ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΕΠΙΣΤΗΜΗ ΔΕΔΟΜΕΝΩΝ»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Ολοκληρωμένη Προσέγγιση Ασφάλειας για την Αρχιτεκτονική Βιομηχανικών Συστημάτων OT/IT Integrated Security Approach for the Architecture of Industrial OT/IT Systems
Ονοματεπώνυμο Φοιτητή	ΘΕΟΔΩΡΙΔΗΣ ΣΤΕΦΑΝΟΣ
Πατρώνυμο	ΕΥΡΙΠΙΔΗΣ
Αριθμός Μητρώου	ΜΠΚΕΔ24014
Επιβλέπων	**ΚΑΡΑΝΤΖΙΑΣ ΑΘΑΝΑΣΙΟΣ, Διδάσκων ΠΜΣ**

Ημερομηνία Παράδοσης Ιούλιος 2026

Τριμελής Εξεταστική Επιτροπή

Δρ. Αθανάσιος Καραντζιάς Διδάσκων ΠΜΣ	Δρ. Σπυρίδων Παπαστεργίου Διδάσκων ΠΜΣ	Παναγιώτης Κοτζανικολάου Καθηγητής

Περιεχόμενα

Περίληψη

Η ταχεία σύγκλιση των πληροφοριακών τεχνολογιών (Information Technology - IT) και των λειτουργικών τεχνολογιών (Operational Technology - OT) έχει αναδιαμορφώσει ριζικά το τοπίο της βιομηχανικής παραγωγής, εισάγοντας εξειδικευμένες απαιτήσεις ασφάλειας και νέους κινδύνους για τις κρίσιμες υποδομές. Η παρούσα διπλωματική εργασία εξετάζει μια ολοκληρωμένη προσέγγιση για την ασφάλεια αρχιτεκτονικών IT/OT, αναλύοντας τόσο τις τεχνολογικές όσο και τις οργανωσιακές πτυχές που απαιτούνται για την αποτελεσματική προστασία σύγχρονων βιομηχανικών συστημάτων. Ειδική έμφαση δίδεται σε διεθνή πρότυπα και βέλτιστες πρακτικές, όπως τα ISO/IEC 27001 και ISO/IEC 27019 για τα πληροφοριακά και ενεργειακά συστήματα, το πλαίσιο NIST SP 800-82 για τα συστήματα βιομηχανικού ελέγχου (ICS) και η προδιαγραφή IEC 62443, η οποία αποτελεί σημείο αναφοράς για την κυβερνοασφάλεια OT.

Επιπλέον, διερευνώνται κρίσιμες έννοιες όπως η διαστρωμάτωση κατά το μοντέλο Purdue, η αρχιτεκτονική άμυνας σε βάθος (Defense-in-Depth), οι μηχανισμοί δικτυακού διαχωρισμού, καθώς και η σημασία των περιβαλλόντων UAT/QA για ασφαλή δοκιμή και αξιολόγηση συστημάτων PLC, HMI και SCADA. Μέσω συστηματικής βιβλιογραφικής επισκόπησης και αξιολόγησης υπαρχόντων πλαισίων, η εργασία αναδεικνύει τις προκλήσεις και τις ευκαιρίες που ανακύπτουν από τη σύγκλιση IT/OT και προτείνει κατευθύνσεις για ολιστική διαχείριση των κυβερνοκινδύνων σε βιομηχανικά περιβάλλοντα. Τα συμπεράσματα υπογραμμίζουν την ανάγκη ανάπτυξης ενιαίων πολιτικών ασφάλειας, οργανωσιακής ωριμότητας και τεχνικών μηχανισμών που ανταποκρίνονται τόσο στις απαιτήσεις της ασφάλειας πληροφοριών όσο και της λειτουργικής ασφάλειας.

Abstract

The rapid convergence of Information Technology (IT) and Operational Technology (OT) has fundamentally reshaped the landscape of industrial production, introducing specialized security requirements and new risks for critical infrastructures. This thesis examines a comprehensive approach to the security of IT/OT architectures, analysing both the technological and organisational dimensions required for the effective protection of modern industrial systems. Particular emphasis is placed on international standards and best practices, such as ISO/IEC 27001 and ISO/IEC 27019 for information and energy systems, the NIST SP 800-82 framework for Industrial Control Systems (ICS), and the IEC 62443 series, which constitutes a key reference for OT cybersecurity.

Furthermore, the thesis explores critical concepts such as the Purdue model layering, defence-in-depth architectures, network segmentation mechanisms, and the importance of UAT/QA environments for the safe testing and validation of PLC, HMI and SCADA systems. Through a systematic literature review and evaluation of existing frameworks, the study highlights the challenges and opportunities arising from IT/OT convergence and proposes directions for holistic cyber risk management in industrial environments. The conclusions underscore the need for unified security policies, organisational maturity and technical mechanisms that address both information security requirements and operational safety.

ΕΙΣΑΓΩΓΗ

Η ασφάλεια των πληροφοριακών και βιομηχανικών συστημάτων αποτελεί σήμερα κεντρικό πυλώνα της επιχειρησιακής συνέχειας (Business continuity) και της ανθεκτικότητας των κρίσιμων υποδομών. Η διείσδυση της ψηφιακής τεχνολογίας στον βιομηχανικό χώρο, σε συνδυασμό με την αυξανόμενη ανάγκη για αυτοματοποίηση, απομακρυσμένο έλεγχο και διαλειτουργικότητα, έχει οδηγήσει σε μία βαθιά και συχνά αναπόφευκτη σύγκλιση μεταξύ των παραδοσιακών IT συστημάτων και των συστημάτων OT, τα οποία μέχρι πρότινος λειτουργούσαν σε απομονωμένα και αυστηρά ελεγχόμενα περιβάλλοντα.

Η παρούσα εργασία επιδιώκει να διερευνήσει συστηματικά τις απαιτήσεις ασφάλειας που ανακύπτουν από την αρχιτεκτονική συνύπαρξη IT και OT, αναδεικνύοντας τα κεντρικά πρότυπα, τις βέλτιστες πρακτικές και τα τεχνικά μέτρα που προτείνονται διεθνώς για την προστασία συστημάτων βιομηχανικού ελέγχου (Industrial Control Systems - ICS). Τα πρότυπα ISO/IEC 27001 και ISO/IEC 27002 αποτελούν τα κορυφαία διεθνή πρότυπα για τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management Systems - ISMS), τα οποία παρέχουν ένα πλαίσιο για τους οργανισμούς ώστε να διαχειρίζονται τους κινδύνους για ευαίσθητα δεδομένα, καθιερώνοντας, εφαρμόζοντας, διατηρώντας και βελτιώνοντας συνεχώς τους ελέγχους ασφάλειας, με έμφαση στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα (Confidentiality, Integrity, and Availability - CIA) των πληροφοριών, και είναι εφαρμόσιμο σε οργανισμούς οποιουδήποτε μεγέθους ή τομέα, ενώ το ISO/IEC 27019 εξειδικεύει τις απαιτήσεις για συστήματα ενέργειας, προσφέροντας ένα κρίσιμο πλαίσιο για τα OT περιβάλλοντα. Παράλληλα, Το ISA/IEC 62443 είναι μια διεθνής σειρά προτύπων που ορίζουν την κυβερνοασφάλεια για τα συστήματα βιομηχανικού αυτοματισμού και ελέγχου (IACS) και παρέχουν ένα δομημένο πλαίσιο για την προστασία των περιβαλλόντων OT, όπως σταθμοί παραγωγής ηλεκτρικής ενέργειας, βιομηχανίες και εγκαταστάσεις επεξεργασίας νερού, από κυβερνοαπειλές, καλύπτοντας διαδικασίες, συστήματα και εξαρτήματα σε όλο τον κύκλο ζωής τους, σε αντίθεση με τα πρότυπα που εστιάζουν στην πληροφορική.

Με βάση τα παραπάνω, στην παρούσα εργασία γίνεται προσπάθεια ανάλυσης στο πως μπορούν τα πρότυπα IEC 62443 και NIST CSF 2.0 να συνδυαστούν σε ένα ενιαίο πλαίσιο διακυβέρνησης και αρχιτεκτονικής ασφάλειας για OT/IT περιβάλλοντα, ποια είναι τα βασικά αρχιτεκτονικά και οργανωσιακά στοιχεία ενός πρακτικά εφαρμόσιμου OT/IT security program για βιομηχανικές εγκαταστάσεις καθώς και πώς επηρεάζουν η Industry 4.0, τα Big Data, η Τεχνητή Νοημοσύνη και η επερχόμενη μετάβαση σε post-quantum κρυπτογραφία τον σχεδιασμό μιας ολοκληρωμένης αρχιτεκτονικής ασφάλειας OT/IT.

ΚΕΦΑΛΑΙΟ 1 - Θεμελιώδεις έννοιες IT/OT και ICS

Το παρόν κεφάλαιο εισάγει τις θεμελιώδεις έννοιες που διέπουν τον χώρο των πληροφοριακών και λειτουργικών τεχνολογιών, καθώς και την τεχνολογική υποδομή των βιομηχανικών συστημάτων ελέγχου. Η κατανόηση της διάκρισης IT/OT, της σταδιακής τους σύγκλισης και των βασικών προκλήσεων ασφάλειας που αναδύονται στα σύγχρονα περιβάλλοντα ICS αποτελεί απαραίτητη προϋπόθεση για τον σχεδιασμό και την αξιολόγηση οποιασδήποτε αρχιτεκτονικής ασφάλειας. Στις επόμενες ενότητες παρουσιάζονται οι βασικές ορολογίες και κατηγορίες συστημάτων, όπως τυποποιούνται από οργανισμούς όπως το NIST και η IEC, καθώς και τα βασικά βιομηχανικά πρωτόκολλα επικοινωνίας. Στόχος είναι να δημιουργηθεί ένα κοινό πλαίσιο αναφοράς, πάνω στο οποίο θα στηριχθούν οι μεταγενέστερες ενότητες που εστιάζουν σε αρχιτεκτονικές IT, OT και ενοποιημένης διακυβέρνησης.

1.1 Ορισμός και διαφοροποίηση IT και OT

Η σαφής διάκριση μεταξύ πληροφοριακών και λειτουργικών τεχνολογιών δεν είναι απλώς ζήτημα ορολογίας, αλλά επηρεάζει άμεσα τον τρόπο με τον οποίο σχεδιάζονται οι έλεγχοι ασφάλειας και οργανώνονται οι ευθύνες μέσα σε έναν οργανισμό. Τα συστήματα IT και OT έχουν αναπτυχθεί ιστορικά με διαφορετικές προτεραιότητες, ρυθμιστικά πλαίσια και τεχνικούς περιορισμούς, γεγονός που οδηγεί σε διαφορετική αντίληψη κινδύνου και ανεκτό επίπεδο διακοπής λειτουργίας. Στο πλαίσιο της παρούσας εργασίας, οι διαφοροποιήσεις αυτές αποτελούν το σημείο εκκίνησης για την ανάπτυξη μιας ενοποιημένης αρχιτεκτονικής ασφάλειας που να λαμβάνει υπόψη και τις δύο όψεις, τόσο στο σχεδιασμό όσο και στην επιχειρησιακή λειτουργία.

Στο πεδίο της κυβερνοασφάλειας, ο όρος Information Technology (IT) περιγράφει συστήματα που έχουν ως πρωτεύον αντικείμενο την επεξεργασία, αποθήκευση και διακίνηση πληροφορίας, και οργανώνονται παραδοσιακά γύρω από έννοιες όπως εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα δεδομένων, όπως αποτυπώνονται σε πλαίσια διαχείρισης ασφάλειας πληροφοριών (ISMS) και σε διεθνή πρότυπα της οικογένειας ISO/IEC 27000 (ISO/IEC 27000 family, Information security management). Αντιθέτως, το Operational Technology (OT) αφορά το σύνολο των μηχανισμών, συσκευών και συστημάτων που αλληλοεπιδρούν άμεσα με φυσικές διεργασίες, όπως αντλίες, βαλβίδες, γραμμές παραγωγής, μονάδες ενέργειας και βιομηχανικές εγκαταστάσεις, όπως ορίζεται από το NIST στον οδηγό για τα συστήματα βιομηχανικού ελέγχου.

Η διαφοροποίηση των δύο αυτών τομέων θεμελιώνεται στις διακριτές προτεραιότητες ασφάλειας. Στο IT κυριαρχεί το τριμερές μοντέλο Confidentiality, Integrity, Availability (CIA), το οποίο τοποθετεί στο επίκεντρο την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων, ενώ η διαθεσιμότητα αποτελεί μεν κρίσιμο στοιχείο, αλλά όχι την πρωτεύουσα απαίτηση. Στον αντίποδα, το OT αντιμετωπίζει τη διαθεσιμότητα και τη λειτουργική ασφάλεια (safety) ως απόλυτες προτεραιότητες. Οποιαδήποτε διακοπή λειτουργίας μπορεί να προκαλέσει καταστροφή εγκαταστάσεων, οικονομικές απώλειες ή ακόμη και κινδύνους για την ανθρώπινη ζωή, όπως περιγράφεται στην IEC 62443-1-1.

Η κατανόηση αυτής της θεμελιώδους διαφοροποίησης είναι αναγκαία, διότι κάθε σύστημα IT ή OT αποτυπώνει διαφορετική φιλοσοφία σχεδιασμού και ανθεκτικότητας. Στο IT οι αναβαθμίσεις, τα patches και η κρυπτογράφηση αποτελούν συμβατικές πρακτικές, ενώ στο OT συχνά δεν είναι δυνατή η εφαρμογή τους λόγω απαιτήσεων συνεχούς λειτουργίας, κάτι που αναφέρεται επανειλημμένα στον οδηγό του NIST για ICS περιβάλλοντα. Επομένως, η διαστρωμάτωση και διασύνδεση των δύο αυτών κόσμων δεν μπορεί να γίνει χωρίς βαθιά κατανόηση της διακριτής τους φύσης.

1.2 Σύγκλιση IT/OT (IT/OT Convergence)

Η σύγκλιση IT/OT αποτελεί μία από τις σημαντικότερες εξελίξεις της Βιομηχανικής Επανάστασης 4.0 και περιγράφει τη σταδιακή ενσωμάτωση πληροφοριακών δεδομένων και επιχειρησιακών διεργασιών με τα συστήματα βιομηχανικού ελέγχου, προκειμένου να επιτευχθεί βελτιστοποίηση, αυτοματοποίηση και επιχειρησιακή διαφάνεια σε πραγματικό χρόνο. Η σύγκλιση αυτή επιτρέπει σε έναν οργανισμό να συλλέγει δεδομένα από βιομηχανικές εγκαταστάσεις, να τα επεξεργάζεται κεντρικά και να προβαίνει σε αποφάσεις που αυξάνουν την παραγωγικότητα και μειώνουν το λειτουργικό κόστος, όπως τεκμηριώνεται στα πλαίσια του NIST για τα ICS.

Οι επιχειρησιακές απαιτήσεις που οδηγούν στη σύγκλιση αφορούν κυρίως την ανάγκη για διαλειτουργικότητα, βελτιωμένη ορατότητα στις παραγωγικές διαδικασίες και δυνατότητα ανάλυσης των δεδομένων με σκοπό την πρόβλεψη βλαβών ή αποκλίσεων. Το NIST τονίζει ότι οι οργανισμοί επιζητούν συντονισμένο έλεγχο και συνεχές monitoring σε συστήματα που παλαιότερα λειτουργούσαν απομονωμένα, επιτρέποντας έτσι την υλοποίηση προηγμένων πρακτικών όπως predictive maintenance και energy optimization.

Η σύγκλιση IT/OT εισάγει σημαντικούς κινδύνους, καθώς η διασύνδεση βιομηχανικών συστημάτων με εταιρικά δίκτυα αυξάνει την επιφάνεια επίθεσης και εκθέτει υποδομές που είχαν σχεδιαστεί για απομονωμένη λειτουργία σε απειλές όπως κακόβουλο λογισμικό και ransomware, οι οποίες προέρχονται από το ευρύτερο οικοσύστημα του εταιρικού IT χώρου. Επιπλέον, πολλές πλατφόρμες OT βασίζονται σε πρωτόκολλα χωρίς μηχανισμούς κρυπτογράφησης ή ισχυρής ταυτοποίησης, αυτό έχει ως αποτέλεσμα η ασφάλεια να εξαρτάται από τη δικτυακή τοπολογία και όχι από τις ίδιες τις συσκευές.

Η δυσκολία υλοποίησης της σύγκλισης είναι επίσης σημαντική. Τα συστήματα OT παρουσιάζουν διαφορετικές χρονικές απαιτήσεις, λειτουργούν σε περιβάλλοντα με απαγόρευση διακοπής λειτουργίας και συχνά δεν υποστηρίζουν ενημερώσεις ή σύγχρονα μέτρα ασφάλειας. Η IEC 62443-3-3 διαπιστώνει ότι η σύγκλιση απαιτεί τη δημιουργία σαφών ορίων ασφάλειας, πολυεπίπεδων ζωνών και μηχανισμών διαχείρισης ταυτότητας που δεν υφίστανται στο κλασικό βιομηχανικό περιβάλλον. Η έλλειψη εξειδικευμένων τεχνικών που κατέχουν γνώσεις και από τους δύο χώρους αποτελεί επίσης βασικό εμπόδιο, όπως σημειώνει η ENISA στη μελέτη της για ICS Security.

Συνοψίζοντας, η σύγκλιση IT/OT δεν αποτελεί απλώς τεχνικό έργο διασύνδεσης συστημάτων, αλλά στρατηγική επιλογή που μεταβάλλει ριζικά το μοντέλο απειλών και την απαιτούμενη ωριμότητα διακυβέρνησης. Οι οδηγοί του NIST για ICS και οι μελέτες για cyber-physical systems υπογραμμίζουν ότι η μετάβαση προς ενοποιημένες υποδομές απαιτεί σαφή οριοθέτηση τομέων ευθύνης, συστηματική διαχείριση κινδύνου και σταδιακή υιοθέτηση αρχών όπως η άμυνα σε βάθος και ο δικτυακός διαχωρισμός. Τα ζητήματα αυτά αναλύονται σε βάθος στα επόμενα κεφάλαια, όπου η σύγκλιση μεταφράζεται σε συγκεκριμένες αρχιτεκτονικές επιλογές για IT, OT και κοινό πλαίσιο ελέγχων.

1.3 Βιομηχανικά Πληροφοριακά Συστήματα και industrial protocols

Τα βιομηχανικά πληροφοριακά συστήματα (Industrial Control Systems - ICS) αποτελούν το τεχνολογικό υπόβαθρο κάθε σύγχρονης βιομηχανικής διεργασίας και περιλαμβάνουν μηχανισμούς αυτοματισμού που επιτρέπουν τον έλεγχο φυσικών υποδομών και τη συλλογή κρίσιμων δεδομένων σε πραγματικό χρόνο. Το NIST τα κατηγοριοποιεί σε PLC, SCADA, DCS και HMI, αποδίδοντας συγκεκριμένο λειτουργικό ρόλο σε κάθε επιμέρους.

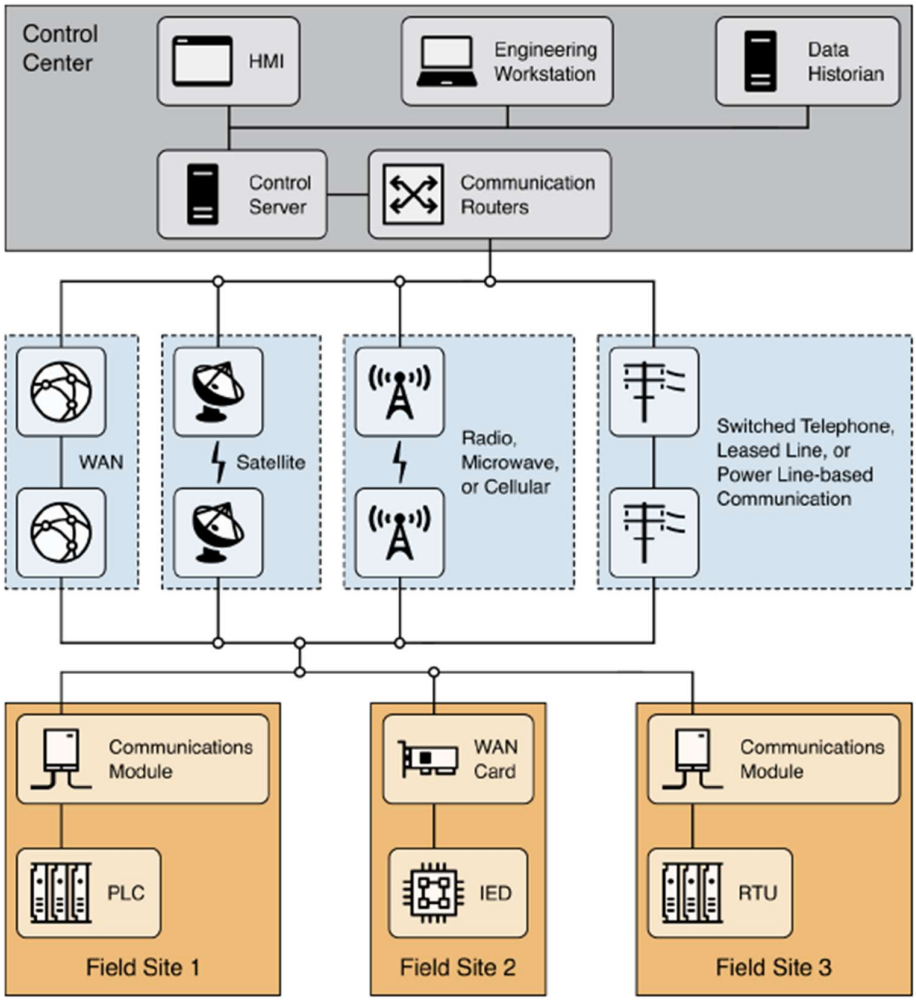
Πέρα από την κλασική ταξινόμηση των ICS, η πρόσφατη βιβλιογραφία εισάγει τον ευρύτερο όρο «cyber-physical systems» (CPS) για να περιγράψει συστήματα στα οποία ψηφιακά στοιχεία ελέγχου συνδέονται στενά με φυσικές διεργασίες μέσω δικτύου αισθητήρων και ενεργοποιητών. Σε αυτά τα συστήματα, η συμπεριφορά του λογισμικού δεν επηρεάζει μόνο τη ροή πληροφοριών, αλλά και πραγματικές φυσικές καταστάσεις, καθιστώντας τις επιθέσεις στην ακεραιότητα των δεδομένων ή στις διαμορφώσεις ελέγχου δυνητικά επικίνδυνες για την ασφάλεια εξοπλισμού και ανθρώπων. Σύμφωνα με το NIST, τα CPS χαρακτηρίζονται από αυστηρές χρονικές απαιτήσεις, πολύπλοκες εξαρτήσεις μεταξύ επιπέδων ελέγχου και έντονη αλληλεπίδραση μεταξύ safety και security, στοιχεία που διαφοροποιούν την προσέγγιση της κυβερνοασφάλειας σε σχέση με τα παραδοσιακά IT συστήματα.

Ένα χαρακτηριστικό παράδειγμα αποτελεί η αλυσίδα αισθητήρα, ελεγκτή, ενεργοποιητή (sensor–controller–actuator chain) όπου κακόβουλες αλλοιώσεις στις μετρήσεις αισθητήρων ή στις εντολές προς ενεργοποιητές μπορούν να οδηγήσουν σε λανθασμένες ενέργειες ελέγχου, ακόμη και αν τα ίδια τα δίκτυα επικοινωνίας εμφανίζονται ως «διαθέσιμα». Η βιβλιογραφία διακρίνει επιθέσεις σε επίπεδο δεδομένων (data-oriented attacks), επιθέσεις στο control logic και επιθέσεις συγχρονισμού/χρονισμού, οι οποίες εκμεταλλεύονται την ανάγκη για πραγματικό χρόνο και προβλέψιμη συμπεριφορά. Αυτές οι κατηγορίες επιθέσεων αναδεικνύουν την ανάγκη συνδυασμού κλασικών μηχανισμών ασφάλειας δικτύου με τεχνικές ανίχνευσης ανωμαλιών στη φυσική συμπεριφορά του συστήματος, ιδιαίτερα σε περιβάλλοντα με κρίσιμες διεργασίες.

Οι Programmable Logic Controllers (PLC) αποτελούν το κυριότερο στοιχείο των αυτοματισμών, καθώς επιτελούν λογικές εντολές και ελέγχουν άμεσα μηχανικές διεργασίες. Η τυποποίησή τους καθορίζεται από την IEC 61131-3, η οποία περιγράφει τις γλώσσες προγραμματισμού και τη λειτουργική φιλοσοφία τους. Παρότι εξαιρετικά σταθερά και αξιόπιστα, τα PLC συχνά στερούνται βασικών μηχανισμών ασφάλειας, καθιστώντας τα ευάλωτα σε επιθέσεις που στοχεύουν την ακεραιότητα ή την ακολουθία εντολών τους.

Τα συστήματα Supervisory Control and Data Acquisition (SCADA) αποτελούν το εποπτικό επίπεδο της βιομηχανικής τεχνολογίας, επιτρέποντας την απομακρυσμένη συλλογή δεδομένων και την επιτήρηση εκτεταμένων γεωγραφικών υποδομών, όπως ενεργειακά δίκτυα και δίκτυα ύδρευσης. Στην εικόνα 1 παρουσιάζονται τα στοιχεία και η γενική διαμόρφωση ενός συστήματος SCADA. Το κέντρο ελέγχου στο επάνω μέρος του διαγράμματος φιλοξενεί έναν διακομιστή ελέγχου και τους δρομολογητές επικοινωνιών. Άλλα στοιχεία του κέντρου ελέγχου περιλαμβάνουν τη διεπαφή ανθρώπου-μηχανής (HMI), τους σταθμούς εργασίας μηχανικών και το σύστημα καταγραφής ιστορικού δεδομένων, τα οποία συνδέονται όλα μέσω ενός τοπικού δικτύου (LAN). Το κέντρο ελέγχου συλλέγει και καταγράφει τις πληροφορίες που συγκεντρώνονται από τις τοποθεσίες πεδίου, εμφανίζει τις πληροφορίες στη διεπαφή HMI και μπορεί να ενεργοποιεί ενέργειες με βάση τα συμβάντα που ανιχνεύονται. Το κέντρο ελέγχου είναι επίσης υπεύθυνο για την κεντρική ειδοποίηση (centralized alarming), τις αναλύσεις τάσεων (trend analyses) και την υποβολή αναφορών (reporting).

Το NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) αναγνωρίζει τα SCADA ως κρίσιμα συστήματα εθνικών υποδομών που απαιτούν εξειδικευμένους μηχανισμούς προστασίας λόγω της δυνατότητας απομακρυσμένου ελέγχου και της ευαίσθητης φύσης των δεδομένων που διακινούν.



Εικόνα 1. Μια γενική διάταξη συστήματος SCADA που απεικονίζει τις συσκευές του κέντρου ελέγχου, τον εξοπλισμό επικοινωνιών και τις τοποθεσίες πεδίου

Τα Distributed Control Systems (DCS) χρησιμοποιούνται κυρίως σε βιομηχανίες συνεχούς παραγωγής και αποτελούν αρχιτεκτονική που διανέμει τον έλεγχο σε επιμέρους υποσυστήματα. Η ISA περιγράφει την οργάνωση των DCS και τον τρόπο με τον οποίο υποστηρίζουν μεγάλης κλίμακας βιομηχανικές διαδικασίες μέσω ιεραρχικής διαχείρισης αυτοματισμών.

Τα Human-Machine Interfaces (HMI) λειτουργούν ως σημεία αλληλεπίδρασης ανθρώπου και συστήματος. Παρά την κρίσιμη λειτουργικότητά τους, αποτελούν συχνό στόχο κυβερνοεπιθέσεων, διότι η πρόσβαση στο HMI μπορεί να επιτρέψει την παραποίηση δεδομένων ή την τροποποίηση των παραμέτρων.

Η λειτουργία των ICS και CPS βασίζεται σε εξειδικευμένα βιομηχανικά πρωτόκολλα επικοινωνίας, τα οποία σχεδιάστηκαν ιστορικά με προτεραιότητα την αξιοπιστία και την απλότητα υλοποίησης και όχι την ενσωματωμένη κυβερνοασφάλεια. Στις πρώτες προδιαγραφές πολλών πρωτοκόλλων, όπως αναδεικνύει ο οδηγός του NIST για ICS, η έλλειψη μηχανισμών αυθεντικοποίησης, κρυπτογράφησης και προστασίας ακεραιότητας θεωρούνταν αποδεκτή, δεδομένου ότι τα συστήματα λειτουργούσαν σε απομονωμένα δίκτυα με αυστηρά ελεγχόμενη πρόσβαση. Η σταδιακή διασύνδεση αυτών των δικτύων με εταιρικά και διακλαδικά περιβάλλοντα έχει ως αποτέλεσμα η ασφάλεια να εξαρτάται πλέον σε μεγάλο βαθμό από την αρχιτεκτονική δικτυακού διαχωρισμού και από εξωτερικούς ελέγχους πρόσβασης, γεγονός που αυξάνει τις απαιτήσεις για σωστό σχεδιασμό ζωνών και διαύλων επικοινωνίας.

Τα παραπάνω συστήματα λειτουργούν μέσω βιομηχανικών πρωτοκόλλων, πολλά εκ των οποίων σχεδιάστηκαν πριν την εποχή της κυβερνοασφάλειας. Για παράδειγμα, το Modbus εξακολουθεί να αποτελεί ευρέως υιοθετημένη οικογένεια προδιαγραφών, ενώ ο οργανισμός Modbus έχει προωθήσει και νεότερη κατεύθυνση “Modbus Security” με αξιοποίηση TLS και πιστοποιητικών X.509 για ασφαλέστερη επικοινωνία.

Το DNP3, ιδιαίτερα διαδεδομένο σε δίκτυα ενέργειας, απέκτησε ασφαλή εκδοχή μόνο μετά το πρότυπο IEEE 1815-2012. Το Profinet, αν και νεότερο, απαιτεί αυστηρή δικτυακή οριοθέτηση και συμμόρφωση με τις απαιτήσεις της IEC 62443-4-2 για να παραμένει ασφαλές.

1.4 Βασικές προκλήσεις ασφάλειας σε βιομηχανικά περιβάλλοντα

Οι προκλήσεις ασφάλειας στα βιομηχανικά περιβάλλοντα δεν είναι ομοιογενείς, αλλά μπορούν να ομαδοποιηθούν σε τεχνικές, οργανωσιακές και κανονιστικές. Σε τεχνικό επίπεδο, κρίσιμα ζητήματα αποτελούν η παρουσία παλαιωμένων συστημάτων χωρίς δυνατότητα ενημέρωσης, η χρήση μη ασφαλών πρωτοκόλλων και οι περιορισμοί σε latency και διαθεσιμότητα που επηρεάζουν την εφαρμογή κλασικών μέτρων IT. Σε οργανωσιακό επίπεδο, η βιβλιογραφία αναδεικνύει την έλλειψη κοινής γλώσσας μεταξύ IT και OT ομάδων, την απουσία τυποποιημένων διαδικασιών αλλαγών και patching, καθώς και την περιορισμένη διαθεσιμότητα προσωπικού με διπλή εξειδίκευση σε αυτοματισμούς και κυβερνοασφάλεια. Τέλος, σε κανονιστικό επίπεδο, η συμμόρφωση με πρότυπα όπως IEC 62443, NERC CIP και τα εθνικά/ευρωπαϊκά πλαίσια για κρίσιμες υποδομές απαιτεί συστηματική τεκμηρίωση και διακυβέρνηση, στοιχεία που συχνά υπολείπονται σε παραδοσιακά βιομηχανικά περιβάλλοντα.

Η ασφάλεια των βιομηχανικών συστημάτων αποτελεί σύνθετο πεδίο, διότι συνδυάζει τεχνολογικούς, λειτουργικούς και ανθρώπινους παράγοντες. Η IEC 62443 και το NIST έχουν επισημάνει ότι τα OT συστήματα αντιμετωπίζουν προκλήσεις που δεν είναι παρούσες στο IT, κυρίως λόγω της φύσης των φυσικών διεργασιών και της ανάγκης για συνεχή λειτουργία.

Ένα από τα σημαντικότερα προβλήματα είναι η ύπαρξη legacy συστημάτων. Πολλές βιομηχανικές εγκαταστάσεις βασίζονται σε συσκευές και λογισμικά δεκαετιών, τα οποία δεν υποστηρίζουν μηχανισμούς ασφάλειας ούτε επιτρέπουν την εύκολη εφαρμογή patches. Η CISA αναφέρει ότι μεγάλος αριθμός περιστατικών ICS οφείλεται σε συστήματα χωρίς δυνατότητα ενημέρωσης, τα οποία παραμένουν εκτεθειμένα σε γνωστές ευπάθειες.

Επιπλέον, τα real time χαρακτηριστικά των OT συστημάτων καθιστούν απαγορευτική τη χρήση εργαλείων ασφάλειας που είναι κοινά στον χώρο του IT όπως deep packet inspection και strong encryption. Αυτό σημαίνει

πως αν εφαρμοστούν τέτοιοι μηχανισμοί θα πρέπει να προσαρμοστούν κατάλληλα καθώς, κάθε καθυστέρηση στην επεξεργασία δεδομένων μπορεί να οδηγήσει σε δυσλειτουργία. Συνεπώς, η ασφάλεια πρέπει να εφαρμόζεται με τρόπο που να μην παρεμβαίνει στη χρονική ακρίβεια των λειτουργιών.

Τέλος, η διάκριση μεταξύ safety και security αποτελεί θεμελιώδες ζήτημα. Ο όρος safety αφορά την προστασία ανθρώπων και εξοπλισμού από ακούσια συμβάντα, ενώ η security σχετίζεται με την προστασία από κακόβουλες ενέργειες. Η IEC 61508 περιγράφει τη λειτουργική ασφάλεια ως διαδικασία αποτροπής ατυχημάτων, αλλά η IEC 62443 τεκμηριώνει ότι μια επιτυχημένη κυβερνοεπίθεση μπορεί να προκαλέσει περιστατικά safety, όπως συνέβη στην περίπτωση του Stuxnet, όπου παραποιήθηκαν βιομηχανικές διεργασίες με αποτέλεσμα φυσικές βλάβες στις εγκαταστάσεις.

Οι παραπάνω παράγοντες καταδεικνύουν ότι η ασφάλεια των βιομηχανικών συστημάτων δεν μπορεί να αντιμετωπιστεί αποσπασματικά, αλλά απαιτεί συντονισμένη προσέγγιση που να ενσωματώνει τεχνικές και οργανωσιακές παραμέτρους. Η IEC 62443 και οι οδηγοί του NIST για ICS προτείνουν ένα συνδυασμό μέτρων, από τον διαχωρισμό δικτύων και τη σκληροποίηση συστημάτων έως τη διαχείριση ευπαθειών, την παρακολούθηση και την προετοιμασία για περιστατικά, με γνώμονα τόσο την ασφάλεια πληροφοριών όσο και τη λειτουργική ασφάλεια. Η παρούσα εργασία αξιοποιεί αυτές τις αρχές ως θεωρητικό υπόβαθρο για τα επόμενα κεφάλαια, όπου οι προκλήσεις που περιγράφηκαν εδώ μεταφράζονται σε συγκεκριμένες αρχιτεκτονικές και λειτουργικά μοντέλα για IT, OT και ενοποιημένο περιβάλλον OT/IT.

