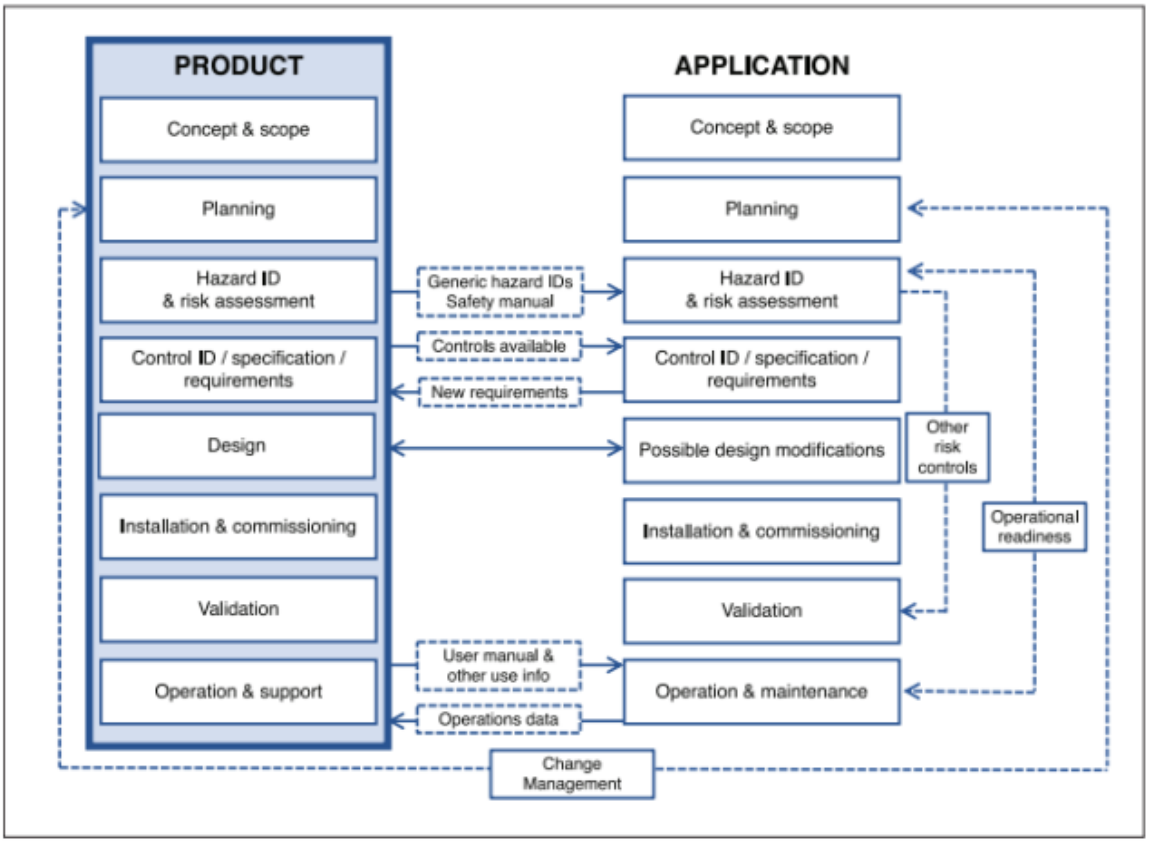

Figure 2. An Example of the Relationship Between Product and Application Lifecycles (Abbreviations: Identification, ID); Note: the contents in the lifecycles may vary.

Table 2. Concept and Scope

At this stage, the concept and scope are examined within well-defined operational, regulatory, and risk environments. The potential requirements and safety controls for managing functional safety are also identified.

Product	Application
• Identify the relevant legislation, regulations, standards, and codes of practice	• Identify the relevant legislation, regulations, standards, and codes of practice
• Identify the equipment under control and its intended use and limits of operation	• Clearly define the concept of operations
• Identify the potential operating environments	• Clearly define the operational parameters
• Identify the communication requirements	• Identify the actual operating environment
• Identify the OPS-specific risk criteria	• Identify the existing or planned communications infrastructure
	• Engage with the relevant regulators
	• Identify the operation-specific risk criteria

Provided from OPS to mine operator:

- All product expectations (as outlined in the product column above)

Provided from mine operator to OPS:

- All application expectations (as outlined in the application column above)

Table 3. Planning

This stage involves developing the process for managing functional safety and assigning the responsibilities for implementing it. See Appendix C for an example outline for a functional safety management plan.

Product	Application
• Document the process for how functional safety should be managed	• Set up the functional safety management plan based on the appropriate functional safety standard(s) where applicable and adapted to the specific application
• Set up the process for managing functional safety based on the appropriate functional safety standard(s) where applicable and adapted to the specific product	• Determine clear roles and responsibilities for all parties throughout the application lifecycle
• Put certified quality management in place (e.g., certified to ISO quality management systems standard, ISO 9001; 2015a)	

Provided from OPS to mine operator:

- Documentation of the rationale for the selection and use of the methodology for managing functional safety

Provided from mine operator to OPS:

- The expected use conditions for the equipment

Table 4. Hazard Identification and Risk Assessment

Robust hazard identification and risk assessment activities are completed at this stage so that the available controls can be identified, and effective decisions can be made about how to apply functional safety. During design, the OPS will typically complete the hazard identification and risk assessment for their product based on industry-wide standards. The mine operator applying the product will then complete their risk assessment with support from the OPS to clarify what risks are mitigated and to identify where they may need to put additional measures in place.

Product

- Identify all of the hazards associated with operating the product in its intended use cases, including foreseeable misuse
- Assess the risks associated with the hazards (use external sources such as ISO 17757 for a list of hazards to consider and a list of risk identification tools)
- Identify the existing controls
- Use an appropriate methodology and the appropriate tools (e.g., ISO 12100 or IEC 31010) to suit the equipment and related systems

Application

- Use a facilitator and group of stakeholders with the appropriate expertise
- Identify all hazards associated with operating the product(s) in the context of the operational scenario, including foreseeable misuse
- Assess the risks associated with the hazards (use external sources such as ISO 17757 for a list of hazards to consider and a list of risk identification tools)
- Identify the existing and proposed controls
- Use an appropriate methodology and the appropriate tools (e.g., ISO 12100 or IEC 31010) to suit the equipment and related systems

Provided from OPS to mine operator:

- A list of hazards considered
- Participation in risk assessment:
  - Communication of outcomes from OPS design risk assessment
  - Participation in the mine operator risk assessment
- A description of the product functionality / use cases and the primary risk controls of the equipment / safety manual

Provided from mine operator to OPS:

- A list of the hazards from the operation to consider

Table 5. Other Risk Controls

Other risk controls—safety-related controls that need to be handled outside of, but in parallel with, the functional safety lifecycle—also need to be considered. For example, these controls may include physical changes such as road width, access control, and signage that are needed to safely accommodate autonomous machines.

Action	Related lifecycle stage
Identified	Hazard identification and risk assessment (Table 4)
Specified	Control identification, specification, and requirements (Table 6)
Managed (in parallel)	Design and possible design modifications (Table 7)
Validated	Validation (Table 8)

Table 6. Control Identification, Specification, and Requirements

At this stage, the functional safety performance requirements and controls are defined and specified so that safety can be embedded in the design or in any design modifications.

Product	Application
• Define the safety function and the required safe state • Evaluate the performance and risk reduction requirements • Specify the safety requirements at the product level	• For existing (i.e., off-the-shelf) systems: – Conduct workshops with the OPS to understand the outcomes of the risk assessment and functional safety analysis to use as an input for the mine operator's risk assessment and procedures to enable safe operation of the system • For systems being modified extensively or a custom system that is being developed: – Conduct workshop(s) to define safety function performance and risk reduction requirements with input from product domain experts – Define the application-specific functional safety requirements, as identified in the layer of protection analysis (LOPA) or equivalent evaluation • Specify the safety requirements at the application level • Verify that the product performance meets the application targets

Provided from OPS to mine operator:

- Documented safety functions, including any safety-critical information, safety-related parts, and risk reduction requirements. These may be defined as integrity levels / performance levels if applicable.

Provided from mine operator to OPS:

- A revised safety requirements specification if modifications are made or the design is done in collaboration with the OPS

Table 7. Design / Possible Design Modifications

At this stage, the product is designed to meet the performance and risk reduction requirements and the functional safety requirements specification. Those applying the solution should verify the product and identify any possible design modifications.

Product (design)	Application (possible design modifications)
• Design the product in accordance with the performance and risk-reduction requirements identified in the control identification, specification, and requirements stage (Table 6) • Verify the design for safety • If the required application safety requirements specification performance target cannot be met, then provide the documentation to demonstrate that all reasonably practicable steps have been taken, any limitations are clearly identified, and the actual performance that can be achieved	• Verify that the product performance meets the performance requirements identified in the control identification, specification, and requirements stage (Table 6) • If required, apply any additional controls • Design the other risk controls identified in risk assessments in previous stages (e.g., road layout, access control)

Provided from OPS to mine operator:

- A listing of the safety functions of the autonomous system and what is required to maintain their integrity over the lifecycle of the machine / system

Provided from mine operator to OPS:

- A revised functional safety requirements specification

Table 8. Installation and Commissioning

This stage involves preparing the autonomous system to be put into service safely, including implementing installation and test plans.

Product	Application
• Develop clear instructions for on-site installation and commissioning • Generate the installation and configuration records • Implement the installation and test plan for safety functions • Run acceptance testing*	• Implement the installation plan for the overall system where applicable • Generate the installation and configuration records • Test the overall system, including the integration of sub-systems an ensuring a record is captured

Provided from OPS to mine operator:

- Installation and site acceptance test plan* for review
- Configuration checklist
- As-built and commissioning records

Provided from mine operator to OPS:

- Feedback on any deviations from installation and test plan or failures
- Configuration records where appropriate (e.g., communications network performance meets specified requirements)

Types of acceptance tests:* ***Factory acceptance test:* *An evaluation of the equipment completed by the vendor before installation to identify whether or not it is operating as specified. It is the final step of the manufacturing process.* ***Site acceptance test:*** *A joint activity between the vendor, integrator, and mine operator to identify whether or not the equipment is operating as specified and if the site is prepared for installation and commissioning. It is signed off by the integrator.* ***User acceptance test:*** *The testing completed by the mine operator to identify whether or not the system works for them and meets the business intent.*

Table 9. Validation

At this stage, procedures are completed to validate that the autonomous system has undergone all relevant assessments and meets all requirements. The product validation and application validation will not happen at the same time unless the OPS and mine operator are developing a custom solution.

Product	Application
• Clearly demonstrate that the product safety requirements have been fulfilled as defined in the product safety requirements specification • Confirm that all verifications and functional safety assessments have been completed as required • Document the residual risks after verification	• Confirm that the overall integrated system application validation is carried out at the mine site, working in conjunction with the OPS • Clearly demonstrate that the application safety requirements have been met as defined in the application safety requirements specification • Confirm that all additional controls required to meet risk reduction factors have been implemented • Confirm that the scope of validation covers the fully integrated system • Confirm that all required verifications and functional safety assessments have been completed

Provided from OPS to mine operator:

- Evidence that the product safety requirements have been met

Provided from mine operator to OPS:

- If the OPS agrees to validate a third-party modification or interface, then any required information that the OPS needs to evaluate the impact of the modification

Table 10. Operational Readiness

Assessing operational readiness is essential before the autonomous system can be safely operated. It is primarily an application process, but it uses input from product development (see also ISO 17757:2019).

Product	Application
• Provide the relevant support documentation and input (see list below of what the OPS provides to the mine operator)	• Confirm that configuration management processes related to functional safety are in place • Identify and procure the safety-critical spares • Confirm that preventive maintenance plans and strategies are in place (e.g., proof testing, inspections, end of life replacement) • Develop a strategy such as bypassing or overriding to manage impaired safety functions • Develop strategies for performance monitoring diagnostics • Recruit and train staff and assess their competencies • Develop and modify the standard operating procedures

Provided from OPS to mine operator:

- Test procedures
- Safety manuals, operating procedures, maintenance instructions, and other information required for operating and maintaining safety functions
- Performance monitoring diagnostics and training

Provided from mine operator to OPS:

- Confirmation that the functional safety-related requirements and specifications from the OPS have been met and are ready to go live

Table 11. Operation and Maintenance

Continuous functional safety management and maintenance are essential once the autonomous system is in operation; it is part of applying the solution, but it also requires support from the product side.

Product (support)	Application (operation and maintenance)
• Manage obsolescence • Provide fault investigation support and support continuous improvement (see change management, Table 12) • Manage incident alerts and advice • Provide training updates	• Manage safety-critical spares • Implement a strategy such as bypassing or overriding to manage impaired safety functions • Maintain a configuration management system for functional safety • Confirm that there is ongoing use of performance monitoring diagnostics • Maintain staff competencies • Verify all controls, including procedures and other risk reduction measures, on an ongoing basis • Revalidate the operational risk assessments periodically • Confirm that there is an appropriate investigation methodology (e.g., incident cause analysis method) in place with competent independent facilitators

Provided from OPS to mine operator:

- The documentation relevant to the support items listed under the product column

Provided from mine operator to OPS:

- Feedback on performance, incidents, and failures

Table 12. Change Management

Change management is a key consideration throughout the lifecycle to make sure that every change that is made allows for the same level of functional safety. Every time changes are made to a product or application, the stages from planning onward may need to be revisited to consider the adjustments. If the mine operator is modifying or developing a system independently from the OPS, some of the expectations under the product column may need to be met on the application side.

Product	Application
• Confirm that the change management process* covers the evaluation of functional safety, including impact analysis • Confirm that any changes made to the product that affect safety functions are communicated to all product owners, and the communications are documented • Reasonably support product owner in the change management process	• Confirm that the change management process covers the evaluation of functional safety, including impact analysis • Establish a mechanism to communicate product changes to the OPS and engage with them • Apply functional safety change management processes to anything that affects the risk profile (e.g., a new use case, environmental changes, new initiating events, or changes to existing events) • Confirm that the change management process defines the appropriate review and approval authorities

Provided from OPS to mine operator:

- An explanation of any changes that are made to the product that affect its safety functions

Provided from mine operator to OPS:

- The identification of opportunities for improvement with details for assessment

** Further detail on change management can be found in the GMG (2019) Guideline for the Implementation of Autonomous Systems in Mining.*

9. ΑΝΑΠΤΥΞΗ, ΕΠΑΛΗΘΕΥΣΗ ΚΑΙ ΕΠΙΚΥΡΩΣΗ ΛΟΓΙΣΜΙΚΟΥ

Το λογισμικό αυτόνομων συστημάτων εκτελεί συχνά λειτουργίες ασφαλείας. Η παρούσα ενότητα περιγράφει γενικές εκτιμήσεις σχετικά με την ανάπτυξη λογισμικού στο πλαίσιο του κύκλου ζωής της λειτουργικής ασφάλειας που περιγράφεται στην ενότητα 8. Επικεντρώνεται στις συμβατικές μεθόδους ανάπτυξης λογισμικού και στα ντετερμινιστικά συστήματα.

9.1. Αρχιτεκτονικές εκτιμήσεις

Οι απαιτήσεις για τις αρχιτεκτονικές λογισμικού των αυτόνομων συστημάτων ποικίλλουν ανάλογα με τη σχέση μεταξύ των στοιχείων ελέγχου και προστασίας.

Ενώ οι αρχιτεκτονικές συστημάτων που έχουν σχεδιαστεί με ξεχωριστά στοιχεία ελέγχου και προστασίας επιτρέπουν στις απαιτήσεις λειτουργικής ασφάλειας να επικεντρωθούν στο σύστημα προστασίας, αυτό δεν είναι πάντα δυνατό ή πρακτικό στις εφαρμογές κινητών μηχανών. Αυτός ο σαφής διαχωρισμός των στοιχείων ελέγχου και προστασίας είναι εφικτός εάν αυτοί που σχεδιάζουν τη λειτουργία προστασίας της ασφάλειας μπορούν να την καθορίσουν και να την υλοποιήσουν χωρίς να έχουν καμία πληροφορία για τη λειτουργία της λειτουργίας ελέγχου (βλέπε παράδειγμα Α). Αυτή η προσέγγιση της λειτουργικής ασφάλειας είναι χαρακτηριστική για τις σταθερές μηχανές σε περιβάλλοντα εργοστασιακού αυτοματισμού.

Εάν η γνώση της κατάστασης της λειτουργίας ελέγχου ή του τι κάνει είναι απαραίτητη για τη διατήρηση της ασφάλειας, είναι πολύ πιο δύσκολο να παραχθεί μια απλή, ανεξάρτητη λειτουργία προστασίας (βλ. Παράδειγμα Β). Σε τέτοιες περιπτώσεις, συνιστάται να στηρίζεται περισσότερο στην ακεραιότητα της λειτουργίας ελέγχου, ωστόσο, για τα αυτόνομα συστήματα, εξακολουθεί να υπάρχει αξιοσημείωτη εξάρτηση από άλλα διοικητικά και μη μέτρα μετριασμού του συστήματος ελέγχου.

Παράδειγμα Α: Κατάσταση όπου τα στοιχεία προστασίας και ελέγχου μπορούν να είναι χωριστά

Ένα υπόγειο σύστημα αυτοματισμού φόρτωσης, μεταφοράς, απόρριψης (δηλαδή το στοιχείο ελέγχου) διαχωρίζεται από την ανθρώπινη αλληλεπίδραση με ένα σύστημα

ελέγχου φραγμού (δηλαδή το στοιχείο προστασίας). Εάν το σύστημα φραγμού παραβιαστεί, το μηχάνημα μεταβαίνει σε μια ασφαλή κατάσταση, η οποία απαιτεί την τήρηση μιας συγκεκριμένης διαδικασίας για την επανέναρξη των αυτόνομων λειτουργιών. Αυτό λειτουργεί επειδή οι άνθρωποι, οι μηχανές και τα οχήματα μπορούν να διαχωριστούν από την αυτόνομη μηχανή.

Παράδειγμα Β: Κατάσταση όπου είναι απαραίτητη η γνώση της κατάστασης της λειτουργίας ελέγχου

Όταν τα συστήματα ελέγχου μηχανών (π.χ. σύστημα διεύθυνσης, πέδησης, πρόωσης) χρησιμοποιούνται ως μέρος ενός αυτόνομου συστήματος μηχανών γύρω από άλλες μηχανές και οχήματα με ανθρώπους μέσα σε αυτά, το αυτόνομο σύστημα πρέπει να γνωρίζει τι κάνει η μηχανή, πού πρέπει να πηγαίνει και πού βρίσκονται άλλα πράγματα, ώστε να μπορεί να ενεργεί ανάλογα. Οι είσοδοι σε αυτά τα συστήματα μπορούν να προέρχονται τόσο από ντετερμινιστικές όσο και από μη ντετερμινιστικές πτυχές. Η ασφάλεια εξαρτάται από τη σωστή λειτουργία των αυτόνομων συστημάτων και των συστημάτων μηχανών και από άλλα μέτρα μετριασμού των κινδύνων. Περισσότερες πληροφορίες σχετικά με τις μη ντετερμινιστικές πτυχές μπορείτε να βρείτε στη Λευκή Βίβλο και τις Κατευθυντήριες Αρχές για τη Λειτουργική Ασφάλεια των Μηχανημάτων Μετακίνησης Γης (2020) των CMEIG, EMESRT και ICMM.

9.2 Σκέψεις για τον κύκλο ζωής

Ο κύκλος ζωής της ανάπτυξης λογισμικού περιλαμβάνεται σε ένα μικρό τμήμα του κύκλου ζωής της λειτουργικής ασφάλειας που προσδιορίζεται στο ενότητα 8 και στο σχήμα 2, και συγκεκριμένα στον κύκλο ζωής του προϊόντος. Ο κύκλος ζωής του λογισμικού εντάσσεται κυρίως στα στάδια του σχεδιασμού/των πιθανών τροποποιήσεων του σχεδιασμού (πίνακας 7) και του προσδιορισμού του ελέγχου, των προδιαγραφών και των απαιτήσεων (πίνακας 6). Ορισμένα στοιχεία της επικύρωσης των απαιτήσεων λογισμικού αποτελούν μέρος του σταδίου επικύρωσης (Πίνακας 9).

Το Σχήμα 3 δείχνει πώς ο κύκλος ζωής της λειτουργικής ασφάλειας εντάσσεται σε ένα βασικό διάγραμμα V-μοντέλου ανάπτυξης λογισμικού. Τα πρότυπα λειτουργικής ασφάλειας χρησιμοποιούν παρόμοια μοντέλα V για την περιγραφή του κύκλου ζωής ανάπτυξης λογισμικού (π.χ. ISO 13849-1:2015, Σχήμα 6 και IEC 61508-3:2010, Σχήμα 6). Αυτός ο κύκλος ζωής αντιστοιχεί καλά με τον κύκλο ζωής της λειτουργικής ασφάλειας που περιγράφεται στην ενότητα 8 και η σχέση μεταξύ των δύο κύκλων ζωής είναι η ακόλουθη:

- Η "προδιαγραφή απαιτήσεων ασφάλειας λογισμικού" αποτελεί μέρος του σταδίου "προσδιορισμός, προδιαγραφή και απαιτήσεις ελέγχου" του Πίνακα 6.
- Η "επικύρωση και δοκιμή αποδοχής" αποτελεί μέρος του σταδίου "επικύρωση" στον πίνακα 9.
- Τα υπόλοιπα βήματα του Σχήματος 3 περιλαμβάνονται στο στάδιο "σχεδιασμός / πιθανές τροποποιήσεις σχεδιασμού" του Πίνακα 7.

Παράδειγμα Α: Κατάσταση όπου τα στοιχεία προστασίας και ελέγχου μπορούν να είναι χωριστά

Ένα υπόγειο σύστημα αυτοματοποίησης φορτίου, μεταφοράς, χωματερή (δηλαδή, το στοιχείο ελέγχου) διαχωρίζεται από την ανθρώπινη αλληλεπίδραση με ένα σύστημα ελέγχου φραγμού (δηλαδή, το στοιχείο προστασίας). Εάν παραβιαστεί το σύστημα φραγμού, το μηχάνημα μεταβαίνει σε ασφαλή κατάσταση, η οποία απαιτεί μια συγκεκριμένη διαδικασία που πρέπει να ακολουθηθεί για την επανεκκίνηση αυτόνομων λειτουργιών. Αυτό λειτουργεί επειδή οι άνθρωποι, μηχανές και τα οχήματα μπορούν να διαχωριστούν από την αυτόνομη μηχανή.

Παράδειγμα Β: Κατάσταση όπου είναι απαραίτητη η γνώση της κατάστασης της λειτουργίας ελέγχου

Όταν τα συστήματα ελέγχου μηχανών (π.χ. σύστημα διεύθυνσης, πέδησης, πρόωσης) χρησιμοποιούνται ως μέρος ενός αυτόνομου συστήματος μηχανών γύρω από άλλες μηχανές και οχήματα με ανθρώπους μέσα σε αυτά, το αυτόνομο σύστημα πρέπει να γνωρίζει τι είναι η μηχανή κάνει, πού πρέπει να πηγαίνει και πού βρίσκονται άλλα

πράγματα, ώστε να μπορεί να ενεργεί ανάλογα. Οι είσοδοι σε αυτά τα συστήματα μπορούν να προέρχονται τόσο από ντετερμινιστικές όσο και από μη ντετερμινιστικές πτυχές. Η ασφάλεια εξαρτάται από τη σωστή λειτουργία του αυτόνομων και μηχανικών συστημάτων και άλλων μέτρων μετριασμού των κινδύνων. Περισσότερες πληροφορίες για τις μη ντετερμινιστικές πτυχές μπορούν να βρεθούν στη Λευκή Βίβλο και τις Κατευθυντήριες αρχές για τη λειτουργική ασφάλεια για τις χωματουργικές εργασίες των CMEIG, EMESRT και ICMM. Machinery (2020).