ΚΕΦΑΛΑΙΟ 2 - Αρχιτεκτονική Ασφάλειας IT και Διαχείριση Κινδύνου

Το παρόν κεφάλαιο εξετάζει την αρχιτεκτονική ασφάλειας στον χώρο των πληροφοριακών συστημάτων, με έμφαση στα πλαίσια διαχείρισης ασφάλειας πληροφοριών, στη διαχείριση κινδύνου και στα μοντέλα ελέγχων που καθορίζουν τις σύγχρονες IT υποδομές. Η ανάλυση βασίζεται σε διεθνή πρότυπα και οδηγούς, όπως τα ISO/IEC 27001 και 27002 για τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών, καθώς και τις σειρές NIST SP 800-53, SP 800-37 και το NIST Cybersecurity Framework (CSF) 2.0, τα οποία παρέχουν δομημένη προσέγγιση στην επιλογή και αξιολόγηση ελέγχων. Η κατανόηση των αρχών αυτών είναι θεμελιώδης, καθώς η προτεινόμενη αρχιτεκτονική OT/IT της εργασίας αξιοποιεί τα IT πρότυπα ως “βάση αναφοράς”, επεκτείνοντάς τα ώστε να καλύψουν τις ιδιαιτερότητες των βιομηχανικών περιβαλλόντων.

2.1 Η έννοια της «αρχιτεκτονικής ασφάλειας» στο IT και ο ρόλος του ISMS

Η έννοια της αρχιτεκτονικής ασφάλειας στο IT αναφέρεται σε μια συστηματική οργάνωση αρχών, πολιτικών, διαδικασιών και τεχνικών ελέγχων που καθορίζουν πώς προστατεύονται τα πληροφοριακά περιουσιακά στοιχεία σε όλο τον κύκλο ζωής τους. Σε αντίθεση με μια “λίστα εργαλείων” ή μια ad-hoc συλλογή μηχανισμών, η αρχιτεκτονική ασφάλειας επιδιώκει να ευθυγραμμίσει τη στρατηγική ασφάλειας με τους επιχειρησιακούς στόχους, ορίζοντας ρητά ποιοι κίνδυνοι είναι αποδεκτοί, ποιοι πρέπει να μετριαστούν και με ποια μέσα. Τα πρότυπα της οικογένειας ISO/IEC 27000 τονίζουν ότι το ISMS λειτουργεί ως πλαίσιο διακυβέρνησης πάνω στο οποίο “κουμπώνουν” οι τεχνικές αρχιτεκτονικές επιλογές, από τα δίκτυα μέχρι τις εφαρμογές και τις υπηρεσίες cloud.

Στον χώρο της κυβερνοασφάλειας, ο όρος «αρχιτεκτονική ασφάλειας IT» δεν περιγράφει απλώς ένα σύνολο τεχνικών εργαλείων, αλλά ένα συνεκτικό σχήμα αρχών, ρόλων, διαδικασιών και ελέγχων που οργανώνουν τη λήψη αποφάσεων γύρω από την προστασία πληροφοριακών πόρων.

Το ISO/IEC 27001:2022 συγκροτεί αυτό το σχήμα μέσα από την απαίτηση για εγκαθίδρυση, εφαρμογή, διατήρηση και συνεχή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), δηλαδή ενός διοικητικού πλαισίου που καθιστά την ασφάλεια αντικείμενο διακυβέρνησης και όχι περιστασιακής τεχνικής παρέμβασης. Συμπληρωματικά, Το ISO/IEC 27000:2018 παρέχει το εννοιολογικό υπόβαθρο (όρους και ορισμούς) που καθιστά δυνατή την κοινή γλώσσα μεταξύ τεχνικών και διοικητικών ρόλων, στοιχείο κρίσιμο ώστε η «ασφάλεια» να μην παραμένει άρρητη υπόθεση αλλά ρητά διαχειρίσιμο πεδίο.

Η έννοια της αρχιτεκτονικής ασφάλειας στο IT αποκτά ιδιαίτερη βαρύτητα στο περιβάλλον σύγχρονων οργανισμών, όπου η κυβερνοασφάλεια αντιμετωπίζεται ως διαρκής διαχείριση κινδύνου και όχι ως «τελική κατάσταση» συμμόρφωσης.

Αυτή η μετατόπιση εκφράζεται και στο NIST Cybersecurity Framework (CSF) 2.0, το οποίο δεν «επιβάλλει» συγκεκριμένους μηχανισμούς, αλλά προσφέρει ταξινομία επιθυμητών αποτελεσμάτων που μπορούν να χρησιμοποιηθούν για κατανόηση, αξιολόγηση και προτεραιοποίηση των προσπαθειών ασφάλειας.

Το CSF 2.0 εισάγει ρητά τη λειτουργία Govern ως ισότιμο, υπογραμμίζοντας ότι η ασφάλεια πρέπει να εντάσσεται σε πλαίσιο λογοδοσίας, πολιτικών και στρατηγικής, στοιχείο που επαναφέρει την «αρχιτεκτονική» στην πρωταρχική της σημασία ως οργάνωση σκοπών και μέσων.

Η προσέγγιση αυτή έχει ιδιαίτερη σημασία για το αντικείμενο της παρούσας εργασίας, διότι επιτρέπει η ίδια λογική ISMS και αρχιτεκτονικής ασφάλειας να επεκταθεί πέρα από τα κλασικά IT συστήματα και να συμπεριλάβει τα OT περιβάλλοντα. Μέσα από την υιοθέτηση κοινών αρχών, όπως η τεκμηριωμένη πολιτική, η διαχείριση κινδύνου και η συστηματική παρακολούθηση, καθίσταται εφικτή η δημιουργία ενοποιημένης αρχιτεκτονικής OT/IT που αντιμετωπίζει τα βιομηχανικά συστήματα ως οργανικό τμήμα του συνολικού οικοσυστήματος ασφάλειας και όχι ως “απομονωμένες” νησίδες.

2.2 Διαχείριση κινδύνου ως θεμέλιο των IT αρχιτεκτονικών ασφάλειας

Η διαχείριση κινδύνου αποτελεί τον άξονα γύρω από τον οποίο οργανώνεται κάθε σύγχρονη αρχιτεκτονική ασφάλειας IT. Τόσο τα διεθνή πρότυπα ISO όσο και οι οδηγίες του NIST συμφωνούν ότι η επιλογή ελέγχων δεν μπορεί να είναι τυχαία ή αποκλειστικά τεχνοκεντρική, αλλά πρέπει να βασίζεται σε συστηματική αναγνώριση

απειλών, ευπαθειών και επιπτώσεων πάνω σε συγκεκριμένα περιουσιακά στοιχεία. Στην πράξη, αυτό σημαίνει ότι η αρχιτεκτονική ασφάλειας λειτουργεί ως “υλοποίηση” αποφάσεων διαχείρισης κινδύνου, μεταφράζοντας τις εκτιμήσεις ρίσκου σε συγκεκριμένες τεχνικές και οργανωσιακές παρεμβάσεις.

Η αρχιτεκτονική ασφάλειας στο IT χρησιμοποιείται, σχεδόν αναγκαστικά, για την ανάλυση την ανάδειξη και την διαχείριση του κινδύνου, διότι η απόλυτη ασφάλεια είναι ανέφικτη και οι οργανισμοί καλούνται να επιλέξουν ελέγχους με βάση προτεραιότητες, επιπτώσεις και αποδεκτό ρίσκο.

Το ISO 31000:2018 προσφέρει γενικές κατευθυντήριες γραμμές για διαχείριση κινδύνου σε επίπεδο οργανισμού, εστιάζοντας στη συστηματική αναγνώριση, ανάλυση, αξιολόγηση, αντιμετώπιση και παρακολούθηση κινδύνων ως επαναληπτική διαδικασία λήψης αποφάσεων.

Σε πιο εξειδικευμένο επίπεδο κυβερνοασφάλειας, το ISO/IEC 27005:2022 παρέχει καθοδήγηση για διαχείριση κινδύνων ασφάλειας πληροφοριών ως υποστήριξη της εφαρμογής ISMS βάσει ISO/IEC 27001, ενισχύοντας τη θέση ότι το ISMS δεν είναι απλή συλλογή πολιτικών, αλλά μηχανισμός λήψης αποφάσεων πάνω στα ρίσκα και τους κινδύνους που αναδεικνύονται.

Στο αμερικανικό κανονιστικό/τεχνικό οικοσύστημα, το NIST SP 800-39 ορίζει την «οργανωσιακή» οπτική της διαχείρισης κινδύνου (organization, mission, information system view), μετατρέποντας τη διαχείριση κινδύνου σε ολοκληρωμένο πρόγραμμα που αφορά λειτουργίες, υποδομές και άτομα.

Το NIST SP 800-30 Rev.1 εξειδικεύει τη μεθοδολογία διεξαγωγής risk assessments και υπογραμμίζει ότι οι αξιολογήσεις κινδύνου αποτελούν μέρος μιας ευρύτερης διαδικασίας risk management, παρέχοντας σε ανώτερα στελέχη πληροφορία για επιλογή κατάλληλων δράσεων.

Το NIST SP 800-37 Rev.2 (Risk Management Framework – RMF) κωδικοποιεί αυτή τη λογική σε πειθαρχημένη διαδικασία που συνδέει κατηγοριοποίηση, επιλογή/εφαρμογή/αξιολόγηση ελέγχων, εξουσιοδότηση και συνεχή παρακολούθηση, δείχνοντας πώς η αρχιτεκτονική ασφάλειας «δένει» με τον κύκλο ζωής του συστήματος.

Η λογική αυτή είναι ιδιαίτερα χρήσιμη όταν επιχειρείται ενοποίηση IT και OT, καθώς παρέχει ένα κοινό “μετα-επίπεδο” συζήτησης για τον κίνδυνο, ανεξάρτητα από το αν οι υποκείμενες τεχνολογίες είναι servers, εφαρμογές επιχειρησιακής ευφυΐας ή συστήματα βιομηχανικού ελέγχου. Χρησιμοποιώντας ένα κοινό πλαίσιο διαχείρισης κινδύνου, όπως το NIST RMF ή οι οδηγίες ISO/IEC 27005, ο οργανισμός μπορεί να αξιολογεί με συνεπή τρόπο τα σενάρια απειλών που αφορούν τόσο IT όσο και OT, και να αποφασίζει πού θα επενδύσει σε πρόσθετους ελέγχους ή πού θα αποδεχτεί ρητά τον κίνδυνο.

2.3 Κατάλογοι ελέγχων και αρχιτεκτονική «στρωμάτων»

Στο επίπεδο της πρακτικής υλοποίησης, οι αρχιτεκτονικές ασφάλειας IT χρειάζονται «λεξιλόγιο ελέγχων», δηλαδή ένα δομημένο σώμα μέτρων που να μπορεί να επιλεγεί, να προσαρμοστεί και να αξιολογηθεί. Το NIST SP 800-53 Rev.5 παρέχει έναν εκτενή κατάλογο ελέγχων ασφάλειας και ιδιωτικότητας, ο οποίος σχεδιάζεται για να είναι ευέλικτος και παραμετροποιήσιμος, ώστε να εφαρμοστεί ως μέρος οργανωσιακής διαδικασίας διαχείρισης κινδύνου του κάθε οργανισμού.

Η ύπαρξη τέτοιων καταλόγων επιτρέπει την ανάπτυξη αρχιτεκτονικών “πολλαπλών στρωμάτων”, στις οποίες διαφορετικές κατηγορίες ελέγχων συνδυάζονται ώστε να παρέχουν άμυνα σε βάθος. Για παράδειγμα, ένας συνδυασμός ελέγχων πρόσβασης (Access Control), ελέγχων διαχωρισμού δικτύων (System and Communications Protection), logging και monitoring (Audit and Accountability, Security Monitoring) και διαδικασιών απόκρισης σε περιστατικά (Incident Response) μπορεί να δομηθεί ως διαδοχικά στρώματα που δυσκολεύουν σημαντικά την επιτυχή εκτέλεση και διάδοση μιας επίθεσης. Το NIST SP 800-53r5 παρέχει τις οικογένειες ελέγχων που υποστηρίζουν αυτόν τον “στρωματοποιημένο” σχεδιασμό, ενώ το ISO/IEC 27002 προσφέρει πρακτικά παραδείγματα εφαρμογής των ελέγχων σε διαφορετικά περιβάλλοντα.

Από την πλευρά των ISO προτύπων, το ISO/IEC 27002:2022 παρέχει πρακτικές ελέγχων (controls) που χρησιμοποιούνται ως σημείο αναφοράς για την υλοποίηση μέτρων ασφάλειας σε οργανισμούς, λειτουργώντας συμπληρωματικά προς τις απαιτήσεις ISMS της ISO/IEC 27001. Τα ISO/IEC 27001–27002 είναι χρήσιμα καθώς

σε αυτά διαχωρίζεται ξεκάθαρα το «τι απαιτείται» από το «πώς υλοποιείται» δεξαμενή ελέγχων/καλών πρακτικών). Εδώ συγκροτείται και μια τυπική λογική «πολλαπλών στρωμάτων»: η αρχιτεκτονική δεν βασίζεται σε έναν μόνο μηχανισμό (π.χ. firewall), αλλά σε συνδυασμό πολιτικών, τεχνικών ελέγχων, διαδικασιών και επιτήρησης που αλληλοσυμπληρώνονται και μπορούν να αξιολογηθούν έναντι κινδύνου. Αυτός ο τρόπος σκέψης ενισχύεται από την έννοια του continuous monitoring, δηλαδή της διαρκούς επίγνωσης της κατάστασης ασφάλειας, την οποία το NIST SP 800-137 παρουσιάζει ως στρατηγική που παρέχει ορατότητα στις υποδομές, στις απειλές, στις ευπάθειες και αποτελεσματικότητα των ελέγχων.

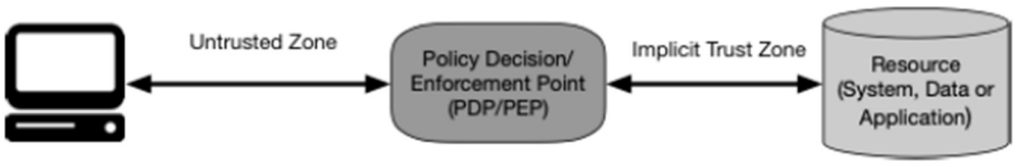
Στα επόμενα κεφάλαια, οι ίδιες αρχές αρχιτεκτονικής “στρωμάτων” θα χρησιμοποιηθούν για να αποτυπωθούν οι ζώνες, οι αγωγοί και οι έλεγχοι των OT περιβαλλόντων, με τρόπο που να επιτρέπει την αντιστοίχισή τους σε καταλόγους ελέγχων όπως το NIST SP 800-53 και τα Foundational Requirements της IEC 62443. Με αυτόν τον τρόπο, η προστασία των βιομηχανικών διεργασιών αποκτά σαφή αναφορά σε διεθνώς αναγνωρισμένα πλαίσια, διευκολύνοντας τόσο την τεχνική υλοποίηση όσο και την τεκμηρίωση της συμμόρφωσης.

2.4 Από το «περιμετρικό» μοντέλο στο Zero Trust

Η μετάβαση από το παραδοσιακό περιμετρικό μοντέλο ασφάλειας προς την προσέγγιση Zero Trust αποτελεί μία από τις σημαντικότερες αλλαγές στη σύγχρονη αρχιτεκτονική ασφάλειας IT. Στο κλασικό μοντέλο, το εσωτερικό δίκτυο θεωρείται κατά βάση αξιόπιστο και η άμυνα επικεντρώνεται στην προστασία ενός σαφώς ορισμένου “περιμετρικού” ορίου, ενώ η πρόσβαση από το εσωτερικό αντιμετωπίζεται συχνά με αυξημένη εμπιστοσύνη. Αντίθετα, η λογική Zero Trust, όπως περιγράφεται στο NIST SP 800-207, απορρίπτει την ιδέα του “εμπιστευόμενου εσωτερικού” και αντιμετωπίζει κάθε αίτημα πρόσβασης ως δυνητικά μη αξιόπιστο, ανεξάρτητα από το πού βρίσκεται ο χρήστης ή η συσκευή (NIST.SP.800-53 Rev 5, Department of Commerce, 2020).

Μία από τις πιο καθοριστικές μεταβολές στις σύγχρονες IT αρχιτεκτονικές είναι η σταδιακή απομάκρυνση από την υπόθεση ότι το εσωτερικό δίκτυο είναι εγγενώς αξιόπιστο, υπόθεση που ιστορικά υποστήριξε το παραδοσιακό περιμετρικό μοντέλο. Το NIST SP 800-207 ορίζει το Zero Trust ως εξελισσόμενο σύνολο παραδειγμάτων που μετακινεί την άμυνα από στατικά, δικτυο-κεντρικά όρια και εστιάζει σε χρήστες, assets και πόρους, και περιγράφει μια Zero Trust Architecture (ZTA) ως εφαρμογή αρχών zero trust στον σχεδιασμό υποδομών. Κεντρική ιδέα του SP 800-207 είναι ότι δεν παρέχεται «απόλυτη εμπιστοσύνη» σε χρήστες ή assets λόγω δικτυακής τοποθεσίας ή ιδιοκτησίας, αλλά απαιτούνται ρητές διεργασίες αυθεντικοποίησης και εξουσιοδότησης, μετατρέποντας την πρόσβαση σε διαρκώς ελεγχόμενη πράξη.

Στο μοντέλο πρόσβασης που παρουσιάζεται στην εικόνα 2, ένας χρήστης χρειάζεται πρόσβαση σε πόρους που είναι πίσω από προστατευμένη περιοχή. Η πρόσβαση χορηγείται μέσω ενός σημείου λήψης αποφάσεων πολιτικής (PDP) και του αντίστοιχου σημείου επιβολής πολιτικής (PEP). Στο OT το “PEP” αντιστοιχεί συχνά σε IDMZ firewall/gateway/jump server και όχι σε endpoint agent σε PLC, άρα το Zero Trust εφαρμόζεται κυρίως στα boundaries/flows.



Εικόνα 2. Zero Trust Access

Για περιβάλλοντα cloud και cloud-native εφαρμογές, το NIST SP 800-207A (2023) προτείνει μοντέλο ZTA για access control, δείχνοντας πώς η λογική zero trust μπορεί να εξειδικευθεί σε σύγχρονες αρχιτεκτονικές microservices.

Αν και το Zero Trust προέκυψε αρχικά ως απάντηση στις προκλήσεις των σύγχρονων IT υποδομών και των cloud περιβαλλόντων, οι βασικές του αρχές είναι ιδιαίτερα σχετικές και με τα OT δίκτυα, όπου δεν είναι εφικτή η

πλήρης εμπιστοσύνη ούτε στο “εσωτερικό” της εγκατάστασης. Η έννοια του Policy Enforcement Point (PEP) που ελέγχει κάθε ροή πρόσβασης μπορεί να υλοποιηθεί σε κρίσιμα σημεία, όπως οι ζώνες IDMZ ή τα jump servers, ελέγχοντας τη διασύνδεση μεταξύ IT και OT και επιβάλλοντας αρχές ελάχιστης προνομιακής πρόσβασης. Στη συνέχεια της εργασίας, οι αρχές Zero Trust θα χρησιμοποιηθούν για να ενισχύσουν την προτεινόμενη αρχιτεκτονική OT/IT, χωρίς να παραβλέπονται οι περιορισμοί διαθεσιμότητας και πραγματικού χρόνου των βιομηχανικών συστημάτων.

2.5 Cloud & Hybrid Security

Η υιοθέτηση υπηρεσιών cloud και υβριδικών υποδομών επεκτείνει σημαντικά τα όρια της αρχιτεκτονικής ασφάλειας IT, καθώς εισάγει νέους τύπους εξαρτήσεων, μοντέλα ευθύνης και διαδρομές δεδομένων. Ο ορισμός του cloud computing από το NIST SP 800-145 αναδεικνύει χαρακτηριστικά όπως η on-demand πρόσβαση σε κοινόχρηστους πόρους και η ευρεία δικτυακή προσβασιμότητα, τα οποία προσφέρουν ευελιξία αλλά ταυτόχρονα δημιουργούν πρόσθετη επιφάνεια επίθεσης. Για τους σκοπούς της παρούσας εργασίας, η κατανόηση των αρχών ασφαλείας σε περιβάλλοντα cloud είναι κρίσιμη, καθώς πολλές επιχειρησιακές λειτουργίες που σχετίζονται με OT, όπως η ανάλυση δεδομένων ή η κεντρική επιτήρηση, υλοποιούνται πλέον σε cloud ή hybrid σενάρια.

Καθώς οι οργανισμοί μεταβαίνουν σε υβριδικά περιβάλλοντα, η IT αρχιτεκτονική ασφάλειας οφείλει να περιγράψει με ακρίβεια τι εννοεί με τον όρο “cloud”. Ο ορισμός του cloud computing από το NIST (SP 800-145) αποτελεί σημείο αναφοράς, καθώς περιγράφει μοντέλο που επιτρέπει ευρεία, on-demand δικτυακή πρόσβαση σε κοινό pool υπολογιστικών πόρων. Παράλληλα, το NIST SP 800-144 αναλύει προκλήσεις ασφάλειας και ιδιωτικότητας σε public cloud και παραθέτει ζητήματα που πρέπει να σταθμίζουν οι οργανισμοί όταν αναθέτουν δεδομένα, εφαρμογές και υποδομές σε cloud περιβάλλοντα.

Στο πεδίο των ISO προτύπων, το ISO/IEC 27017:2015 παρέχει οδηγίες ελέγχων ασφάλειας ειδικά για την παροχή και χρήση cloud υπηρεσιών, δίνοντας μεγαλύτερη βάση σε ελέγχους που σχετίζονται με το cloud πέρα από τις γενικές κατευθύνσεις του ISO/IEC 27002. Για ζητήματα προστασίας προσωπικών δεδομένων σε public cloud, το ISO/IEC 27018:2019 καθορίζει εργαλεία ελέγχου και κατευθύνσεις για μέτρα προστασίας των προσωπικών δεδομένων ώστε οι οργανισμοί να ευθυγραμμίζονται με τις αρχές ιδιωτικότητας, ενισχύοντας την κατανόηση ότι η αρχιτεκτονική ασφάλειας cloud δεν είναι μόνο τεχνικό αλλά και κανονιστικό/δεοντολογικό ζήτημα.

Σε επίπεδο υλοποίησης, η αρχιτεκτονική ασφάλειας cloud προϋποθέτει σαφή κατανομή ευθυνών μεταξύ παρόχου και πελάτη, διότι η ασφάλεια προκύπτει από συνεργασία αρμοδιοτήτων. Αυτό αποτυπώνεται και ρητά σε επίσημο ενημερωτικό κείμενο του U.S. Department of Defense (Cybersecurity Information Sheet) για το cloud shared responsibility model, όπου τονίζεται ότι τόσο ο πελάτης όσο και ο πάροχος είναι υπόλογοι για την ασφάλεια και ότι τα αποτελέσματα ασφάλειας εξαρτώνται από την κατανόηση και τήρηση αυτών των ευθυνών.

2.6 Υλοποίηση Zero Trust Architecture

Το NIST SP 800-207 περιγράφει μια Zero Trust Architecture ως συνδυασμό αρχών και λογικών συστατικών που μεταφέρουν το κέντρο βάρους της άμυνας από τα στατικά όρια δικτύου στα ίδια τα αιτήματα πρόσβασης, στους χρήστες και στα assets. Στον πυρήνα του μοντέλου βρίσκονται τρία βασικά στοιχεία, το Policy Engine, ο Policy Administrator και το Policy Enforcement Point, τα οποία συνεργάζονται για να αξιολογούν συνεχώς την αξιοπιστία κάθε αιτήματος με βάση πολιτικές, σήματα ταυτοποίησης και πληροφορίες για την κατάσταση της συσκευής. Η αρχιτεκτονική αυτή δεν επιβάλλει συγκεκριμένη τεχνολογία, αλλά προσφέρει ένα λογικό πλαίσιο που μπορεί να υλοποιηθεί με διαφορετικούς συνδυασμούς proxy, gateway, identity provider και μηχανισμών παρακολούθησης.

Η μετάβαση από τις υποθέσεις σε πιο ρεαλιστικά μοντέλα αποτελεί κομβικό σημείο στη σύγχρονη IT αρχιτεκτονική, ιδίως σε περιβάλλοντα cloud/hybrid και απομακρυσμένης πρόσβασης.

Το NIST SP 800-207 ορίζει το Zero Trust ως σύνολο παραδειγμάτων που μεταφέρουν την άμυνα από στατικά όρια δικτύου προς χρήστες, assets, resources, και παρουσιάζει τα λογικά συστατικά μιας ZTA (όπως policy engine, policy administrator, policy enforcement). Στο ίδιο κείμενο, το NIST περιγράφει ως αφετηρία μετάβασης τη σταδιακή υλοποίηση πολιτικών πρόσβασης που βασίζονται σε συνεχή αξιολόγηση (ταυτότητα, κατάσταση

συσκευής) και όχι σε απλή αναγνώριση της τοποθεσίας της συσκευής/χρήστη στο δίκτυο. Για multi-cloud/hybrid σενάρια, το NIST SP 800-207A εξειδικεύει ένα μοντέλο ZTA για access control που επιδιώκει granular πολιτικές σε επίπεδο εφαρμογής, συμβατές με runtime απαιτήσεις τέτοιων περιβαλλόντων.

Έστω ένας οργανισμός με on-prem εφαρμογή οικονομικής διαχείρισης (ERP) και χρήστες που συνδέονται από εταιρικά laptops και από BYOD σε εξαιρετικές περιπτώσεις, όπου ο στόχος είναι να μειωθεί ο κίνδυνος κλοπής διαπιστευτηρίων και lateral movement.

Η υλοποίηση ZTA, σύμφωνα με τη λογική του SP 800-207, μπορεί να θεμελιωθεί σε τρία επίπεδα: (α) ισχυρή ταυτοποίηση χρήστη, (β) αξιολόγηση της συσκευής, (γ) επιβολή πολιτικής στο σημείο πρόσβασης (Policy Enforcement Point, PEP), ώστε κάθε αίτημα να κρίνεται δυναμικά. Στην πράξη, αυτό μεταφράζεται σε χρήση μηχανισμών ισχυρής αυθεντικοποίησης σύμφωνα με τις απαιτήσεις assurance levels, όπως ορίζονται στο NIST SP 800-63B-4 (2025) για τα Authenticator Assurance Levels και τους τεχνικούς όρους αυθεντικοποίησης. Στη συνέχεια, το PEP μπορεί να υλοποιηθεί ως reverse proxy / application gateway μπροστά από την εφαρμογή, ώστε η πρόσβαση να επιτρέπεται μόνο μετά από την αποδοχή του policy (policy engine) που λαμβάνει σήματα ταυτοποίησης και posturing, όπως προϋποθέτει η λογική των ZTA components στο SP 800-207.

Τέλος, το μοντέλο ολοκληρώνεται με συνεχή παρακολούθηση της αποτελεσματικότητας των ελέγχων και της κατάστασης των assets, όπως περιγράφεται στο πρόγραμμα ISCM του NIST SP 800-137, ώστε η ZTA να μην είναι «στατική ρύθμιση» αλλά διαρκής αξιολόγηση κινδύνου.

Για τα OT περιβάλλοντα, η υλοποίηση Zero Trust επικεντρώνεται λιγότερο σε agents πάνω σε PLCs και περισσότερο σε ισχυρά Policy Enforcement Points στα όρια μεταξύ ζωνών, όπως gateways στην Industrial DMZ, jump servers και ασφαλείς διακομιστές απομακρυσμένης πρόσβασης. Με αυτόν τον τρόπο, οι αρχές συνεχούς αυθεντικοποίησης και ελάχιστης προνομιακής πρόσβασης μπορούν να εφαρμοστούν χωρίς να απαιτούνται παρεμβάσεις στα ίδια τα συστήματα ελέγχου, τα οποία συχνά έχουν περιορισμένες δυνατότητες για σύγχρονους μηχανισμούς ασφάλειας. Η λογική αυτή θα αξιοποιηθεί στα επόμενα κεφάλαια για τον σχεδιασμό της γέφυρας IT/OT και της συνολικής αρχιτεκτονικής ασφαλείας.

2.6.1 Identity Access Management στην πράξη

Στην αρχιτεκτονική ασφάλειας IT, η ταυτοποίηση λειτουργεί ως πρωτεύον σημείο ελέγχου, επειδή μεγάλο μέρος των επιθέσεων επιχειρεί είτε κατάχρηση των προσβάσεων ενός χρήστη είτε κλοπή/παραποίηση διαπιστευτηρίων.
Το NIST SP 800-63B-4 (2025) ορίζει τεχνικές απαιτήσεις για επίπεδα διασφάλισης αυθεντικοποίησης (AALs) και έτσι δίνει «μετρήσιμη γλώσσα» για το τι σημαίνει ισχυρή αυθεντικοποίηση και πότε απαιτείται.

Σε ένα περιβάλλον, για παράδειγμα, με Windows/AD ή αντίστοιχο directory, οι διαχειριστικοί λογαριασμοί αποτελούν διαφορετική κατηγορία κινδύνου από τους απλούς χρήστες, συνεπώς η αρχιτεκτονική μπορεί να προβλέπει (α) ξεχωριστά identities για administrators, (β) ισχυρότερους μηχανισμούς αυθεντικοποίησης, (γ) χρονικά περιορισμένη απόδοση προσβάσεων (just-in-time).

2.6.2 Telemetry, logging και SIEM: υλοποίηση αρχιτεκτονικής monitoring

Καμία αρχιτεκτονική δεν είναι πειστική αν δεν μπορεί να παραγάγει logs (evidence) και να υποστηρίξει έγκαιρη ανίχνευση/απόκριση, διότι η ασφάλεια είναι δυναμική και όχι στατική. Το NIST SP 800-137 ορίζει τη συνεχή παρακολούθηση (ISCM) ως πρόγραμμα που προσφέρει ορατότητα σε assets, επίγνωση απειλών και ευπαθειών, και ορατότητα στην αποτελεσματικότητα των ελέγχων, άρα αποτελεί θεμέλιο της αρχιτεκτονικής σε επίπεδο λειτουργικής ωριμότητας.

Για αξιολόγηση του ίδιου του ISCM προγράμματος, το NIST SP 800-137A δίνει μεθοδολογία assessment, ώστε η παρακολούθηση να μην είναι «απλή συλλογή logs», αλλά αξιολογήσιμος μηχανισμός διαχείρισης κινδύνου. Στο χαμηλότερο επίπεδο πρακτικής υλοποίησης, το NIST SP 800-92 παρέχει οδηγίες για log management σε επιχειρησιακό περιβάλλον, δηλαδή για σχεδιασμό, υλοποίηση και συντήρηση πρακτικών καταγραφής και διαχείρισης αρχείων καταγραφής.

Ένας οργανισμός μπορεί να ορίσει, με βάση το SP 800-92, ποιες κατηγορίες γεγονότων είναι κρίσιμες (authentication, privilege changes, endpoint detections, admin actions) και να τις μεταφέρει σε κεντρικό σύστημα συσχέτισης/ανάλυσης (SIEM), διασφαλίζοντας ακεραιότητα, επάρκεια χρόνου διατήρησης και δυνατότητα αναζήτησης. Η αποτελεσματικότητα αυτής της υλοποίησης τεκμηριώνεται όταν εντάσσεται σε ISCM πρόγραμμα (SP 800-137), δηλαδή όταν ο οργανισμός ορίζει μετρικές και ρυθμό αξιολόγησης που τροφοδοτούν αποφάσεις risk management.

Η οργανωσιακή ολοκλήρωση έρχεται όταν το incident response δεν αντιμετωπίζεται ως «έκτακτο γεγονός», αλλά ως τμήμα της διαχείρισης κινδύνου, όπως περιγράφει το NIST SP 800-61 Rev.3 (2025), το οποίο συνδέει το incident response με τις λειτουργίες του CSF 2.0. Αντίστοιχα, σε διεθνές επίπεδο τυποποίησης, η ISO/IEC 27035-1:2023 παρέχει γενική αλλά δομημένη καθοδήγηση για incident management, ώστε η αρχιτεκτονική να συνοδεύεται από διαδικασίες προετοιμασίας, ανίχνευσης και απόκρισης.

2.6.3 Secure Software Development LifeCycle (SSDLC) και supply chain αρχιτεκτονική

Στα σύγχρονα περιβάλλοντα, η αρχιτεκτονική ασφάλειας δεν τελειώνει στο runtime επίπεδο, γιατί μεγάλο ποσοστό κινδύνου εισάγεται ήδη στη φάση ανάπτυξης και προμήθειας λογισμικού και υπηρεσιών. Το NIST SP 800-218 (SSDF v1.1) προτείνει θεμελιώδεις πρακτικές ασφαλούς ανάπτυξης, με στόχο τη μείωση του κινδύνου ευπαθειών λογισμικού, και αποτελεί primary source για το πώς ένα SDLC «εμπλουτίζεται» με ασφάλεια. Παράλληλα, το NIST SP 800-161 Rev.1 παρέχει καθοδήγηση για Cybersecurity Supply Chain Risk Management (C-SCRM), ενσωματώνοντάς το στη διαχείριση κινδύνου σε όλα τα επίπεδα του οργανισμού.

Αν ένας οργανισμός, για παράδειγμα, αναπτύσσει microservices και τα τρέχει σε Kubernetes, η αρχιτεκτονική ασφάλειας μπορεί να περιλάβει service-to-service προστασία μέσω service mesh, με πολιτικές πρόσβασης σε επίπεδο εφαρμογής και κρυπτογράφηση μεταξύ υπηρεσιών, όπως περιγράφει το NIST SP 800-204A για ασφαλή ανάπτυξη microservices με service mesh. Η ίδια αρχιτεκτονική αποκτά «ρίζες» όταν η αλυσίδα παραγωγής λογισμικού ακολουθεί SSDF πρακτικές (SP 800-218), ώστε ο κώδικας, τα dependencies και οι διαδικασίες build/release να τεκμηριώνονται και να ελέγχονται ως προς τον κίνδυνο.

Τέλος, η αξιολόγηση προμηθευτών, υπηρεσιών και προϊόντων εντάσσεται σε C-SCRM πρόγραμμα (SP 800-161r1), ώστε η αρχιτεκτονική να καλύπτει όχι μόνο «τι τρέχει», αλλά και «από πού προέρχεται» και «πώς ελέγχεται» αυτό που τρέχει.

2.7 Segmentation και trust zones ως αρχιτεκτονική

Η τμηματοποίηση δικτύων (segmentation) και η δημιουργία ζωνών εμπιστοσύνης αποτελούν ένα από τα παλαιότερα αλλά και πιο αποτελεσματικά εργαλεία αρχιτεκτονικής ασφάλειας, καθώς περιορίζουν την κίνηση επιτιθέμενων και μειώνουν την έκταση των περιστατικών. Στο επίπεδο του IT, η τμηματοποίηση μπορεί να υλοποιηθεί με συνδυασμό VLANs, ACLs, firewalls και λογικών trust zones, οι οποίες διαχωρίζουν κρίσιμες υπηρεσίες, διαχειριστικά συστήματα και ευαίσθητα δεδομένα από το υπόλοιπο εταιρικό δίκτυο. Η ίδια λογική επεκτείνεται στα OT περιβάλλοντα μέσω της έννοιας των ζωνών και αγωγών που εισάγει η IEC 62443, όπου οι ζώνες ομαδοποιούν assets με παρόμοιο επίπεδο εμπιστοσύνης και οι αγωγοί ορίζουν ελεγχόμενες οδούς επικοινωνίας μεταξύ τους (ANSI/ISA-62443-3-2-2020).