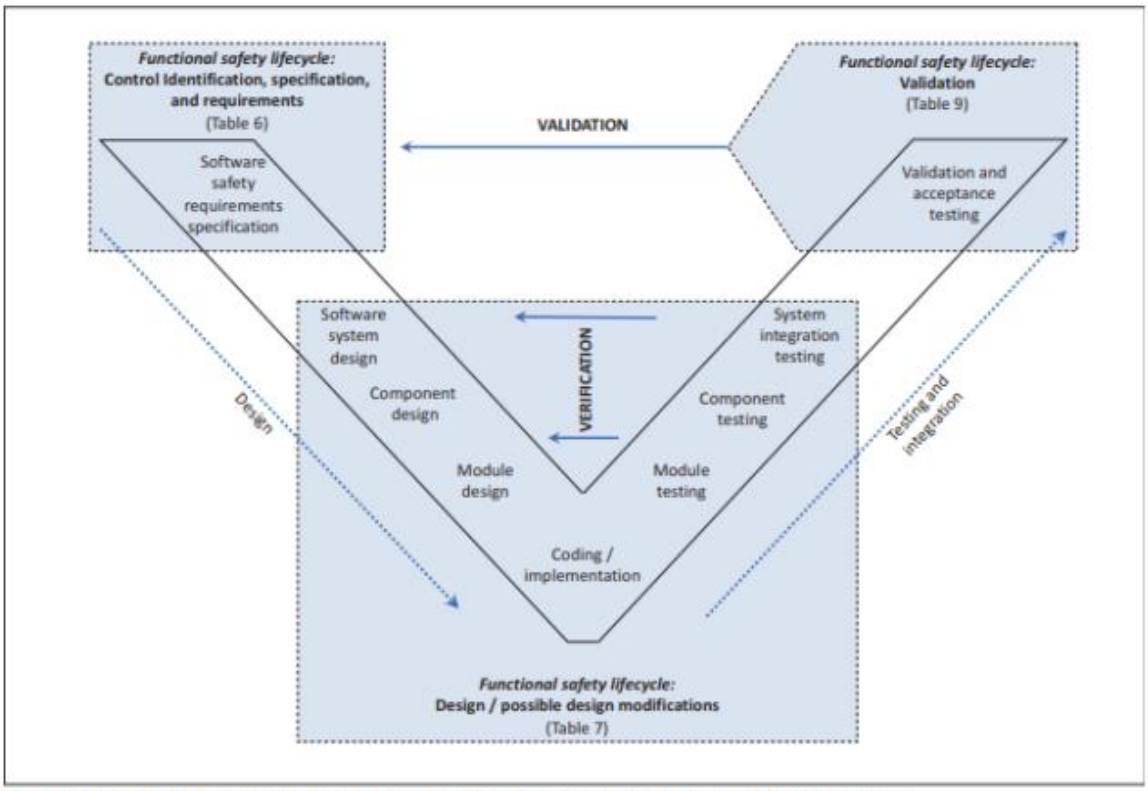

Figure 3. The Relationship between the Functional Safety Lifecycle and a Software Development V-Model Lifecycle Diagram

9.3 Ανάπτυξη συμβατικών στοιχείων συστήματος

Συνιστάται να αναπτύσσεται το λογισμικό με βάση τις απαιτήσεις απόδοσης της λειτουργίας ασφαλείας για έναν συγκεκριμένο έλεγχο και λαμβάνοντας υπόψη τα σχετικά πρότυπα (π.χ. ISO 13849, IEC 61508, ISO 19014). Όταν δημοσιευθεί, το ISO/DIS 19014-4, Μηχανήματα κίνησης γης - Λειτουργική ασφάλεια - Μέρος 4: Σχεδιασμός και αξιολόγηση του λογισμικού και της μετάδοσης δεδομένων για τα μέρη του συστήματος ελέγχου που σχετίζονται με την ασφάλεια, θα είναι πιθανότατα το πιο σχετικό πρότυπο (https:// www.iso.org/standard/70718.html). Οι απαιτήσεις επιδόσεων

ασφαλείας προσδιορίζονται συχνά από τη μείωση του κινδύνου που απαιτείται στο στάδιο "Προσδιορισμός, προδιαγραφή και απαιτήσεις ελέγχου" του κύκλου ζωής της λειτουργικής ασφάλειας (Πίνακας 6).

Για παράδειγμα, το πρότυπο ISO 13849-1:2015 περιλαμβάνει ανάλυση του βαθμού εξάρτησης από τις λειτουργίες ασφαλείας, καθορίζοντας τις απαιτήσεις επιδόσεων με τον καθορισμό των επιπέδων επιδόσεων (PL). Τα PL επισημαίνονται με α-ε, με το ε να αντιπροσωπεύει την υψηλότερη εξάρτηση από τη λειτουργία όσον αφορά την ασφάλεια. Βλέπε προσάρτημα Δ για ένα παράδειγμα των πιθανών δραστηριοτήτων ανάπτυξης λογισμικού για τα κατανεμημένα PLs με βάση το ISO 13849-12015. Ορισμένοι προγραμματιστές συστημάτων ενδέχεται να χρησιμοποιούν τεχνικές/μεθόδους όπως αυτές.

Τα λάθη που γίνονται κατά την ανάπτυξη λογισμικού μπορούν να μειωθούν με τον περιορισμό της χρήσης της γλώσσας προγραμματισμού. Μια επιλογή είναι η χρήση γλωσσών περιορισμένης μεταβλητότητας (LVLs). Για παράδειγμα, τα διαγράμματα λειτουργικών μπλοκ χρησιμοποιούνται για την κατασκευή προγραμμάτων με τη σύνδεση προκαθορισμένων λειτουργικών μπλοκ, μειώνοντας έτσι τα περιθώρια για σφάλματα. Όταν χρησιμοποιούνται πιο γενικές γλώσσες προγραμματισμού, είναι σύνηθες να χρησιμοποιείται ένα υποσύνολο γλώσσας, που σημαίνει ότι χρησιμοποιούνται μόνο ορισμένες από τις πτυχές μιας γλώσσας ή ότι χρησιμοποιούνται με συγκεκριμένο τρόπο. Για παράδειγμα, η Motor Industry Software Reliability Association (MISRA) έχει αναπτύξει κατευθυντήριες γραμμές για κοινά χρησιμοποιούμενες γλώσσες:

- MISRA C, Κατευθυντήριες γραμμές για τη χρήση της γλώσσας C σε κρίσιμα συστήματα (2013), η οποία έχει πλέον επικαιροποιηθεί για να αντιμετωπίσει τις ανησυχίες σχετικά με την ασφάλεια (2016).
- MISRA C++: Κατευθυντήριες γραμμές για τη χρήση της γλώσσας C++ σε κρίσιμα συστήματα (2008)

Αυτά τα υποσύνολα χρησιμοποιούνται πλέον ευρέως και υποστηρίζονται από εργαλεία. Αν και τα υποσύνολα δεν ορίζονται για όλες τις γλώσσες και υπάρχουν και άλλες παραλλαγές αυτών που ορίζονται, η χρήση ενός υποσυνόλου που επιβάλλεται από εργαλεία είναι καλή πρακτική.

10. ΔΙΑΧΕΙΡΙΣΗ ΙΚΑΝΟΤΗΤΩΝ

Όσοι διαχειρίζονται τη λειτουργική ασφάλεια αναμένεται να είναι επαρκώς ικανοί όσον αφορά τις γνώσεις, τις δεξιότητες, την εμπειρία και τη συμπεριφορά τους. Η παρούσα ενότητα παρέχει καθοδήγηση για τις εξορυκτικές επιχειρήσεις σχετικά με την αξιολόγηση της ικανότητας. Οι πιθανές απαιτήσεις επάρκειας περιλαμβάνουν τα εξής:

- Προσδιορισμός των σχετικών φάσεων του κύκλου ζωής της ασφάλειας
- Προσδιορισμός των καθηκόντων που πρέπει να εκτελεστούν στις φάσεις αυτές
- Ορισμός κριτηρίου ικανότητας για κάθε εργασία
- Ανάθεση των καθηκόντων σε ρόλους
- Ανάθεση των ρόλων σε τμήματα ή άτομα
- Ανάπτυξη και εκτέλεση σχεδίου αξιολόγησης
- Προγραμματισμός και προληπτική διαχείριση των κενών
- Διεξαγωγή περιοδικών αξιολογήσεων για να επιβεβαιωθεί ότι οι ικανότητες παραμένουν έγκυρες
- Διαχείριση των ικανοτήτων των νεοεισερχομένων
- Περιοδική επανεξέταση των καθηκόντων και των κριτηρίων για να επιβεβαιωθεί ότι παραμένουν επίκαιρα

Η καθοδήγηση για την επιτυχή εφαρμογή ενός σχεδίου διαχείρισης ικανοτήτων σε μια επιχείρηση περιλαμβάνει τα εξής βήματα:

- Αναπτύξτε τα κριτήρια ικανοτήτων ώστε να περιλαμβάνουν απαιτήσεις που αποδεικνύουν γνώσεις, δεξιότητες, εμπειρία και συμπεριφορές. Η απόδειξη αυτή θα πρέπει να υπερβαίνει τα μαθήματα κατάρτισης και τις πιστοποιήσεις, οι οποίες δεν είναι πάντα ολοκληρωμένες.
- Χρησιμοποιήστε σαφή γλώσσα στο πλαίσιο των κριτηρίων ικανοτήτων.
- Αντιστοιχίστε το επίπεδο λεπτομέρειας και αυστηρότητας των κριτηρίων ικανοτήτων με το επίπεδο επιδόσεων ασφαλείας που απαιτεί το προϊόν ή η εφαρμογή και το δυναμικό της να προκαλέσει βλάβη.
- Εξετάστε πώς να αξιολογήσετε τη γνώση τομέα βάσει των κριτηρίων επάρκειας. Για παράδειγμα, ενώ μπορεί να είναι καλό να υπάρχει ένας εμπειρογνώμονας λειτουργικής ασφάλειας επί του σκάφους, η εμπειρογνωμοσύνη τους πρέπει να

συμπληρώνεται από τη γνώση των εξορυκτικών εργασιών και των αυτόνομων συστημάτων.

- Ενσωμάτωση κριτηρίων ικανότητας σε υπάρχοντα συστήματα. Ορισμένες εταιρείες διαθέτουν ένα πλαίσιο ή σύστημα ικανότητας (π.χ. διαχείριση κινδύνων για την υγεία και την ασφάλεια με την εργασία σε περιορισμένο χώρο).
- Συνεργασία με OPS για βοήθεια με επίσημη εκπαίδευση, προσομοίωση κατάρτισης, κοινές αξιολογήσεις κατά την εργασία και παράδοση, εάν δεν υπάρχει επαρκής ικανότητα στο πλαίσιο της επιχείρησης.
- Επιτρέψτε στη διαδικασία ανάπτυξης κριτηρίων να αποκαλύψει κενά ικανοτήτων. Τα κενά ικανότητας μπορούν στη συνέχεια να αντιμετωπιστούν μέσω στρατηγικών όπως η συνεργασία μεταξύ των μελών της ομάδας που πληρούν συλλογικά τις απαιτήσεις ικανότητας για μια δεδομένη εργασία.

Η συνιστώμενη βιβλιογραφία που εξετάζει λεπτομερώς τη διαχείριση των ικανοτήτων λειτουργικής ασφάλειας περιλαμβάνει:

- Ινστιτούτο Μηχανικής και Τεχνολογίας (2016), Κριτήρια ικανότητας για ασκούμενους συστημάτων που σχετίζονται με την ασφάλεια
- Η Εκτελεστική Αρχή Υγείας και Ασφάλειας του Ηνωμένου Βασιλείου (2006, 2007), Διαχείριση ικανοτήτων για συστήματα που σχετίζονται με την ασφάλεια

11. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Η κυβερνοασφάλεια είναι ένα αναδυόμενο ζήτημα που μπορεί να επηρεάσει σημαντικά τις λειτουργίες ασφάλειας των αυτόνομων συστημάτων και, ως εκ τούτου, θα πρέπει να λαμβάνεται υπόψη καθ' όλη τη διάρκεια του κύκλου ζωής τους. Επειδή τα αυτόνομα συστήματα βασίζονται σε μεγάλο βαθμό στο λογισμικό, οι απειλές που επηρεάζουν τη λειτουργία των αισθητήρων, το σχεδιασμό του λογισμικού, τη δια λειτουργικότητα του συστήματος και την αλληλεπίδραση ανθρώπου-μηχανής έχουν τη δυνατότητα να επηρεάσουν τη λειτουργική ασφάλεια. Υπάρχουν επίσης απειλές κυβερνοασφάλειας που στοχεύουν ειδικά τα συστήματα ασφαλείας.

Τα μέτρα κυβερνοασφάλειας θα πρέπει να διατηρούν τη λειτουργικότητα ασφαλείας του αυτόνομου συστήματος. Το σύστημα θα πρέπει να είναι σχεδιασμένο ώστε να ενεργεί για τη διατήρηση της ασφάλειας ως ύψιστης προτεραιότητας εάν του αποστέλλονται μηνύματα που θα μπορούσαν να οδηγήσουν σε μη ασφαλή λειτουργία. Η ασφάλεια των διεπαφών ελέγχου θα πρέπει να εξετάζεται και να διαχειρίζεται ως μέρος της διαδικασίας διαχείρισης κινδύνου λειτουργικής ασφάλειας και θα πρέπει να καλύπτει τις απαιτήσεις συμμόρφωσης, πιστοποίησης και μετριασμού του κινδύνου ακολουθώντας τη μεθοδολογία "στο μέτρο του ευλόγως εφικτού". Συνιστάται η διενέργεια εκτίμησης κινδύνου σχετικά με τις απειλές κυβερνοασφάλειας με τη χρήση πληροφοριών από το μοντέλο απειλών αυτόνομων συστημάτων MM-ISAC (http://www.mmisac.org/).

Η συνιστώμενη βιβλιογραφία για την ασφάλεια στον κυβερνοχώρο περιλαμβάνει:

IEC TR 63069:2019 *Μέτρηση, έλεγχος και αυτοματοποίηση βιομηχανικής διαδικασίας - Πλαίσιο για λειτουργική ασφάλεια και ασφάλεια* (Διεθνής Ηλεκτροτεχνική Επιτροπή, 2019a)

IEC TR 63074:2019 *Ασφάλεια μηχανημάτων - Πτυχές ασφαλείας σχετικά με τη λειτουργική ασφάλεια των συστημάτων ελέγχου που σχετίζονται με την ασφάλεια* (Διεθνής Ηλεκτροτεχνική Επιτροπή, 2019d)

ISA TR 84.00.09_2017 *Κυβερνοασφάλεια σε σχέση με τον κύκλο ζωής της λειτουργικής ασφάλειας* (Διεθνής Εταιρεία Αυτοματισμού, 2017)

Αναλυτικότερες οδηγίες για την ασφάλεια στον κυβερνοχώρο θα αναπτυχθούν μέσω του έργου GMG System Safety for Autonomous Mining και της ομάδας εργασίας GMG-MMISAC Cybersecurity.

12. ΤΕΚΜΗΡΙΩΣΗ ΔΙΑΣΦΑΛΙΣΗΣ

Ο φορέας εκμετάλλευσης του ορυχείου και το OPS θα πρέπει να συνεργάζονται σχετικά με την τεκμηρίωση και την ανάλυση διασφάλισης που είναι κατάλληλες για το σύστημα. Οι επιλογές που πρέπει να εξεταστούν περιλαμβάνουν:

- Παραπομπές σε ή συμμόρφωση με τα σχετικά διεθνή πρότυπα, συμπεριλαμβανομένων, κατά περίπτωση, των προτύπων λειτουργικής ασφάλειας
- Αποτελέσματα της ανάλυσης κινδύνων και επικινδυνότητας
- Ένας κατάλογος των λειτουργιών ασφαλείας, περιγραφή της λειτουργικότητάς τους και των ασφαλών καταστάσεων λειτουργίας
- Οι περιορισμοί του συστήματος ή οι στόχοι ασφαλείας που είναι απαραίτητοι για την ασφαλή λειτουργία του συστήματος στον τόπο εγκατάστασης
- Έκθεση επικύρωσης ότι όλες οι λειτουργίες ασφαλείας λειτουργούν κατά τη διάρκεια της θέσης σε λειτουργία επί τόπου (όπου αυτό είναι εφικτό)
- Εάν οι λειτουργίες ασφαλείας δεν είναι δυνατόν να δοκιμαστούν επί τόπου, αποδεικτικά στοιχεία επικύρωσης των εν λόγω λειτουργιών ασφαλείας
- Αποτελέσματα αιτιώδους ανάλυσης, για παράδειγμα ανάλυση τρόπων αστοχίας και επιδράσεων (FMEA), ανάλυση δέντρου σφαλμάτων (FTA) και θεωρητική ανάλυση διεργασιών συστημάτων (STPA).
- Επισκόπηση της διαδικασίας ανάπτυξης λογισμικού που μπορεί να χρησιμοποιεί μεθόδους όπως αυτές του ISO 19014, του ISO 13849 ή του IEC 61508.

Σημειώστε ότι ορισμένα έγγραφα ενδέχεται να μην μπορούν να διαμοιραστούν λόγω των απαιτήσεων προστασίας της πνευματικής ιδιοκτησίας για το OPS. Σε τέτοιες περιπτώσεις, το OPS και ο φορέας εκμετάλλευσης του ορυχείου θα πρέπει να συμφωνήσουν σε έναν κατάλληλο μηχανισμό για την παροχή επαρκούς διαβεβαίωσης για την ασφάλεια του προϊόντος στον φορέα εκμετάλλευσης του ορυχείου.

Μπορεί επίσης να είναι χρήσιμο για το OPS να παρέχει μια υψηλού επιπέδου επισκόπηση της διαχείρισης του κύκλου ζωής των προϊόντων του OPS στον φορέα εκμετάλλευσης του ορυχείου.

13. ΜΗ ΝΤΕΤΕΡΜΙΝΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ

Στην παρούσα κατάσταση, η εξορυκτική βιομηχανία είναι συνηθισμένη σε συστήματα που είναι κυρίως ντετερμινιστικά, δηλαδή ανταποκρίνονται σε γνωστές και κατανοητές καταστάσεις, τρόπους αστοχίας και συνθήκες. Με βάση τις τρέχουσες τάσεις στην εξέλιξη της εξόρυξης και άλλων βιομηχανιών, είναι πιθανό να επικρατήσουν μη ντετερμινιστικά συστήματα και πτυχές των συστημάτων. Ένα μη ντετερμινιστικό σύστημα είναι ένα σύστημα όπου οι αποφάσεις προέρχονται από πολύπλοκους αλγορίθμους αισθητήρων και επεξεργασίας ή/και περιλαμβάνουν μηχανική μάθηση. Παραδείγματα μη ντετερμινιστικών συστημάτων περιλαμβάνουν:

- Συστήματα αντίληψης (συμπεριλαμβανομένων των συστημάτων αποφυγής σύγκρουσης)
- Τεχνολογία GPS (συμπεριλαμβανομένων των γεωφράξεων)
- Συστήματα σχεδιασμού διαδρομής με βάση την τεχνητή νοημοσύνη

Τα υφιστάμενα πρότυπα περιλαμβάνουν την απόδοση επιπέδων απόδοσης ή ακεραιότητας και μπορούν να εφαρμοστούν πιο άμεσα σε ντετερμινιστικά συστήματα. Επειδή τα μη ντετερμινιστικά συστήματα αντιδρούν σε συνθήκες με βάση την πιθανότητα, οι αντιδράσεις αυτές δεν μπορούν να ποσοτικοποιηθούν με τη χρήση αυτών των μεθόδων. Η Λευκή Βίβλος και οι κατευθυντήριες αρχές για τη λειτουργική ασφάλεια των χωματουργικών μηχανημάτων (2020) των CMEIG, EMESRT και ICMM προσφέρουν ορισμένες οδηγίες υψηλού επιπέδου σχετικά με την κατεύθυνση της εξορυκτικής βιομηχανίας όσον αφορά τα μη ντετερμινιστικά συστήματα. Περιγράφουν:

- **Μια προσωρινή προσέγγιση μέχρι να υπάρξουν νέα πρότυπα**: Μια αξιολόγηση με βάση τον κίνδυνο που συνδυάζει παραδοσιακές και εξελισσόμενες τεχνικές διαχείρισης κινδύνου, μια ισχυρή διαδικασία ανάπτυξης, ένα εκτεταμένο πλαίσιο δοκιμών και επικύρωσης του συστήματος και μια ισχυρή δέσμευση και συνεργασία μεταξύ των σχετικών ενδιαφερομένων μερών. ("Προτεινόμενη προσέγγιση για την αξιολόγηση συστημάτων με μη ντετερμινιστικές πτυχές", CMEIG, EMESRT και ICMM, 2020).
- **Η προσέγγιση στην αυτοκινητοβιομηχανία:** ISO/PAS 21448:2019 Οδικά οχήματα - Ασφάλεια της προβλεπόμενης λειτουργικότητας προορίζεται να

εφαρμοστεί για την αξιολόγηση των μη ντετερμινιστικών πτυχών των συστημάτων που σχετίζονται με την ασφάλεια μέσω "εκτεταμένης επικύρωσης σε μια σειρά περιπτώσεων χρήσης/κατάχρησης". ("Προσέγγιση άλλων βιομηχανιών", CMEIG, EMESRT και ICMM, 2020).

- **Σχετικές εργασίες τυποποίησης για χωματουργικά μηχανήματα**: Η επιτροπή ISO/TC 127 για τα χωματουργικά μηχανήματα διεξάγει κάποιες εργασίες για την αντιμετώπιση της σημερινής έλλειψης τυποποίησης στον τομέα αυτό, συμπεριλαμβανομένης της προσαρμογής της προσέγγισης της ασφάλειας της προβλεπόμενης λειτουργικότητας στην αυτοκινητοβιομηχανία για τα χωματουργικά οχήματα (ISO/TC 127/SC2 WG 24; https://www.iso.org/committee/52180.html).

14. ΜΕΛΛΟΝΤΙΚΕΣ ΕΡΓΑΣΙΕΣ

Επειδή η λειτουργική ασφάλεια των αυτόνομων συστημάτων στα ορυχεία είναι ένα ταχέως εξελισσόμενο θέμα, η παρούσα κατευθυντήρια γραμμή αναμένεται επίσης να εξελίσσεται και να προσθέτει κάθε κατάλληλη λεπτομέρεια με την πάροδο του χρόνου, ώστε να ευθυγραμμίζεται με τα νέα και επικαιροποιημένα πρότυπα και να λαμβάνει υπόψη τις αναδυόμενες έννοιες και τεχνολογικές εξελίξεις. Ένα ξεχωριστό έργο της GMG για την ασφάλεια συστημάτων βρίσκεται επίσης σε εξέλιξη και θα συμπληρώσει την παρούσα κατευθυντήρια γραμμή εξετάζοντας παρακείμενα θέματα όπως η περίπτωση ασφάλειας και η διαχείριση κινδύνων, οι ανθρώπινοι παράγοντες, η ολοκλήρωση και η επαλήθευση και επικύρωση.

15. ΠΟΡΟΙ ΚΑΙ ΑΝΑΦΟΡΕΣ

Construction and Mining Equipment Industry Group (CMEIG), Earth Moving Equipment Safety Round Table (EMESRT) και International Council on Mining and Metals (ICMM). (2020). Λευκή Βίβλος και κατευθυντήριες αρχές για τη λειτουργική ασφάλεια των μηχανημάτων χωματουργικών εργασιών. Ανακτήθηκε από https://www.cmeig.com.au/working-groups/engineering/.