Στην υβριδική αρχιτεκτονική (on-prem + cloud + SaaS), η τμηματοποίηση (segmentation) δεν αποτελεί απλώς τεχνική βελτιστοποίησης δικτύου αλλά θεμελιώδη μηχανισμό μείωσης κινδύνου, επειδή περιορίζει τις δυνατές διαδρομές κίνησης (paths) ανάμεσα σε πόρους διαφορετικού επιπέδου κρισιμότητας και διαφορετικού security posture. Η έννοια αυτή ευθυγραμμίζεται με την παραδοχή ότι τα συστήματα που βρίσκονται στο εσωτερικό δίκτυο θα πρέπει να αντιμετωπίζονται αξιόπιστα και ασφαλή, αλλά ως σύνολο πόρων που απαιτούν ρητή πολιτική πρόσβασης και ελέγχου.

Η έννοια των trust zones στην πράξη αντιστοιχεί σε ρητά ορισμένα σύνορα (boundaries) όπου εφαρμόζονται διαφορετικοί κανόνες πρόσβασης, διαφορετικές απαιτήσεις αυθεντικοποίησης και διαφορετικές απαιτήσεις παρακολούθησης, ώστε να ελαχιστοποιείται το «implicit trust» μεταξύ ανομοιογενών τμημάτων του οργανισμού.

Η CISA, μέσω του Zero Trust Maturity Model, πραγματεύεται τη μετάβαση προς Zero Trust ως οργανωσιακό και τεχνικό πρόγραμμα και αντιμετωπίζει το “Network/Environment” ως πυλώνα στον οποίο η τμηματοποίηση, η απομόνωση και ο έλεγχος ροών αποτελούν ουσιώδεις επιλογές σχεδιασμού.

2.7.1 Από το “macro-segmentation” στο “microsegmentation”

Στο κλασικό enterprise δίκτυο, η τμηματοποίηση ξεκινά συχνά ως macro-segmentation (π.χ. VLANs/VRFs/υποδίκτυα και firewall boundaries) για να ελέγχει την κίνηση μεταξύ δικτύων ή των hosts με διαφορετική στάση ασφάλειας, ακριβώς όπως περιγράφεται στον οδηγό του NIST για firewalls και firewall policy.

Στην ίδια λογική τα firewall policies πρέπει να ορίζουν ρητά πώς χειρίζεται η υποδομή την εισερχόμενη και εξερχόμενη κίνηση ανά κατηγορία διευθύνσεων/υπηρεσιών. Ωστόσο, σε υβριδικά περιβάλλοντα με έντονη εσωτερική κίνηση workload-to-workload, η ασφάλεια δεν κρίνεται μόνο από τα σύνορα (client-to-server) αλλά και από τις επικοινωνίες που επιτρέπουν lateral movement μετά από ένα αρχικό compromise.

Στο NIST SP 800-207, η microsegmentation αναγνωρίζεται ως ένα από τα χαρακτηριστικά deployment μοντέλα Zero Trust, στο οποίο η επιβολή πολιτικής προσεγγίζει τον πόρο ή το workload και όχι μόνο το κεντρικό περίγραμμα.

Η CISA τοποθετεί τη microsegmentation ως πρακτική καθοδήγηση στο πλαίσιο Zero Trust και μάλιστα την πραγματεύεται ρητά σε πρόσφατο guidance, όπου η microsegmentation αντιμετωπίζεται ως τρόπος περιορισμού των επιτρεπτών επικοινωνιών με αποτέλεσμα τη μείωση της επιφάνειας lateral movement σε σύγχρονες υποδομές.

Για να σταθεί η τμηματοποίηση ως τμήμα μιας αρχιτεκτονικής ασφάλειας (και όχι ως «δικτυακή αισθητική»), πρέπει να θεμελιώνεται σε αποτύπωση assets, σε χαρτογράφηση επικοινωνιών (data flows) και στον ορισμό των επιτρεπτών επικοινωνιών που είναι αναγκαίες για επιχειρησιακή λειτουργία.

Η τεκμηρίωση αυτή ευθυγραμμίζεται με την έννοια της “information flow enforcement” ως κατηγορίας ελέγχου, δηλαδή με την ανάγκη να ρυθμίζεται «πού μπορεί να ταξιδέψει» η πληροφορία μέσα και μεταξύ συστημάτων, κάτι που το NIST SP 800-53 Rev.5 πραγματεύεται ως δομικό στοιχείο ελέγχων.

Εξίσου κρίσιμο είναι ότι το 800-53 δεν λειτουργεί ως λίστα τεχνολογιών, αλλά ως γλώσσα ελέγχων που επιτρέπει στον οργανισμό να αποδείξει ότι ο σχεδιασμός τμηματοποίησης αντιστοιχεί σε ρητές απαιτήσεις ασφάλειας και σε μετρήσιμες πρακτικές εφαρμογής.

Στην πράξη, μια ώριμη τεκμηρίωση segmentation ξεκινά από την ταξινόμηση των πόρων σε ζώνες (π.χ. User Zone, Application Zone, Data Zone, Management Zone) και συνεχίζει με “allow-lists” ροών που επιτρέπουν μόνο τις ελάχιστες αναγκαίες επικοινωνίες, ώστε να υπηρετείται η αρχή του “least functionality” και να περιορίζονται οι μη αναγκαίες διαδρομές. Η αρχή αυτή ταιριάζει οργανικά με το Zero Trust, επειδή η απουσία implicit trust μεταξύ ζωνών σημαίνει ότι κάθε ροή πρέπει να τεκμηριώνεται ως επιχειρησιακά αναγκαία και να επιβάλλεται μέσω PEPs που βρίσκονται «εγγύτερα» στους πόρους.

Στο πλαίσιο OT/IT, η μετάβαση από macro-segmentation σε πιο λεπτό επίπεδο τμηματοποίησης δεν σημαίνει απαραίτητα την υλοποίηση πλήρους microsegmentation όπως σε cloud-native περιβάλλοντα, αλλά την προσεκτική δημιουργία μικρότερων λειτουργικών “κυψελών” (cell/area zones) με σαφώς ορισμένα boundaries και κανόνες ροής. Έτσι, ένα περιστατικό σε ένα σύστημα engineering ή σε έναν σταθμό HMI δεν μπορεί να εξαπλωθεί ανεξέλεγκτα σε ολόκληρη την εγκατάσταση, ενώ ταυτόχρονα διατηρείται η απαραίτητη διαθεσιμότητα για την παραγωγή. Η αρχή αυτή αποτελεί θεμέλιο της προτεινόμενης αρχιτεκτονικής στο Κεφάλαιο 3, όπου το μοντέλο Purdue και οι ζώνες IEC 62443 χρησιμοποιούνται ως οδηγός για τη σχεδίαση ασφαλούς τοπολογίας.

ΚΕΦΑΛΑΙΟ 3 - Αρχιτεκτονική Ασφάλειας OT και IEC 62443

Το παρόν κεφάλαιο εξετάζει τις αρχιτεκτονικές ασφάλειας που εφαρμόζονται στα περιβάλλοντα OT και στα συστήματα βιομηχανικού ελέγχου, εστιάζοντας στη δομή, τη διαστρωμάτωση και τους μηχανισμούς διαχωρισμού που απαιτούνται για την προστασία κρίσιμων διεργασιών. Η ανάλυση βασίζεται σε διεθνώς αναγνωρισμένα πλαίσια, όπως το NIST SP 800-82r3, το οποίο παρέχει κατευθύνσεις για την ασφάλεια OT, και η σειρά IEC 62443, η οποία εισάγει έννοιες όπως ζώνες, αγωγοί και επίπεδα ασφάλειας. Στόχος είναι να παρουσιαστεί πώς μοντέλα όπως το Purdue και οι επεκτάσεις του, σε συνδυασμό με πρακτικές τμηματοποίησης και defense-in-depth, μπορούν να μεταφραστούν σε εφαρμόσιμες αρχιτεκτονικές για πραγματικά βιομηχανικά περιβάλλοντα.

Το NIST ορίζει το OT ως σύνολο προγραμματιζόμενων συστημάτων/συσκευών που αλληλεπιδρούν με το φυσικό περιβάλλον (ή διαχειρίζονται συσκευές που αλληλεπιδρούν με αυτό), άρα η επιπτώσεις από μια κυβερνοεπίθεση μπορεί να μεταφραστεί σε φυσικές συνέπειες μέσω μεταβολής διεργασιών. Στον ίδιο οδηγό τονίζεται ότι οι OT τεχνολογίες εντάσσονται συχνά σε κρίσιμες υποδομές και χαρακτηριστικά όπως επίδοση, αξιοπιστία και φυσική ασφάλεια είναι προτεραιότητες και διαφοροποιούν τη διαχείριση ασφάλειας από τις κλασικές πρακτικές IT.

Αυτή η διαφοροποίηση δεν είναι απλώς “τεχνική λεπτομέρεια”, αλλά συνιστά μετατόπιση του κέντρου βάρους από την εμπιστευτικότητα προς τη διαθεσιμότητα, την ακεραιότητα των διεργασιών και τη διασφάλιση λειτουργίας, όπως αποτυπώνεται στον τρόπο που το NIST προσεγγίζει τις OT ιδιαιτερότητες.

Η βιομηχανική πραγματικότητα δείχνει ότι τα “industrial networks” δεν είναι μία ενιαία κατηγορία αλλά περιλαμβάνουν instrumentation, control και automation δίκτυα σε διαφορετικούς τομείς (χημική διεργασία, utilities, discrete manufacturing), ενώ η ISA χρησιμοποιεί τον όρο IACS (Industrial Automation and Control Systems) για να οριοθετήσει αυτό το πεδίο. Παράλληλα επισημαίνεται ότι το IACS περιλαμβάνει συστήματα ελέγχου σε εργοστάσια και εγκαταστάσεις, αλλά και κλάδους με γεωγραφικά διασπαρμένες λειτουργίες όπως υποσταθμούς και δίκτυα σωλήνων για μεταφορά υλικών, στοιχείο που προετοιμάζει το έδαφος για την αρχιτεκτονική συζήτηση περί ζωνών, ορίων και ελεγχόμενης διασύνδεσης.

3.1 Η ιδιαιτερότητα του OT ως πεδίο ασφάλειας

Η ασφάλεια στα OT περιβάλλοντα διαφοροποιείται ουσιαστικά από την κλασική κυβερνοασφάλεια IT, διότι οι συνέπειες ενός περιστατικού δεν περιορίζονται σε απώλεια δεδομένων, αλλά μπορεί να επηρεάσουν άμεσα φυσικές διεργασίες, εξοπλισμό και ανθρώπινες ζωές. Το NIST SP 800-82r3 επισημαίνει ότι η λογική που εκτελείται σε OT συστήματα έχει άμεσο αντίκτυπο στον φυσικό κόσμο, με αποτέλεσμα τα αντικείμενα της ασφάλειας να περιλαμβάνουν safety, αξιοπιστία και διαθεσιμότητα κρίσιμων λειτουργιών, πέρα από την κλασική τριάδα CIA. Αντίστοιχα, ο Brooks και ο Craig υπογραμμίζουν ότι η “ανεκτικότητα σε downtime” σε OT περιβάλλοντα είναι εξαιρετικά χαμηλή και ότι η εισαγωγή μέτρων ασφάλειας πρέπει να γίνεται με τρόπο που να μην διαταράσσει τον έλεγχο σε πραγματικό χρόνο.

Η ασφάλεια σε περιβάλλοντα Operational Technology (OT) δεν αφορά πρωτίστως την προστασία της πληροφορίας ως αφηρημένου αντικειμένου, αλλά τη διασφάλιση της συνεχούς και ορθής της λειτουργίας ενός φυσικού συστήματος, στο οποίο η πληροφορία λειτουργεί ως εντολή, μέτρηση και ανάδραση.

Σε αυτό το πλαίσιο, το λεξιλόγιο της κυβερνοασφάλειας (π.χ. «διαθεσιμότητα», «ακεραιότητα») μετατοπίζεται σημασιολογικά: η διαθεσιμότητα στο OT μεταφράζεται σε αδιάλειπτη παραγωγή/παροχή υπηρεσίας, ενώ η ακεραιότητα σημαίνει «ορθή εντολή προς διεργασία» και «ορθή απεικόνιση κατάστασης» προς τους χειριστές.

Ο NIST υπογραμμίζει ότι η ασφάλεια OT οφείλει να λαμβάνει υπόψη μοναδικές απαιτήσεις απόδοσης, αξιοπιστίας και ασφάλειας (safety), οι οποίες διαφοροποιούν ουσιωδώς το πεδίο από τα τυπικά IT περιβάλλοντα. Η σύνδεση OT με IT λειτουργίες (monitoring, record keeping, maintenance, planning) δεν είναι πλέον «ευκολία», αλλά συχνά επιχειρησιακή απαίτηση, με συνέπεια την αύξηση του κινδύνου από πρόσθετους διαύλους επίθεσης μέσω του IT και των συνδέσεών του στο Διαδίκτυο.

Η κεντρική ένταση που διατρέχει τη βιβλιογραφία του OT είναι η σχέση Safety vs Security: μέτρα ασφάλειας πληροφοριών (π.χ. επιθετικό scanning, συχνές αλλαγές συστημάτων) μπορεί να δημιουργήσουν επιχειρησιακό κίνδυνο ή downtime, άρα να πλήξουν στόχους safety/availability.

Γι' αυτό, η κλασική «IT-λογική» της άμεσης διόρθωσης μέσω patching απαιτεί προσαρμογή στο OT, όπου έχουν καταγραφεί περιπτώσεις αστοχιών patches και λειτουργικών προβλημάτων.

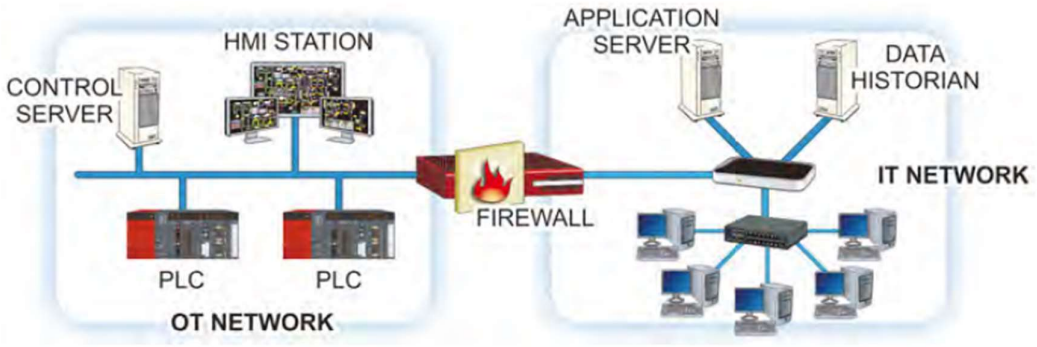
Το IEC TR 62443-2-3 επισημαίνει επίσης ότι ακόμη και «ελεγμένα» patches μπορεί να προκαλέσουν λειτουργικά ζητήματα λόγω διαφορών μεταξύ εγκαταστάσεων και ότι η δημιουργία πλήρως ισοδύναμου test environment μπορεί να είναι πρακτικά απαγορευτική.

Το NIST SP 800-82r3 συνοψίζει τα βασικά αυτά χαρακτηριστικά σε μια σειρά στόχων, όπως ο περιορισμός της λογικής πρόσβασης στα OT δίκτυα, η προστασία των επιμέρους συστατικών από εκμετάλλευση, η διατήρηση λειτουργικότητας σε αντίξοες συνθήκες και η δυνατότητα γρήγορης αποκατάστασης μετά από περιστατικό. Για να επιτευχθούν οι στόχοι αυτοί, προτείνονται αρχές όπως η πολυστρωματική τοπολογία με πολλαπλά επίπεδα, η αυστηρή διαχωριστική γραμμή μεταξύ corporate και OT δικτύων και η ενσωμάτωση της κυβερνοασφάλειας σε ευρύτερα προγράμματα safety και αξιοπιστίας. Αυτά τα θεμέλια καθοδηγούν τις αρχιτεκτονικές αποφάσεις που αναλύονται στις επόμενες υποενότητες, από το μοντέλο Purdue έως τις ζώνες και τους αγωγούς της IEC 62443.

3.2 Τα «επίπεδα» του OT/IT.

Η έννοια της "επιπεδοποίησης" στα βιομηχανικά δίκτυα στοχεύει στη διακριτή οργάνωση των λειτουργιών ελέγχου, εποπτείας και επιχειρησιακής διαχείρισης σε επίπεδα με διαφορετικές απαιτήσεις ασφάλειας και διαθεσιμότητας. Το κλασικό μοντέλο Purdue, όπως παρουσιάζεται τόσο στο NIST SP 800-82r3 όσο και στο βιβλίο Practical Industrial Cybersecurity, απεικονίζει αυτή τη διαστρωμάτωση σε επίπεδα 0 έως 4, διαχωρίζοντας τις φυσικές διεργασίες και τον άμεσο έλεγχο από τις επιχειρησιακές εφαρμογές και τα εταιρικά πληροφοριακά συστήματα. Η προσέγγιση αυτή επιτρέπει τον ορισμό σαφών ορίων και interfaces μεταξύ OT και IT, τα οποία αποτελούν κρίσιμα σημεία εφαρμογής ελέγχων ασφάλειας.

Η κλασική σύλληψη της ασφαλούς βιομηχανικής αρχιτεκτονικής στηρίζεται στη λογική των επιπέδων και των ορίων, η καλύτερη σχεδίαση για ένα εργοστάσιο είναι να διατηρούνται OT και IT διακριτά λογικά και φυσικά και να αποφεύγεται διαδρομή από το Internet προς OT (εικόνα 3).



Εικόνα 3. Φυσικός διαχωρισμός μεταξύ OT και IT δικτύων.

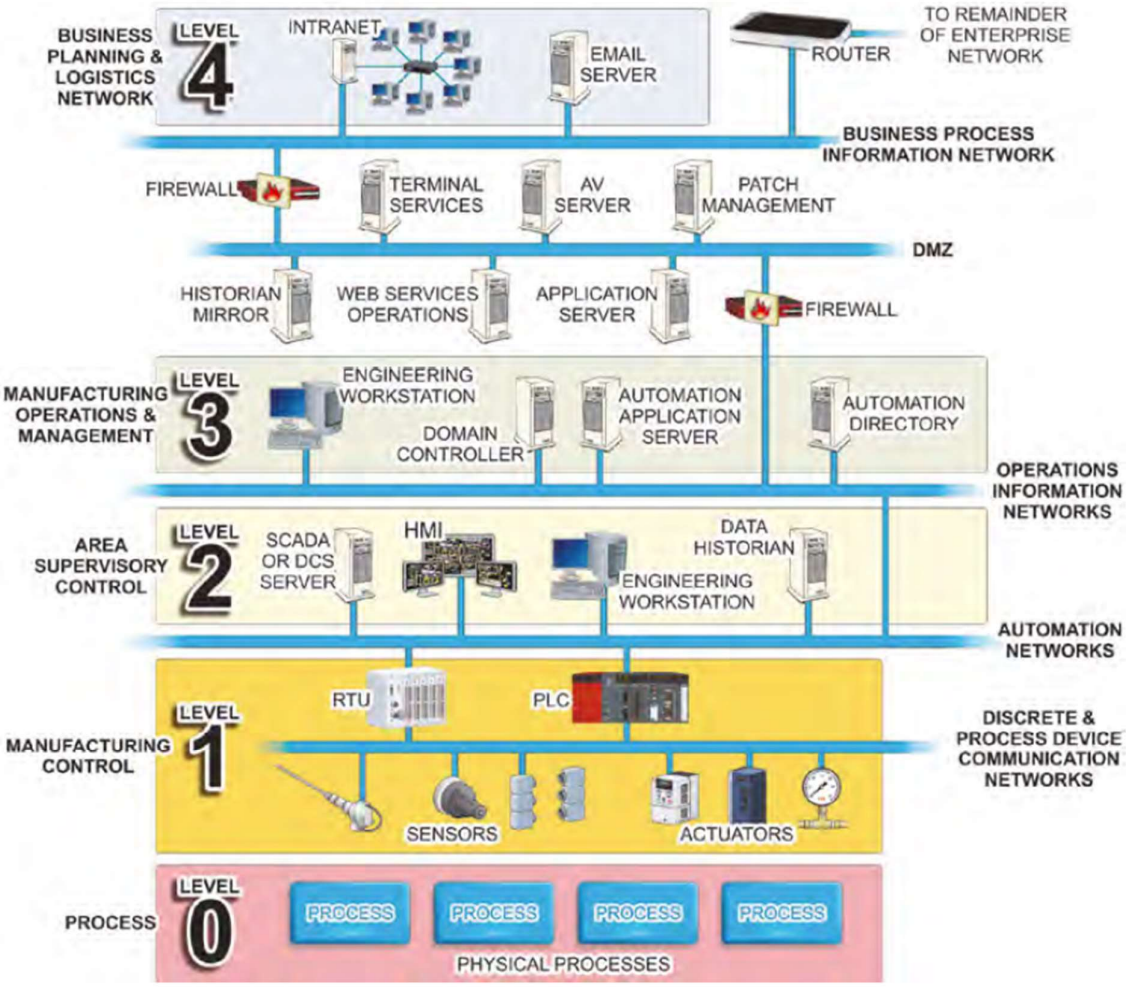
Επειδή η τάση σύνδεσης των δικτύων OT και IT έχει αυξηθεί σε σημαντικό βαθμό, η Διεθνής Εταιρεία Αυτοματισμού (ISA) έχει αναπτύξει ένα σύνολο προτύπων γνωστών ως ISA-95 για τον καθορισμό της αυτοματοποιημένης ανταλλαγής πληροφοριών μεταξύ δικτύων επιχειρήσεων και βιομηχανικών συστημάτων ελέγχου.

Η αρχική έκδοση αυτού του προτύπου αναφερόταν ως Perdue Enterprise Reference Architecture for ICS cybersecurity και χρησιμοποιείται για την ομαδοποίηση τμημάτων δικτύων IT/OT σε ζώνες ασφαλείας. Αυτό το σύνολο προτύπων καθιερώνει μια διαδικασία ενσωμάτωσης πέντε επιπέδων:

Επίπεδο 0: Φυσική προστασία (Physical Protection)
Επίπεδο 1: Ανίχνευση και χειρισμός της διαδικασίας παραγωγής (Production Process Sensing and Manipulation)
Επίπεδο 2: Αυτοματοποιημένος έλεγχος της διαδικασίας παραγωγής (Automated Control of the Production Process)
Επίπεδο 3: Έλεγχος ροής εργασίας (Workflow Control)
Επίπεδο 4: Βασικός προγραμματισμός εργοστασίου (Basic Plant Scheduling)

Τα επίπεδα 0, 1 και 2 ισχύουν για τις λειτουργίες ICS του οργανισμού που παρέχονται από τα συστήματα SCADA ή DCS, ενώ το επίπεδο 4 αντιστοιχεί στις επιχειρηματικές λειτουργίες του οργανισμού που παρακολουθούν τη λειτουργία του δικτύου της επιχείρησης. Οι λειτουργίες του επιπέδου 3 παρέχουν τη διεπαφή ανταλλαγής πληροφοριών μεταξύ των δικτύων OT και IT.

Ωστόσο, όταν η διασύνδεση καθίσταται αναγκαία, προτείνεται η ελαχιστοποίηση των διασυνδέσεων σε ένα «single point of contact» που λειτουργεί ως ελεγχόμενος διάδρομος επικοινωνίας μεταξύ εταιρικού IT και OT.



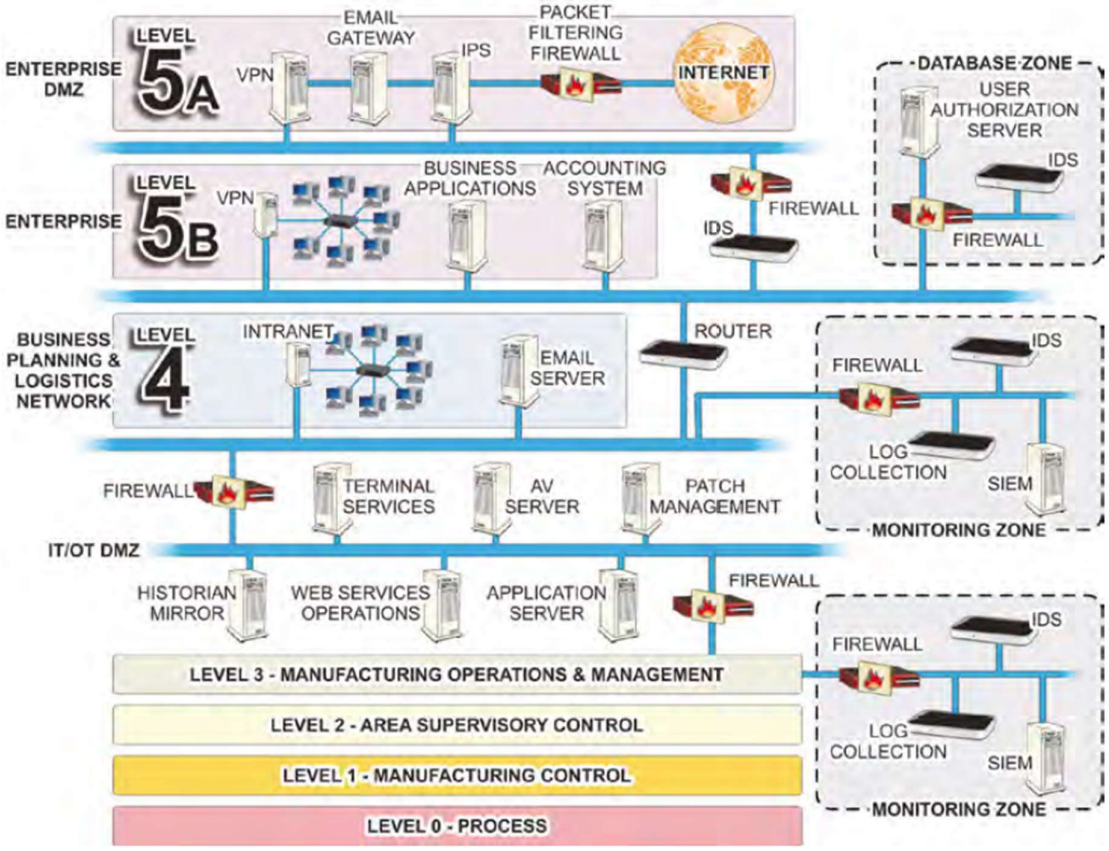
Εικόνα 4. Purdue Model levels

Στη σύγχρονη πρακτική, το «Purdue ως ιεραρχία» συχνά επεκτείνεται για να περιλάβει cloud/WAN και IIoT, χωρίς να εγκαταλείπεται η βασική αρχή της τμηματοποίησης και της αμυντικής διαβάθμισης (defense-in-depth).

Το υπουργείο ενέργειας των Η.Π.Α. κάνει αναφορά στο infrastructure topic, Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation, για το επίπεδο 3.5. Το επίπεδο αυτό δεν είχε αρχικά

σχεδιαστεί στο πλαίσιο του μοντέλου Purdue, ωστόσο, με τη συνεχή σύγκλιση των τομέων OT και IT, αυτό το επίπεδο είναι απαραίτητο για τη διασφάλιση του διαχωρισμού των επικοινωνιών. Πρόκειται για ένα μέτριο αλλά κρίσιμο επίπεδο καθώς συμπεριλαμβάνει τις προσβάσεις που δίνονται σε εξωτερικούς συνεργάτες και προμηθευτές για υποστήριξη των OT συσκευών.

Οι C. Brooks & P. Craig αναφέρουν ότι δεν υπάρχει ακόμη καθολικά αποδεκτό πρότυπο ISA-95/IIoT integration, αλλά αναπτύσσονται υβριδικές λύσεις που ενσωματώνουν IIoT διατηρώντας segmentation και ελεγχόμενη ροή δεδομένων. Ιδιαίτερο ενδιαφέρον έχει η «επιχειρησιακή» εκδοχή του Purdue, όπως το SANS ICS410 που περιγράφεται από τους C. Brooks & P. Craig, όπου τα επίπεδα 0–2 διαχωρίζονται σε σιλό (cells/lines/processes), ενσωματώνονται safety systems, και οι λειτουργίες Level 3 (engineering stations, remote access, staging) τμηματοποιούνται περαιτέρω.



Εικόνα 5. Εκτεταμένο Purdue model με 5ο επίπεδο συμπερίληψης του enterprise δικτύου.

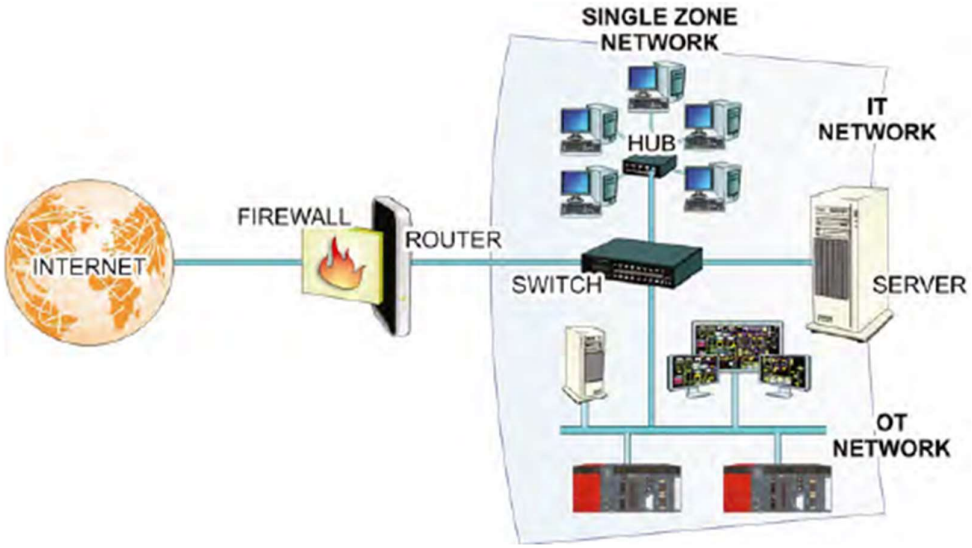
Στο ίδιο πλαίσιο, οι DMZs τοποθετούνται στρατηγικά ώστε να επιτυγχάνεται «A-to-B push» και «B-to-C pull» χωρίς άμεσο A-to-C, ως μηχανισμός μείωσης κινδύνου πλευρικής κίνησης.

3.3 Ζώνες και «αγωγοί» (Zones & Conduits)

Η IEC 62443 μετατρέπει την έννοια της επιπεδοποίησης σε πιο λεπτομερή αρχιτεκτονική, εισάγοντας τις έννοιες των ζωνών (zones) και αγωγών (conduits) ως βασικά δομικά στοιχεία. Μια ζώνη ομαδοποιεί assets με παρόμοια απαιτούμενα επίπεδα ασφάλειας και κοινό επίπεδο εμπιστοσύνης, ενώ ένας αγωγός αποτελεί τον ελεγχόμενο δρόμο επικοινωνίας μεταξύ δύο ή περισσότερων ζωνών, στον οποίο εφαρμόζονται συγκεκριμένοι έλεγχοι πρόσβασης και προστασίας ροής. Με αυτόν τον τρόπο, η αρχιτεκτονική δεν περιορίζεται στη φυσική τοπολογία, αλλά αποκτά λογική δομή που μπορεί να τεκμηριωθεί, να αξιολογηθεί και να ελεγχθεί στο πλαίσιο risk-based διαχείρισης.

Η τμηματοποίηση στο OT δεν είναι απλώς τεχνική VLAN/Firewall είναι η μορφοποίηση του συστήματος σε ζώνες διαφορετικής κρισιμότητας και διαφορετικών απαιτήσεων, ώστε να αποτραπεί η ανεξέλεγκτη διάδοση διαταραχών στα επιμέρους επίπεδα.

Οι C. Brooks & P. Craig τονίζουν ότι οι «flat topologies» χωρίς segmentation (εικόνα 6), αν και έχουν σε μεγάλο βαθμό χαμηλότερο κόστος, επιτρέπουν σε επιθέσεις ή disturbances να εξαπλώνονται γρήγορα μετά την αρχική παραβίαση, κάτι που στο OT αποκτά δυσανάλογη σοβαρότητα λόγω φυσικού αντικτύπου.



Εικόνα 6. Flat network configuration

Όταν συμβαίνουν καθυστερήσεις σε ένα περιβάλλον IT (όπως η εμφάνιση της κλεψύδρας των Windows στην οθόνη), η παραγωγικότητα των χρηστών μειώνεται. Ωστόσο, εάν παρόμοιες καθυστερήσεις συμβούν σε ένα περιβάλλον OT, συμβαίνουν άσχημα πράγματα:

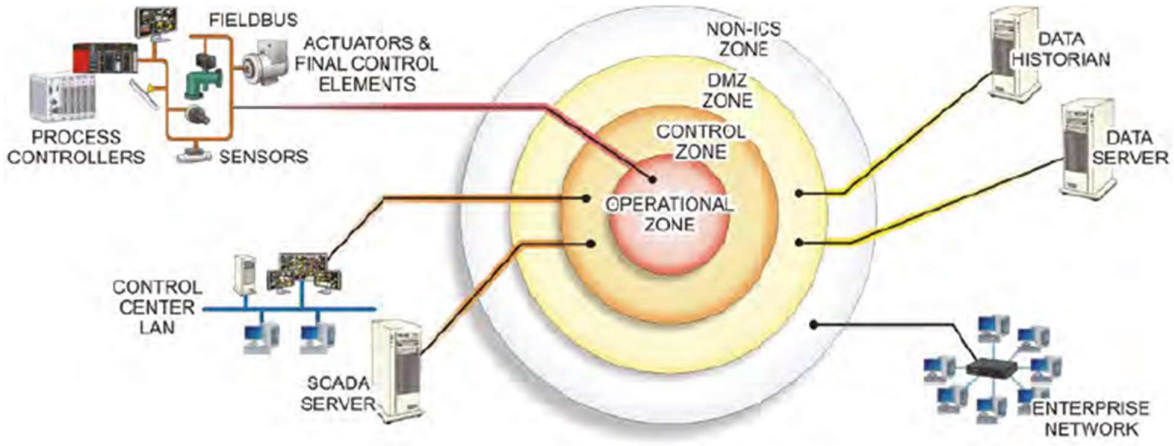
- Η παραγωγή διακόπτεται.
- Τα προϊόντα δεν πληρούν τα πρότυπα ποιότητας και πρέπει να απορριφθούν.
- Ο εξοπλισμός παραγωγής υφίσταται ζημιά ή καταστρέφεται.
- Το προσωπικό τραυματίζεται ή σκοτώνεται.

Τα εταιρικά δίκτυα πληροφορικής συνήθως ενέχουν σημαντικά μεγαλύτερο κίνδυνο για την ασφάλεια σε σύγκριση με τα αντίστοιχα δίκτυα OT.

Τα δίκτυα OT τείνουν να λειτουργούν σε συσκευές, λειτουργικά συστήματα, εφαρμογές και δίκτυα που είναι λιγότερο γνωστά από αυτά που χρησιμοποιούνται στα δίκτυα πληροφορικής. Επιπλέον, τα δίκτυα OT ιστορικά δεν έχουν συνδεθεί με κανέναν τρόπο στο δημόσιο Διαδίκτυο.

Η ISA (Global Cybersecurity Alliance) περιγράφει πρακτικούς κανόνες σχεδίασης, όπως ότι μια ζώνη μπορεί να έχει περισσότερους από έναν conduits, ενώ ένας conduit δεν πρέπει να διατρέχει πάνω από μία ζώνη, ώστε να αποφεύγονται «αδιαφανείς» διαδρομές επικοινωνίας.