Παγκόσμια ομάδα κατευθυντήριων γραμμών για την εξόρυξη (2019). Κατευθυντήρια γραμμή για την εφαρμογή αυτόνομων συστημάτων στα ορυχεία (2019). Κατευθυντήρια γραμμή αριθ. 20181008_Implementation_of_Autonomous_Systems-GMG-AM-v01-r01. Ανακτήθηκε από https://gmggroup.org/wp-content/uploads/2019/06/20181008_Implementation_of_Autonomous_Systems-GMG-AM-v01-r01.pdf

Κυβέρνηση της Δυτικής Αυστραλίας Υπουργείο Ορυχείων, Ρύθμισης Βιομηχανίας και Ασφάλειας (2015). Ασφαλής κινητή αυτόνομη εξόρυξη στη Δυτική Αυστραλία [Κώδικας πρακτικής]. Ανακτήθηκε από http://www.dmp.wa.gov.au/Documents/Safety/MSH_COP_SafeMobile AutonomousMiningWA.pdf

Ινστιτούτο Μηχανικής και Τεχνολογίας (2016). Κώδικας πρακτικής: Κριτήρια επάρκειας για επαγγελματίες που ασχολούνται με συστήματα που σχετίζονται με την ασφάλεια. Ανακτήθηκε από https://shop.theiet.org/code-of-practice-competence-for-safety-related-systems-practitioners.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2010α). Λειτουργική ασφάλεια ηλεκτρικών/ηλεκτρονικών/προγραμματιζόμενων ηλεκτρονικών συστημάτων σχετικών με την ασφάλεια - Μέρος 1: Γενικές απαιτήσεις (Πρότυπο αριθ. IEC 61508-1:2010). Ανακτήθηκε από https://webstore.iec.ch/publication/5515.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2010β). Λειτουργική ασφάλεια ηλεκτρικών/ηλεκτρονικών/προγραμματιζόμενων ηλεκτρονικών συστημάτων που σχετίζονται με την ασφάλεια - Μέρος 2: Απαιτήσεις για ηλεκτρικά/ηλεκτρονικά/προγραμματιζόμενα ηλεκτρονικά συστήματα που σχετίζονται με την ασφάλεια (Πρότυπο αριθ. IEC 61508-2:2010). Ανακτήθηκε από https://webstore.iec.ch/publication/5516

Διεθνής Ηλεκτροτεχνική Επιτροπή (2010c). Λειτουργική ασφάλεια ηλεκτρικών/ηλεκτρονικών/προγραμματιζόμενων ηλεκτρονικών συστημάτων σχετικών με την ασφάλεια - Μέρος 3: Απαιτήσεις λογισμικού (Πρότυπο αριθ. IEC 61508-3:2010). Ανακτήθηκε από https://webstore.iec.ch/publication/5517.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2010δ). Λειτουργική ασφάλεια ηλεκτρικών/ηλεκτρονικών/προγραμματιζόμενων ηλεκτρονικών συστημάτων σχετικών με την ασφάλεια - Μέρος 4: Ορισμοί και συντομογραφίες (Πρότυπο αριθ. IEC 61508-4:2010). Ανακτήθηκε από https://webstore.iec.ch/publication/5518

Διεθνής Ηλεκτροτεχνική Επιτροπή (2010ε). Λειτουργική ασφάλεια ηλεκτρικών/ηλεκτρονικών/προγραμματιζόμενων ηλεκτρονικών συστημάτων σχετικών με την ασφάλεια - Μέρος 5: Παραδείγματα μεθόδων για τον προσδιορισμό των επιπέδων ακεραιότητας ασφάλειας (Πρότυπο αριθ. IEC 61508-5:2010). Ανακτήθηκε από https://webstore.iec.ch/publication/5519.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2010στ). Λειτουργική ασφάλεια ηλεκτρικών/ηλεκτρονικών/προγραμματιζόμενων ηλεκτρονικών συστημάτων σχετικών με την ασφάλεια - Μέρος 6: Κατευθυντήριες γραμμές για την εφαρμογή των προτύπων IEC 61508-2 και IEC 61508-3 (Πρότυπο αριθ. IEC 61508-6:2010). Ανακτήθηκε από https://webstore.iec.ch/publication/5520

Διεθνής Ηλεκτροτεχνική Επιτροπή (2010g). Λειτουργική ασφάλεια ηλεκτρικών/ηλεκτρονικών/προγραμματιζόμενων ηλεκτρονικών συστημάτων σχετικών με την ασφάλεια - Μέρος 7: Επισκόπηση τεχνικών και μέτρων (IEC 61508-7:2010). Ανακτήθηκε από https://webstore.iec.ch/publication/5521.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2015β). Ασφάλεια μηχανημάτων - Λειτουργική ασφάλεια των σχετικών με την ασφάλεια ηλεκτρικών, ηλεκτρονικών και προγραμματιζόμενων ηλεκτρονικών συστημάτων ελέγχου (Πρότυπο αριθ. IEC 62061:2005 +AMD1:2012+AMD2:2015 CSV). Ανακτήθηκε από https://webstore.iec.ch/publication/22797.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2016). Ηλεκτρικά συστήματα μετάδοσης κίνησης ρυθμιζόμενων στροφών - Μέρος 5-2: Απαιτήσεις ασφάλειας - Λειτουργικές (Πρότυπο αριθ. IEC 61800-5-2:2016). Ανακτήθηκε από https://webstore.iec.ch/publication/24556.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2019α). Μέτρηση, έλεγχος και αυτοματισμός βιομηχανικών διεργασιών - Πλαίσιο για λειτουργική ασφάλεια και προστασία (Πρότυπο αριθ. IEC TR 63069:2019). Ανακτήθηκε από https://webstore.iec.ch/publication/31421.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2019β). Διαχείριση κινδύνων - Τεχνικές εκτίμησης κινδύνων (Πρότυπο αρ. IEC 31010:2019). Ανακτήθηκε από https://webstore.iec.ch/publication/59809.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2019γ). Ασφάλεια μηχανημάτων - Αισθητήρες που σχετίζονται με την ασφάλεια και χρησιμοποιούνται για την προστασία ατόμων (Πρότυπο αρ. IEC TS 62998-1:2019). Ανακτήθηκε από https://webstore.iec.ch/publication/31009.

Διεθνής Ηλεκτροτεχνική Επιτροπή (2019δ). Ασφάλεια μηχανημάτων - Πτυχές ασφάλειας που σχετίζονται με τη λειτουργική ασφάλεια των συστημάτων ελέγχου που σχετίζονται με την ασφάλεια (Πρότυπο αριθ. IEC TR 63074:2019). Ανακτήθηκε από https://webstore.iec.ch/publication/31572.

Διεθνής Οργανισμός Τυποποίησης (2007α). Μηχανήματα χωματουργικών εργασιών - Μηχανήματα με ελαστικά - Απαιτήσεις οδήγησης (Πρότυπο αριθ. ISO 5010: 2007) Ανακτήθηκε από https://www.iso.org/standard/45105.html.

Διεθνής Οργανισμός Τυποποίησης (2010). Ασφάλεια μηχανημάτων - Γενικές αρχές σχεδιασμού - Εκτίμηση και μείωση κινδύνων (Πρότυπο αριθ. ISO 12100-2:2010). Ανακτήθηκε από https://www.iso.org/standard/51528.html.

Διεθνής Οργανισμός Τυποποίησης (2011α). Μηχανήματα χωματουργικά - Τροχοφόρα ή υψηλής ταχύτητας μηχανήματα με ερπύστριες από καουτσούκ - Απαιτήσεις επιδόσεων και διαδικασίες δοκιμής για συστήματα πέδησης (Πρότυπο αριθ. ISO 3450: 2011) Ανακτήθηκε από https://www.iso.org/standard/42076.html.

Διεθνής Οργανισμός Τυποποίησης (2011β). Ρομπότ και ρομποτικές συσκευές - Απαιτήσεις ασφάλειας για βιομηχανικά ρομπότ - Μέρος 1: Ρομπότ (Πρότυπο αριθ. ISO 10218-1:2011) Ανακτήθηκε από https://www.iso.org/standard/51330.html

Διεθνής Οργανισμός Τυποποίησης (2012α). Χωματουργικά μηχανήματα - Απαιτήσεις ασφάλειας για συστήματα τηλεχειρισμού (Πρότυπα αρ. ISO 15817:2012) Ανακτήθηκε από https://www.iso.org/standard/46237.html.

Διεθνής Οργανισμός Τυποποίησης (2012β). Ασφάλεια μηχανημάτων - Μέρη συστημάτων ελέγχου που σχετίζονται με την ασφάλεια - Μέρος 2: Επικύρωση (Πρότυπο αριθ. ISO 13849-2:2012). Ανακτήθηκε από https://www.iso.org/standard/53640.html.

Διεθνής Οργανισμός Τυποποίησης (2015α). Συστήματα διαχείρισης ποιότητας - Απαιτήσεις (Πρότυπο αριθ. ISO 9001:2015). Ανακτήθηκε από https://www.iso.org/standard/62085.html.

Διεθνής Οργανισμός Τυποποίησης (2015β). Ασφάλεια μηχανημάτων - Μέρη συστημάτων ελέγχου που σχετίζονται με την ασφάλεια - Μέρος 1: Γενικές αρχές σχεδιασμού (Πρότυπο αριθ. ISO 13849-1:2015). Ανακτήθηκε από https://www.iso.org/standard/69883.html.

Διεθνής Οργανισμός Τυποποίησης (2015γ). Μηχανική συστημάτων και λογισμικού - Διαδικασίες κύκλου ζωής συστήματος (Πρότυπο αρ. ISO/ IEC/IEEE 15288: 2015) Ανακτήθηκε από https://www.iso.org /standard/63711.html

Διεθνής Οργανισμός Τυποποίησης (2017α). Μηχανήματα χωματουργικών εργασιών - Συστήματα ανίχνευσης αντικειμένων και βοηθήματα ορατότητας - Απαιτήσεις επιδόσεων και δοκιμές (Πρότυπα αριθ. ISO 16001: 2017) Ανακτήθηκε από https://www.iso.org/standard/63688.html.

Διεθνής Οργανισμός Τυποποίησης (2017β). Χωματουργικά μηχανήματα - Ασφάλεια - Μέρος 1: Γενικές απαιτήσεις (Πρότυπο αριθ. ISO 20474-1: 2017) Ανακτήθηκε από https:// www.iso.org/standard/60734.html

Διεθνής Οργανισμός Τυποποίησης (2017γ). Διαχείριση ποιότητας - Κατευθυντήριες γραμμές για τη διαχείριση διαμόρφωσης (Πρότυπο αριθ. ISO 10007:2017). Ανακτήθηκε από https://www.iso.org/standard/70400.html

Διεθνής Οργανισμός Τυποποίησης (2018α). Μηχανήματα χωματουργικά και οικοδομικά - Ηλεκτρομαγνητική συμβατότητα (ΗΜΣ) μηχανημάτων με εσωτερική ηλεκτρική τροφοδοσία - Μέρος 1: Γενικές απαιτήσεις ΗΜΣ υπό τυπικές περιβαλλοντικές συνθήκες (Πρότυπο αριθ. ISO 13766-1:2018) Ανακτήθηκε από https://www.org/standard/67347.html.

Διεθνής Οργανισμός Τυποποίησης (2018β). Μηχανήματα χωματουργικά και οικοδομικά - Ηλεκτρομαγνητική συμβατότητα (ΗΜΣ) μηχανών με εσωτερική ηλεκτρική τροφοδοσία - Μέρος 2: Πρόσθετες απαιτήσεις ΗΜΣ για λειτουργική ασφάλεια (Πρότυπο αριθ. ISO 13766-2:2018) Ανακτήθηκε από https://www.iso.org/standard/67403.html.

Διεθνής Οργανισμός Τυποποίησης (2018γ). Χωματουργικά μηχανήματα - Λειτουργική ασφάλεια - Μέρος 1: Μεθοδολογία για τον προσδιορισμό των σχετικών με την ασφάλεια τμημάτων του συστήματος ελέγχου και των απαιτήσεων επιδόσεων (Πρότυπο αριθ. ISO 19014-1:2018). Ανακτήθηκε από https://www.iso.org/standard/70715.html.