Αυτός ο σχεδιασμός των ζωνών (εικόνα 7)επιτρέπει να εφαρμοστεί στην πράξη η αρχή της ελάχιστης αναγκαίας επικοινωνίας, αντί δηλαδή να ορίζεται τι απαγορεύεται (deny-lists), ορίζεται τι επιτρέπεται (allow-lists) ανά ζώνη και ανά ροή.



Εικόνα 7. ICS Security zones.

Οι C. Brooks & P. Craig περιγράφουν ρητά ότι μια allowlist στρατηγική ενσωματώνει «least privilege» και «need-to-know» ως κριτήριο πρόσβασης σε τμήματα του δικτύου (Practical Industrial Cybersecurity, Charles J. Brooks, Philip A. Craig Jr.,2022).

Οι Brooks και Craig συνδέουν άμεσα τη σχεδίαση ζωνών και αγωγών με στρατηγική defense-in-depth, προτείνοντας τα firewalls και τα OT-specific gateways να υλοποιούν αυστηρές πολιτικές allow-listing για κάθε conduit. Σε μια τέτοια προσέγγιση, η ροή δεδομένων επιτρέπεται μόνο μεταξύ συγκεκριμένων source/destination ζωνών, θυρών και πρωτοκόλλων, ενώ οποιαδήποτε μη αναγνωρισμένη ή μη τεκμηριωμένη ροή αποκλείεται εξ ορισμού, μειώνοντας σημαντικά τις δυνατότητες lateral movement. Η εφαρμογή αυτής της λογικής σε όλη την αρχιτεκτονική δημιουργεί μια αλληλουχία σημείων επιβολής πολιτικής, τα οποία μπορούν να ελέγχονται και να τεκμηριώνονται ως evidence της ασφάλειας της αρχιτεκτονικής.

3.4 Foundational Requirements και Security Levels

Η οικογένεια IEC 62443 οργανώνει τις τεχνικές απαιτήσεις σε επτά «Foundational Requirements» (FRs), οι οποίες λειτουργούν ως ελάχιστοι άξονες ασφαλείας για συστήματα βιομηχανικού αυτοματισμού.

Τα FRs περιλαμβάνουν Identification & Authentication Control, Use Control, System Integrity, Data Confidentiality, Restricted Data Flow, Timely Response to Events και Resource Availability.

Σκοπός αυτής της τυποποίησης είναι να μπορεί ένας οργανισμός να «χαρτογραφήσει» τεχνικούς ελέγχους (π.χ. αυθεντικοποίηση, επιβολή ροών, monitoring) σε συγκεκριμένες απαιτήσεις συμμόρφωσης, μειώνοντας την «απόσταση» μεταξύ σχεδίασης και ελέγχου.

Παράλληλα, η IEC 62443 εισάγει κλίμακα Security Levels (SL 1–4) που κλιμακώνει το επίπεδο προστασίας από τυχαία κακή χρήση έως εξελιγμένους επιθέσεις με πρόσβαση σε πόρους.

Η κλιμάκωση αυτή επιτρέπει η ίδια αρχιτεκτονική «ζωνών» να αποκτά διαβαθμίσεις προστασίας ανάλογες με την κρισιμότητα της διεργασίας και την απειλητική υπόθεση (threat model).

Ο συνδυασμός των Foundational Requirements με τα επίπεδα ασφάλειας επιτρέπει την αντιστοίχιση συγκεκριμένων τεχνικών ελέγχων σε στοχευμένα επίπεδα προστασίας για κάθε ζώνη ή αγωγό. Το NIST SP 800-82r3 αξιοποιεί αυτή την τυποποίηση, παρέχοντας OT-specific overlay πάνω στο NIST SP 800-53r5, ώστε οι έλεγχοι πρόσβασης, προστασίας ροής, καταγραφής και ανίχνευσης ανωμαλιών να μπορούν να συνδεθούν με συγκεκριμένους FR και SL. Για τον σχεδιαστή αρχιτεκτονικής, αυτή η χαρτογράφηση λειτουργεί ως γέφυρα ανάμεσα σε “λογικές” απαιτήσεις ασφαλείας και συγκεκριμένες υλοποιήσεις ελέγχων σε IT και OT επίπεδο.

3.5 Πρακτική υλοποίηση αρχιτεκτονικών OT ασφάλειας

Στην πράξη, η ασφαλής OT αρχιτεκτονική επιδιώκει να δημιουργήσει σαφή όρια (boundaries) που επιτρέπουν την απαραίτητη κίνηση των δεδομένων, χωρίς να επιτρέπουν τη «διάχυση» των κινδύνων του IT προς το OT.

Στο σημείο αυτό η έννοια του boundary protection αποκτά ειδικό βάρος, επειδή η OT/IT διαλειτουργικότητα αυξάνει παράλληλα και τις κυβερνοαπειλές.

Μια ώριμη στρατηγική υλοποίησης ξεκινά από τη χαρτογράφηση των ροών και των εξαρτήσεων «as-operated», καθώς ο πραγματικός κίνδυνος στο OT συχνά αναδύεται από κρυφές διασυνδέσεις και operational dependencies που δεν αποτυπώνονται σε ιδεατά διαγράμματα.

Η CISA συστήνει ρητά τη δημιουργία ακριβούς «as-operated OT network map» και την αναγνώριση OT/IT inter-dependencies ως προϋπόθεση ανθεκτικότητας.

Σε τεχνικό επίπεδο, η τμηματοποίηση μπορεί να επιτευχθεί με φυσικά firewalls/routers, ACLs και VLANs, ενώ τεχνικές όπως VPNs και data diodes (βλ. Παράρτημα A.2.1) μπορούν να συμβάλουν στη διαβάθμιση επικοινωνίας σε πολλαπλά επίπεδα OSI.

Οι C. Brooks & P. Craig επισημαίνουν ότι η παραδοσιακή υλοποίηση segmentation μέσω firewall/ACL είναι αποδεδειγμένη, αλλά μπορεί να γίνει χρονοβόρα και επιρρεπής σε ανθρώπινο σφάλμα, επειδή απαιτεί λεπτομερή γνώση θυρών/πρωτοκόλλων και σύνταξης ρυθμίσεων.

Η ίδια πηγή συνδέει άμεσα το segmentation με τον περιορισμό του βάθους διείσδυσης (depth) και της διάδοσης (propagation) μιας επίθεσης, κάτι που αποτελεί «πρώτη αρχή» για OT.

3.6 Remote access σε βιομηχανικό περιβάλλον

Η πίεση για απομακρυσμένη διαχείριση και συντήρηση συχνά οδηγεί σε άνοιγμα remote access προς OT, κυρίως για λόγους κόστους και διαθεσιμότητας ειδικευμένου προσωπικού.

Ωστόσο, η απομακρυσμένη πρόσβαση αποτελεί «παράθυρο» εισόδου για μη εξουσιοδοτημένη πρόσβαση, malware ή άλλου είδους επίθεσης και το πρόβλημα στο OT εντείνεται επειδή το OT διαθέτει συχνά λιγότερα αμυντικά εργαλεία από το enterprise IT.

Για τον λόγο αυτό, οι C. Brooks & P. Craig συνιστούν κρυπτογραφημένα πρωτόκολλα, ισχυρή αυθεντικοποίηση (token/MFA) και VPNs για κάθε μορφή απομακρυσμένης πρόσβασης που σχετίζεται με ICS, καθώς και διπλή αυθεντικοποίηση σε enterprise επίπεδο καθώς και έλεγχος επικοινωνιών μέσα από firewall προς το OT.

Η CISA, στο πλαίσιο ransomware απειλών, ενσωματώνει την απομακρυσμένη πρόσβαση στη γενικότερη «υγιεινή» με MFA ως ουσιώδες μέτρο τόσο για OT όσο και για IT δίκτυα.

Σε επίπεδο σχεδίασης, αυτό πρακτικά συνεπάγεται ότι οι απομακρυσμένες συνδέσεις δεν «τερματίζουν» βαθιά στο OT, αλλά διέρχονται από ελεγχόμενες ζώνες (π.χ. remote access zone/DMZ) όπου εφαρμόζονται policy enforcement, καταγραφή, και αυστηρός έλεγχος επικοινωνιών.

3.7 Διαχείριση ευπαθειών και patching στο OT

Η διαχείριση ευπαθειών στο OT είναι δύσκολη όχι επειδή «δεν χρειάζεται», αλλά επειδή η ίδια η δομή του OT (legacy, real-time constraints, vendor dependencies) καθιστά το patching μια πράξη υψηλού επιχειρησιακού ρίσκου.

Οι C. Brooks & P. Craig αναφέρουν ότι patching είναι συνήθης, συνεχής δραστηριότητα στο enterprise IT, αλλά «δεν ισχύει το ίδιο» στο ICS/OT, ενώ επισημαίνουν τον υψηλό αριθμό ευπαθειών και πιθανότητα προβληματικών patches σε OT λειτουργικά.

Το IEC TR 62443-2-3 εξειδικεύει την πραγματικότητα αυτή με τεχνικούς όρους, προτείνει εναλλακτικές όταν δεν είναι εφικτό πλήρες offline testing, όπως reliance σε vendor testing και προσεκτικά ελεγχόμενο rollout σε παραγωγικό περιβάλλον με σχέδιο που ελαχιστοποιεί common mode failures.

Στην ίδια λογική, το πρότυπο επιμένει ότι η εγκατάλειψη patching «πρέπει να αποφεύγεται» και ότι η ηγεσία μπορεί να επιλέξει ρητά την αποδοχή πρόσθετου ρίσκου μόνο με συνειδητή στάθμιση.

Επιπλέον, το IEC TR 62443-2-3 δίνει έμφαση στο backup/restore ως αναγκαίο συμπλήρωμα του patching, διότι έχουν υπάρξει περιπτώσεις όπου patches προκάλεσαν διαταραχή λειτουργίας, άρα η δυνατότητα επαναφοράς σε «known good state» είναι οργανικό τμήμα του patch lifecycle.

Σημαντικό στοιχείο εδώ είναι και η χρήση «sandbox/digital twin» για δοκιμές, καθώς στο OT το επιθετικό scanning και το testing μπορεί να οδηγήσουν σε downtime γι' αυτό στην βιβλιογραφία αναφέρονται ότι τέτοιες δοκιμές τείνουν να γίνονται σε digital-twin ή sandbox περιβάλλον πριν μεταφερθούν στο operational.

3.8 Ανθεκτικότητα σε επιθέσεις

Η CISA περιγράφει ως κρίσιμη την αναγνώριση «critical processes» που πρέπει να συνεχίσουν αδιάλειπτα και προτείνει τη δημιουργία και τακτική δοκιμή workarounds ή manual controls, ώστε οι ICS/OT λειτουργίες να μπορούν να απομονωθούν και να συνεχίσουν χωρίς πρόσβαση στο IT δίκτυο, αν απαιτηθεί.

Στο ίδιο κείμενο, η CISA προτείνει ρητά robust network segmentation μεταξύ IT και OT και απομονωμένα backups, ως μέτρα που μειώνουν την πιθανότητα «severe business degradation» σε περίπτωση ransomware επίθεσης. Η CISA τονίζει επίσης ότι η πλειονότητα ransomware επιθέσεων εκμεταλλεύεται γνωστές ευπάθειες και κοινές αδυναμίες, προτείνοντας πρακτικές όπως timely updates (όπου είναι αυτό εφικτό), application allowlisting, περιορισμό λογαριασμών και MFA. Σε επίπεδο απόκρισης, η CISA προτείνει ως πρώτες ενέργειες την άμεση απομόνωση επηρεασμένων συστημάτων και, μόνο αν δεν είναι δυνατός ο αποσυνδετικός χειρισμός, το power-down για περιορισμό εξάπλωσης.

Αυτή η προσέγγιση συνδέεται οργανικά με το IEC TR 62443-2-3, όπου η επαναφορά από backup παρουσιάζεται ως δομημένη διαδικασία χωρίς «fixed rules», αλλά με αρχή αναλογικότητας προς την κρισιμότητα και τους αποδεκτούς χρόνους αποκατάστασης.

Χαρακτηριστικές επιθέσεις, όπως οι εκστρατείες του Sandworm Group εναντίον ενεργειακών δικτύων στην Ουκρανία, αναδεικνύουν πώς η ανεπαρκής τμηματοποίηση και η έλλειψη σαφών ζωνών επιτρέπουν σε έναν επιτιθέμενο να μετακινηθεί από IT σε OT συστήματα και να διαταράξει φυσικές διεργασίες. Η σχετική βιβλιογραφία περιγράφει τη χρήση κακόβουλου λογισμικού για να αποκτηθεί έλεγχος σε SCADA/OT περιβάλλοντα, με αποτέλεσμα εκτεταμένες διακοπές παροχής ενέργειας, γεγονός που ενισχύει την ανάγκη για πολυστρωματική άμυνα και σαφείς DMZ μεταξύ επιχειρησιακού και βιομηχανικού δικτύου.

3.9 Ασφάλεια βιομηχανικών πρωτοκόλλων

Το Modbus, ως ιστορικά διαδεδομένο βιομηχανικό πρωτόκολλο, αποτυπώνει την ένταση μεταξύ απλότητας/διαλειτουργικότητας και σύγχρονων απαιτήσεων ασφάλειας.

Η τεκμηρίωση του Modbus TCP/IP επισημαίνει ότι ο server «περιμένει Modbus request» στο TCP port 502, στοιχείο που στην πράξη διευκολύνει την αναγνώριση υπηρεσιών αλλά και τη στόχευση όταν εκτίθεται ακατάλληλα. Ακριβώς επειδή τα κλασικά προφίλ Modbus δεν σχεδιάστηκαν με ενσωματωμένη κρυπτογράφηση/ αυθεντικοποίηση, η κοινότητα έχει προχωρήσει σε προδιαγραφές ασφάλειας για Modbus/TCP που αξιοποιούν TLS και ορίζουν νέο port (802) για «secure Modbus» μεταφορά. Ενδεικτικά, η Modbus κοινότητα συγκεντρώνει τις επίσημες προδιαγραφές και αναφέρεται ρητά στο Modbus Security και στη χρήση port 802 ως μέρος των σχετικών κειμένων.

Η σημασία για την OT αρχιτεκτονική δεν είναι «να κρυπτογραφήσουμε τα πάντα», αλλά να αναγνωρίσουμε ότι όπου επιτρέπονται flows Modbus μεταξύ ζωνών, οι απαιτήσεις Restricted Data Flow και Identification/ Authentication αποκτούν άμεση τεχνική έκφραση μέσω ασφαλών προφίλ (TLS) και αυστηρής πολιτικής επιτρεπτών εντολών/λειτουργιών.

ΚΕΦΑΛΑΙΟ 4 - Ενοποιημένη Διακυβέρνηση και OT/IT Operating Model

Στο παρόν κεφάλαιο εξετάζεται η διακυβέρνηση και η οργάνωση της ασφάλειας σε περιβάλλοντα όπου συνυπάρχουν OT και IT, με στόχο τη δημιουργία ενός ενοποιημένου πλαισίου πολιτικών, ρόλων και αρχιτεκτονικών αποφάσεων. Η ανάλυση αντλεί από προσεγγίσεις όπως το NIST Cybersecurity Framework (CSF) 2.0, τα πρότυπα ISO/IEC 27001–27002 και τις κατευθυντήριες οδηγίες της IEC 62443 για τη διακυβέρνηση των IACS, καθώς και από πρακτικές προσεγγίσεις που περιγράφονται στη βιβλιογραφία για ICS και Industry 4.0. Στόχος είναι να παρουσιαστεί πώς ένα ενιαίο πλαίσιο διακυβέρνησης μπορεί να συνδέσει τις απαιτήσεις ασφάλειας, τις αρχιτεκτονικές αποφάσεις και το λειτουργικό μοντέλο υλοποίησης σε έναν συνεκτικό OT/IT Security Program.

Όταν λέμε ενοποιημένη διακυβέρνηση (governance) και ενοποιημένη αρχιτεκτονική ασφάλειας (security architecture) για OT/IT, εννοούμε ότι ο οργανισμός δεν χειρίζεται την ασφάλεια ως δύο παράλληλα σύμπαντα (“IT security” από τη μία και “plant/OT security” από την άλλη), αλλά ως ένα ενιαίο σύστημα αποφάσεων, τεκμηρίωσης και τεχνικών ορίων όπου διοικητικά (governance) ορίζει ποιος αποφασίζει, με ποια κριτήρια, με ποια ανοχή κινδύνου, με ποια τεκμήρια και με ποια διαδικασία αναθεώρησης (λογική ISMS) και αρχιτεκτονικά (architecture) ορίζει πού επιτρέπεται να υπάρχουν συνδέσεις μεταξύ του IT και OT, ποιες ροές επιτρέπονται, με ποια επίπεδα προστασίας, και με ποια αποδεικτικά στοιχεία συμμόρφωσης (λογική zones & conduits και security levels).

Το κρίσιμο ζήτημα είναι ότι η ενοποίηση δεν σημαίνει “να εφαρμόσουμε τα μέτρα που εφαρμόζονται στο IT αυτούσια στο OT”, αντίθετα, σημαίνει να έχουμε κοινή μέθοδο που λαμβάνει υπόψη τις OT ιδιαιτερότητες (performance, reliability, safety) και μεταφράζει τις απαιτήσεις ασφάλειας σε λειτουργικά αποδεκτά controls.

4.1 Ενοποιημένη διακυβέρνηση κινδύνου

Η διακυβέρνηση κινδύνου σε ένα περιβάλλον OT/IT δεν μπορεί να αντιμετωπίζει τα δύο πεδία ως απομονωμένα “σιλό”, καθώς οι επιχειρησιακές διαδικασίες και οι τεχνολογικές εξαρτήσεις τα συνδέουν στενά. Το NIST SP 800-82r3 προτείνει ρητά τη θεώρηση των OT συστημάτων ως οργανικό μέρος του συνολικού προγράμματος κυβερνοασφάλειας του οργανισμού, επισημαίνοντας ότι η διαχείριση κινδύνου πρέπει να καλύπτει τόσο τις ψηφιακές όσο και τις φυσικές επιπτώσεις. Αντίστοιχα, τα πρότυπα ISO/IEC 27001 και 27002 παρέχουν ένα πλαίσιο ISMS που μπορεί να επεκταθεί ώστε να περιλαμβάνει assets, διαδικασίες και απαιτήσεις από τον χώρο του OT, αρκεί να προσαρμοστούν κατάλληλα οι ορισμοί του scope και του risk context.

Η σύγκλιση OT/IT, αν και ξεκινάει από τεχνολογικές επιλογές (διασυνδέσεις, data flows, cloud/remote access), παράγει πρωτίστως ένα πρόβλημα διακυβέρνησης κινδύνου, ποιος αποφασίζει, με ποια κριτήρια, με ποια τεκμήρια και με ποιον τρόπο αποδεικνύεται ότι οι αποφάσεις ασφάλειας είναι συνεπείς, αναθεωρήσιμες και λειτουργικά αποδεκτές. Το ISO/IEC 27001 ορίζει ακριβώς αυτήν τη λογική ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), δηλαδή ενός πλαισίου απαιτήσεων για εγκαθίδρυση, εφαρμογή, συντήρηση και συνεχή βελτίωση της ασφάλειας ως οργανωσιακής λειτουργίας. Στην ίδια κατεύθυνση, το NIST CSF 2.0 δεν επιβάλλει τεχνικές λύσεις, αλλά προσφέρει μια ταξινόμηση των αποτελεσμάτων (outcomes) για την κατανόηση, την αξιολόγηση, την ιεράρχηση και την επικοινωνία των τρόπων εφαρμογής του framework κυβερνοασφάλειας σε οποιονδήποτε οργανισμό. Η αξία του CSF στο μεικτό OT/IT περιβάλλον έγκειται ακριβώς στη γλωσσική του λειτουργία, επιτρέπει δηλαδή να συζητηθεί ο κίνδυνος με κοινό λεξιλόγιο ανάμεσα σε IT security, engineering και operations, χωρίς να προϋποτίθεται τεχνική ομοιογένεια.

Ωστόσο, στο OT η κυβερνοασφάλεια δεν μπορεί να εξαντληθεί σε “προστασία δεδομένων”, διότι τα OT συστήματα είναι άμεσα δεμένα με απαιτήσεις διαθεσιμότητας, αξιοπιστίας και safety. Το NIST SP 800-82 Rev.3 υπογραμμίζει ότι η ασφάλεια OT πρέπει να σχεδιάζεται λαμβάνοντας υπόψη αυτές τις, μοναδικές, απαιτήσεις, οι οποίες διαφοροποιούν την επιλογή και το ρυθμό εφαρμογής των μέτρων. Η ίδια διάκριση, σε πιο πρακτικό ύφος, αποτυπώνεται και στη βιβλιογραφία των C. Brooks & P. Craig, σε OT περιβάλλοντα, πολιτικές και risk mitigation δεν μπορούν να αγνοούν πιθανές συνέπειες όπως προσωπική ασφάλεια, ασφάλεια εξοπλισμού, περιβαλλοντική επίπτωση και απώλεια παραγωγής, άρα ο κίνδυνος οφείλει να μετράται με όρους διεργασίας και όχι μόνο με όρους πληροφορίας.

Μεθοδολογικά, αυτό σημαίνει ότι μια “ενοποιημένη” πολιτική ασφάλειας δεν είναι ενιαίο κείμενο γενικών απαγορεύσεων, αλλά ένα σύστημα στο οποίο τα επιχειρησιακά όρια του OT (π.χ. downtime intolerance, αλλαγές μόνο σε προγραμματισμένα maintenance windows, vendor dependencies) μεταφράζονται σε συγκεκριμένες επιλογές αλλαγών, εξαιρέσεων και αποδεκτού ρίσκου. Οι C. Brooks & P. Craig χρησιμοποιούν το CSF ως “χάρτη” ανάπτυξης πολιτικών και διαδικασιών, αλλά επισημαίνουν ρητά ότι το CSF συνήθως υποστηρίζει τις IT πολιτικές, ενώ πρότυπα όπως η IEC 62443 εφαρμόζονται εξειδικευμένα στο OT περιβάλλον.

Πρακτικά, η ενοποιημένη διακυβέρνηση για OT/IT οφείλει τεκμηρίωση αρχικά σε πολιτικές/διαδικασίες που περιγράφουν σκοπό, πεδίο, ρόλους, ευθύνες και δέσμευση διοίκησης, έπειτα σε “profiles” ή τομεακές εφαρμογές πλαισίων, ώστε διαφορετικά τμήματα (enterprise IT, plant OT, safety) να έχουν αναγνωρίσιμες υποχρεώσεις, και τέλος σε τεκμηρίωση ορίων/ροών, ώστε η αρχιτεκτονική να είναι ελέγξιμη. Ο C. Brooks & P. Craig, αναπτύσσοντας τις λειτουργίες του CSF (Identify, Protect, Detect, Respond, Recover), το συνδέουν άμεσα με το governance, το risk strategy και το supply chain risk management ως τμήματα της αναγνωριστικής λειτουργίας, δείχνοντας ότι οι αποφάσεις ασφάλειας προηγούνται της τεχνικής υλοποίησης και δεν έπονται αυτής.

Στο σημείο αυτό, αξίζει να προστεθεί ότι η διακυβέρνηση στο OT/IT δεν περιορίζεται στο εσωτερικό του οργανισμού. Το “Good Practices for Supply Chain Cybersecurity” (June 2023) εντοπίζει ως δομικό πρόβλημα την έλλειψη σταθερής εταιρικής διακυβέρνησης και τυποποιημένων πολιτικών για supplier relationships και vulnerability handling, προτείνοντας μια στρατηγική συνεχή χαρτογράφηση εξαρτήσεων ICT/OT supply chain.

Το ίδιο κείμενο συσχετίζει ρητά τη διαχείριση supply chain κινδύνου με PDCA (Plan-Do-Check-Act) κύκλο συνεχούς βελτίωσης, στοιχείο που ταιριάζει απολύτως με τη λογική ISMS και τη λειτουργική πραγματικότητα βιομηχανικών οργανισμών που οφείλουν να επανεξετάζουν τις παραδοχές τους καθώς αλλάζει συνεχώς το τεχνολογικό τοπίο αλλά και τοπίο επιθέσεων.

Η ENISA, στη μελέτη “Good Practices for Supply Chain Cybersecurity”, επισημαίνει ότι η κυβερνοασφάλεια OT/IT δεν περιορίζεται στις εσωτερικές λειτουργίες, αλλά επεκτείνεται σε ολόκληρη την αλυσίδα εφοδιασμού, από προμηθευτές εξοπλισμού μέχρι παρόχους υπηρεσιών. Προτείνεται η ενσωμάτωση των supply chain κινδύνων στις διαδικασίες διακυβέρνησης, με σαφείς πολιτικές για αξιολόγηση προμηθευτών, δικαιώματα audit, διαχείριση ευπαθειών και συμβατικές απαιτήσεις ασφάλειας, στο πλαίσιο ενός κύκλου PDCA που ευθυγραμμίζεται με το ISMS. Σε ένα ενοποιημένο OT/IT περιβάλλον, αυτό σημαίνει ότι η διοίκηση πρέπει να βλέπει vendors λογισμικού, integrators αυτοματισμού και παρόχους cloud ως μέρος του ίδιου οικοσυστήματος κινδύνου και όχι ως απομονωμένους τεχνικούς συνεργάτες.

4.2 Αρχιτεκτονική-γέφυρα OT/IT

Η αρχιτεκτονική-γέφυρα OT/IT αποσκοπεί στη δημιουργία ενός συνεκτικού “χάρτη” που περιγράφει πώς οι διαδικασίες, τα assets και οι ροές δεδομένων συνδέουν τον κόσμο του IT με τον κόσμο του OT. Σε αντίθεση με τις καθαρά τεχνικές τοπολογίες, η αρχιτεκτονική αυτή πρέπει να ενσωματώνει επιχειρησιακές απαιτήσεις, περιορισμούς safety, επιδόσεις σε πραγματικό χρόνο και ρυθμιστικές υποχρεώσεις, ώστε οι αποφάσεις για συνδέσεις και ροές να λαμβάνονται με πλήρη επίγνωση των συνεπειών. Πλαίσια όπως το NIST SP 800-82r3 και η σειρά IEC 62443 παρέχουν το θεωρητικό υπόβαθρο για να αποτυπωθεί αυτή η γέφυρα με όρους ζωνών, αγωγών και target security levels.

Η μετάβαση από τη διακυβέρνηση στην εφαρμογή απαιτεί μια κοινή αρχιτεκτονική περιγραφή του συστήματος ένα “συντακτικό” με το οποίο να περιγράφονται assets, λειτουργίες, όρια εμπιστοσύνης και επιτρεπτές ροές. Το NIST SP 800-82 Rev.3 παρέχει το θεσμικό υπόβαθρο αυτής της ανάγκης, ορίζοντας το OT ως σύνολο προγραμματιζόμενων συστημάτων που αλληλεπιδρούν με το φυσικό περιβάλλον και τονίζοντας ότι τα προτεινόμενα μέτρα πρέπει να είναι συμβατά με performance/reliability/safety περιορισμούς.

Στην OT πρακτική, η περιγραφή ξεκινά συχνά από ιεραρχικά/λειτουργικά μοντέλα (π.χ. Purdue/ISA-95) που καθιστούν ορατές τις θέσεις των λειτουργιών ελέγχου, εποπτείας και επιχειρησιακής διαχείρισης. Οι C. Brooks & P. Craig δείχνουν ότι, ακριβώς επειδή οι “flat” τοπολογίες επιτρέπουν γρήγορη διάδοση συμβάντων, η αρχιτεκτονική οφείλει να διατηρεί διακριτές ζώνες/στρώματα και να ενσωματώνει αμυντική διαβάθμιση.

Το αποφασιστικό βήμα, όμως, από την “τοπογραφία” προς την “ασφάλεια” παρέχεται από την IEC 62443. Η ISA περιγράφει τη σειρά ISA/IEC 62443 ως ολιστική προσέγγιση που γεφυρώνει operations και IT και συνδέει process safety με cybersecurity, παρέχοντας απαιτήσεις και διαδικασίες για την εγκαθίδρυση και διατήρηση ηλεκτρονικά ασφάλειας

Στο εκπαιδευτικό υλικό του Wally Magda, η μετάβαση αποτυπώνεται μέσω του ορισμού του System under Consideration (SuC) και της κατάτμησής του σε zones και conduits, με ρητή στόχευση σε target security levels ως αποτέλεσμα risk-based συλλογισμού. Το εκπαιδευτικό υλικό του Wally Magda για τη χρήση της ISA/IEC 62443 τονίζει ότι ο σαφής ορισμός του System under Consideration και η διάσπασή του σε ζώνες και αγωγούς αποτελούν όχι μόνο τεχνική άσκηση αλλά και μέσο διακυβέρνησης. Η τεκμηρίωση κάθε ζώνης με όρια, σημεία πρόσβασης, επιτρεπτές ροές, υποθέσεις και εξαρτήσεις λειτουργεί ως “σκελετός τεκμηρίωσης” (evidence spine), πάνω στον οποίο μπορούν να ελεγχθούν η συμμόρφωση, οι εξαιρέσεις και οι αλλαγές στην αρχιτεκτονική. Με αυτόν τον τρόπο, η αρχιτεκτονική-γέφυρα OT/IT συνδέεται άμεσα με το ISMS και το πρόγραμμα διαχείρισης κινδύνου, καθώς κάθε αλλαγή σε ροές ή οριακές γραμμές πρέπει να τεκμηριώνεται, να εγκρίνεται και να παρακολουθείται.

Εδώ η αρχιτεκτονική αποκτά “λογικό-νομική” ισχύ, κάθε ζώνη και κάθε αγωγός τεκμηριώνονται με όρια, σημεία πρόσβασης, ροές δεδομένων, υποθέσεις και εξαρτήσεις, ώστε η πολιτική να μετατρέπεται σε ελέγξιμη αρχιτεκτονική και όχι σε γενικόλογη πρόθεση.

Στην ίδια λογική, οι C. Brooks & P. Craig τονίζει ότι όταν η σύνδεση IT - OT είναι επιχειρησιακά αναγκαία, πρέπει να περιορίζεται σε ελάχιστα και αυστηρά ελεγχόμενα σημεία επαφής, ώστε να μειώνεται η επιφάνεια επίθεσης και να είναι διαχειρίσιμη η επιβολή πολιτικής. Συνεπώς, η αρχιτεκτονική-γέφυρα OT/IT μπορεί να αποδοθεί ως σύνθεση. Τα “επίπεδα” (ως λειτουργικός χάρτης) επιτρέπουν να οριστούν κατανοητά τα επιχειρησιακά τμήματα μετασχηματίζουν τον χάρτη σε κανόνες επιτρεπτών ροών, με στόχο την προστασία και απαιτήσεις που μπορούν να ελεγχθούν και να συντηρηθούν σε βάθος χρόνου.

4.3 Λειτουργικό μοντέλο υλοποίησης

Καμία αρχιτεκτονική OT/IT, όσο καλά σχεδιασμένη και αν είναι, δεν μπορεί να παραμείνει αποτελεσματική χωρίς ένα σαφές λειτουργικό μοντέλο που να ορίζει ρόλους, ευθύνες, διαδικασίες και τεκμήρια. Η εμπειρία σε ICS περιβάλλοντα δείχνει ότι πολλά περιστατικά ασφάλειας δεν οφείλονται σε τεχνική αδυναμία, αλλά σε ασάφεια σχετικά με το ποιος “κατέχει” τον κίνδυνο, ποιος εγκρίνει αλλαγές και ποιος είναι υπεύθυνος για την τήρηση των διαδικασιών patching, monitoring και incident response. Γι’ αυτό, πρότυπα όπως το IEC TR 62443-2-3 προτείνουν ρητά τον ορισμό ownership και RACI για βασικές δραστηριότητες ασφαλείας στο OT, όπως η διαχείριση ευπαθειών και η εφαρμογή patches. Η ενοποιημένη ασφάλεια OT/IT δεν μπορεί να επιτευχθεί μόνο με τεχνική σχεδίαση απαιτεί ένα λειτουργικό μοντέλο που ορίζει ρόλους, διαδικασίες και τεκμήρια συμμόρφωσης. Οι C. Brooks & P. Craig περιγράφουν τις πολιτικές, διαδικασίες και οδηγίες ως governance στοιχεία που παρέχουν στους εργαζόμενους επαρκή καθοδήγηση για να εκτελούν τα καθήκοντά τους εντός του οργανισμού και αναπτύσσει την ιδέα ότι η κυβερνοασφάλεια σε ICS απαιτεί σαφή standards, exemptions και exceptions, δηλαδή μηχανισμούς που επιτρέπουν ελεγχόμενη απόκλιση όταν η λειτουργία το επιβάλλει.

Ένα από τα πιο καθαρά παραδείγματα “operating model” στη βιομηχανική ασφάλεια δίνεται από το IEC TR 62443-2-3 στο πλαίσιο patch management, όχι επειδή το patching είναι το μόνο θέμα, αλλά επειδή συμπυκνώνει όλες τις οργανωσιακές ενστάσεις του OT, υποχρέωση βελτίωσης ασφάλειας, περιορισμοί δοκιμών, ανάγκη business case, και κατανομή ευθυνών ανάμεσα σε IT, OT, safety, engineering, maintenance και suppliers. Το IEC TR 62443-2-3 ορίζει ότι η επιτυχία ενός IACS patch management program απαιτεί υποστήριξη και συμμετοχή πολλών stakeholder groups, και ότι η πρώτη αναγκαία πράξη είναι ο σαφής ορισμός και η επικοινωνία ownership, accountability, ρόλων και ευθυνών. Επιπλέον, προτείνει ρητά τη χρήση πινάκων RACI/RASCI για αντιστοίχιση δραστηριοτήτων (monitoring vulnerabilities, evaluation, testing, deployment, reporting, auditing) σε ρόλους, ώστε να αποφεύγεται η “σιωπηρή” υπόθεση ότι κάποιος άλλος είναι υπεύθυνος.

Το operating model πρέπει να ορίζει ποιος “κατέχει” το risk, ποιος το αξιολογεί, ποιος εγκρίνει εξαιρέσεις, ποιος εφαρμόζει τεχνικούς ελέγχους, και ποιος συντηρεί τα evidence artifacts (network maps, zone/conduit

documentation, access reviews, incident logs). Η τεκμηρίωση zones/conduits που αναφέρει ο Magda (όρια, access points, flows, SL-T, policies, assumptions, dependencies) λειτουργεί ως “evidence spine” για τον έλεγχο της αρχιτεκτονικής.

Παράλληλα, ο Magda σημειώνει ότι ο καθορισμός Target Security Level (SL-T) είναι αποτέλεσμα risk assessment και ότι η ανοχή κινδύνου (risk tolerance) είναι ευθύνη της διοίκησης, άρα το operating model οφείλει να προβλέπει ρητό σημείο όπου η διοίκηση εγκρίνει (ή απορρίπτει) το υπόλοιπο ρίσκο που παραμένει μετά τους ελέγχους.

Η διάσταση της εφοδιαστικής αλυσίδας ενισχύει ακόμη περισσότερο την ανάγκη λειτουργικού μοντέλου. Στο “Good Practices for Supply Chain Cybersecurity” επισημαίνεται ότι η αποτελεσματική προσέγγιση απαιτεί στρατηγική, up-to-date policies, επαρκείς πόρους και ομάδες supply chain risk που περιλαμβάνουν executives από cyber, procurement, legal, ενώ υπογραμμίζει την ανάγκη ανάθεσης ευθύνης/εξουσίας σε προσωπικό και δημιουργίας ρητών συνεργατικών δομών. Στην ωριμότερη εκδοχή του, το ίδιο κείμενο προτείνει περιοδικές αξιολογήσεις/ελέγχους προμηθευτών και “right to audit” ρήτρες στις συμβάσεις ώστε να υπάρχει καταγεγραμμένη η εικόνα μεταβολών ρίσκου.

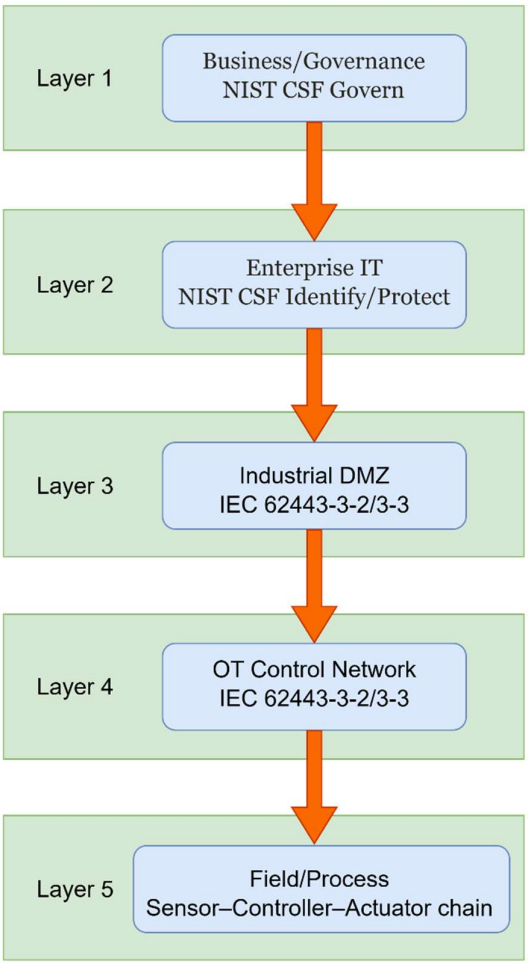
Εδώ υπάρχει μια άμεση γέφυρα προς ISO/IEC 27001 και ISO/IEC 27002, τα οποία το ίδιο κείμενο χρησιμοποιεί ως πηγή ελέγχων για supplier relationships και governance, άρα ως τεκμηριωτική βάση για να μεταφερθεί η supply chain ασφάλεια από την “καλή πρόθεση” στην “συμβατική υποχρέωση”.

Τέλος, το operating model αποκτά νοηματική ολοκλήρωση όταν οργανωθεί ως κύκλος συνεχούς βελτίωσης (PDCA), διότι τόσο το ISMS λογικά (διακυβέρνηση/βελτίωση) όσο και το CSF (profiles, ιεράρχηση, outcomes) προϋποθέτουν αναθεώρηση με βάση νέα δεδομένα και τις μεταβολές του οργανισμού. Το NIST CSF 2.0 παρουσιάζει ακριβώς αυτήν τη λειτουργία, αποτελεί “μακρόβιο” πλαίσιο που υποστηρίζει ότι η αξιολόγηση δεν πρέπει να είναι μια στατική “λύση”. Οι C. Brooks & P. Craig, στο αντίστοιχο κεφάλαιο governance, περιγράφουν ρητά τις λειτουργίες Identify, Protect, Detect, Respond, Recover ως οδικό χάρτη πολιτικής που ευθυγραμμίζει δραστηριότητες ασφάλειας με επιχειρησιακές απαιτήσεις, ανοχή κινδύνου και πόρους, δηλαδή ως πρακτική μορφή συνεχούς κύκλου.

4.4 Προτεινόμενο μοντέλο αρχιτεκτονικής ασφάλειας OT/IT

Συνοψίζοντας τις αρχές και τα πρότυπα που παρουσιάστηκαν στις προηγούμενες ενότητες, στην παρούσα ενότητα προτείνεται ένα στρωματοποιημένο μοντέλο αρχιτεκτονικής ασφάλειας για περιβάλλοντα OT/IT. Το προτεινόμενο «Layered OT/IT Security Architecture Model» επιδιώκει να συνδυάσει τη δομική λογική ζωνών και αγωγών της σειράς IEC 62443 με τις λειτουργίες του NIST Cybersecurity Framework, παρέχοντας μια ενιαία, πρακτικά εφαρμόσιμη αναπαράσταση της αρχιτεκτονικής άμυνας σε βάθος. Κάθε επίπεδο αντιστοιχεί σε έναν σαφώς ορισμένο χώρο ευθύνης και τεχνικών ελέγχων, ενώ ταυτόχρονα συνδέεται με συγκεκριμένες κατηγορίες του NIST CSF (όπως Govern, Identify και Protect) και με τις απαιτήσεις των IEC 62443-3-2 και IEC 62443-3-3 για την οργάνωση και προστασία των βιομηχανικών δικτύων.

Στο Σχήμα 1 απεικονίζονται τα πέντε διακριτά επίπεδα του μοντέλου, Business/Governance, Enterprise IT, Industrial DMZ, OT Control Network και Field/Process. Στο ανώτερο επίπεδο (Layer 1) τοποθετείται η επιχειρησιακή διακυβέρνηση και η λειτουργία Govern του NIST CSF, η οποία καθορίζει το πλαίσιο πολιτικών, ρόλων και στρατηγικών αποφάσεων που επηρεάζουν συνολικά την αρχιτεκτονική ασφάλειας. Το δεύτερο επίπεδο (Layer 2) αντιστοιχεί στο εταιρικό πληροφοριακό περιβάλλον (Enterprise IT) και συνδέεται κυρίως με τις λειτουργίες Identify και Protect του NIST CSF, καθώς εδώ εδράζονται οι κεντρικές υπηρεσίες πληροφορικής και οι βασικοί μηχανισμοί ελέγχου πρόσβασης και προστασίας.



Σχήμα 1 Layered OT/IT Security Architecture Model

Το τρίτο επίπεδο (Layer 3) αποτελεί την Industrial DMZ, η οποία λειτουργεί ως ενδιάμεση ζώνη μεταξύ IT και OT, σύμφωνα με τις κατευθυντήριες γραμμές των IEC 62443-3-2 και 62443-3-3. Στο επίπεδο αυτό φιλοξενούνται οι υπηρεσίες που απαιτούν ελεγχόμενη διασύνδεση, όπως historians, jump hosts και συστήματα συλλογής δεδομένων, με στόχο την ασφαλή ροή πληροφορίας χωρίς άμεση έκθεση των OT δικτύων.

Το τέταρτο επίπεδο (Layer 4) αντιστοιχεί στο OT Control Network, δηλαδή στα ίδια τα δίκτυα ελέγχου (SCADA, DCS, PLC), τα οποία οργανώνονται σε ζώνες και αγωγούς σύμφωνα με το IEC 62443-3-2 και προστατεύονται με αντίστοιχους τεχνικούς ελέγχους όπως segmentation, firewalling και OT-aware monitoring.

Τέλος, το πέμπτο επίπεδο (Layer 5) αφορά το Field/Process Layer, όπου υλοποιείται η αλυσίδα sensor–controller–actuator και οι φυσικές διεργασίες, και στο οποίο η αρχιτεκτονική ασφάλειας εστιάζει κυρίως στη μείωση της επιφάνειας έκθεσης, στη φυσική προστασία και στην ασφαλή παραμετροποίηση των πεδικών διατάξεων.

Επίπεδο	**Περιγραφή**	**Ενδεικτικά στοιχεία / έλεγχοι**
Επίπεδο 1: Business &	Επίπεδο επιχειρησιακής διακυβέρνησης και στρατηγικής, όπου	Στρατηγικές πολιτικές ασφάλειας.

Governance Layer	καθορίζονται οι στόχοι ασφάλειας, τα επίπεδα αποδοχής κινδύνου και οι βασικές αρχές αρχιτεκτονικής OT/IT.	Οργανωτική δομή (CISO, OT governance board). Ευθυγράμμιση με NIST CSF (Govern) και IEC 62443-2-1.
Επίπεδο 2: Enterprise IT Layer	Εταιρικό πληροφοριακό περιβάλλον που υποστηρίζει τις επιχειρησιακές λειτουργίες και αποτελεί το κύριο σημείο ενσωμάτωσης με τα OT δεδομένα σε επίπεδο business.	AD/identity services, email, ERP, HR, collaboration. IT security controls (IAM, EDR, SIEM). Διαχωρισμός από OT μέσω firewalls/segmentation.
Επίπεδο 3: Industrial DMZ Layer	Ενδιάμεση ζώνη μεταξύ IT και OT, η οποία φιλοξενεί υπηρεσίες που απαιτούν ελεγχόμενη διασύνδεση, παρέχοντας buffer και επιπλέον επίπεδο προστασίας.	OT/enterprise historians, jump hosts, OT application proxies, update/patch servers για OT, OT monitoring collectors. Διπλά firewalls, αυστηροί κανόνες πρόσβασης, one-way data flows όπου είναι εφικτό.
Επίπεδο 4: OT Control Network Layer	Πυρήνας των βιομηχανικών δικτύων ελέγχου, όπου λειτουργούν τα SCADA, DCS, PLC networks, οργανωμένα σε ζώνες ασφάλειας με βάση την κρισιμότητα και τη λειτουργία.	PLCs, RTUs, SCADA/DCS servers, engineering workstations. Ζώνες και conduits κατά IEC 62443-3-2. Network segmentation, OT firewalls, OT IDS/IPS, application whitelisting, hardening συστημάτων.
Επίπεδο 5: Field / Process Layer	Επίπεδο φυσικών διεργασιών και διατάξεων πεδίου, όπου υλοποιούνται τα συστήματα ασφαλείας.	Αισθητήρες, actuators, field devices, safety instrumented systems (SIS), fieldbuses. Φυσική ασφάλεια, ελαχιστοποίηση επιφάνειας έκθεσης, ασφαλείς ρυθμίσεις επικοινωνίας και πρόσβασης.

ΚΕΦΑΛΑΙΟ 5 - Ανθεκτικότητα, IR & Business Continuity για OT/IT

Το παρόν κεφάλαιο εστιάζει στην ανθεκτικότητα ενός ενοποιημένου περιβάλλοντος OT/IT, μέσα από τις διαδικασίες incident response, business continuity και disaster recovery. Η προσέγγιση που ακολουθείται βασίζεται σε διεθνή πρότυπα και οδηγίες, όπως το NIST SP 800-82r3 για την ασφάλεια OT, το NIST SP 800-61 για το incident handling, το NIST SP 800-34 και 800-184 για contingency και cyber event recovery, καθώς και το ISO 22301 για Business Continuity Management Systems. Στόχος είναι να αναδειχθεί πώς ένα OT-aware πρόγραμμα IR/BC/DR μπορεί να διασφαλίσει τη συνέχιση κρίσιμων βιομηχανικών διεργασιών, ιεραρχώντας safety, διαθεσιμότητα και αποκατάσταση εμπιστοσύνης στα συστήματα μετά από ένα περιστατικό.

5.1 Incident Response σε βιομηχανικά OT/ICS

Η διαχείριση περιστατικών σε OT/ICS περιβάλλοντα ακολουθεί τον κλασικό κύκλο preparation, detection and analysis, containment, eradication, recovery και post-incident activities, αλλά πρέπει να προσαρμοστεί στις ιδιαιτερότητες της φυσικής διεργασίας και των περιορισμών safety. Το NIST SP 800-82r3 προτείνει την ύπαρξη OT-specific incident response capability, ευθυγραμμισμένη με το NIST SP 800-61, ώστε η ομάδα IR να μπορεί να λαμβάνει αποφάσεις λαμβάνοντας υπόψη επιπτώσεις σε ανθρώπινη ασφάλεια, περιβάλλον και κρίσιμο εξοπλισμό. Σε αντίθεση με καθαρά IT σενάρια, σε πολλές περιπτώσεις η “τέλεια” τεχνική αποκατάσταση υποχωρεί μπροστά στην ανάγκη ελεγχόμενης υποβάθμισης λειτουργίας ή χειροκίνητης λειτουργίας της εγκατάστασης.

Στα βιομηχανικά περιβάλλοντα manufacturing, η έννοια “incident response” δεν μπορεί να νοηθεί ως καθαρά ψηφιακή διαδικασία χειρισμού συμβάντων (π.χ. απομόνωση endpoints, επαναφορά λογαριασμών, restoration συστημάτων), διότι το OT συνδέεται άμεσα με φυσική διεργασία, με δεσμεύσεις real-time λειτουργίας και με απαιτήσεις safety. Το NIST SP 800-82 Rev.3 επιμένει ότι οι OT/ICS πρακτικές κυβερνοασφάλειας οφείλουν να σχεδιάζονται με σεβασμό σε performance, reliability και safety constraints, άρα η απόκριση σε περιστατικό δεν επιτρέπεται να παράγει μεγαλύτερο λειτουργικό κίνδυνο από το ίδιο το περιστατικό.

Η σύγχρονη καθοδήγηση του NIST στο NIST SP 800-61 Rev.3 μετακινεί το κέντρο βάρους από ένα «στατικό εγχειρίδιο βημάτων» προς μια λογική ενοποίησης του incident response μέσα στη συνολική διαχείριση κινδύνου όπως περιγράφεται στο NIST CSF 2.0. Το σημαντικό εδώ (και κρίσιμο για OT) είναι ότι το IR δεν αντιμετωπίζεται ως ad hoc αντίδραση, αλλά ως ικανότητα που διαχέεται στις λειτουργίες Govern–Identify–Protect–Detect–Respond–Recover, πράγμα που διευκολύνει την κοινή γλώσσα OT/IT για το τι σημαίνει «ετοιμότητα», «ανίχνευση», «μετριασμός» και «ανάκαμψη».

Στο manufacturing, η πρακτική “OT-aware” απόκρισης προϋποθέτει ότι η ομάδα IR διαθέτει όχι μόνο τεχνική επάρκεια αλλά και επιχειρησιακή γνώση: ποια τμήματα της διεργασίας είναι κρίσιμα, ποια είναι τα ασφαλή modes λειτουργίας, ποιες αλλαγές μπορούν να εφαρμοστούν χωρίς να θιγεί η σταθερότητα, και ποια γεγονότα αποτελούν «κανονικές αποκλίσεις» (process noise) έναντι «κακόβουλης παρέμβασης». Αυτή η απαίτηση «ενσωμάτωσης της IR σκέψης στο risk management» είναι ακριβώς ο στόχος του NIST SP 800-61 Rev.3 όταν δηλώνει ότι οι συστάσεις του πρέπει να ενσωματώνονται στη συνολική διαχείριση κυβερνοκινδύνου με βάση το CSF 2.0.

Στη βιβλιογραφία για ICS επισημαίνεται ότι ένα αποτελεσματικό IR plan σε OT περιβάλλον πρέπει να ξεκαθαρίζει από πριν προτεραιότητες, όπως αν σε ένα περιστατικό προτιμάται ταχεία επιστροφή σε λειτουργία ή διατήρηση forensic δεδομένων για root-cause analysis. Το NIST SP 800-82r3 προτείνει η ανάλυση κάθε περιστατικού να λαμβάνει υπόψη αν η απενεργοποίηση συστημάτων, η αποσύνδεση δικτύων ή η ενεργοποίηση χειροκίνητων λειτουργιών δημιουργεί μεγαλύτερους κινδύνους για safety και διαθεσιμότητα από την ίδια την κυβερνοεπίθεση. Για τον λόγο αυτό, συνιστάται η εκτέλεση στοχευμένων OT risk assessments κατά τη φάση containment, ώστε οι ενέργειες απομόνωσης (π.χ. φυσική αποσύνδεση ενός segment) να ζυγίζονται έναντι των επιχειρησιακών και safety συνεπειών.

Επιπλέον, το OT incident response δεν μπορεί να στηριχθεί αποκλειστικά σε παραδοσιακή IT τηλεμετρία. Η έννοια «ανίχνευση» πρέπει να συνδεθεί με επιτρεπτές ροές και συμπεριφορές στη βιομηχανική ζώνη (π.χ. επικοινωνίες πρωτοκόλλων, αλλαγές configuration, ανωμαλίες σε HMI/engineering workstations, ασυνήθιστα remote sessions). Η ανάγκη αυτής της “contextual” ανίχνευσης αιτιολογείται από το ίδιο το OT προφίλ όπου

πολλά OT assets δεν υποστηρίζουν agents, τα lifecycle windows είναι περιορισμένα και οι παρεμβάσεις πρέπει να είναι ελάχιστα επεμβατικές.

Τέλος, η απόκριση σε OT περιστατικό οφείλει να παράγει τεκμήρια (evidence) που τροφοδοτούν τη διακυβέρνηση, μεταβολές σε rulesets, αναθεώρηση επιτρεπτών ροών, ενημέρωση των “lessons learned” και επικαιροποίηση διαδικασιών. Αυτή η λογική κλεισίματος του κύκλου (response → learning → governance update) βρίσκεται στο επίκεντρο τόσο της προσέγγισης του CSF 2.0 όσο και της φιλοσοφίας του NIST SP 800-61 Rev.3.

5.2 Business Continuity & Disaster Recovery σε OT/IT

Η επιχειρησιακή συνέχεια σε περιβάλλοντα OT/IT απαιτεί συνδυασμό business continuity planning (BCP) και disaster recovery planning (DRP), με στόχο να διασφαλιστεί ότι κρίσιμες διεργασίες μπορούν να συνεχίσουν ή να επανέλθουν εντός αποδεκτών ορίων χρόνου και ποιότητας. Το ISO 22301 παρέχει το γενικό πλαίσιο BCMS, ενώ το NIST SP 800-34 και το NIST SP 800-184 εξειδικεύουν την προσέγγιση σε επίπεδο πληροφοριακών και OT συστημάτων, δίνοντας έμφαση σε συντονισμένο IR/BC/DR σχεδιασμό. Σε ένα βιομηχανικό περιβάλλον, τα recovery objectives πρέπει να συνδέονται άμεσα με τις διεργασίες παραγωγής, την ασφάλεια προσωπικού και τις ρυθμιστικές απαιτήσεις, και όχι μόνο με την αποκατάσταση IT υπηρεσιών. Σε βιομηχανικά περιβάλλοντα, η επιχειρησιακή συνέχεια δεν είναι απλή «επιστροφή των πληροφοριακών συστημάτων σε λειτουργία», αλλά δυνατότητα διατήρησης ή γρήγορης αποκατάστασης της παραγωγικής ικανότητας σε αποδεκτό επίπεδο. Το ISO 22301 περιγράφει τις απαιτήσεις ενός Business Continuity Management System (BCMS) ακριβώς ως συστηματική προσέγγιση για ανθεκτικότητα απέναντι σε διαταραχές, με έμφαση στον κύκλο ζωής σχεδιασμού, υλοποίησης, αξιολόγησης και βελτίωσης.

Η διάκριση BCP/DR αποκτά ειδικό νόημα στο OT. Το DR (ως τεχνική αποκατάσταση υποδομών) είναι αναγκαίο αλλά ανεπαρκές, διότι η παραγωγή μπορεί να απαιτεί όχι μόνο servers και δίκτυα, αλλά και ασφαλή επαναφορά παραμέτρων διεργασίας, επανασυγχρονισμό ελέγχου, επαλήθευση ποιότητας και ασφαλή restart sequences. Για τον λόγο αυτό, ο σχεδιασμός continuity πρέπει να ενσωματώνει «σενάρια λειτουργικής υποβάθμισης» (degraded mode), χειροκίνητες διαδικασίες (workarounds), και σαφείς αποφάσεις για το πότε μια γραμμή μπαίνει σε safe state ή πότε επιτρέπεται περιορισμένη λειτουργία. Το NIST SP 800-61 Rev.3, εστιάζοντας σε risk management, οδηγεί ακριβώς σε αυτήν τη συλλογιστική ότι δηλαδή, τα σχέδια απόκρισης/ανάκαμψης δεν είναι “IT-only”, αλλά μέρος ολοκληρωμένης μείωσης επιχειρησιακού αντίκτυπου.

Το NIST SP 800-82r3 προτείνει ο καθορισμός RTO και RPO να γίνεται σε επίπεδο βιομηχανικών διεργασιών και όχι μόνο σε επίπεδο συστημάτων, π.χ. μέγιστος αποδεκτός χρόνος χωρίς καταγραφή σε historian ή χωρίς λειτουργική πρόσβαση σε HMI. Η βιβλιογραφία για ICS BCP/DR τονίζει ότι αυτές οι παράμετροι μπορεί να δικαιολογούν επενδύσεις σε εφεδρικό εξοπλισμό, εναλλακτικά σημεία λειτουργίας (hot/warm sites) ή ειδικές διαδικασίες “degraded mode” όπου η παραγωγή συνεχίζεται με μειωμένη δυναμικότητα αλλά με διασφαλισμένη ασφάλεια. Σε κάθε περίπτωση, τα RTO/RPO πρέπει να αντικατοπτρίζουν τόσο οικονομικές απώλειες από downtime όσο και επιπτώσεις σε ποιότητα, traceability και συμμόρφωση με κανονιστικά πλαίσια.

Σε σύγχρονα OT περιβάλλοντα, ο πιο συχνός καταλύτης για επιχειρησιακή ασυνέχεια είναι το ransomware, όχι μόνο λόγω κρυπτογράφησης δεδομένων, αλλά λόγω παράπλευρης διαταραχής σε διασυνδεδεμένα IT/OT επίπεδα. Η CISA στο “Rising Ransomware Threat to OT Assets” τονίζει ότι οι επιθέσεις ransomware έχουν δείξει αυξανόμενο κίνδυνο σοβαρής επιχειρησιακής υποβάθμισης για κρίσιμες υποδομές και OT περιβάλλοντα, γεγονός που καθιστά τα μέτρα συνέχειας (offline backups, σχέδια αποκατάστασης, περιορισμό lateral movement, έλεγχο απομακρυσμένης πρόσβασης) θεμέλιο ανθεκτικότητας.

Το NIST SP 800-82r3, στο Appendix E, υπογραμμίζει τη σημασία αξιόπιστων backup μηχανισμών για OT δεδομένα, συμπεριλαμβανομένων configuration files, recipes, setpoints, logs και historian snapshots, καθώς και τη χρήση immutable storage ώστε να δυσκολεύεται η αλλοίωση από ransomware. Οι Brooks και Craig προτείνουν τακτικές δοκιμές restore, ιδανικά σε test ή digital-twin περιβάλλον, ώστε να επιβεβαιώνεται ότι τα backups μπορούν πράγματι να επαναφέρουν συστήματα σε “known good state” χωρίς να εισάγουν νέους λειτουργικούς κινδύνους. Η αποθήκευση αντιγράφων σε φυσικά και λογικά απομονωμένες τοποθεσίες (offline

ή off-site) αποτελεί κρίσιμο μέτρο για την ανθεκτικότητα απέναντι σε καταστροφικά περιστατικά ή εκστρατείες ransomware.

Το κρίσιμο σημείο για το BCP δεν «έρχεται μετά» την αρχιτεκτονική ασφάλειας αλλά απορρέει από αυτήν. Όταν η αρχιτεκτονική ορίζει ζώνες, ροές και όρια, τότε ο σχεδιασμός continuity μπορεί να γίνει συγκεκριμένος. Ποιες λειτουργίες πρέπει να αποκατασταθούν πρώτες, ποια δεδομένα είναι κρίσιμα (π.χ. recipes, setpoints, historian snapshots, quality/traceability), ποια είναι τα ελάχιστα απαιτούμενα για ασφαλές restart, και ποιες συνδέσεις πρέπει να παραμείνουν κλειστές μέχρι να υπάρξει επιβεβαιωμένη αποκατάσταση εμπιστοσύνης. Αυτό το “recovery with controlled re-trust” είναι πρακτικά η γέφυρα ανάμεσα σε cybersecurity recovery και παραγωγική ανάκαμψη.

5.3 Continuity ξεπερνώντας τρίτους και supply chain

Στις βιομηχανίες, ειδικά σε γραμμές παραγωγής υψηλής εξειδίκευσης, η επιχειρησιακή συνέχεια δεν εξαρτάται μόνο από εσωτερικές ομάδες IT/OT, αλλά και από τρίτους, integrators, vendors, συμβάσεις συντήρησης, remote diagnostics, ανταλλακτικά, ενημερώσεις λογισμικού και διαδικασίες escalation. Η ευαλωτότητα εδώ είναι διπλή, τεχνική, επειδή οι προμηθευτές συχνά χρειάζονται πρόσβαση, και οργανωσιακή, επειδή η κρίσιμη γνώση troubleshooting μπορεί να βρίσκεται εκτός του οργανισμού.

Η ENISA στο “Good Practices for Supply Chain Cybersecurity” αντιμετωπίζει τη supply chain κυβερνοασφάλεια ως ICT/OT ζήτημα εταιρικής διακυβέρνησης και συνεχούς βελτίωσης, περιγράφοντας ότι η αποτελεσματική διαχείριση κινδύνου απαιτεί δέσμευση από ανώτατη διοίκηση, σαφείς ρόλους/πόρους και διαδικασίες που μπορούν να οργανωθούν σε PDCA κύκλο. Αυτό είναι καθοριστικό για το business continuity, αν δεν υπάρχει governance των προμηθευτικών σχέσεων και των διαδικασιών remote support, τότε οι χρόνοι αποκατάστασης (RTO) και τα σενάρια ανάκαμψης παραμένουν θεωρητικά. Η ENISA επισημαίνει ότι η συνέχεια λειτουργίας σε OT/IT περιβάλλοντα εξαρτάται σε μεγάλο βαθμό από την ανθεκτικότητα της εφοδιαστικής αλυσίδας, συμπεριλαμβανομένων vendors αυτοματισμού, παρόχων remote support και cloud υπηρεσιών. Στο “Good Practices for Supply Chain Cybersecurity” προτείνονται μηχανισμοί όπως συμβατικές απαιτήσεις για BC/DR δυνατότητες των προμηθευτών, κοινές δοκιμές σε σενάρια διακοπής remote support και σαφώς καθορισμένοι RTO/RPO σε επίπεδο υπηρεσιών που παρέχονται στον τελικό βιομηχανικό πελάτη. Η ενσωμάτωση αυτών των απαιτήσεων στο ISMS και στο BCMS επιτρέπει πιο ρεαλιστικό σχεδιασμό συνέχειας, καθώς λαμβάνει υπόψη εξωτερικούς περιορισμούς και αλληλεξαρτήσεις.

Στο ίδιο πλαίσιο, μια ώριμη στρατηγική επιχειρησιακής συνέχειας ενσωματώνει ρητά διαδικασίες διαχείρισης κύκλου ζωής (lifecycle management) για όλα τα κρίσιμα OT components, σε στενή σύνδεση με το πρόγραμμα διαχείρισης κινδύνου προμηθευτών (C-SCRM). Το NIST SP 800-161r1 προτείνει τη διατήρηση ενημερωμένου καταλόγου (asset and component inventory) που να περιλαμβάνει, για κάθε asset, πληροφορίες όπως η ημερομηνία αρχικής εγκατάστασης, η τρέχουσα έκδοση λογισμικού/firmware, η πολιτική υποστήριξης του κατασκευαστή και η αναμενόμενη ημερομηνία end-of-support. Πρακτικά, αυτό υλοποιείται μέσω τακτικών κύκλων αναθεώρησης (π.χ. ετήσιας ή εξαμηνιαίας αξιολόγησης) κατά τους οποίους η ομάδα OT σε συνεργασία με procurement/IT security αξιολογεί ποια συστήματα εισέρχονται σε φάση obsolescence, εκτιμά τις λειτουργικές και τις επιπτώσεις που σχετίζονται με την ασφάλεια και καταρτίζει σχέδιο μετάβασης με πλήρη αντικατάσταση (replacement), σταδιακή μετάβαση (migration) σε νέα πλατφόρμα ή εφαρμογή αντισταθμιστικών μέτρων (compensating controls) όπου η αντικατάσταση δεν είναι άμεσα εφικτή.

Ένα ακόμη πρακτικό στοιχείο της στρατηγικής continuity σε συνθήκες obsolescence είναι η προνοητική διαχείριση ανταλλακτικών (spares management). Σε αντίθεση με τα τυπικά IT περιβάλλοντα, όπου ο εξοπλισμός ανανεώνεται σχετικά συχνά, στα OT συστήματα είναι συνηθισμένο να διατηρείται στόλος PLCs, RTUs ή βιομηχανικών servers που έχουν πλέον αποσυρθεί από την αγορά. Η διακοπή παραγωγής συγκεκριμένων μοντέλων από τον vendor συνεπάγεται ότι μια μεμονωμένη βλάβη μπορεί να οδηγήσει σε παρατεταμένη διακοπή αν δεν υπάρχουν διαθέσιμα ανταλλακτικά. Τα NIST 800-82r3 και 800-161r1 συνιστούν, στο πλαίσιο της continuity και του C-SCRM, την υιοθέτηση πολιτικής διατήρησης ελάχιστου αποθέματος ανταλλακτικών για κρίσιμα components, με τεκμηριωμένα κριτήρια επιλογής (κρισιμότητα διεργασίας, χρόνος παραγγελίας, πιθανότητα αστοχίας) και προγραμματισμένες αναθεωρήσεις καθώς πλησιάζουν σε τέλος κύκλου ζωής. Στην πράξη, αυτό μπορεί να περιλαμβάνει αποθήκευση έτοιμων, προ-διαμορφωμένων spare units για κεντρικούς

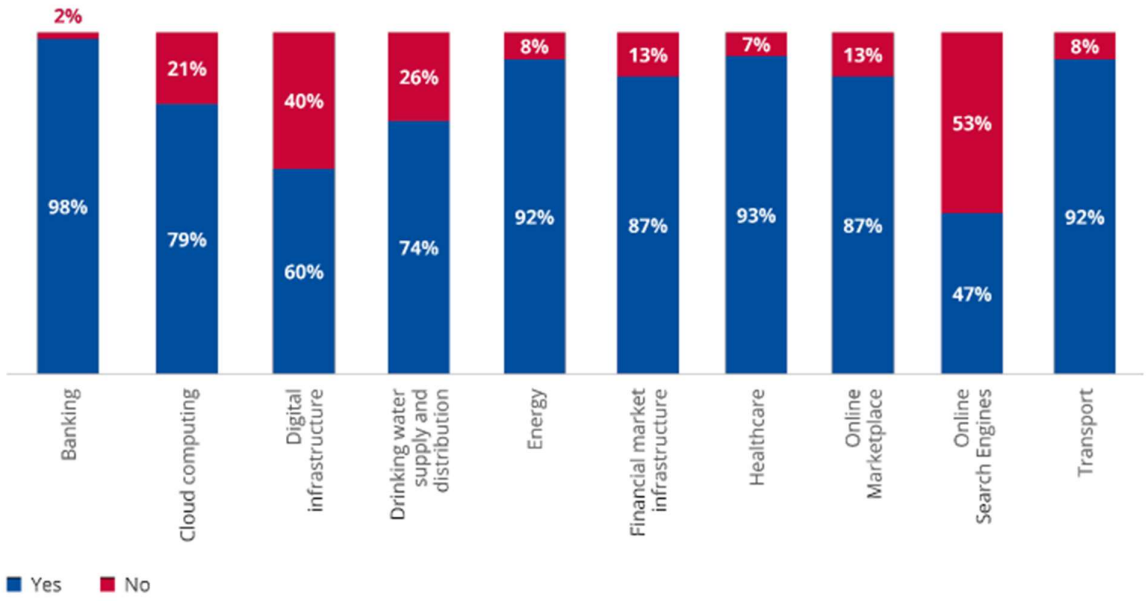
SCADA servers ή PLC racks, ώστε η αντικατάσταση σε περίπτωση βλάβης να μπορεί να γίνει εντός ωρών αντί για ημέρες ή εβδομάδες.

Συνολικά, η πρακτική διαχείριση obsolescence και end-of-support στην εφοδιαστική αλυσίδα OT/IT δεν είναι απλώς θέμα «αναβάθμισης όταν χαλάσει», αλλά ενσωμάτωση του κύκλου ζωής των προϊόντων στον σχεδιασμό επιχειρησιακής συνέχειας και στις διαδικασίες C-SCRM. Οργανισμοί που αντιμετωπίζουν τη γήρανση εξοπλισμού με προληπτικό, risk-based τρόπο – συνδυάζοντας lifecycle inventories, σχέδια μετάβασης, compensating controls και διαχείριση ανταλλακτικών – είναι σε σαφώς καλύτερη θέση να απορροφήσουν τόσο τεχνικές αστοχίες όσο και κυβερνοεπιθέσεις σε παλαιωμένα συστήματα, χωρίς να θέτουν σε κίνδυνο τη βασική βιομηχανική λειτουργία.

Σε πρακτικό επίπεδο, η σημασία της προνοητικής διαχείρισης κύκλου ζωής και επιχειρησιακής συνέχειας αναδεικνύεται ξεκάθαρα σε περιστατικά αστοχίας κρίσιμου εξοπλισμού, ακόμη και όταν υπάρχουν τυπικά συμβόλαια υποστήριξης. Σε πραγματική περίπτωση βιομηχανικού περιβάλλοντος, αστοχία σε server διπλού επεξεργαστή, ο οποίος υποστήριζε κρίσιμες λειτουργίες, οδήγησε τελικά σε πλήρη αντικατάσταση motherboard. Παρότι ο οργανισμός διέθετε premium support συμβόλαιο με τυπική δέσμευση «4 ωρών για αντικατάσταση», στην πράξη ο χρόνος αποκατάστασης έφτασε περίπου τις 38 ώρες, διότι το SLA όριζε ότι ο χρόνος μετρά από τη στιγμή που θα επιβεβαιωθεί το ελαττωματικό εξάρτημα. Προηγήθηκε πολύωρη διαδικασία συλλογής logs, ανοίγματος case, αποστολής οδηγιών troubleshooting από τον vendor (αφαίρεση και εναλλαγή RAM DIMMs, μεταφορά CPU μεταξύ sockets, εναλλαγή θέσεων RAM) και τελικά αποστολής του ανταλλακτικού, η οποία εξαρτήθηκε επιπλέον από τη διαθεσιμότητα του τοπικού συνεργάτη. Στο συγκεκριμένο παράδειγμα, η παραγωγική γραμμή δεν επηρεάστηκε επειδή ο server ήταν μέλος cluster δύο hosts και υπήρχε επαρκής πλεονασμός, ωστόσο η εμπειρία ανέδειξε στην πράξη ότι το «4 ώρες υποστήριξη» δεν ταυτίζεται με «4 ώρες συνολικός χρόνος διακοπής».