Διεθνής Οργανισμός Τυποποίησης (2018δ). Χωματουργικά μηχανήματα - Λειτουργική ασφάλεια - Μέρος 3: Περιβαλλοντικές επιδόσεις και απαιτήσεις δοκιμής ηλεκτρονικών και ηλεκτρικών εξαρτημάτων που χρησιμοποιούνται σε μέρη του συστήματος ελέγχου που σχετίζονται με την ασφάλεια (Πρότυπο αριθ. ISO 19014-3:2018). Ανακτήθηκε από https://www.iso.org/standard/70717.html

Διεθνής Οργανισμός Τυποποίησης (2018ε). Διαχείριση κινδύνων-Κατευθυντήριες γραμμές (Πρότυπο αριθ. ISO 31000:2018). Ανακτήθηκε από https://www.iso.org/standard/65694.html.

Διεθνής Οργανισμός Τυποποίησης (2018στ). Οδικά οχήματα-Λειτουργική ασφάλεια-Μέρος 1: Λεξιλόγιο (Πρότυπο Αρ. ISO 26262-1: 2018). Ανακτήθηκε από https://www.iso.org/standard/68383.html

Διεθνής Οργανισμός Τυποποίησης (2019α). Μηχανοκίνητα μηχανήματα και εξόρυξη-ασφάλεια αυτόνομων και ημιαυτόνομων συστημάτων μηχανών (Πρότυπο Αρ. 17757: 2019). Ανακτήθηκε από https://www.iso.org/standard/76126.html

Διεθνής Οργανισμός Τυποποίησης (2019b). Οδικά οχήματα - Ασφάλεια της προβλεπόμενης λειτουργικότητας (Πρότυπο αριθ. ISO/ PAS 21448: 2019) Ανακτήθηκε από https://www.iso.org/standard /70939.html

Διεθνής Εταιρεία Αυτοματισμού (2017) Κυβερνοασφάλεια σε σχέση με τον κύκλο ζωής της λειτουργικής ασφάλειας. (Πρότυπο Αρ. ISA-TR84.00.09). Ανακτήθηκε από https://www.isa.org/store/isa-tr840009-2017,-cybersecurity-related-to-the-functional-safety-lifecycle/56889051

MISRA (2013). Οδηγίες για τη χρήση της γλώσσας C σε κρίσιμα συστήματα (Αρ. Κατευθυντήριων γραμμών MISRA C: 2012). Ανακτήθηκε από https://www.misra.org.uk/Publications/tabid/57/Default.aspx

MISRA (2016). Πρόσθετες οδηγίες ασφαλείας για το MISRA C: 2012 (Αρ. Κατευθυντήριων γραμμών MISRA C: 2012 - Τροπολογία 1) Ανακτήθηκε από https://www.misra.org.uk/Publications/tabid/57/Default.aspx

MISRA (2008). Οδηγίες για τη χρήση της γλώσσας C ++ σε κρίσιμα συστήματα. (Οδηγία ΑΡΙΘ. MISRA C ++) Ανακτήθηκε από https://www.misra.org.uk/Publications/tabid/57/Default.aspx

Στέλεχος Υγείας και Ασφάλειας του Ηνωμένου Βασιλείου (2006). Διαχειριστική ικανότητα για συστήματα που σχετίζονται με την ασφάλεια, Μέρος 1: Βασικές οδηγίες. Ανακτήθηκε από http://www.hse.gov.uk/humanfactors/topics/mancomppt1.pdf

Στέλεχος Υγείας και Ασφάλειας του Ηνωμένου Βασιλείου (2007). Διαχειριστική ικανότητα για συστήματα που σχετίζονται με την ασφάλεια, Μέρος 2: Συμπληρωματικό υλικό. Ανακτήθηκε από http://www.hse.gov.uk/humanfactors/topics/mancomppt2.pdf

Αμυντική τυποποίηση του Ηνωμένου Βασιλείου (2017). Διαχείριση ασφάλειας για αμυντικά συστήματα. Τεύχος 7. (Πρότυπο Αρ. MOD DEF STAN 00-56).

ΠΡΟΣΑΡΤΗΜΑ Α: ΛΕΙΤΟΥΡΓΙΚΗ ΑΣΦΑΛΕΙΑ ΣΤΗ ΣΥΝΟΛΙΚΗ ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Η συνολική ασφάλεια βασίζεται σε στοιχεία ενός συστήματος ασφαλείας να σχεδιάζονται και να λειτουργούν με ασφάλεια. Η λειτουργική ασφάλεια είναι μέρος του ευρύτερου πλαισίου της συνολικής ασφάλειας, το οποίο αποτελείται από τα ακόλουθα επίπεδα:

- Οι κοινωνικές προσδοκίες για την ασφάλεια. Αυτό που θεωρείται ασφαλές αποφασίζεται από κοινωνικά καθορισμένες περιγραφές για τους κινδύνους που θεωρούνται ανεκτοί σε σχέση με τα οφέλη από τη λειτουργία ενός συστήματος. Αυτές οι κοινωνικές προσδοκίες εκφράζονται μέσω της νομοθεσίας και του κοινού δικαίου.
- Τα συστήματα διαχείρισης της ασφάλειας τίθενται σε εφαρμογή για να επιβεβαιώσουν ότι ένα σύστημα λειτουργεί με ασφάλεια. Αυτά περιλαμβάνουν τη διαχείριση κινδύνων, έκτακτης ανάγκης και αλλαγών και την καθιέρωση κουλτούρας ασφάλειας.
- Η ασφάλεια συστήματος επιβεβαιώνει ότι ο συνολικός σχεδιασμός ενός συστήματος είναι ασφαλής. Η λειτουργική ασφάλεια αποτελεί μέρος αυτού του επιπέδου και αναφέρεται σε "ένα σύστημα ή εξοπλισμό που λειτουργεί σωστά ως απάντηση στις εισόδους του" (πηγή: www.iec.ch).

Το σχήμα Α1 απεικονίζει ορισμένα παραδείγματα για το τι μπορεί να είναι σε κάθε στρώμα.

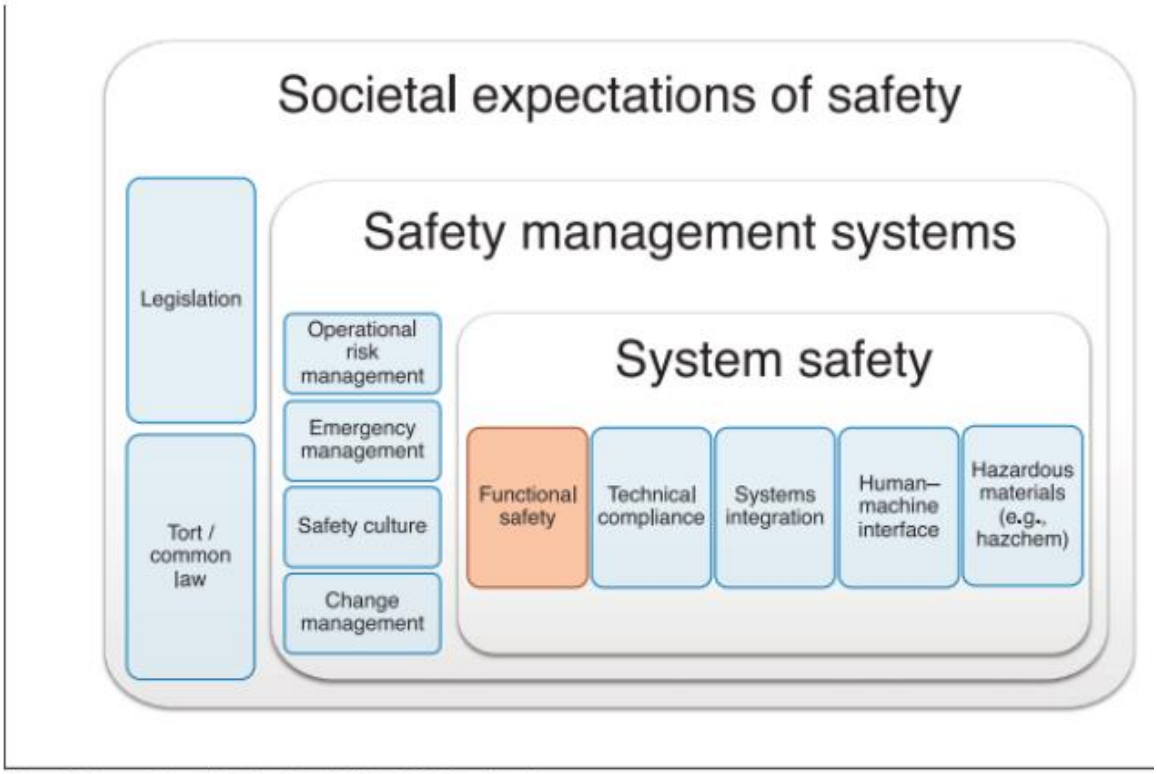

Figure A1. Layers of Overall Safety (Provided by a GMG Contributor)

ΠΑΡΑΡΤΗΜΑ Β: ΠΕΡΙΛΗΨΗ ΠΡΟΤΥΠΩΝ

Οι ακόλουθες περιγραφές συνοψίζουν το περιεχόμενο και το πεδίο εφαρμογής των βασικών και μη βασικών προτύπων που σχετίζονται με τη λειτουργική ασφάλεια. Τα βασικά πρότυπα αφορούν διάφορες πτυχές της εφαρμογής της λειτουργικής ασφάλειας σε αυτόνομα συστήματα εξόρυξης. Τα μη βασικά πρότυπα δεν αφορούν ειδικά τη λειτουργική ασφάλεια για αυτόνομα συστήματα στα ορυχεία, αλλά είναι σχετικά με τις διαδικασίες και τις δραστηριότητες που τα περιβάλλουν ή παρέχουν οδηγίες για άλλες βιομηχανίες που θα μπορούσαν να προσαρμοστούν στα ορυχεία. Είναι ταξινομημένα αριθμητικά.

Πλήρεις παραπομπές σε αυτά τα πρότυπα και πλήρεις αριθμοί προτύπων υπάρχουν στο Ενότητα 15. Επισημαίνεται ότι για τα μη βασικά πρότυπα, παρατίθενται μόνο τα γενικά τμήματα των προτύπων που αποτελούνται από πολλά μέρη, εκτός εάν ορίζεται διαφορετικά.

Β.1. Βασικά πρότυπα

ISO 12100 Ασφάλεια μηχανημάτων - Γενικές αρχές σχεδιασμού - Εκτίμηση και μείωση κινδύνων (Διεθνής Οργανισμός Τυποποίησης, 2010)

Το παρόν πρότυπο ορίζει τη γενική ορολογία, τις αρχές και τις μεθόδους εκτίμησης των κινδύνων που σχετίζονται με διάφορους τύπους σταθερών και κινητών μηχανημάτων. Παρέχει έναν κατάλογο κοινών κινδύνων και προορίζεται να χρησιμοποιηθεί σε συνδυασμό με άλλα πρότυπα ασφαλείας για συγκεκριμένες εφαρμογές (π.χ. τύπου Β και τύπου Γ).

ISO 13849 Ασφάλεια μηχανημάτων - Μέρη συστημάτων ελέγχου που σχετίζονται με την ασφάλεια (Διεθνής Οργανισμός Τυποποίησης 2015β, 2012β)

Αυτό το πρότυπο που αποτελείται από δύο μέρη παρέχει καθοδήγηση σχετικά με το σχεδιασμό, την ενσωμάτωση και την επικύρωση του υλικού και του λογισμικού των συστημάτων ελέγχου που σχετίζονται με την ασφάλεια και χρησιμοποιούνται σε

διάφορους τύπους μηχανημάτων. Επικεντρώνεται κυρίως σε σταθερά μηχανήματα, αλλά μπορεί επίσης να εφαρμοστεί σε συστήματα που χρησιμοποιούνται σε κινητό εξοπλισμό. Η αξιολόγηση των κινδύνων χρησιμοποιείται για τον καθορισμό των απαιτούμενων PL των συστημάτων ελέγχου, και οι επιτυγχανόμενες PL αναλύονται μέσω της αξιολόγησης της αρχιτεκτονικής του συστήματος, συμπεριλαμβανομένης της αξιοπιστίας των χρησιμοποιούμενων εξαρτημάτων και της ικανότητας ανίχνευσης σφαλμάτων. Παραπέμπει σε ορισμένες έννοιες από άλλα πρότυπα, όπως το IEC 61508, και προτείνει τη χρήση ενός διαγράμματος κινδύνου ανά εφαρμογή για τον καθορισμό των απαιτήσεων επιδόσεων.