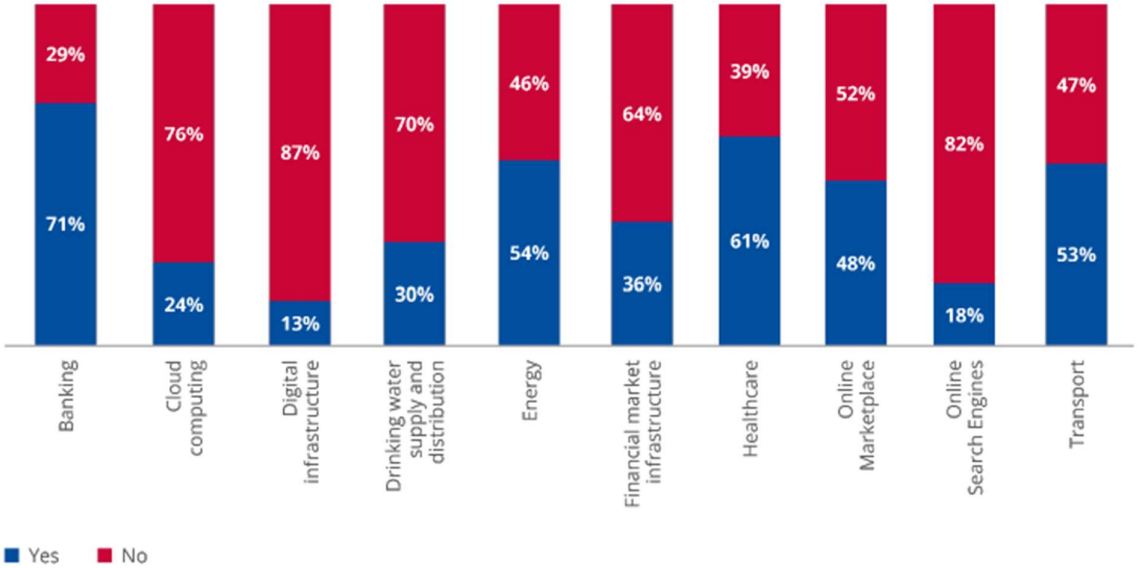
Το περιστατικό αυτό είναι απόλυτα εναρμονισμένο με τις παρατηρήσεις τόσο του NIST όσο και της ENISA ότι οι οργανισμοί συχνά υποεκτιμούν τον πραγματικό χρόνο αποκατάστασης όταν εξαρτώνται πλήρως από SLA προμηθευτών, χωρίς να έχουν σχεδιάσει επαρκή πλεονασμό ή εναλλακτικά σενάρια λειτουργίας. Στο πλαίσιο της επιχειρησιακής συνέχειας, το μάθημα που προκύπτει είναι διπλό. Αφενός, τα SLA με vendors πρέπει να αναλύονται προσεκτικά ως προς τις πραγματικές προϋποθέσεις ενεργοποίησης και τους χρόνους διάγνωσης αφετέρου, η αρχιτεκτονική σχεδίαση (π.χ. clusters, failover hosts, εφεδρικά HMI/SCADA nodes) πρέπει να θεωρεί δεδομένο ότι σε ένα σοβαρό περιστατικό ο χρόνος αποκατάστασης μπορεί να είναι πολύ μεγαλύτερος από τον ονομαστικό χρόνο ανταπόκρισης που αναγράφεται στη σύμβαση. Η ύπαρξη επαρκούς πλεονασμού και εναλλακτικών διαδρομών λειτουργίας, όπως στο παραπάνω παράδειγμα, είναι συχνά ο καθοριστικός παράγοντας που αποτρέπει μια τεχνική αστοχία ή καθυστέρηση vendor από το να εξελιχθεί σε πλήρες περιστατικό διακοπής παραγωγής.

Από ερεύνα που έχει γίνει σε οργανισμούς στην ΕΕ, το 86% έχει εφαρμόσει πολιτικές για την ασφάλεια στον κυβερνοχώρο της εφοδιαστικής αλυσίδας ICT/OT. Μόνο το 14 % των οργανισμών που συμμετείχαν στην έρευνα δεν διαθέτει εγκεκριμένες πολιτικές ασφάλειας που αφορούν τρίτους, δηλαδή συνεργάτες, πωλητές ή προμηθευτές (ENISA, GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY, June 2023). Η έρευνα διαπιστώνει ότι όσο μεγαλύτερος είναι ο οργανισμός, τόσο πιο πιθανό είναι να έχει θεσπίσει μια τέτοια πολιτική.



Γράφημα 1. Πολιτικές διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας της εφοδιαστικής αλυσίδας των ICT/OT ανά τομέα.

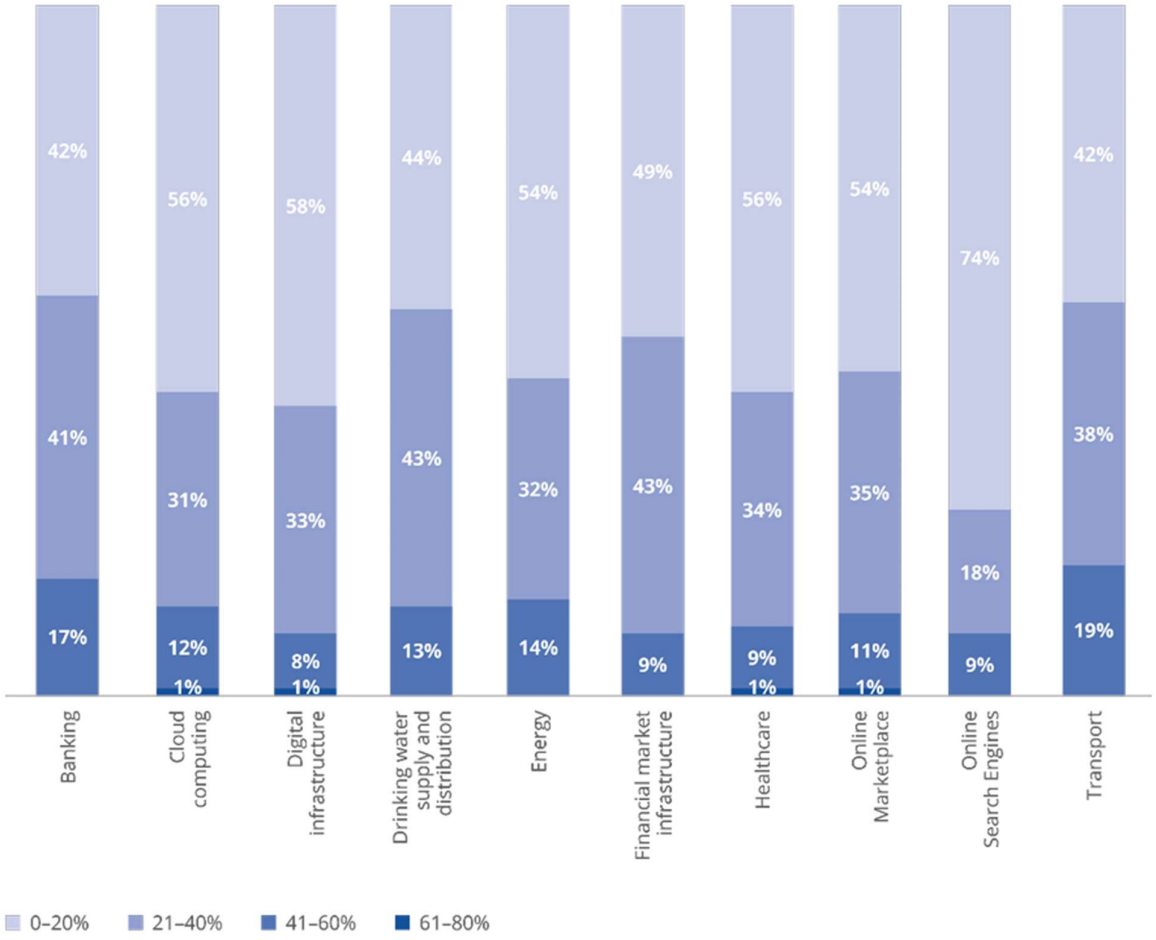
Παρά την ύπαρξη σχετικών πολιτικών κυβερνοασφάλειας, οι οργανισμοί δεν φαίνεται να επενδύουν στην ασφάλεια του κυκλώματος εφοδιασμού των ICT/OT. Μόνο το 47% των οργανισμών που συμμετείχαν στην έρευνα στην ΕΕ έχει διαθέσει προϋπολογισμό για την ασφάλεια του κυκλώματος εφοδιασμού των ICT/OT (Γράφημα 1), ενώ η πλειοψηφία των οργανισμών που συμμετείχαν στην έρευνα (53%) δεν διαθέτει εγκεκριμένο προϋπολογισμό για τέτοια θέματα (ENISA, GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY, June 2023). Ο τραπεζικός τομέας βρίσκεται στην πρώτη θέση, με το υψηλότερο ποσοστό ειδικών προϋπολογισμών για την ασφάλεια του κυκλώματος εφοδιασμού των ICT/OT (Γράφημα 2).



Γράφημα 2 προϋπολογισμός για την ασφάλεια στον κυβερνοχώρο της εφοδιαστικής αλυσίδας ICT/OT ανά τομέα.

Στην ίδια έρευνα είναι ξεκάθαρο αυτό που αναφέρεται παραπάνω για το asset management και το visibility των assets τα οποία είναι με τις τελευταίες ενημερώσει. Τα στοιχεία της έρευνας έδειξαν ότι η πλειοψηφία (52%) διαθέτει αυστηρή πολιτική εγκατάστασης ενημερώσεων ασφαλείας, σύμφωνα με την οποία μόνο το 0 έως 20%

των περιουσιακών τους στοιχείων δεν καλύπτεται. Από την άλλη πλευρά, το 13,5% των οργανισμών που συμμετείχαν στην έρευνα δεν έχει ορατότητα όσον αφορά την εγκατάσταση ενημερώσεων στο 50% ή περισσότερο των περιουσιακών στοιχείων πληροφοριών τους (ENISA, GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY, June 2023). Εάν οι asset owners δεν μπορούν να παρακολουθούν πιθανές ευπάθειες ή να λαμβάνουν αντίστοιχες ειδοποιήσεις ευπάθειας από τους προμηθευτές τους, ή εάν δεν κατανοούν τους κινδύνους που ενέχουν οι ευπάθειες των προϊόντων στο επιχειρησιακό τους πλαίσιο, δεν μπορούν να σχεδιάσουν και να εφαρμόσουν επαρκή προγράμματα διαχείρισης ενημερώσεων προκειμένου να διασφαλίσουν τον μετριασμό των αντίστοιχων κινδύνων.



Γράφημα 3 Επισκόπηση της ενημέρωσης λογισμικού των περιουσιακών στοιχείων ανά τομέα.

Η προσέγγιση της ENISA για την κυβερνοασφάλεια της εφοδιαστικής αλυσίδας δεν περιορίζεται σε αποσπασματικούς ελέγχους προμηθευτών, αλλά οργανώνεται ως ένα ενιαίο σύστημα διακυβέρνησης που καλύπτει στρατηγική, διαχείριση κινδύνου, σχέσεις με προμηθευτές, χειρισμό ευπαθειών και ποιότητα προϊόντων και υπηρεσιών σε όλο το εύρος της αλυσίδας αξίας. Το κρίσιμο σημείο είναι ότι η ασφάλεια της εφοδιαστικής αλυσίδας δεν αντιμετωπίζεται ως μια εξωτερική δραστηριότητα procurement, αλλά ως οργανωτική λειτουργία που πρέπει να ενσωματώνεται στο συνολικό σύστημα κυβερνοασφάλειας του οργανισμού, με σαφή σύνδεση με ρόλους, ευθύνες, risk assessment, απαιτήσεις συμβάσεων και συνεχές monitoring. Η παρατήρηση αυτή είναι ιδιαίτερα σημαντική για περιβάλλοντα OT/IT, όπου ένας προμηθευτής δεν επηρεάζει μόνο την πληροφοριακή ασφάλεια, αλλά δυνητικά και τη διαθεσιμότητα κρίσιμων βιομηχανικών διεργασιών.

Σε αυτό το πλαίσιο, η ENISA δίνει ιδιαίτερη βαρύτητα στη δημιουργία ενός strategic corporate approach, δηλαδή μιας εταιρικής πολιτικής για την ασφάλεια της εφοδιαστικής αλυσίδας με άμεση εμπλοκή της διοίκησης, σαφή κατανομή αρμοδιοτήτων και σύνδεση με τις γενικότερες λειτουργίες third-party risk

management. Το στοιχείο αυτό συνδέεται άμεσα με τη φιλοσοφία του ISO/IEC 27002:2022, το οποίο δεν αντιμετωπίζει τους προμηθευτές μόνο ως εξωτερικούς συνεργάτες αλλά ως πηγές κινδύνου που πρέπει να καλύπτονται από τεκμηριωμένες πολιτικές, διαδικασίες ανάθεσης, ελέγχους πρόσβασης, απαιτήσεις παρακολούθησης υπηρεσιών και ρήτρες ασφάλειας στις συμβάσεις. Ειδικά οι έλεγχοι του ISO/IEC 27002:2022 που αφορούν supplier relationships, information security in supplier agreements, management of information security in the ICT supply chain και monitoring/review of supplier services ενισχύουν σημαντικά την άποψη ότι η ασφάλεια της εφοδιαστικής αλυσίδας δεν είναι μεμονωμένο τεχνικό θέμα, αλλά οργανωσιακή ευθύνη που απαιτεί lifecycle governance.

Η δεύτερη σημαντική διάσταση αφορά το supply chain risk management με risk-based λογική. Η ENISA υπογραμμίζει ότι οι οργανισμοί δεν πρέπει απλώς να ζητούν πιστοποιήσεις ή δηλώσεις συμμόρφωσης από τους προμηθευτές, αλλά να εφαρμόζουν μια συνεχή διαδικασία αναγνώρισης, αξιολόγησης, αντιμετώπισης και παρακολούθησης των κινδύνων που προέρχονται από προϊόντα, λογισμικό, υπηρεσίες και εξωτερικούς παρόχους. Αυτό είναι ιδιαίτερα κρίσιμο σε OT περιβάλλοντα, όπου οι τεχνολογικές εξαρτήσεις είναι μακροχρόνιες, τα προϊόντα έχουν πολυετή κύκλο ζωής και οι αδυναμίες ενός vendor μπορεί να μεταφραστούν σε αδυναμία patching, καθυστέρηση ανταλλακτικών ή αδυναμία τεχνικής υποστήριξης κατά τη διάρκεια περιστατικού. Η σύνδεση με το ISO/IEC 27002:2022 είναι και εδώ εμφανής, καθώς οι έλεγχοι του προτύπου επιβάλλουν την αναγνώριση των απαιτήσεων ασφάλειας πριν από την προμήθεια, την αξιολόγηση των παρόχων με βάση το επίπεδο έκθεσης και την επαναξιολόγηση των προμηθευτών καθ’ όλη τη διάρκεια της συνεργασίας.

Ιδιαίτερα ώριμη είναι και η τρίτη διάσταση του πλαισίου της ENISA, δηλαδή το supplier relationship management. Η λογική εδώ είναι ότι η ασφάλεια δεν μπορεί να διασφαλιστεί μόνο πριν από την ανάθεση, αλλά πρέπει να συνοδεύει όλη τη διάρκεια της σχέσης με τον προμηθευτή, από την επιλογή και τις συμβατικές ρήτρες έως την παρακολούθηση της απόδοσης, τη διαχείριση μεταβολών, την ανταλλαγή πληροφοριών για συμβάντα και τη διαδικασία τερματισμού της συνεργασίας. Το ISO/IEC 27002:2022 ενισχύει αυτή τη λογική, προτείνοντας όχι μόνο contractual controls αλλά και ενεργή παρακολούθηση της συμμόρφωσης και των delivered services, κάτι που πρακτικά μεταφράζεται σε periodic review meetings, supplier audits, security KPIs, reassessment questionnaires και διαδικασίες απομάκρυνσης πρόσβασης όταν λήγει μια συνεργασία.

Ένα ακόμη σημείο στο οποίο αξίζει να σταθεί η ανάλυση είναι το vulnerability handling, όπου η ENISA αναγνωρίζει ότι η εφοδιαστική αλυσίδα είναι από τη φύση της ένας μηχανισμός διάχυσης ευπαθειών και όχι μόνο προϊόντων ή υπηρεσιών. Η έκθεση τονίζει ότι χωρίς ορατότητα στην κατάσταση patching, στις γνωστές ευπάθειες των assets και στις διαδικασίες ειδοποίησης από τους vendors, οι οργανισμοί αδυνατούν να εφαρμόσουν αποτελεσματικό vulnerability management, ιδιαίτερα σε OT περιβάλλοντα όπου η άμεση εγκατάσταση patches δεν είναι πάντα εφικτή. Η σημασία αυτού του σημείου είναι διπλή, αφενός ενισχύει την ανάγκη για test environments και staging πριν την εφαρμογή patches σε production OT υποδομές, αφετέρου συνδέει τη διαχείριση ευπαθειών με τις υποχρεώσεις των suppliers να κοινοποιούν έγκαιρα vulnerabilities, mitigations και ασφαλείς διαδικασίες αναβάθμισης. Εδώ το ISO/IEC 27002:2022 λειτουργεί συμπληρωματικά, γιατί δίνει το γενικό πλαίσιο για vulnerability management, change management και configuration control, ενώ η ENISA το εξειδικεύει στην αλυσίδα προμηθευτών.

Τέλος, εξαιρετικά σημαντική είναι η πέμπτη διάσταση που αφορά την ποιότητα προϊόντων και πρακτικών των suppliers και service providers. Η ENISA επισημαίνει ότι η ασφάλεια της εφοδιαστικής αλυσίδας εξαρτάται όχι μόνο από το αν ένας οργανισμός ελέγχει τους άμεσους προμηθευτές του, αλλά και από το κατά πόσο οι ίδιοι οι προμηθευτές ακολουθούν ασφαλείς πρακτικές ανάπτυξης, διαχείρισης ποιότητας, vulnerability disclosure και secure maintenance. Το σημείο αυτό είναι ιδιαίτερα συμβατό με τη σύγχρονη λογική του ISO/IEC 27002:2022, καθώς και με τη broader τάση προς secure-by-design και secure-by-default προϊόντα. Για βιομηχανικά περιβάλλοντα OT, αυτό σημαίνει ότι ο οργανισμός δεν πρέπει να ενδιαφέρεται μόνο για την παράδοση του προϊόντος, αλλά για το κατά πόσο ο vendor διαθέτει ώριμες διαδικασίες secure development, σαφές vulnerability disclosure process, υποστήριξη για patch availability και μακροχρόνιο lifecycle support. Με άλλα λόγια, η ποιότητα του supplier δεν αποτιμάται μόνο εμπορικά ή τεχνικά, αλλά και κυβερνοασφαλιστικά.

Με βάση όλα τα παραπάνω συμπεραίνουμε ότι η ασφάλεια της εφοδιαστικής αλυσίδας δεν μπορεί να αντιμετωπίζεται ως μια περιφερειακή απαίτηση συμμόρφωσης, αλλά ως πολυεπίπεδη λειτουργία διακυβέρνησης και ανθεκτικότητας που διατρέχει οριζόντια procurement, legal, IT, OT, risk management και incident response. Αυτό είναι ιδιαίτερα κρίσιμο διότι ένα ολοκληρωμένο πλαίσιο ασφάλειας για OT/IT περιβάλλοντα οφείλει να ενσωματώνει όχι μόνο τεχνικούς ελέγχους, αλλά και δομές διακυβέρνησης προμηθευτών, συμβατικές απαιτήσεις, risk-based αξιολόγηση και μηχανισμούς συνεχούς εποπτείας των εξαρτήσεων από την εφοδιαστική αλυσίδα.

ΚΕΦΑΛΑΙΟ 6 – Αξιολόγηση, Συμμόρφωση & Πιστοποιήσεις OT/IT

Στο παρόν κεφάλαιο εξετάζεται πώς οι απαιτήσεις ασφάλειας που περιγράφηκαν στα προηγούμενα κεφάλαια μεταφράζονται σε συγκεκριμένους ελέγχους, τεκμήρια και δραστηριότητες αξιολόγησης σε ένα OT/IT περιβάλλον. Η ανάλυση βασίζεται στον OT overlay του NIST SP 800-82r3 πάνω στο NIST SP 800-53, στις κατηγορίες του NIST Cybersecurity Framework 2.0 και στις Foundational Requirements και Security Levels της IEC 62443, ώστε να δημιουργηθεί μια συνεκτική εικόνα "τι ελέγχουμε, πώς το ελέγχουμε και πώς το αποδεικνύουμε". Επιπλέον, παρουσιάζονται ιδιαιτερότητες των OT audits και οι περιορισμοί των δοκιμών διείσδυσης σε βιομηχανικά περιβάλλοντα, με έμφαση στη χρήση αντισταθμιστικών μέτρων και στην τεκμηρίωση της ανθεκτικότητας.

6.1 Mapping controls και τεκμηρίωση συμμόρφωσης

Η χαρτογράφηση ελέγχων (mapping) αποτελεί τον συνδετικό κρίκο ανάμεσα στα υψηλού επιπέδου πλαίσια (NIST CSF, ISO/IEC 27001–27002, IEC 62443) και στην πραγματική εικόνα των μέτρων που εφαρμόζονται σε ένα OT/IT περιβάλλον. Ο OT overlay του NIST SP 800-82r3 πάνω στο NIST SP 800-53 παρέχει OT-specific "συζητήσεις" για κάθε έλεγχο και προτείνει πότε απαιτούνται αντισταθμιστικά μέτρα (compensating controls) λόγω τεχνικών ή λειτουργικών περιορισμών των OT συστημάτων. Σε συνδυασμό με τα Foundational Requirements της IEC 62443, αυτό επιτρέπει τη δημιουργία ενός πρακτικού πίνακα που συνδέει CSF outcomes, FR/SL και συγκεκριμένους ελέγχους, μαζί με τα αντίστοιχα αποδεικτικά στοιχεία. Η συμμόρφωση σε μεικτά περιβάλλοντα OT/IT δεν είναι "checklist", αλλά διαδικασία μετασχηματισμού ενός πλαισίου αρχών σε ελέγξιμα τεκμήρια, πολιτικές, διαδικασίες, ρόλους, logs, αρχεία αλλαγών, αρχιτεκτονικά σχέδια, και αποτελέσματα δοκιμών/ασκήσεων. Το ISO/IEC 27001, ως διεθνές πρότυπο ISMS, δίνει τις απαιτήσεις ώστε η διαχείριση κινδύνου και οι έλεγχοι ασφάλειας να μην είναι αποσπασματικοί, αλλά οργανωμένοι, ελεγχόμενοι και αντικείμενο συνεχούς βελτίωσης.

Το mapping, ως μέθοδος, μπορεί να διατυπωθεί ως εξής: το CSF 2.0 ορίζει "τι outcomes θέλουμε", το ISO/IEC 27001 ορίζει "πώς οργανώνουμε το σύστημα διαχείρισης ώστε να τα πετυχαίνουμε", και το ISA/IEC 62443 προσφέρει "πώς το υλοποιούμε τεχνικά/μηχανικά στο IACS με τρόπο που αξιολογείται και συντηρείται". Το αποτέλεσμα είναι ένα σύνολο evidence που μπορεί να σταθεί σε audit: risk assessment, scope definition, τεκμηρίωση αρχιτεκτονικών ορίων, πολιτικές απομακρυσμένης πρόσβασης, διαδικασίες incident management, και τεστ αποκατάστασης.

Τέλος, η "συμμόρφωση" σε OT/IT είναι άρρηκτα δεμένη με το supply chain. Εδώ, το ISO/IEC 27036 (ιδίως το 27036-1) λειτουργεί ως θεωρητική και πρακτική γέφυρα: ορίζει το πλαίσιο εννοιών και καθοδήγησης για ασφάλεια σε σχέσεις προμηθευτών, κάτι που είναι κρίσιμο όταν vendor access και lifecycle dependencies είναι συστατικά στοιχεία της OT λειτουργίας.

6.2 Πιστοποιήσεις και σχήματα συμμόρφωσης στο OT οικοσύστημα

Οι έλεγχοι (audits) σε OT περιβάλλοντα δεν μπορούν να βασίζονται αποκλειστικά σε κλασικές IT πρακτικές, καθώς η διαθεσιμότητα, η ασφάλεια και οι φυσικοί περιορισμοί επηρεάζουν άμεσα τι μπορεί να ελεγχθεί και πώς. Το NIST SP 800-82r3, στον OT overlay του NIST SP 800-53, εισάγει OT-specific συστάσεις για τον τρόπο που πρέπει να σχεδιάζονται οι αξιολογήσεις ελέγχων (CA-2), η συνεχής παρακολούθηση (CA-7) και η διαχείριση ευρημάτων (CA-5) ώστε να μην διαταράσσεται η λειτουργία κρίσιμων διεργασιών. Αντίστοιχα, η IEC 62443 και το υλικό του Magda για SuC/zones & conduits τονίζουν ότι τα audits πρέπει να πατούν πάνω σε καλά τεκμηριωμένη αρχιτεκτονική (ζώνες, αγωγοί, SL-T) και σε σαφώς ορισμένα evidence spines. Η σειρά ISA/IEC 62443 έχει αποκτήσει βαρύτητα ακριβώς επειδή παρέχει μια ολιστική προσέγγιση κυβερνοασφάλειας για IACS: γεφυρώνει operations με IT και συνδέει process safety με cybersecurity. Σε αντίθεση με "γενικά" πρότυπα ISMS, η IEC 62443 δομεί το πρόβλημα με ρόλους/αντικείμενα OT: asset owners, system integrators, product suppliers, και απαιτήσεις που σχετίζονται με zones/conduits, security levels, secure product development και τεχνικά χαρακτηριστικά συστατικών.

Για τις πιστοποιήσεις, ένα πρακτικό σημείο αναφοράς είναι τα σχήματα ISASecure, τα οποία λειτουργούν ως certification schemes ευθυγραμμισμένα με IEC 62443. Το ISASecure περιγράφει ότι οι αξιολογήσεις προϊόντων και διαδικασιών γίνονται από certification bodies με διαπίστευση (ISO/IEC 17065) και ότι το σχήμα πιστοποιεί

off-the-shelf προϊόντα και lifecycle πρακτικές σύμφωνα με τη σειρά ISA/IEC 62443. Ο OT-specific σχολιασμός στο NIST SP 800-82r3 για τον έλεγχο CA-7 (continuous monitoring) επισημαίνει ότι οι τεχνικές που χρησιμοποιούνται σε IT (εντατική active scanning, agent-based έλεγχοι) μπορεί να είναι ακατάλληλες ή και επικίνδυνες για OT συστήματα. Προτείνονται αντισταθμιστικές προσεγγίσεις, όπως η χρήση παθητικών εργαλείων παρακολούθησης δικτύου, περιοδικά manual log reviews και αξιοποίηση test/digital-twin περιβαλλόντων για πιο “βαριές” δοκιμές, ώστε να στηρίζεται η συνεχής αξιολόγηση χωρίς να τίθεται σε κίνδυνο η ασφάλεια ή η διαθεσιμότητα. Τα ευρήματα αυτής της παρακολούθησης πρέπει να τροφοδοτούνται σε ένα structured plan of action and milestones (CA-5), με σαφή καταγραφή των περιπτώσεων όπου επιλέγονται compensating controls αντί της “βέλτιστης” αλλά μη εφαρμόσιμης λύσης.

Σημαντικό εδώ είναι να μην παρουσιαστεί η πιστοποίηση ως αυτοσκοπός. Η αξία της σε OT/IT έγκειται στη μετατροπή αφηρημένων απαιτήσεων σε “assurance”: απαιτήσεις τεκμηρίωσης, ελέγχου διαδικασιών, traceability και επαληθευσιμότητας. Αυτό είναι ιδιαίτερα κρίσιμο σε manufacturing περιβάλλοντα όπου οι αλυσίδες εξάρτησης (vendors, updates, remote support) είναι ενδογενείς και το security posture κρίνεται τόσο από τον operator όσο και από τον προμηθευτή.

6.3 Penetration testing σε OT

Οι δοκιμές διείσδυσης σε OT περιβάλλοντα αποτελούν ειδική κατηγορία αξιολόγησης, καθώς ο κίνδυνος να προκληθούν ανεπιθύμητες διακοπές ή και καταστροφικές αστοχίες είναι πολύ μεγαλύτερος σε σύγκριση με τα IT δίκτυα. Ο Brooks και ο Craig επισημαίνουν ότι σε ICS περιβάλλοντα, κάθε ενεργή δοκιμή που μπορεί να επηρεάσει controllers, field devices ή κρίσιμα δίκτυα πρέπει είτε να εκτελείται σε απομονωμένα lab / staging περιβάλλοντα είτε να πραγματοποιείται με αυστηρό change control και παρουσία operations/safety προσωπικού. Για τον λόγο αυτό, πολλοί οργανισμοί προτιμούν μια υβριδική προσέγγιση που συνδυάζει configuration reviews, passive reconnaissance και περιορισμένο, “χειρουργικό” penetration testing σε συγκεκριμένα τμήματα της αρχιτεκτονικής.

Η ωριμότητα ασφάλειας σε OT/IT δεν αποδεικνύεται από ένα έγγραφο πολιτικής, αλλά από τη δυνατότητα του οργανισμού να επαναλαμβάνει αξιόπιστα κρίσιμες λειτουργίες: να αξιολογεί κίνδυνο, να επιβάλλει όρια, να ανιχνεύει αποκλίσεις, να αποκρίνεται, και να ανακάμπτει με ελεγχόμενο τρόπο. Το NIST CSF 2.0 στηρίζεται σε αυτήν την επαναληπτική λογική: επιδιώκει να βοηθήσει οργανισμούς να κατανοήσουν, να προτεραιοποιήσουν και να επικοινωνήσουν τις προσπάθειες κυβερνοασφάλειας ως outcomes, άρα να μπορούν να μετρήσουν πρόοδο και να την αναθεωρούν.

Το incident management, ως πεδίο audit, αποκτά επιπλέον θεσμική υποστήριξη από το ISO/IEC 27035-1:2023, το οποίο ορίζει βασικές αρχές και διαδικασίες για structured προσέγγιση προετοιμασίας, ανίχνευσης, αναφοράς, αξιολόγησης και απόκρισης σε περιστατικά, καθώς και “lessons learned” που επιστρέφουν στη βελτίωση του συστήματος. Σε OT/IT, αυτή η «επιστροφή γνώσης» είναι κομβική, διότι μετατρέπει ένα περιστατικό από μεμονωμένο γεγονός σε μηχανισμό αναθεώρησης αρχιτεκτονικών ροών, προμηθευτικών πρακτικών και διαδικασιών αλλαγών.

Ιδιαίτερη θέση στην ωριμότητα έχει το patch/vulnerability handling, επειδή είναι σημείο τριβής μεταξύ IT ρυθμού αλλαγής και OT ανάγκης σταθερότητας. Το IEC TR 62443-2-3 (patch management in the IACS environment) αναδεικνύει ότι η ανταλλαγή πληροφορίας patches μεταξύ asset owners και product suppliers πρέπει να ακολουθεί ορισμένη δομή και ότι οι δραστηριότητες patching απαιτούν συντονισμό και διαδικασίες που είναι συμβατές με τη λειτουργία του IACS. Αυτό ακριβώς είναι “engineering feedback loop”: οι έλεγχοι δεν ορίζονται μία φορά, αλλά επανεξετάζονται με βάση ευπάθειες, incidents, changes και νέες εξαρτήσεις.

Το τελικό συμπέρασμα του κεφαλαίου είναι ότι η συμμόρφωση και η πιστοποίηση, όταν εντάσσονται σε ενοποιημένη προσέγγιση OT/IT, λειτουργούν ως εργαλεία διακυβέρνησης και μηχανικής: ορίζουν απαιτήσεις, παράγουν evidence, και στηρίζουν συνεχές improvement. Ο οργανισμός κερδίζει όχι μόνο “compliance posture”, αλλά ικανότητα πρόβλεψης/αντοχής: να απορροφά διαταραχές, να περιορίζει εξάπλωση, να αποκαθιστά παραγωγή και να μαθαίνει με τρόπο συστηματικό.

ΚΕΦΑΛΑΙΟ 7 – OT/IT Security Program και GRC

Η σύγκλιση των Information Technology (IT) και Operation Technology (OT) έχει δημιουργήσει ένα συνεκτικό αλλά ιδιαίτερα σύνθετο περιβάλλον, όπου η ασφάλεια δεν μπορεί να αντιμετωπίζεται μόνο ως ζήτημα τεχνικών ελέγχων, αλλά ως οργανωσιακός μηχανισμός διακυβέρνησης κινδύνου και συμμόρφωσης. Οι κλασικές προσεγγίσεις που βασίζονται αποκλειστικά σε IT-centric μέτρα δεν επαρκούν για βιομηχανικά δίκτυα και Industrial Control Systems, τα οποία δίνουν προτεραιότητα στη διαθεσιμότητα, την ασφάλεια και τον ντετερμινιστικό έλεγχο φυσικών διεργασιών. Για τον λόγο αυτό, η σύγχρονη πρακτική προτείνει την υιοθέτηση ενός ολοκληρωμένου OT/ICS Security Program, το οποίο στηρίζεται σε αρχές Governance, Risk and Compliance (GRC) και αξιοποιεί πρότυπα όπως το NIST Cybersecurity Framework 2.0, το NIST SP 800-82r3 και την οικογένεια IEC 62443 για να επιτύχει συνεπή διαχείριση κινδύνου σε IT και OT.

Στο κεφάλαιο αυτό παρουσιάζεται πώς μπορεί να δομηθεί ένα τέτοιο πρόγραμμα ασφάλειας OT/IT με κέντρο το GRC, ξεκινώντας από τη θεμελιώδη έννοια της διακυβέρνησης, προχωρώντας στην ενοποίηση και αξιοποίηση πλαισίων και προτύπων, αναλύοντας τις πρακτικές risk management σε περιβάλλοντα ζωνών και conduits και καταλήγοντας στην ουσιαστική αντιμετώπιση της συμμόρφωσης μέσω αποδεικτικών στοιχείων και audits. Η ανάλυση βασίζεται σε πρόσφατες εργασίες που προτείνουν ολοκληρωμένα IT/OT GRC frameworks, σε οδηγίες οργανισμών όπως NIST και ENISA, καθώς και σε case studies εφαρμογής της IEC 62443 σε πολυεθνικούς οργανισμούς.

7.1 GRC σε περιβάλλοντα OT/IT

Ο όρος Governance, Risk and Compliance περιγράφει ένα ενιαίο πλαίσιο μέσα από το οποίο ο οργανισμός καθορίζει ποιος αποφασίζει για την ασφάλεια, πώς αναγνωρίζονται και αντιμετωπίζονται οι κίνδυνοι και με ποιον τρόπο αποδεικνύεται η συμμόρφωση με εσωτερικές και εξωτερικές απαιτήσεις. Σε περιβάλλοντα OT/ICS αυτό το πλαίσιο αποκτά επιπλέον διαστάσεις, καθώς η παραβίαση ενός συστήματος μπορεί να μεταφραστεί σε πραγματικές φυσικές συνέπειες, όπως βλάβες εξοπλισμού, περιβαλλοντικά συμβάντα ή κίνδυνο για την ανθρώπινη ασφάλεια, και όχι μόνο σε απώλεια δεδομένων ή φήμης. Η βιβλιογραφία υπογραμμίζει ότι παραδοσιακά μοντέλα διακυβέρνησης που εστιάζουν μόνο σε IT assets δεν μπορούν να συλλάβουν επαρκώς τις ιδιαιτερότητες των industrial systems, με αποτέλεσμα κενά μεταξύ αρμοδιοτήτων, ελλιπή ορατότητα στο διοικητικό επίπεδο και ασυνεπή συντονισμό μεταξύ IT και OT ομάδων.

Η έκδοση 2.0 του NIST Cybersecurity Framework επιχειρεί να καλύψει αυτό το κενό, εισάγοντας τη νέα λειτουργία Govern, η οποία τοποθετεί τη διακυβέρνηση του κυβερνοκινδύνου στο ίδιο επίπεδο με τους υπόλοιπους επιχειρηματικούς κινδύνους και καθιστά σαφές ότι η ασφάλεια δεν είναι μόνο τεχνικό ζήτημα, αλλά και θέμα στρατηγικής, οργανωσιακού πλαισίου και εποπτείας. Η λειτουργία Govern δομείται γύρω από αποτελέσματα όπως η κατανόηση του οργανωσιακού context, η διαμόρφωση risk management strategy, ο καθορισμός risk appetite και tolerance και η σαφής ανάθεση ρόλων, ευθυνών και αρμοδιοτήτων, τα οποία ενημερώνουν την υλοποίηση των υπόλοιπων λειτουργιών Identify, Protect, Detect, Respond και Recover. Αυτή η προοπτική είναι ιδιαίτερα σημαντική για OT περιοχές, όπου αποφάσεις όπως η απομόνωση ζωνών, οι κανόνες πρόσβασης σε engineering workstations ή η στρατηγική patching παίζουν ρόλο τόσο στον κυβερνοκίνδυνο όσο και στην επιχειρησιακή συνέχεια και την ασφάλεια.

Παράλληλα, μελέτες που έχουν ως στόχο την ενοποίηση IT και OT διακυβέρνησης προτείνουν ολοκληρωμένα I-GRC frameworks, στα οποία τα πρότυπα IT ασφάλειας όπως το ISO/IEC 27001 παρέχουν γενικό έδαφος για την αντιμετώπιση κινδύνων, ενώ τα OT-εξειδικευμένα πρότυπα όπως η IEC 62443 καλύπτουν ζητήματα όπως η ασφάλεια αυτοματισμών, η ακεραιότητα των ελέγχων και η τμηματοποίηση των control networks. Αυτή η συνδυαστική προσέγγιση επιτρέπει την ευθυγράμμιση των τεχνικών controls με τους επιχειρηματικούς στόχους, τη διευκόλυνση της συμμόρφωσης με ρυθμιστικές απαιτήσεις και τη βελτίωση των διαδικασιών incident response σε IT και OT. Ειδικά σε κρίσιμες υποδομές, όπου το OT είναι πυρήνας της παρεχόμενης υπηρεσίας, η υιοθέτηση ενός τέτοιου GRC πλαισίου είναι προϋπόθεση για βιώσιμη, όχι απλώς “συμμορφωτική” ασφάλεια.

7.2 Πλαίσια και πρότυπα για τη διακυβέρνηση OT/IT ασφάλειας

Η πρακτική υλοποίηση ενός OT/IT Security Program βασισμένου σε GRC δεν μπορεί να στηρίζεται σε ένα μόνο πρότυπο ή πλαίσιο, αλλά σε συνδυασμό συμπληρωματικών αναφορών που καλύπτουν τόσο την υψηλού επιπέδου στρατηγική όσο και τους τεχνικούς ελέγχους. Το NIST Cybersecurity Framework 2.0 προσφέρει ένα γενικό, ευέλικτο πλαίσιο διαχείρισης κυβερνοκινδύνου, στο οποίο οι λειτουργίες Govern, Identify, Protect, Detect, Respond και Recover μεταφράζουν τις απαιτήσεις διακυβέρνησης και ασφάλειας σε συγκεκριμένα αποτελέσματα. Τα αποτελέσματα αυτά υποστηρίζονται από Informative References που συνδέουν κάθε υποκατηγορία με συγκεκριμένα controls από πρότυπα όπως το NIST SP 800-53, το ISO/IEC 27001 και την IEC 62443, επιτρέποντας στους οργανισμούς να κάνουν συστηματικό mapping μεταξύ στρατηγικών στόχων, ελέγχων και αποδεικτικών στοιχείων. Σε περιβάλλοντα OT, όπου οι οργανισμοί διαθέτουν ήδη ετερογενή εσωτερικά πρότυπα, αυτό το mapping λειτουργεί ως κοινή γλώσσα μεταξύ διοίκησης, compliance και τεχνικών ομάδων.

Το NIST SP 800-82r3 εξειδικεύει τις γενικές αρχές του NIST CSF για OT/ICS περιβάλλοντα, παρέχοντας συγκεκριμένη καθοδήγηση για αρχιτεκτονικές άμυνας σε βάθος, μηχανισμούς segmentation, διαχείριση αλλαγών, patching και continuous monitoring με τρόπο που λαμβάνει υπόψη περιορισμούς διαθεσιμότητας και ασφάλειας. Στο παράρτημα του προτύπου βρίσκεται ένα OT overlay των ελέγχων του NIST SP 800-53, όπου για κάθε control και enhancement περιγράφεται πώς πρέπει να προσαρμοστεί στο OT, πότε μπορεί να είναι τεχνικά μη εφαρμόσιμο και πώς μπορούν να αξιοποιηθούν αντισταθμιστικά μέτρα, όπως ενισχυμένος φυσικός έλεγχος πρόσβασης ή διαδικαστικές δικλείδες ασφαλείας. Το overlay αυτό αποτελεί ουσιαστικό εργαλείο για asset owners και integrators που προσπαθούν να εφαρμόσουν ελέγχους διακυβέρνησης, risk assessment, continuous monitoring και incident response σε περιβάλλοντα όπου ο άμεσος επηρεασμός παραγωγής ή ασφάλειας δεν είναι αποδεκτός.

Παράλληλα, η οικογένεια IEC 62443 λειτουργεί ως πρότυπο αναφοράς για την ασφάλεια Industrial Automation and Control Systems, καλύπτοντας τόσο διοικητικές όσο και τεχνικές πτυχές. Η αναθεωρημένη IEC 62443-2-1:2024 περιγράφει αναλυτικά πώς ένας asset owner μπορεί να δομήσει και να λειτουργήσει ένα Security Management System για OT, με οκτώ βασικά στοιχεία προγράμματος, τα οποία περιλαμβάνουν οργανωτικά μέτρα, πολιτικές και διαδικασίες, διαχείριση αλλαγών, σχέδια συνέχειας και ανάκαμψης, εκπαίδευση και διαχείριση προμηθευτών. Τα επόμενα μέρη, όπως η IEC 62443-3-2 και 3-3, επεκτείνουν το πλαίσιο, καθορίζοντας πώς εκτελείται risk assessment σε επίπεδο ζωνών και conduits, πώς ορίζονται τα Security Levels και ποιες τεχνικές απαιτήσεις πρέπει να πληροί κάθε ζώνη για να επιτευχθεί το αντίστοιχο SL.

Ευρωπαϊκοί οργανισμοί, όπως η ENISA, συμπληρώνουν τις παραπάνω αναφορές με οδηγίες για τη διαχείριση κινδύνου και την εφαρμογή μέτρων σε φορείς κρίσιμων υπηρεσιών, σύμφωνα με το κανονιστικό πλαίσιο της ΕΕ. Οι οδηγίες αυτές τονίζουν την ανάγκη υιοθέτησης συστηματικής μεθοδολογίας risk management, τη σαφή διατύπωση risk appetite από τα διοικητικά όργανα και τη σύνδεση της πολιτικής κινδύνου με αναλύσεις επιχειρησιακών επιπτώσεων, καθώς και την τακτική επανεξέταση και τεκμηρίωση του risk treatment plan. Επιπλέον, καθορίζουν ποια αποδεικτικά στοιχεία αναμένονται για να θεωρηθούν επαρκείς οι διαδικασίες risk management και αναθεώρησης από ρυθμιστικές αρχές. Σε συνδυασμό με το NIST CSF και την IEC 62443, οι οδηγίες ENISA προσφέρουν ειδικά για ευρωπαϊκούς οργανισμούς μια συνεκτική γέφυρα μεταξύ τεχνικών απαιτήσεων και κανονιστικών υποχρεώσεων.

Τέλος, πρωτοβουλίες όπως η ISAGCA και case studies από βιομηχανίες όπως η Campari Group δείχνουν στην πράξη πώς η IEC 62443-2-1 μπορεί να χρησιμοποιηθεί ως πλαίσιο διακυβέρνησης σε παγκόσμιο επίπεδο, ορίζοντας ρόλους και ευθύνες σε εταιρικό και εργοστασιακό επίπεδο, συνδέοντας ωριμότητα διαδικασιών με συγκεκριμένες απαιτήσεις και υλοποιώντας σταδιακή ανάπτυξη πολιτικών και διαδικασιών OT ασφάλειας. Η εμπειρία αυτή αναδεικνύει τη μετάβαση από μια προσέγγιση “checklist-συμμόρφωσης” προς μια προσέγγιση βασισμένη στην ωριμότητα, τη συνεχή βελτίωση και τη μετρήσιμη μείωση κινδύνου. Έτσι, η διακυβέρνηση OT ασφάλειας αποκτά ουσιαστικό περιεχόμενο, με σαφή αναφορά σε δομές, διαδικασίες και μετρικές, αντί για γενικές δηλώσεις προθέσεων.

7.3 Governance: δομή, ρόλοι και ενιαίο OT/IT πρόγραμμα ασφάλειας

Η διακυβέρνηση της ασφάλειας σε ένα περιβάλλον OT/IT δεν αφορά μόνο το ποιος "κατέχει" τα συστήματα, αλλά και το πώς λαμβάνονται αποφάσεις, πώς καθορίζονται προτεραιότητες και πώς εξασφαλίζεται ότι οι τεχνικές και οργανωτικές παρεμβάσεις υποστηρίζουν τους επιχειρησιακούς στόχους. Στο πλαίσιο του NIST CSF 2.0, η λειτουργία Govern αναγνωρίζει ότι ο κυβερνοκίνδυνος είναι ένας από τους βασικούς επιχειρηματικούς κινδύνους που πρέπει να παρακολουθούνται σε επίπεδο διοικητικού συμβουλίου, με σαφή διατύπωση των αποφάσεων για risk appetite, risk tolerance, και της σχέσης τους με τη στρατηγική και τις επενδύσεις της εταιρείας. Η λειτουργία αυτή καλύπτει επίσης θέματα όπως η διαχείριση κινδύνων στην εφοδιαστική αλυσίδα, η ενσωμάτωση της ασφάλειας σε κύκλους ζωής ψηφιακών προϊόντων και η συνεχής βελτίωση της στρατηγικής ασφάλειας βάσει απόδοσης και νέων απειλών, στοιχεία που είναι ιδιαίτερα κρίσιμα για OT, όπου οι υποδομές είναι μακρόβιες και συχνά εξαρτημένες από προμηθευτές.

Στη βιβλιογραφία για OT/ICS GRC αναδεικνύεται η ανάγκη δημιουργίας διεπιστημονικής δομής διακυβέρνησης, με Steering Committees ή Security Boards που περιλαμβάνουν εκπροσώπους από OT engineering, operations, ασφάλεια, συμμόρφωση και IT, ώστε να διασφαλίζεται ότι οι αποφάσεις για πολιτικές, επενδύσεις και προτεραιότητες μέτρων λαμβάνουν υπόψη τόσο τις επιχειρησιακές όσο και τις τεχνικές και ρυθμιστικές διαστάσεις. Τέτοιες δομές επιτρέπουν τη συνεχή αναθεώρηση του προγράμματος ασφάλειας, τη σύνδεση των δεικτών απόδοσης (KPIs/KRIs) με τους επιχειρησιακούς στόχους και τη διασφάλιση ότι οι αποφάσεις για παρεμβάσεις σε OT περιβάλλοντα λαμβάνονται με γνώμονα τις πραγματικές επιπτώσεις στην παραγωγή και την ασφάλεια. Σε αυτό το πλαίσιο, η IEC 62443-2-1 προβλέπει ρητά την ύπαρξη σαφούς οργανωσιακής δομής ασφάλειας, με ορισμένους ρόλους, διαδικασίες συντονισμού και μηχανισμούς λογοδοσίας σε εταιρικό και τοπικό επίπεδο.

Ένα χαρακτηριστικό στοιχείο ώριμης διακυβέρνησης είναι η δυνατότητα της διοίκησης να γεφυρώνει τη θεωρία με την πράξη, δηλαδή να εξασφαλίζει ότι οι πολιτικές και οι αποφάσεις της μεταφράζονται σε συγκεκριμένα μέτρα και διαδικασίες στο επίπεδο των εγκαταστάσεων. Case studies εφαρμογής της IEC 62443 δείχνουν ότι οργανισμοί που κατάφεραν να ορίσουν σαφείς ρόλους σε corporate και plant επίπεδο, να εκδώσουν κατευθυντήριες γραμμές για σχέδια συνέχειας και ανάκαμψης, διαδικασίες change management και εκπαιδευτικά προγράμματα OT ασφάλειας, ήταν σε θέση να αναπτύξουν σταδιακά πολιτικές και διαδικασίες OT ασφάλειας που εφαρμόζονται ομοιόμορφα σε παγκόσμιο επίπεδο, ανεξάρτητα από τις τοπικές ιδιαιτερότητες. Αυτή η προσέγγιση συνδέει την έννοια της διακυβέρνησης με μετρήσιμα επίπεδα ωριμότητας, επιτρέποντας την αντικειμενική αξιολόγηση της προόδου ενός OT/IT Security Program.

Τα πραγματικά περιστατικά κυβερνοεπιθέσεων σε κρίσιμες υποδομές δείχνουν επίσης τις συνέπειες αποτυχημένης ή αποσπασματικής διακυβέρνησης. Σε επιθέσεις ransomware σε αγωγούς ενέργειας και άλλες βιομηχανικές εγκαταστάσεις, η έλλειψη ενοποιημένου IT/OT governance, η ανεπαρκής ορατότητα σε πραγματικό χρόνο και η απουσία δοκιμασμένων σχεδίων απόκρισης οδήγησαν σε εκτεταμένες διακοπές λειτουργίας, αυξημένο κόστος ανάκαμψης και έντονη πίεση από ρυθμιστικές αρχές και κοινή γνώμη. Αντίθετα, μελέτες αγοράς και βέλτιστων πρακτικών για OT/ICS security προτείνουν ότι η εφαρμογή ισχυρού OT GRC πλαισίου, με σαφείς γραμμές ευθύνης, ενιαίο risk register και τακτικές ασκήσεις incident response που περιλαμβάνουν και OT, αποτελεί βασική προϋπόθεση για αποτελεσματική άμυνα σε βάθος και ανθεκτικότητα σε επιθέσεις.

7.4 Διαχείριση κινδύνου: OT ιδιαιτερότητες, Security Levels και ενοποιημένο risk register

Η διαχείριση κινδύνου σε OT περιβάλλοντα διαφοροποιείται σημαντικά από την αντίστοιχη σε καθαρά IT πλαίσια, καθώς οι απειλές και οι ευπάθειες πρέπει να αξιολογούνται σε σχέση με συνέπειες που περιλαμβάνουν όχι μόνο απώλεια δεδομένων, αλλά και διακοπή υπηρεσίας, υλικές ζημιές, περιβαλλοντικές επιπτώσεις και κίνδυνο για την ανθρώπινη ζωή. Το NIST SP 800-82r3 τονίζει ότι η risk assessment διαδικασία για OT πρέπει να λαμβάνει υπόψη τις συγκεκριμένες λειτουργικές απαιτήσεις, όπως η ανάγκη συνεχούς λειτουργίας, οι περιορισμένες δυνατότητες patching, η χρήση παλαιού εξοπλισμού και η ύπαρξη μη δικτυακών ή δυσπρόσιτων στοιχείων, όπως πεδία αισθητήρων και απομακρυσμένοι σταθμοί. Παράλληλα, η ENISA, στο πλαίσιο του ευρωπαϊκού κανονιστικού πλαισίου, προτείνει μια δομημένη προσέγγιση risk management που

περιλαμβάνει τεκμηριωμένη μεθοδολογία, καθορισμό risk tolerance και risk criteria, τεκμηρίωση και τακτική αναθεώρηση του risk treatment plan, με έγκριση και αποδοχή του υπολειπόμενου κινδύνου από τα αρμόδια διοικητικά σώματα.

Η IEC 62443-3-2 εισάγει μια συστηματική προσέγγιση στην αξιολόγηση και αντιμετώπιση κινδύνου σε OT, χρησιμοποιώντας την έννοια του System under Consideration, την κατάτμηση σε ζώνες και conduits και τον καθορισμό Security Levels για κάθε ζώνη ή conduit. Η σχέση μεταξύ του αρχικού (unmitigated) κινδύνου και του αποδεκτού (tolerable) κινδύνου εκφράζεται μέσω ενός Cyber Risk Reduction Factor, ο οποίος αντιστοιχίζεται σε Security Level Target μέσω προκαθορισμένου πίνακα, διευκολύνοντας τη μετάφραση των αποτελεσμάτων του risk assessment σε συγκεκριμένες απαιτήσεις ασφαλείας. Αυτή η προσέγγιση επιτρέπει στους οργανισμούς να ορίζουν διαφορετικά επίπεδα προστασίας για ζώνες υψηλής κρισιμότητας, όπως safety συστήματα ή κρίσιμες διεργασίες, και για λιγότερο κρίσιμα συστήματα, όπως υποστήριξη ποιότητας ή αναλύσεις δεδομένων, ανάλογα με τις συνέπειες αστοχίας.

Πρόσφατες επιστημονικές εργασίες για την ενοποίηση IT και OT GRC προτείνουν ένα Integrated IT-OT GRC Framework, στο οποίο τα μοντέλα κινδύνου και συμμόρφωσης ευθυγραμμίζονται, έτσι ώστε ένα κοινό risk register να καλύπτει IT και OT assets, ενώ τα χρησιμοποιούμενα πρότυπα (ISO/IEC 27001 για IT, IEC 62443 για OT) αντιμετωπίζονται ως συμπληρωματικά μέσα επίτευξης των ίδιων υψηλού επιπέδου στόχων. Οι συγγραφείς επισημαίνουν ότι παραδοσιακά IT-centric μοντέλα κινδύνου αποτυγχάνουν να ενσωματώσουν περιορισμούς όπως οι απαιτήσεις real-time, η ασφάλεια και η ανάγκη για deterministic control και προτείνουν ότι η ενσωμάτωση της IEC 62443 στο GRC πλαίσιο επιτρέπει την καλύτερη αποτύπωση και αντιμετώπιση αυτών των παραγόντων. Με αυτόν τον τρόπο, η risk management διαδικασία παύει να είναι κατακερματισμένη και δημιουργεί ενιαία εικόνα κινδύνου για IT και OT.

Σε πρακτικό επίπεδο, η εφαρμογή των παραπάνω αρχών φαίνεται σε πραγματικά σενάρια αξιολόγησης κινδύνου σε βιομηχανικές εγκαταστάσεις. Για παράδειγμα, σε μια βιομηχανία χημικών ουσιών, οι ζώνες που περιλαμβάνουν Safety Instrumented Systems και κρίσιμα control loops αξιολογήθηκαν ως υψηλής κρισιμότητας, με σοβαρές συνέπειες σε περίπτωση αστοχίας, ενώ ζώνες που αφορούσαν συστήματα ποιότητας ή analytics κρίθηκαν λιγότερο κρίσιμες από άποψη ασφάλειας αλλά σημαντικές από άποψη οικονομικού και ρυθμιστικού κινδύνου. Με βάση αυτή την ανάλυση, ορίστηκαν υψηλότερα Security Levels για τις πρώτες ζώνες, με αυστηρή φυσική και λογική απομόνωση, περιορισμένη χρήση ενεργών δοκιμών διείσδυσης και έμφαση σε αναλύσεις διαμόρφωσης και αλλαγών, ενώ οι λιγότερο κρίσιμες ζώνες υπέστησαν πιο εκτεταμένες δοκιμές και αυτοματοποιημένες σαρώσεις ευπαθειών. Το αποτέλεσμα ήταν ένα πιο ρεαλιστικό και στοχευμένο πρόγραμμα μέτρων, ευθυγραμμισμένο με τον πραγματικό επιχειρησιακό κίνδυνο κάθε τμήματος του συστήματος.

7.5 Συμμόρφωση, audits και αποδείξεις σε OT/IT περιβάλλοντα

Η συμμόρφωση σε ένα OT/IT Security Program δεν εξαντλείται στην ικανοποίηση μιας λίστας ελέγχου, αλλά αφορά στη συνεπή και αποδείξιμη ευθυγράμμιση των πρακτικών ασφαλείας με κανονιστικές απαιτήσεις, κλαδικά πρότυπα και εσωτερικές πολιτικές. Σε κλάδους κρίσιμων υποδομών, οι οργανισμοί καλούνται ταυτόχρονα να αποδείξουν συμμόρφωση με ευρωπαϊκές απαιτήσεις, όπως αυτές της NIS2, με κλαδικά ή εθνικά πρότυπα και με τις ίδιες τις πολιτικές και τα risk appetite statements που έχουν εγκρίνει τα διοικητικά τους όργανα. Σε αυτό το πλαίσιο, η συμμόρφωση συνδέεται στενά με το Governance, καθώς η αποδοχή υπολειπόμενου κινδύνου, η έγκριση του risk treatment plan και η παρακολούθηση της αποτελεσματικότητας των μέτρων αποτελούν ευθύνη της διοίκησης και όχι μόνο της τεχνικής ομάδας ασφάλειας.

Το NIST CSF 2.0 παρέχει ένα χρήσιμο εργαλείο για την υποστήριξη της συμμόρφωσης, μέσω των Informative References που συνδέουν κάθε υποκατηγορία με συγκεκριμένους ελέγχους από άλλα πρότυπα. Οι οργανισμοί μπορούν να χρησιμοποιήσουν αυτό το mapping για να δημιουργήσουν πίνακες που συνδέουν τα επιθυμητά outcomes, όπως η έγκαιρη ανίχνευση και απόκριση σε συμβάντα ή η προστασία κρίσιμων assets, με συγκεκριμένους ελέγχους από το NIST SP 800-53, την IEC 62443 ή το ISO/IEC 27001, καθώς και με τα αντίστοιχα αποδεικτικά στοιχεία που απαιτούνται για audits. Στο πλαίσιο OT, αυτά τα evidence artifacts μπορεί να περιλαμβάνουν εγκεκριμένες αλλαγές σε firewalls και conduits, δοκιμασμένα σχέδια backup και restore, αναφορές incident response, καταγραφές πρόσβασης σε συστήματα ελέγχου και αξιολογήσεις προμηθευτών

και τρίτων. Με αυτόν τον τρόπο, η συμμόρφωση δεν είναι αφηρημένη αλλά συνδέεται με συγκεκριμένα τεκμήρια από την πραγματική λειτουργία της εγκατάστασης.

Η IEC 62443-2-1 και το NIST SP 800-82r3 υπογραμμίζουν ότι οι διαδικασίες audit και αξιολόγησης σε OT περιβάλλοντα πρέπει να σχεδιάζονται προσεκτικά, ώστε να ελαχιστοποιούν τον λειτουργικό κίνδυνο. Σε πολλές περιπτώσεις, οι ενεργές δοκιμές που είναι σύνηθες σε IT περιβάλλοντα είναι ακατάλληλες ή επικίνδυνες για OT, και έτσι οι αξιολογήσεις βασίζονται σε ανασκοπήσεις τεκμηρίωσης, αναλύσεις διαμόρφωσης, συνεντεύξεις και παρατήρηση, με περιορισμένη και αυστηρά ελεγχόμενη χρήση ενεργών δοκιμών. Αυτή η προσέγγιση δεν μειώνει την αξία των audits, αλλά απαιτεί υψηλότερο επίπεδο ωριμότητας σε διαδικασίες και τεκμηρίωση, ώστε οι auditors να μπορούν να αξιολογήσουν την αποτελεσματικότητα των μέτρων χωρίς να διακινδυνεύσουν την ασφάλεια ή τη διαθεσιμότητα των διεργασιών.

Πρόσφατες οδηγίες για την αντιμετώπιση ransomware σε οργανισμούς με OT υποδομές υπογραμμίζουν επίσης ότι η ουσιαστική συμμόρφωση απαιτεί περισσότερο από γενικές αναφορές σε segmentation και backups. Οργανισμοί που είχαν σε ισχύ πολιτικές για τμηματοποίηση δικτύων και αντίγραφα ασφαλείας, αλλά δεν διέθεταν πρακτική απομόνωση κρίσιμων ζωνών ή offline/immutable backups, διαπίστωσαν ότι σε πραγματικές επιθέσεις η ανάκαμψη ήταν αργή και επώδυνη, με σημαντικές επιχειρησιακές διακοπές και αυξημένο κόστος. Αντίθετα, αναλύσεις δείχνουν ότι οργανισμοί με σωστά απομονωμένα, μη τροποποιήσιμα αντίγραφα ασφαλείας και καλά σχεδιασμένη τμηματοποίηση με zero trust αρχές ανέκαμψαν πιο γρήγορα και είχαν πολύ μικρότερη πιθανότητα να πληρώσουν λύτρα. Αυτές οι παρατηρήσεις αναδεικνύουν ότι η συμμόρφωση πρέπει να αξιολογείται βάσει πραγματικών δοκιμών και απόδοσης και όχι μόνο βάσει ύπαρξης πολιτικών και διαδικασιών στα χαρτιά.

Συνολικά, η διάσταση της συμμόρφωσης σε ένα OT/IT Security Program συνδέεται άρρηκτα με τη διακυβέρνηση και τη διαχείριση κινδύνου. Ένα ώριμο GRC πλαίσιο για OT/ICS δεν περιορίζεται στην ικανοποίηση τυπικών απαιτήσεων, αλλά αξιοποιεί πρότυπα όπως το NIST CSF 2.0, το NIST SP 800-82r3, την IEC 62443-2-1 και τις οδηγίες ENISA και CISA, ώστε να δομεί διαδικασίες και τεκμήρια που επιτρέπουν την ουσιαστική αξιολόγηση και συνεχή βελτίωση της ασφάλειας. Έτσι, καταλήγουμε στην παραδοχή ότι η επιτυχία ενός OT/IT Security Program δεν κρίνεται μόνο από το εάν υπάρχουν πολιτικές ή εάν συμπληρώνονται ερωτηματολόγια, αλλά από το εάν ο οργανισμός μπορεί να αποδείξει, με συνεκτικό τρόπο, ότι διαχειρίζεται τον κυβερνοκίνδυνο με τρόπο συμβατό με τους επιχειρησιακούς του στόχους και τις ρυθμιστικές του υποχρεώσεις.

7.6 Προτεινόμενο OT/IT framework

Στο πλαίσιο της παρούσας εργασίας προτείνεται ένα ολοκληρωμένο πλαίσιο GRC για περιβάλλοντα OT/IT, το οποίο επιδιώκει να ενοποιήσει τις απαιτήσεις διακυβέρνησης, διαχείρισης κινδύνου και συμμόρφωσης σε ένα ενιαίο λειτουργικό μοντέλο. Το προτεινόμενο «OT/IT Integrated GRC Framework for Industrial Environments» βασίζεται σε τρεις διακριτούς αλλά αλληλοεξαρτώμενους πυλώνες, τη διακυβέρνηση (Governance), τη διαχείριση κινδύνου (Risk Management) και τη συμμόρφωση/ελέγχους (Compliance & Controls). Η λογική του πλαισίου ευθυγραμμίζεται με τις αρχές του NIST Cybersecurity Framework 2.0, ιδίως με τη λειτουργία Govern, και ενσωματώνει τις ειδικές απαιτήσεις των προτύπων IEC 62443-2-1 και IEC 62443-3-2 για τα βιομηχανικά περιβάλλοντα.

Επίπεδο	Βασικά Στοιχεία
Επίπεδο 1: Governance	• Καθορισμός ρόλων και αρμοδιοτήτων (CISO, OT managers, Διοίκηση) • Διαμόρφωση και έγκριση ενιαίων πολιτικών ασφάλειας IT/OT • Ορισμός risk appetite και στρατηγικής κυβερνοασφάλειας • Ευθυγράμμιση με τη λειτουργία Govern του NIST CSF 2.0 • Εφαρμογή απαιτήσεων IEC 62443-2-1 για OT security program και PDCA κύκλο
Επίπεδο 2:	• Ενοποιημένο μητρώο κινδύνων IT/OT (integrated risk register) • Κοινή μεθοδολογία αναγνώρισης, ανάλυσης και αξιολόγησης κινδύνων

Risk Management	• Χαρτογράφηση κινδύνων σε Security Levels (SL-T) και απαιτήσεις προστασίας • Ανάλυση ζωνών και conduits σύμφωνα με IEC 62443-3-2 • Ενσωμάτωση διαδικασιών Cybersecurity Supply Chain Risk Management (C-SCRM) βάσει NIST SP 800-161r1
Επίπεδο 3: Compliance & Controls	• Χαρτογράφηση απαιτήσεων προτύπων (ISO/IEC 27001/27002, IEC 62443, NIST CSF, NIST SP 800-82/53) σε συγκεκριμένους ελέγχους • Δημιουργία ενιαίου «χάρτη ελέγχων» IT/OT (control matrix) • Καθορισμός και παρακολούθηση KPIs/KRIs για την απόδοση της ασφάλειας • Συνεχές monitoring και αναφορά προς τη διοίκηση • Υλοποίηση εσωτερικών/εξωτερικών ελέγχων (audits) και υποστήριξη προγραμμάτων πιστοποίησης.

Ο πρώτος πυλώνας, Governance, εστιάζει στον καθορισμό της στρατηγικής και των δομών διακυβέρνησης για την ασφάλεια OT/IT. Σε αυτό το επίπεδο ορίζονται ο ρόλος της διοίκησης, η σχέση μεταξύ CISO, OT managers και παραγωγικών διευθύνσεων, οι πολιτικές ασφάλειας για IT και OT, το risk appetite και οι βασικές αρχές διακυβέρνησης της εφοδιαστικής αλυσίδας και των τρίτων μερών. Η λειτουργία αυτή εναρμονίζεται με τις κατευθύνσεις του NIST CSF 2.0 για το Govern, αλλά και με τις απαιτήσεις του IEC 62443-2-1 για τη δόμηση ενός OT security program με σαφώς καθορισμένους ρόλους, διαδικασίες και κύκλους PDCA.

Ο δεύτερος πυλώνας, Risk Management, αποτελεί το σημείο στο οποίο ενοποιούνται οι διαδικασίες εκτίμησης και αντιμετώπισης κινδύνων μεταξύ IT και OT. Σε αυτό το επίπεδο συγκροτείται ένα κοινό μητρώο κινδύνων (integrated risk register) που καλύπτει τόσο κινδύνους πληροφορικής όσο και κινδύνους λειτουργικών τεχνολογιών, με διασύνδεση προς την ανάλυση κινδύνων IEC 62443-3-2 (ζώνες, conduits, Security Levels) και προς τις κατηγορίες Identify/Protect/Detect/Respond/Recover του NIST CSF. Παράλληλα, ενσωματώνονται πρακτικές C-SCRM σύμφωνα με το NIST SP 800-161r1 και τις κατευθυντήριες της ENISA για την εφοδιαστική αλυσίδα, ώστε η αξιολόγηση κινδύνου να καλύπτει τόσο εσωτερικά assets όσο και εξαρτήσεις από προμηθευτές.

Ο τρίτος πυλώνας, Compliance & Controls, επικεντρώνεται στη χαρτογράφηση των κανονιστικών και προτυποποιητικών απαιτήσεων και στη μετάφρασή τους σε συγκεκριμένους ελέγχους, δείκτες και διαδικασίες παρακολούθησης. Σε αυτό το επίπεδο γίνεται η συσχέτιση των απαιτήσεων των ISO/IEC 27001 και 27002, του NIST CSF 2.0, των NIST SP 800-82/53 και της σειράς IEC 62443 με τις πολιτικές και τις διαδικασίες του οργανισμού, δημιουργώντας έναν ενιαίο «χάρτη ελέγχων» για IT και OT. Επιπλέον, εδώ εντάσσονται οι μηχανισμοί μέτρησης (KPIs/KRIs για OT/IT ασφάλεια), οι εσωτερικοί και εξωτερικοί έλεγχοι συμμόρφωσης, τα προγράμματα πιστοποίησης και η αναφορά προς τη διοίκηση και τις ρυθμιστικές αρχές. Με αυτόν τον τρόπο, το προτεινόμενο πλαίσιο GRC λειτουργεί ως γέφυρα μεταξύ της υψηλού επιπέδου στρατηγικής και των πρακτικών αρχιτεκτονικών και λειτουργικών αποφάσεων που αναλύονται στα προηγούμενα κεφάλαια.

ΚΕΦΑΛΑΙΟ 8 – OT/IT Security για AI, Big Data & Industry 4.0

8.1 Η τέταρτη βιομηχανική επανάσταση ως νέο τοπίο κινδύνου

Η τέταρτη βιομηχανική επανάσταση, γνωστή ευρέως ως Industry 4.0, αναδιαμορφώνει ριζικά τον τρόπο με τον οποίο λειτουργούν βιομηχανικές εγκαταστάσεις και κρίσιμες υποδομές, εισάγοντας μαζική ψηφιακή διασύνδεση, τεχνητή νοημοσύνη, ανάλυση μεγάλων δεδομένων και Industrial Internet of Things ως αναπόσπαστα στοιχεία της παραγωγικής διαδικασίας. Η υπόσχεση αυτής της μετάβασης είναι πραγματική, αυτοματοποίηση, προβλεπτική συντήρηση, ευέλικτη παραγωγή και ανταγωνιστικότητα μέσω δεδομένων πραγματικού χρόνου. Ωστόσο, η ίδια αυτή σύγκλιση ψηφιακού και φυσικού κόσμου δημιουργεί μια ποιοτικά νέα επιφάνεια επίθεσης που, σε αντίθεση με τις παραδοσιακές απειλές πληροφορικής, επεκτείνεται σε φυσικές διεργασίες, βιομηχανικό εξοπλισμό και κρίσιμα συστήματα ελέγχου.

Τα στατιστικά δεδομένα αποκαλύπτουν μια εικόνα ταχύτατης επιδείνωσης. Σύμφωνα με έρευνα της Telstra International σε συνεργασία με την Omdia Research το 80% των βιομηχανικών οργανισμών παγκοσμίως

ανέφερε σημαντική αύξηση περιστατικών ασφάλειας κατά τη διάρκεια του 2024, αντιπροσωπεύοντας μια εκρηκτική άνοδο σε σύγκριση με τα προηγούμενα χρόνια. Εξίσου ανησυχητικό είναι το γεγονός ότι το 75% των επιθέσεων ξεκίνησε από IT συστήματα με στόχο OT υποδομές, αντικατοπτρίζοντας ακριβώς τις νέες αρχιτεκτονικές πραγματικότητες της Industry 4.0. Η σύγκλιση IT/OT δεν αυξάνει μόνο την παραγωγικότητα, αλλά μεταφέρει ταυτόχρονα τους κινδύνους της εταιρικής πληροφορικής απευθείας στο εσωτερικό των βιομηχανικών δικτύων. Παράλληλα, οι ερευνητές εντόπισαν σχεδόν ~180.000 συσκευές ICS/OT εκτεθειμένες μηνιαία παγκοσμίως (Bitsight, 2025), με γνωστές ευπάθειες και παλαιωμένο firmware, ενώ μεταξύ 2024 και 2025 ο αριθμός των εκτεθειμένων ICS συσκευών στο ανοικτό διαδίκτυο αυξήθηκε κατά 12% (Bitsight, 2025).

Το παρόν κεφάλαιο εξετάζει τρεις αλληλένδετες διαστάσεις αυτής της νέας πραγματικότητας. Πρώτον, πώς η Industry 4.0 και το IIoT αναδιαμορφώνουν την επιφάνεια επίθεσης σε OT περιβάλλοντα και τι σημαίνει αυτό για τη δομή ασφάλειας. Δεύτερον, πώς τα Big Data και η Τεχνητή Νοημοσύνη λειτουργούν ταυτόχρονα ως εργαλεία άμυνας και ως νέοι φορείς κινδύνου. Τρίτον, ποια είναι η επικείμενη απειλή των κβαντικών υπολογιστών για την κρυπτογραφία των OT συστημάτων και πώς πρέπει οι οργανισμοί να προετοιμαστούν σήμερα για μια μετάβαση που θα οριστικοποιηθεί αύριο.