ISO 17757 Χωματουργικά μηχανήματα και ορυχεία - Ασφάλεια αυτόνομων και ημιαυτόνομων συστημάτων μηχανών (Διεθνής Οργανισμός Τυποποίησης, 2019)

Το παρόν πρότυπο παρέχει τις γενικές απαιτήσεις ασφαλείας και τους προβληματισμούς για αυτόνομα και ημιαυτόνομα κινητά μηχανήματα που χρησιμοποιούνται σε εφαρμογές χωματουργικών εργασιών και εξόρυξης.

ISO 19014 Χωματουργικά μηχανήματα - Λειτουργική ασφάλεια (Διεθνής Οργανισμός Τυποποίησης, 2018γ, 2018δ)

Πρόκειται για ένα πρότυπο πέντε τμημάτων που καλύπτει την εφαρμογή της λειτουργικής ασφάλειας σε κινητά μηχανήματα που χρησιμοποιούνται σε εφαρμογές κατασκευών και εξόρυξης. Το πρώτο και το τρίτο μέρος έχουν δημοσιευθεί, ενώ τα άλλα τρία βρίσκονται υπό ανάπτυξη. Πολλές έννοιες είναι παρόμοιες με εκείνες των προτύπων ISO 13849 και IEC 61508. Το πρότυπο αυτό χρησιμοποιεί μια προσέγγιση βάσει του κλάδου και του κινδύνου για τον προσδιορισμό των PL μηχανών των χρησιμοποιούμενων συστημάτων ελέγχου που σχετίζονται με την ασφάλεια. Αντιμετωπίζει τις ανησυχίες σχετικά με τις περιβαλλοντικές συνθήκες και παρέχει περαιτέρω λεπτομέρειες σχετικά με τον τρόπο ανάλυσης πολύπλοκων ενσωματωμένων συστημάτων ελέγχου μηχανών που περιλαμβάνουν τη χρήση ολοκληρωμένων ηλεκτρικών, υδραυλικών και πνευματικών συστημάτων σε χωματουργικά μηχανήματα.

ISO 31000 Διαχείριση κινδύνων (Διεθνής Οργανισμός Τυποποίησης, 2018e)

Το πρότυπο αυτό παρέχει γενικές αρχές και κατευθυντήριες γραμμές για τη δημιουργία ενός πλαισίου για τη διαχείριση του κινδύνου διεργασιών σε ολόκληρο τον οργανισμό και διερευνά διάφορες έννοιες και μεθοδολογίες αξιολόγησης κινδύνου.

IEC 31010 Διαχείριση κινδύνου - Τεχνικές εκτίμησης κινδύνου (Διεθνής Ηλεκτροτεχνική Επιτροπή, 2019β)

Το πρότυπο αυτό (πρότυπο με διπλό λογότυπο με το ISO) παρέχει καθοδήγηση σχετικά με τον εντοπισμό κινδύνων και τις τεχνικές εκτίμησης κινδύνου.

IEC 61508 Λειτουργική ασφάλεια ηλεκτρικών / ηλεκτρονικών / προγραμματιζόμενων ηλεκτρονικών (Η/Ε/ΠΕ) συστημάτων που σχετίζονται με την ασφάλεια (Διεθνής Ηλεκτροτεχνική Επιτροπή, 2010a-2010g)

Πρόκειται για ένα ευρύ πρότυπο που αποτελείται από επτά μέρη και καλύπτει διάφορες πτυχές που πρέπει να λαμβάνονται υπόψη όταν τα συστήματα Η/Ε/ΠΕ χρησιμοποιούνται για την εκτέλεση λειτουργιών ασφαλείας. Έχει ιδιαίτερη σημασία για τις αρχές της διαχείρισης του κύκλου ζωής. Προορίζεται για την υποστήριξη της ανάπτυξης προτύπων λειτουργικής ασφάλειας συγκεκριμένων εφαρμογών ή τομέων και επικεντρώνεται μόνο σε ηλεκτρικά και ηλεκτρονικά συστήματα. Δεν εξετάζει τις ανησυχίες που σχετίζονται με τους μηχανικούς ελέγχους ή τις απαιτήσεις του ανθρώπινου παράγοντα που σχετίζονται με το σχεδιασμό των συστημάτων Η/Ε/ΠΕ. Οι απαιτήσεις σχεδιασμού συστημάτων εκφράζονται με τη χρήση SIL.

IEC 62061 Ασφάλεια μηχανημάτων - Λειτουργική ασφάλεια ηλεκτρικών, ηλεκτρονικών και προγραμματιζόμενων ηλεκτρονικών συστημάτων ελέγχου (Διεθνής Ηλεκτροτεχνική Επιτροπή, 2015)

Πρόκειται για μια προσαρμογή του προτύπου IEC 64508 που αφορά ειδικά τα σταθερά μηχανήματα στα οποία οι απαιτήσεις σχεδιασμού εξαρτημάτων που σχετίζονται με την ασφάλεια εκφράζονται με τη χρήση SIL.

Β.2 Μη βασικά πρότυπα

Πρότυπο Άμυνας 00-56 Απαιτήσεις διαχείρισης ασφάλειας για αμυντικά συστήματα (Τυποποίηση Άμυνας Ηνωμένου Βασιλείου, 2017)

Το παρόν πρότυπο ορίζει γενικές έννοιες και αρχές που πρέπει να λαμβάνουν υπόψη οι προγραμματιστές συστημάτων υλικού και λογισμικού κατά την ανάπτυξη ενός συστήματος ασφαλείας. Χρησιμοποιεί ορισμένες πτυχές παρόμοιες με μεθοδολογίες που παρουσιάζονται στο IEC 61508, με έμφαση στις συμβάσεις και τις ευθύνες του αναδόχου.

ISO 3450 Χωματουργικά μηχανήματα - Τροχοφόρα μηχανήματα ή μηχανήματα με τροχούς από καουτσούκ υψηλής ταχύτητας - Απαιτήσεις επιδόσεων και διαδικασίες δοκιμής για συστήματα πέδησης (Διεθνής Οργανισμός Τυποποίησης, 2011α)

Το παρόν πρότυπο καθορίζει τις απαιτήσεις επιδόσεων και τις διαδικασίες δοκιμής για τα συστήματα πέδησης κινητών μηχανημάτων.

ISO 5010 Χωματουργικά μηχανήματα - Μηχανήματα με ελαστικά καουτσούκ - Απαιτήσεις οδήγησης (Διεθνής Οργανισμός Τυποποίησης, 2007α)

Το παρόν πρότυπο καθορίζει τα κριτήρια επιδόσεων και δοκιμών που χρησιμοποιούνται για την αξιολόγηση της ικανότητας διεύθυνσης των τροχοφόρων κινητών μηχανημάτων.

ISO 10218 Ρομπότ και ρομποτικές συσκευές - Απαιτήσεις ασφάλειας για βιομηχανικά ρομπότ - Μέρος 1: Ρομπότ (Διεθνής Οργανισμός Τυποποίησης, 2011β)

Το πρότυπο αυτό καλύπτει τις απαιτήσεις ασφαλείας που σχετίζονται με τα βιομηχανικά ρομπότ, συμπεριλαμβανομένων των πιθανών κινδύνων και των μέτρων για τη μείωση ή την εξάλειψή τους.

ISO 13766 Μηχανήματα χωματουργικών και οικοδομικών εργασιών - Ηλεκτρομαγνητική συμβατότητα (ΗΜΣ) μηχανημάτων με εσωτερική ηλεκτρική τροφοδοσία (Διεθνής Οργανισμός Τυποποίησης, 2018α, 2018β)

Πρόκειται για ένα πρότυπο που αποτελείται από δύο μέρη και επικεντρώνεται στην ηλεκτρομαγνητική συμβατότητα. Το πρώτο μέρος αφορά τις γενικές απαιτήσεις συμβατότητας του εξοπλισμού. Το δεύτερο μέρος επικεντρώνεται στις μεθόδους δοκιμής και τα κριτήρια αποδοχής για τα μέρη των συστημάτων ελέγχου που σχετίζονται με την ασφάλεια (λειτουργική ασφάλεια) και χρησιμοποιούνται σε κινητά μηχανήματα.

ISO / IEC / IEEE 15288 - Μηχανική συστημάτων και λογισμικού - Διαδικασίες κύκλου ζωής συστήματος (Διεθνής Οργανισμός Τυποποίησης, 2015γ)

Το πρότυπο αυτό θεσπίζει ένα κοινό πλαίσιο ελέγχων διεργασιών που μπορεί να χρησιμοποιηθεί από οργανισμούς κατά την απόκτηση ή την προμήθεια συστημάτων.

ISO 15817 Χωματουργικά μηχανήματα - Απαιτήσεις ασφάλειας για συστήματα τηλεχειρισμού (Διεθνής Οργανισμός Τυποποίησης, 2012α)

Το παρόν πρότυπο καθορίζει τις βασικές απαιτήσεις ασφαλείας για τον τηλεχειρισμό κινητών μηχανημάτων από τον χειριστή. Δεν εφαρμόζεται σε αυτόνομα συστήματα που είναι ικανά να λειτουργούν χωρίς τη βοήθεια του χειριστή.

ISO 16001 Μηχανήματα χωματουργικών εργασιών - Συστήματα ανίχνευσης αντικειμένων και βοηθήματα ορατότητας - Απαιτήσεις επιδόσεων και δοκιμές (Διεθνής Οργανισμός Τυποποίησης, 2017α)

Το παρόν πρότυπο καθορίζει τις γενικές απαιτήσεις και τις μεθόδους για την αξιολόγηση και τη δοκιμή των επιδόσεων των συστημάτων ανίχνευσης αντικειμένων που χρησιμοποιούνται σε κινητά μηχανήματα.

ISO 20474 Χωματουργικά μηχανήματα - Ασφάλεια (Διεθνής Οργανισμός Τυποποίησης 2017β)

Αυτό το πρότυπο 15 τμημάτων καθορίζει τις γενικές απαιτήσεις ασφαλείας για τα χωματουργικά μηχανήματα. Το πρώτο μέρος περιέχει γενικές απαιτήσεις και τα μέρη που ακολουθούν αφορούν ειδικά τους επιμέρους τύπους μηχανημάτων και τις ειδικές λειτουργίες και εφαρμογές τους. Καθορίζει τα κατάλληλα τεχνικά μέτρα για την εξάλειψη ή τη μείωση των κινδύνων από τους σχετικούς κινδύνους. Παραπέμπει στη χρήση του ISO 17757 για αυτόνομα συστήματα.

ISO 21448 Οδικά οχήματα - Ασφάλεια της προβλεπόμενης λειτουργικότητας (Διεθνής Οργανισμός Τυποποίησης, 2019γ)

Το παρόν πρότυπο συμπληρώνει το ISO 26262- προορίζεται να εφαρμόζεται όταν η επίγνωση της κατάστασης είναι κρίσιμη για την ασφάλεια και προέρχεται από πολύπλοκους αλγορίθμους αισθητήρων και επεξεργασίας (π.χ. συστήματα επέμβασης έκτακτης ανάγκης, προηγμένα συστήματα υποβοήθησης οδηγού), όπου μπορεί να μην είναι δυνατόν να καθοριστεί βαθμολογία SIL ή PL.

ISO 26262 Οδικά οχήματα - Λειτουργική ασφάλεια (Διεθνής Οργανισμός Τυποποίησης, 2018στ)

Πρόκειται για ένα πρότυπο 10 τμημάτων που επικεντρώνεται στην εφαρμογή της λειτουργικής ασφάλειας σε ηλεκτρικά και ηλεκτρονικά συστήματα αυτοκινήτων. Πολλές έννοιες προέρχονται από το πρότυπο IEC 61508 με τη χρήση μιας βιομηχανικής προσέγγισης με βάση τον κίνδυνο για τον προσδιορισμό των επιπέδων ακεραιότητας

ασφάλειας αυτοκινήτων (ASIL) των χρησιμοποιούμενων συστημάτων ελέγχου που σχετίζονται με την ασφάλεια.

IEC 61800 - Συστήματα ηλεκτροκίνησης ρυθμιζόμενης ταχύτητας (Διεθνής Ηλεκτροτεχνική Επιτροπή, 2016)

Πρόκειται για ένα πρότυπο εννέα τμημάτων που επικεντρώνεται σε διάφορες πτυχές του σχεδιασμού συστημάτων μετάδοσης κίνησης εναλλασσόμενου και συνεχούς ρεύματος, συμπεριλαμβανομένων των θεμάτων ασφάλειας, των απαιτήσεων διασύνδεσης, της ηλεκτρομαγνητικής συμβατότητας και της ενεργειακής απόδοσης. Το πιο σχετικό έγγραφο αυτής της σειράς είναι το IEC 61800-5-2:2016, Συστήματα ηλεκτροκίνησης ρυθμιζόμενων στροφών - Μέρος 5-2: Απαιτήσεις ασφαλείας - Λειτουργικές.

IEC 62998 - Ασφάλεια μηχανημάτων - Αισθητήρες που σχετίζονται με την ασφάλεια και χρησιμοποιούνται για την προστασία ατόμων (Διεθνής Ηλεκτροτεχνική Επιτροπή, 2019β)

Πρόκειται για μια τεχνική προδιαγραφή απαιτήσεων για την ανάπτυξη και ενσωμάτωση συστημάτων αισθητήρων που σχετίζονται με την ασφάλεια και την προστασία των ανθρώπων.

ΠΑΡΑΡΤΗΜΑ Γ: ΠΑΡΑΔΕΙΓΜΑ ΣΧΕΔΙΟΥ ΔΙΑΧΕΙΡΙΣΗΣ ΛΕΙΤΟΥΡΓΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Ο πίνακας Γ1 είναι ένα παράδειγμα που περιγράφει τα περιεχόμενα που πρέπει να ληφθούν υπόψη σε ένα σχέδιο διαχείρισης λειτουργικής ασφάλειας. Επισημαίνεται ότι οι λεπτομέρειες θα διαφέρουν ανάλογα με το πλαίσιο και ότι το περιεχόμενο του σχεδίου διαχείρισης λειτουργικής ασφάλειας θα πρέπει να προσαρμόζεται ανάλογα με το συγκεκριμένο προϊόν ή εφαρμογή. Σημειώστε επίσης ότι μια σειρά από άλλες διαδικασίες μπορεί επίσης να πληρούν τα κριτήρια του σχεδίου διαχείρισης λειτουργικής ασφάλειας.

Σημειώστε ότι τα στοιχεία που περιέχονται στον πίνακα Γ1 μπορεί να είναι ενσωματωμένα σε μια συνολική διαδικασία και όχι να υπάρχουν ως ξεχωριστό σχέδιο διαχείρισης της λειτουργικής ασφάλειας.

Table C1. Functional Safety Management Plan

1. Introduction

1.1 Scope

- Consider system and application

1.2 Standards

- Identify functional safety standards utilized

2. Organization

2.1 Roles and responsibilities

2.2 Competency

- Develop strategy for internal competency management

2.3 Communications

- Define interface points between OPS and mine operator, and se requirements for documentation exchanged

2.4 Supplier management

3. Safety management

3.1 Lifecycle

- Outline functional safety lifecycle to be followed

3.2 Phase activities

- Plan for each phase, including identifying inputs, outputs, and dependencies

3.3 Change management

3.4 Configuration management

3.5 Hazard log / risk register

4. Technical delivery

4.1 Design principles applied

- Structure software and hardware techniques employed (e.g., architecture)

4.2 Installation and commissioning

4.3 Verification

4.4 Validation

- Conduct site-specific safety validation exercise

4.5 Cybersecurity

4.6 Safety constraints

5. Operations and maintenance

5.1 Change management

- Detail how to maintain the risk register during production phase

5.2 Configuration management

- Define requirements for configuration management in operation and maintenance

5.3 In-service performance management

- Define requirements for ongoing safety management and continuous improvement

5.4 Management of actions

5.5 Emergency preparedness

6. Assurance

6.1 Audits

6.2 Functional safety assessments

- Define requirements for functional safety assessment

ΠΑΡΑΡΤΗΜΑ Δ: ΠΙΘΑΝΕΣ ΔΡΑΣΤΗΡΙΌΤΗΤΕΣ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΛΟΓΙΣΜΙΚΟΥ

Οι πίνακες Δ.1 και Δ.2 παραθέτουν τις πιθανές δραστηριότητες για την ανάπτυξη λογισμικού και τη σχέση τους με τα PLs, όπως αυτά ορίζονται στο ISO 13849-1:2015. Επισημαίνεται ότι οι πίνακες αυτοί δεν προορίζονται για σκοπούς ελέγχου, διότι οι δραστηριότητες και οι απαιτήσεις θα διαφέρουν σημαντικά ανάλογα με τη διαδικασία ανάπτυξης. Μπορούν να χρησιμοποιηθούν για να βοηθήσουν στην κατανόηση και τον εντοπισμό ορισμένων από τις δραστηριότητες που ενδέχεται να ισχύουν.

Σημειώστε ότι το ISO 13849-1:2015 βρίσκεται υπό αναθεώρηση κατά τη στιγμή της δημοσίευσης και οι πληροφορίες αυτές θα είναι ξεπερασμένες μόλις κυκλοφορήσει η επόμενη έκδοση. Σημειώστε επίσης ότι άλλες προσεγγίσεις και πρότυπα για την ανάπτυξη λογισμικού μπορεί να είναι πιο κατάλληλα για συγκεκριμένα συστήματα.

Table D.1. Safety-Related Embedded Software (SRESW)

#	Activity	PL				
		a	b	c	d	e
1	Software safety lifecycle with verification and validation activities	✓	✓	✓	✓	✓
2	Documentation of specification and design	✓	✓	✓	✓	✓
3	Modular and structured design and coding	✓	✓	✓	✓	✓
4	Control of systematic failures	✓	✓	✓	✓	✓
5	Where using software-based measures for control of random hardware failures, verification of correct implementation	✓	✓	✓	✓	✓
6	Functional testing (e.g., black-box testing)	✓	✓	✓	✓	✓
7	Appropriate software safety lifecycle activities after modifications	✓	✓	✓	✓	✓
8	Project management and quality management system comparable to (e.g., ISO 9001)	✓	✓	✓	✓	✓
9	Documentation of all relevant activities during software safety lifecycle	✓	✓	✓	✓	✓
10	Configuration management to identify all configuration items and documents related to an SRESW release			✓	✓	✓
11	Structured specification with safety requirements and design			✓	✓	✓
12	Use of suitable programming languages and computer-based tools with confidence from use			✓	✓	✓
13	Modular and structured programming, separation in non-safety-related software, limited module sizes with fully defined interfaces, use of design and coding standards			✓	✓	✓
14	Coding verification by walk-through / review with control flow analysis			✓	✓	✓
15	Extended functional testing (e.g., grey-box testing, performance testing, or simulation)			✓	✓	✓
16	Impact analysis and appropriate software safety lifecycle activities after modifications			✓	✓	✓
17	Structural test coverage (statements) 100% (Note: in addition to ISO 13849 requirements)			✓	✓	✓

Table D.2. Safety-Related Applied Software (SRASW)

#	Activity	PL				
		a	b	c	d	e
1	Software safety lifecycle with verification and validation activities	✓	✓	✓	✓	✓
2	Documentation of specification and design	✓	✓	✓	✓	✓
3	Modular and structured design and coding	✓	✓	✓	✓	✓
4	Functional Testing	✓	✓	✓	✓	✓
5	Appropriate development activities after modifications	✓	✓	✓	✓	✓
The safety-related software specification should be reviewed, made available to people involved in the lifecycle, and contain the description of:						
6	Safety functions with required PL and associated operating modes	✓	✓	✓	✓	✓
7	Performance criteria (e.g., reaction times)	✓	✓	✓	✓	✓
8	Hardware architecture with external signal interfaces	✓	✓	✓	✓	✓
9	Detection and control of external failure	✓	✓	✓	✓	✓
Selection of tools, libraries, languages:						
10	Suitable tools with "confidence from use." The tool should comply with the appropriate safety standard; if two diverse components with diverse tools are used, confidence from use may be sufficient. Technical features that detect conditions that could cause systematic error (such as data type mismatch, ambiguous dynamic memory allocation, incomplete called interfaces, recursion, pointer arithmetic) should be used.			✓	✓	✓
11	Whenever reasonable and practicable, validated function block libraries should be used, either safety-related function block libraries provided by the tool manufacturer (highly recommended for PL = e) or validated application-specific FB libraries.			✓	✓	✓
12	A justified limited variability language (LVL) subset suitable for a modular approach should be used (e.g., the accepted subset of IEC 61131-3 languages). Graphical languages (e.g., function block diagram, ladder diagram) are highly recommended.			✓	✓	✓
Software design should feature:						
13	Semi-formal methods to describe data and control flow(e.g., state diagram or program flow chart)			✓	✓	✓
14	Modular and structured programming predominantly realized by function blocks deriving from safety-related validated function block libraries			✓	✓	✓
15	Function blocks of limited size of coding			✓	✓	✓
16	Code execution inside function block that should have one entry and one exit point			✓	✓	✓
17	Architecture model of three stages: inputs, processing, outputs			✓	✓	✓
18	Assignment of a safety output at only one program location			✓	✓	✓
19	Use of techniques for detection of external failure and for defensive programming within input, processing, and output blocks that lead to a safe state			✓	✓	✓

Table D.2. Continued

#	Activity	PL				
		a	b	c	d	e
Where SRASW and non-SRASW are combined in one component:						
20	SRASW and non-SRASW should be coded in different function blocks with well-defined data links			✓	✓	✓
21	There should be no logical combination of non-safety-related and safety-related data that could lead to the downgrading of the integrity of safety-related signals (e.g., combining safety-related and non-safety-related signals by a logical "OR" where the result controls safety-related signals)			✓	✓	✓
Software implementation / coding:						
22	Code should be readable, understandable and testable using symbolic variables instead of explicit hardware addresses			✓	✓	✓
23	Justified or accepted coding guidelines should be used			✓	✓	✓
24	Data integrity and plausibility checks (e.g., range checks) available on application layer (defensive programming) should be used			✓	✓	✓
25	Code should be tested by simulation			✓	✓	✓
26	Verification should be by control and data flow analysis for PLd or PLe				✓	✓
Testing:						
27	The appropriate validation method is black-box testing of functional behavior and performance criteria (e.g., timing performance)			✓	✓	✓
28	For PLd and PLe, test case execution from boundary value analysis is recommended				✓	✓
29	Test planning is recommended and should include test cases with completion criteria and required tools			✓	✓	✓
30	Input / output testing should confirm that safety-related signals are correctly used within SRASW			✓	✓	✓
31	Structural test coverage (statements) 100% (Note: in addition to ISO 13849 requirements)			✓	✓	✓
Documentation:						
32	All lifecycle and modification activities should be documented	✓	✓	✓	✓	✓
33	Documentation should be complete, available, readable, and understandable	✓	✓	✓	✓	✓
34	Code documentation within source text should contain module headers with legal entity, functional and I/O description, and version of used library function blocks, and sufficient comments on networks and declaration lines			✓	✓	✓
Configuration management:						
35	It is highly recommended that procedures and data backup be established to identify and archive documents, software modules, verification/validation results, and tool configuration related to a specific SRASW version	✓	✓	✓	✓	✓
Modifications:						
36	After modifications of SRASW, impact analysis should be performed to confirm correct specification. Appropriate lifecycle activities should be performed after modifications. Access rights to modifications should be controlled, and modification history should be documented.	✓	✓	✓	✓	✓