8.2 Industry 4.0, IIoT και η επέκταση της επιφάνειας επίθεσης σε OT

Η Industry 4.0 δεν αποτελεί μια ενιαία τεχνολογία, αλλά ένα οικοσύστημα σύγκλισης, Industrial Internet of Things, cloud computing, edge computing, ασύρματα δίκτυα, ψηφιακά δίδυμα, προβλεπτική συντήρηση και αυτοματοποιημένα συστήματα παρακολούθησης συνδυάζονται για να δημιουργήσουν ένα fully connected, data-driven εργοστάσιο. Σε αυτό το μοντέλο, ο εξοπλισμός παραγωγής, οι αισθητήρες, τα PLCs, τα συστήματα SCADA και τα enterprise IT συστήματα αντιμετωπίζονται ως ενιαίο οικοσύστημα, ανταλλάσσοντας δεδομένα σε πραγματικό χρόνο για βελτιστοποίηση της παραγωγής. Σε αυτό το πλαίσιο, εκτιμάται ότι στις ΗΠΑ, τη Λατινική Αμερική και την Ευρώπη το 70% των OT συστημάτων σε βιομηχανικές εγκαταστάσεις σύντομα θα είναι συνδεδεμένα με εταιρικά IT δίκτυα, αυξημένο από 50%. Σε Ασία και Ωκεανία η μετάβαση προχωρεί με παρόμοιο ρυθμό.

Αυτή η μαζική διασύνδεση δημιουργεί νέους τύπους έκθεσης που διαφέρουν ποιοτικά από τις παραδοσιακές IT απειλές. Το κλασικό μοντέλο του "air gap" μεταξύ OT και IT δικτύων έχει πρακτικά εκλείψει σε κάθε οργανισμό που έχει υιοθετήσει Industry 4.0 αρχιτεκτονικές: οι ροές δεδομένων μεταξύ αισθητήρων, cloud analytics platforms και enterprise dashboards δημιουργούν αναρίθμητα σημεία διέλευσης στο παραδοσιακό IT/OT boundary. Η έρευνα της Omdia αποκαλύπτει ότι το 43% των μεγάλων περιστατικών ασφάλειας εντοπίζεται στο Level 4 (επίπεδο εταιρικού σχεδιασμού) του stack ISA-95, ακριβώς εκεί όπου η συνδεσιμότητα είναι μεγαλύτερη λόγω αναγκών Industry 4.0. Παράλληλα, η ταχεία ανάπτυξη IIoT συσκευών όπως αισθητήρες, μετρητές, actuators, edge gateways εισάγει μαζικά νέα endpoints που στις περισσότερες περιπτώσεις δεν έχουν σχεδιαστεί με ενσωματωμένη ασφάλεια, χρησιμοποιούν μη κρυπτογραφημένα πρωτόκολλα και αδυνατούν να δεχθούν updates.

Το πρόβλημα δεν αφορά μόνο τα ίδια τα τελικά σημεία. Η αλυσίδα εφοδιασμού λογισμικού αποτελεί μια από τις κεντρικότερες επικίνδυνες περιοχές της Industry 4.0 εποχής. Βιομηχανικά συστήματα ενσωματώνουν ολοένα και περισσότερο στοιχεία τρίτων κατασκευαστών, από firmware έως βιβλιοθήκες επικοινωνίας και cloud connector software, χωρίς συστηματική τεκμηρίωση των εξαρτημάτων και των γνωστών ευπαθειών τους. Αυτή η αδιαφάνεια στη δομή του λογισμικού είναι αυτό που καθιστά τα Software Bill of Materials (SBOM) κρίσιμα εργαλεία. Το IEC 62443-4-1 απαιτεί διαδικασίες διαχείρισης κινδύνου για εξωτερικά components (SM-9, SM-10), και η χρήση SBOM επιτρέπει τον άμεσο εντοπισμό εκτεθειμένων components όταν εμφανίζεται νέα ευπάθεια, μετατρέποντας τη διαχείριση ευπαθειών από "ανθρωπιστική δραστηριότητα" σε αυτοματοποιήσιμη, risk-based διαδικασία.

Μια ακόμη κρίσιμη διάσταση της Industry 4.0 αρχιτεκτονικής είναι η ασφαλής μεταφορά δεδομένων μεταξύ OT και IT, ιδιαίτερα για historians, SCADA analytics και cloud platforms. Η παραδοσιακή αρχιτεκτονική Industrial DMZ, με δύο firewalls διαφορετικών vendors, proxy services στη ζώνη DMZ και strict default-deny rules και προς τα δύο δίκτυα, παραμένει η βέλτιστη δομή για segmentation. Ωστόσο, σε Industry 4.0 σενάρια η απλή DMZ δεν αρκεί, τα unidirectional security gateways (data diodes), ιδιαίτερα στα αρχιτεκτονικά μοντέλα "push from OT", εξασφαλίζουν φυσική μονοκατευθυντικότητα ροής δεδομένων, καθιστώντας αδύνατη οποιαδήποτε

ανατροφοδότηση από IT προς OT. Σε περιβάλλοντα υψηλής κρισιμότητας, όπως πυρηνικές εγκαταστάσεις, αγωγοί ενέργειας ή συστήματα νερού, αυτή η αρχιτεκτονική επιλογή δεν είναι υπερβολή, αλλά αναγκαιότητα.

8.3 Big Data Analytics και ασφάλεια σε OT/ICS

Η ανάδυση της βιομηχανικής ανάλυσης μεγάλων δεδομένων αποτελεί από μόνη της μια επανάσταση για τα OT περιβάλλοντα. Για πρώτη φορά, ο τεράστια όγκος δεδομένων που παράγουν PLCs, DCS, αισθητήρες και SCADA historians, δεδομένα που στο παρελθόν αποθηκεύονταν σε silos χωρίς δυνατότητα ανάλυσης, πλέον μπορούν να επεξεργαστούν σε πραγματικό χρόνο για να εντοπίσουν ανωμαλίες, να προβλέψουν βλάβες και να ανιχνεύσουν επιθέσεις πριν αυτές επηρεάσουν φυσικές διεργασίες. Από την σκοπιά της κυβερνοασφάλειας, το Big Data Analytics έχει μεταμορφώσει το τοπίο ανίχνευσης απειλών. Σύμφωνα με έρευνα που δημοσιεύτηκε στο journal Nature Scientific Reports, τα μοντέλα ανάλυσης κινδύνου βάσει Big Data επιτυγχάνουν AUC 0.95 σε δοκιμές ανίχνευσης, με μέσο precision 0.87 σε πολλαπλές κατηγορίες απειλών, αποδεικνύοντας ότι η τεχνολογία αυτή προσφέρει αξιόπιστη βάση για πρώιμη προειδοποίηση.

Το πλέον κρίσιμο χαρακτηριστικό της Big Data analytics για OT είναι η δυνατότητα baseline modelingδηλαδή με ανάλυση ιστορικών δεδομένων λειτουργίας, τα συστήματα αναγνωρίζουν το κανονικό εύρος τιμών κάθε παραμέτρου, ταχύτητα κινητήρων, πίεση αγωγών, συχνότητα εντολών σε PLCs, πρότυπα επικοινωνίας Modbus ή DNP3 και ανιχνεύουν αποκλίσεις που δεν ταιριάζουν σε κανένα γνωστό σχέδιο κανονικής λειτουργίας. Αυτή η προσέγγιση είναι ιδιαίτερα αποτελεσματική σε OT περιβάλλοντα, επειδή τα συστήματα industrial control είναι εξαιρετικά ντετερμινιστικά. Ένα PLC υπό κανονικές συνθήκες εκτελεί το ίδιο ακριβώς σύνολο εντολών σε κυκλική ακολουθία, κάτι που καθιστά τις αποκλίσεις πολύ πιο εύκολα ανιχνεύσιμες σε σύγκριση με τον πολυμορφισμό των IT δικτύων. Τεχνολογίες όπως το sequence-to-sequence autoencoder με LSTM units έχουν αποδείξει σε εργαστηριακά περιβάλλοντα ότι μπορούν να ανιχνεύσουν πολύπλοκες επιθέσεις χειρισμού δεδομένων, επιτυγχάνοντας recall 0.86 σε σύνολα επιθέσεων που αποτελούν σοβαρές προκλήσεις για παραδοσιακά συστήματα ανίχνευσης.

Ωστόσο, η ενσωμάτωση Big Data analytics σε OT/ICS δεν είναι χωρίς κινδύνους. Το πρώτο πρόβλημα είναι αρχιτεκτονικό, τα OT historian databases, όπως OSIsoft PI, Honeywell PHD, GE Proficy, αποθηκεύουν time-series βιομηχανικά δεδομένα σε proprietary formats που δεν είναι συμβατά με σύγχρονα cloud analytics engines χωρίς να προηγηθεί επεξεργασία για την μεταφορά τους. Αυτά τα δεδομένα, παγιδευμένα σε OT silo, δεν μπορούν να φτάσουν στο analytics layer χωρίς ανάπτυξη custom connectors και επίλυση του IT/OT security boundary. Το δεύτερο πρόβλημα είναι ότι αν και τα big data tools αυξάνουν τις δυνατότητες ανίχνευσης για τους αμυνόμενους, αυξάνουν ταυτόχρονα τις δυνατότητες των επιτιθέμενων, σύγχρονοι threat actors χρησιμοποιούν AI για να εκμαιεύσουν βιομηχανικά δεδομένα μέσω OT συστημάτων και να εκπαιδεύσουν ιδιωτικά μοντέλα για να δημιουργήσουν εξελιγμένες επόμενες επιθέσεις, μετατοπίζοντας τον στόχο από τη διακοπή λειτουργίας στην κλοπή βιομηχανικής πληροφορίας. Το τρίτο πρόβλημα αφορά τη νομική και τεχνική διαχείριση των δεδομένων, logs από OT συστήματα που περιέχουν πληροφορίες προσωπικού, κινήσεις εξοπλισμού ή ευαίσθητες διεργασίες παραγωγής εμπίπτουν σε κανονισμούς όπως ο GDPR, περιορίζοντας χρόνους φύλαξης και τρόπους επεξεργασίας, και δημιουργώντας τριβή μεταξύ compliance και forensic.

Ο σωστός σχεδιασμός pipeline αρχιτεκτονικής για OT Big Data πρέπει να λαμβάνει υπόψη όλες αυτές τις διαστάσεις. Η καλύτερη πρακτική που αναδεικνύεται στη βιβλιογραφία συνδυάζει μονοκατευθυντικά gateways ή historian replication σε DMZ για ασφαλή εξαγωγή δεδομένων, time-series databases (InfluxDB, Timescale) ως ενδιάμεσο buffer layer στη DMZ με store-and-forward δυνατότητες σε περίπτωση network outage, και ασφαλή σύνδεση με enterprise analytics platforms μέσω ελεγχόμενων API με αυστηρή πιστοποίηση και κρυπτογράφηση. Αυτή η "push-only" αρχιτεκτονική - δηλαδή δεδομένα που κινούνται μόνο από OT προς IT και ποτέ αντίστροφα ελαχιστοποιεί τον κίνδυνο υβριδικής επίθεσης χωρίς να εμποδίζει τη ροή αναλυτικών δεδομένων.

8.4 Τεχνητή Νοημοσύνη στην OT/ICS ασφάλεια

Η Τεχνητή Νοημοσύνη αλλάζει το τοπίο της OT ασφάλειας ταυτόχρονα και από τις δύο πλευρές της σύγκρουσης. Ως εργαλείο άμυνας, το AI και το Machine Learning επιτρέπουν για πρώτη φορά τη δυναμική δημιουργία baseline στην συμπεριφορά των δικτύων OT, την ανίχνευση zero-day απειλών μέσω αποκλίσεων από γνωστά

πρότυπα και τη σημαντική μείωση false positives που παραδοσιακά επιβαρύνουν τις ομάδες SOC. Ένα unsupervised ML σύστημα που εκπαιδεύεται στα πρότυπα επικοινωνίας ενός PLCs μπορεί να εντοπίσει ότι ένα συγκεκριμένο device εκδίδει εντολές εκτός της φυσιολογικής ακολουθίας του ακόμη και αν η εντολή από μόνη της φαίνεται έγκυρη, επειδή η αλληλουχία και η χρονική κατανομή διαφέρουν από το baseline. Η αγορά λύσεων AI για OT ασφάλεια βρίσκεται σε φάση ταχείας ανάπτυξης, καθώς όλο και περισσότεροι οργανισμοί επενδύουν σε AI-assisted ανίχνευση απειλών για βιομηχανικά περιβάλλοντα

Η ενσωμάτωση AI/ML σε OT ασφάλεια όμως δεν είναι άνευ προβλημάτων. Η CISA, σε συνεργασία με NSA, ASD's ACSC και άλλες εθνικές υπηρεσίες ασφάλειας, εξέδωσε τον Δεκέμβριο του 2025 κοινές οδηγίες για την ασφαλή ενσωμάτωση Τεχνητής Νοημοσύνης σε OT περιβάλλοντα, αναγνωρίζοντας τέσσερις βασικές αρχές, κατανόηση των κινδύνων AI, αξιολόγηση του επιχειρηματικού use case, δημιουργία AI governance πλαισίου και ενσωμάτωση oversight και failsafe μηχανισμών. Η κεντρική ανησυχία είναι ότι ένα AI σύστημα που λαμβάνει αποφάσεις σε OT περιβάλλον μπορεί να έχει απρόβλεπτες επιπτώσεις στη φυσική ασφάλεια αν δεν υποστηρίζεται από ανθρώπινη εποπτεία και δυνατότητα αναστροφής. Ο ρόλος του AI στο OT πρέπει να παραμένει decision support, και όχι autonomous decision-making, τουλάχιστον στα σημεία όπου αποφάσεις μπορεί να επηρεάσουν φυσικές διεργασίες.

Η άλλη όψη του νομίσματος είναι η χρήση AI από τους επιτιθέμενους. Οι σύγχρονοι threat actors χρησιμοποιούν AI για να αυτοματοποιήσουν την αναγνώριση ευπαθειών σε εκτεθειμένα ICS, να δημιουργήσουν εξελιγμένα phishing campaigns κατά OT ομάδων και, πιο ανησυχητικά, για adversarial attacks κατά ML μοντέλων που χρησιμοποιούνται στην ανίχνευση απειλών. Μια adversarial attack είναι μια εσκεμμένη χειραγώγηση των εισόδων ενός ML μοντέλου έτσι ώστε το μοντέλο να παράγει λανθασμένο αποτέλεσμα, στο πλαίσιο OT ασφάλειας, αυτό θα μπορούσε να σημαίνει ότι ένα σύστημα anomaly detection "πείθεται" να χαρακτηρίσει κακόβουλη δραστηριότητα ως φυσιολογική, αδειάζοντας ουσιαστικά τον ανιχνευτικό μηχανισμό. Τεχνικές όπως το data poisoning (η εισαγωγή κακόβουλων δεδομένων στη φάση εκπαίδευσης του μοντέλου) και το prompt injection σε AI συστήματα που εξετάζουν logs ή αναφορές, αποτελούν πραγματικές απειλές για την αξιοπιστία AI-assisted ανίχνευσης.

Για την αντιμετώπιση αυτών των νέων κινδύνων, το NIST ανέπτυξε το AI Risk Management Framework 1.0 (AI RMF), το οποίο δομείται γύρω από τέσσερις λειτουργίες, Govern, Map, Measure και Manage, ανάλογα με τη δομή του CSF. Σε OT πλαίσιο, η εφαρμογή του AI RMF σημαίνει ότι κάθε AI σύστημα που αναπτύσσεται σε βιομηχανικό περιβάλλον πρέπει να υπόκειται σε structured risk assessment κατά τη φάση σχεδιασμού, να εξετάζεται από τεχνικές και λειτουργικές ομάδες για σχεδιαστικά ελαττώματα και ανεπιθύμητες συμπεριφορές, να διαθέτει explainability μηχανισμούς ώστε οι ομάδες OT να κατανοούν τις αποφάσεις του και να ενσωματώνεται σε σχέδια incident response, ώστε σε περίπτωση παραβίασης ή malfunction να υπάρχει σαφής διαδικασία deactivation και αναστροφής σε manual control. Η Τεχνητή Νοημοσύνη στα OT περιβάλλοντα απαιτεί ένα governance πλαίσιο επικαλυπτόμενο τόσο με τις απαιτήσεις ασφάλειας του NIST CSF 2.0 όσο και με τις operational safety απαιτήσεις της IEC 62443, δημιουργώντας ένα integrated AI+OT security framework που δεν υπήρχε πριν από πέντε χρόνια.

8.5 Digital Twins σαν εργαλείο ασφάλειας και δοκιμής

Μία από τις πιο υποσχόμενες τεχνολογικές εξελίξεις στην τομή Industry 4.0 και OT ασφάλειας είναι η χρήση Digital Twins, δηλαδή, εικονικών αντιγράφων φυσικών βιομηχανικών συστημάτων ως πλατφόρμα για δοκιμές ασφάλειας, red team ασκήσεις και συνεχή επαλήθευση ελέγχων χωρίς διακοπή της παραγωγής. Η ανάγκη για αυτό το εργαλείο είναι εμφανής, παραδοσιακές δοκιμές διείσδυσης σε OT περιβάλλοντα ενέχουν σοβαρό κίνδυνο για τη φυσική ασφάλεια και τη διαθεσιμότητα, καθώς ακόμη και μια απλή σάρωση δικτύου μπορεί να προκαλέσει σφάλμα ή αστάθεια σε εύθραυστο legacy εξοπλισμό. Το κόστος ενός πλήρους penetration test σε OT εγκατάσταση, συμπεριλαμβανομένων του συντονισμού maintenance windows και των πιθανών διαταραχών παραγωγής, μπορεί να ξεπεράσει τα 100.000 δολάρια ανά εκτίμηση.

Ένα Digital Twin, αντίθετα, αναπαράγει την αρχιτεκτονική ενός OT δικτύου PLCs, HMIs, SCADA servers, communication paths σε ένα ασφαλές εικονικό περιβάλλον στο οποίο μπορούν να εκτελούνται επιθέσεις, να δοκιμάζονται αλλαγές configuration και να αξιολογούνται τα αποτελέσματα παρεμβάσεων χωρίς οποιαδήποτε επίπτωση στη λειτουργία. Ερευνητές από το Πανεπιστήμιο Eindhoven ανέπτυξαν ένα Digital Twin framework

για cybersecurity testing βιομηχανικών δικτύων σε εγκαταστάσεις χημικής βιομηχανίας, αναπαράγοντας λεπτομερώς ένα σύστημα μεθανόλης-αζώτου και εκτελώντας επιθέσεις command injection, spoofing και χειρισμού δεδομένων αισθητήρων με χρήση Python scripts επικοινωνίας EtherNet/IP (ENIP). Παράλληλα, το NIST IR 8356 εξετάζει cybersecurity challenges ειδικά για Digital Twins, καθορίζοντας ότι η ψηφιακή αντανάκλαση ενός OT συστήματος απαιτεί ισχυρή πιστοποίηση, access controls και cryptographic integrity για να μην μετατραπεί η ίδια σε attack vector.

Πέρα από τη χρήση για δοκιμές, τα Digital Twins χρησιμοποιούνται ολοένα περισσότερο για continuous configuration monitoring με σύγκριση του "golden state" ενός OT συστήματος (το αναμενόμενο configuration) με τον digital twin σε πραγματικό χρόνο, είναι δυνατός ο αυτόματος εντοπισμός unauthorized configuration changes που θα μπορούσαν να αποτελούν πρώιμο δείκτη παραβίασης ή σφάλματος. Αυτή η δυνατότητα είναι ιδιαίτερα πολύτιμη σε IEC 62443 ελέγχους CM (Configuration Management), όπου απαιτείται τεκμηρίωση της αναμενόμενης κατάστασης κάθε asset και έγκαιρη ανίχνευση αποκλίσεων. Ο συνδυασμός Digital Twins με AI-driven anomaly detection δημιουργεί ένα continuous security assurance μοντέλο το οποίο υπερβαίνει την παραδοσιακή περιοδική επαλήθευση και ευθυγραμμίζεται με τις απαιτήσεις continuous monitoring του NIST CSF 2.0.

8.6 Post-Quantum Cryptography

Η κβαντική απειλή στην ασφάλεια OT συστημάτων αποτελεί μια από τις λιγότερο ορατές αλλά μακροπρόθεσμα ίσως καταστροφικότερες προκλήσεις που αντιμετωπίζει το πεδίο. Κβαντικοί υπολογιστές επαρκούς ισχύος, γνωστοί ως Cryptographically Relevant Quantum Computers (CRQC), θα έχουν τη δυνατότητα να σπάσουν τις ασύμμετρες κρυπτογραφικές αλγορίθμους RSA και ECC που υπόκεινται στη μεγάλη πλειονότητα των σύγχρονων IT και OT ασφαλών επικοινωνιών. Οι εκτιμήσεις εμπειρογνωμόνων τοποθετούν το λεγόμενο "Q-Day", δηλαδή την ημερομηνία κατά την οποία ένας CRQC θα μπορέσει να σπάσει τον RSA-2048, στο παράθυρο 2030 - 2040. Αυτό σημαίνει ότι το πρόβλημα φαίνεται μακρινό, αλλά η μετάβαση σε post-quantum κρυπτογραφία, ειδικά σε OT περιβάλλοντα, δεν μπορεί να αναβληθεί ασφαλώς.

Ο λόγος για τον οποίο το πρόβλημα είναι ήδη παρόν αφορά τη στρατηγική "Harvest Now, Decrypt Later" (HNDL). Κρατικοί και άλλοι κατεστημένοι threat actors υλοποιούν ήδη αυτή τη στρατηγική, συλλέγουν και αποθηκεύουν κρυπτογραφημένες επικοινωνίες OT συστημάτων σήμερα, ιδιαίτερα από κρίσιμες υποδομές, ενέργεια, αμυντικές βιομηχανίες, με σκοπό να τα αποκρυπτογραφήσουν μόλις τεθεί σε λειτουργία ένας CRQC. Δεδομένου ότι μεγάλες κρυπτογραφικές μεταβάσεις σε πολύπλοκες υποδομές απαιτούν πέντε έως δέκα χρόνια για πλήρη υλοποίηση, και δεδομένου ότι δεδομένα βιομηχανικής σημασίας κρατούν την αξία τους για δεκαετίες, η εξίσωση για την αναγκαιότητα άμεσης δράσης γράφεται ως εξής. Αν x είναι ο χρόνος ζωής των δεδομένων, y ο χρόνος μετάβασης σε PQC και z ο χρόνος έως το Q-Day, τότε ισχύει y + τρέχων έτος > z - x, άρα η μετάβαση είναι ήδη καθυστερημένη για μακρόβια ευαίσθητα δεδομένα. Ο Αύγουστος 2024 ήταν ορόσημο, το NIST εξέδωσε τρία εγκεκριμένα PQC πρότυπα, ML-KEM (FIPS 203), ML-DSA (FIPS 204) και SLH-DSA (FIPS 205), παρέχοντας για πρώτη φορά σταθερή βάση για μετάβαση.

Η πρόκληση για OT είναι σημαντικά δυσκολότερη από ό,τι για IT. Η CISA, σε ειδική αναφορά για post-quantum OT, επισημαίνει ότι η εφαρμογή PQC σε OT είναι "a significant and enduring challenge" για κρίσιμες υποδομές, για πολλούς λόγους. Πρώτον, ο υπολογιστικός φόρτος των lattice-based αλγορίθμων (ML-KEM, ML-DSA) είναι σημαντικά μεγαλύτερος από τον αντίστοιχο των κλασικών αλγορίθμων, κάτι που μπορεί να ξεπεράσει τις υπολογιστικές δυνατότητες παλαιών PLCs, microcontrollers και embedded devices. Δεύτερον, πολλά legacy OT components δεν υποστηρίζουν firmware update καθόλου ή μόνο υπό αυστηρά ελεγχόμενες συνθήκες χωρίς εγγύηση λειτουργικής συμβατότητας. Τρίτον, η OT εφοδιαστική αλυσίδα εκτείνεται σε δεκάδες vendors με διαφορετικά roadmaps quantum-readiness, και η τυπική προσέγγιση "αντικατέστησε τον αλγόριθμο" απαιτεί σε OT "αντικατέστησε τον εξοπλισμό", που συχνά σημαίνει εκατομμύρια ευρώ και χρόνια σχεδιασμού.

Οι αρμόδιες αρχές και ειδικοί προτείνουν μια σταδιακή, risk-based στρατηγική μετάβασης. Ο Βρετανικός NCSC καθορίζει ότι η μετάβαση σε PQC πρέπει να ξεκινήσει τώρα για συστήματα με μακρά ζωή δεδομένων, και δεδομένα μεγάλης αξίας, αναφέροντας ρητά IIoT και OT ως ειδικές προκλήσεις που απαιτούν ξεχωριστό σχεδιασμό μετάβασης. Η CISA συστήνει στους asset owners να απαιτούν "crypto-agile features" από νέες αγορές εξοπλισμού, δηλαδή δυνατότητα αντικατάστασης κρυπτογραφικών αλγορίθμων μέσω firmware update

χωρίς ανάγκη αντικατάστασης hardware, και να εξετάσουν hybrid cryptography λύσεις ως ενδιάμεσο βήμα, συνδυάζοντας κλασικούς και PQC αλγορίθμους σε VPN tunnels και control center επικοινωνίες. Κρίσιμη ενέργεια είναι επίσης η διεξαγωγή cryptographic inventory, καταγραφή κάθε συστήματος που χρησιμοποιεί δημόσιους κλειδιά, εντοπισμός legacy RSA/ECC χρήσεων σε industrial protocols όπως TLS, DNP3 Secure Authentication ή IEC 62351 ώστε να υπάρχει σαφής εικόνα της έκθεσης πριν τεθεί σε εφαρμογή το migration plan.

Τα σύγχρονα πρότυπα IEC 62443 εξελίσσονται για να αντιμετωπίσουν αυτή την πραγματικότητα ενώ οι τρέχουσες υλοποιήσεις encryption που απαιτεί η IEC 62443 για εμπιστευτικότητα δεδομένων και ακεραιότητα συστημάτων βασίζονται σε κλασικούς αλγορίθμους που δεν είναι quantum-resistant, η τάση κατευθύνεται σαφώς στην αντικατάστασή τους με PQC-ready εκδόσεις. Αυτό σημαίνει ότι οι οργανισμοί που σχεδιάζουν σήμερα νέα OT συστήματα ή εκσυγχρονίζουν υπάρχοντα δεν μπορούν πλέον να αγνοούν την quantum-readiness ως κριτήριο αξιολόγησης, τοποθετώντας την post-quantum κρυπτογραφία στο επίκεντρο των στρατηγικών αποφάσεων για OT ασφάλεια της επόμενης δεκαετίας.

8.7 Security Framework για AI-ready OT

Η ανάλυση των προηγούμενων ενοτήτων αναδεικνύει ένα κεντρικό συμπέρασμα: η ασφάλεια OT/IT στην εποχή της Industry 4.0 δεν μπορεί να αντιμετωπίζεται ως σύνολο ανεξάρτητων τεχνολογικών μέτρων, αλλά ως ολοκληρωμένο πλαίσιο που καλύπτει ταυτόχρονα αρχιτεκτονικές, governance, τεχνολογία, διαδικασίες και μεταβατικές στρατηγικές. Ένα AI-ready OT security framework πρέπει να ενσωματώνει ιεραρχικά, βασικά μέτρα ασφάλειας (asset inventory, segmentation, identity management) σύμφωνα με IEC 62443 και NIST SP 800-82, αρχιτεκτονικές ασφαλούς ροής δεδομένων για Big Data pipelines (DMZ, data diodes, historian replication), AI/ML anomaly detection με ανθρώπινη εποπτεία και AI governance σύμφωνα με CISA/NIST AI RMF, digital twin-based testing και continuous configuration validation, και post-quantum cryptography transition planning βάσει PQC standards.

Η ολοκλήρωση αυτή δεν είναι θεωρητική άσκηση. Το ποσοστό οργανισμών παγκοσμίως που έχει εντάξει την OT ασφάλεια στην αποκλειστική αρμοδιότητα του CISO/CSO παρουσίασε ραγδαία άνοδο τα τελευταία χρόνια (16% το 2022, 52% το 2025), με μια πρώτη ένδειξη ωρίμανσης το 2026 να καταγράφεται πτώση στο 40%, καθώς οι οργανισμοί αρχίζουν να αναδιανέμουν την ευθύνη και σε χαμηλότερα ιεραρχικά επίπεδα αν συνυπολογιστεί και ο CIO, το 60% των οργανισμών αναφέρει CISO ή CIO ως τελικό υπεύθυνο OT ασφάλειας το 2026, έναντι 69% το 2025 (Fortinet, 2026), αντικατοπτρίζοντας μια σαφή οργανωσιακή τάση ενοποίησης της διακυβέρνησης. Οι οργανισμοί που αναπτύσσουν σήμερα Industry 4.0 υποδομές χωρίς να ενσωματώνουν αυτό το ολοκληρωμένο πλαίσιο θα βρεθούν αντιμέτωποι στα επόμενα χρόνια με ρυθμιστικές απαιτήσεις (NIS2, NIST PQC mandates για ρυθμιζόμενες βιομηχανίες), τεχνολογικές αναγκαιότητες (quantum migration, AI governance) και λειτουργικούς κινδύνους (AI-powered επιθέσεις, supply chain exposures) για τους οποίους μια αποσπασματική προσέγγιση δεν θα επαρκεί. Η ασφάλεια του OT στην Industry 4.0 δεν είναι πλέον μια τεχνική παρένθεση στη βιομηχανική στρατηγική, είναι αναπόσπαστη συνιστώσα της ίδιας της βιωσιμότητας του μοντέλου Industry 4.0.

ΚΕΦΑΛΑΙΟ 9 – Συμπεράσματα και Μελλοντικές Κατευθύνσεις

Η παρούσα διπλωματική εργασία εκκίνησε από μια θεμελιώδη διαπίστωση που διατρέχει ολόκληρο το σώμα της έρευνας: τα συστήματα Λειτουργικής Τεχνολογίας που για δεκαετίες λειτουργούσαν σε απομόνωση από τα δίκτυα πληροφορικής έχουν εισέλθει πλέον σε ένα νέο ψηφιακό οικοσύστημα, αναπόφευκτα διασυνδεδεμένο, τεχνολογικά εκτεθειμένο και ρυθμιστικά απαιτητικό. Η σύγκλιση IT/OT δεν είναι πλέον στρατηγική επιλογή αλλά λειτουργική αναγκαιότητα, και η ασφάλεια αυτής της σύγκλισης αποτελεί ένα από τα πιο πολύπλοκα και κρίσιμα προβλήματα της σύγχρονης κυβερνοασφάλειας. Τα δεδομένα που αναλύθηκαν στη διάρκεια της εργασίας δεν αφήνουν περιθώριο εφησυχασμού: το 96% των περιστατικών OT ασφάλειας προέρχεται από παραβιάσεις IT συστημάτων, ενώ το 60% των οργανισμών παγκοσμίως βίωσε ένα τουλάχιστον σημαντικό περιστατικό OT κατά τη διάρκεια του 2025 (βλ. #54 TXOne Networks, 2026 Annual OT/ICS Cybersecurity Report). Αυτά τα αριθμητικά στοιχεία δεν είναι απλώς στατιστικά — αντικατοπτρίζουν ένα δομικό χάσμα μεταξύ της ψηφιακής επιτάχυνσης που επέβαλε η Industry 4.0 και της ωριμότητας ασφάλειας που οι βιομηχανικοί οργανισμοί έχουν μέχρι σήμερα καταφέρει να αναπτύξουν.

Η ανάλυση που αναπτύχθηκε στα κεφάλαια της εργασίας κάλυψε συστηματικά τις διαστάσεις αυτού του χάσματος: από τις διαφορές αρχιτεκτονικής, φιλοσοφίας ασφάλειας και ιεράρχησης προτεραιοτήτων μεταξύ IT και OT, στις πρακτικές μεθόδους αξιολόγησης και αντιμετώπισης κινδύνου, στα βέλτιστα αρχιτεκτονικά μοντέλα προστασίας, στη διακυβέρνηση και τα πλαίσια GRC, και τέλος στις νέες τεχνολογικές προκλήσεις και ευκαιρίες που φέρνουν η Industry 4.0, η Τεχνητή Νοημοσύνη και οι κβαντικοί υπολογιστές. Η θεματολογία αυτή ακολουθεί μια συνεκτική εσωτερική λογική: από το γενικό στο ειδικό, από τη θεωρία στην πράξη, από τα σημερινά εργαλεία στις αύριες απειλές. Η δομή αυτή δεν είναι τυχαία — αντικατοπτρίζει την πραγματική ακολουθία που πρέπει να ακολουθεί κάθε οργανισμός όταν επιχειρεί να αντιμετωπίσει σοβαρά και συστηματικά την ασφάλεια των βιομηχανικών του συστημάτων.

Το κεντρικό εύρημα που αναδύεται από το σύνολο της ανάλυσης είναι ότι η αποτελεσματική ασφάλεια IT/OT δεν επιτυγχάνεται μέσω της μηχανικής εφαρμογής ενός προτύπου ή ενός τεχνικού εργαλείου, αλλά μέσω της ολοκλήρωσης τεσσάρων αλληλένδετων επιπέδων: ορατότητας, αρχιτεκτονικής, διακυβέρνησης και ωριμότητας. Χωρίς πλήρη και ακριβή γνώση των assets που υπάρχουν σε ένα OT δίκτυο, κανένα μέτρο ασφάλειας δεν μπορεί να εφαρμοστεί αποτελεσματικά. Χωρίς αρχιτεκτονική άμυνας σε βάθος — ζωνοποίηση, DMZ, segmentation — η τεχνολογία ανίχνευσης δεν έχει δομή πάνω στην οποία να χτιστεί. Χωρίς διακυβέρνηση που να εκφράζει σαφές risk appetite, ρόλους και λογοδοσία σε επίπεδο διοίκησης, οι τεχνικές παρεμβάσεις παραμένουν αποσπασματικές και ευάλωτες σε αλλαγές προσωπικού ή οργανωτικές αναδιαρθρώσεις. Και χωρίς μετρήσιμη ωριμότητα — δηλαδή συστηματική και τεκμηριωμένη βελτίωση μέσω σαφών κύκλων αξιολόγησης και προόδου — οποιοδήποτε πρόγραμμα ασφάλειας κινδυνεύει να εκπέσει σε "paper compliance", γεμάτο πολιτικές και διαδικασίες που δεν επαληθεύονται ποτέ στην πράξη.

Εξίσου σημαντικό εύρημα είναι ότι η IEC 62443 και το NIST CSF 2.0 δεν αποτελούν ανταγωνιστικά πλαίσια αλλά βαθιά συμπληρωματικά: το NIST CSF 2.0 — και ειδικά η νέα λειτουργία Govern που εισήχθη στην έκδοση 2.0 — παρέχει τον στρατηγικό σκελετό για τη διαχείριση κυβερνοκινδύνου σε επίπεδο οργανισμού, σε γλώσσα κατανοητή από τη διοίκηση, ενώ η IEC 62443 προσφέρει τον OT-specific τεχνικό και οργανωτικό σκελετό για την υλοποίηση στο επίπεδο των εγκαταστάσεων και των βιομηχανικών συστημάτων. Η συνδυαστική χρήση τους, με mapping των λειτουργιών NIST CSF στις απαιτήσεις IEC 62443, αποτελεί τη βέλτιστη πρακτική που αναδείχθηκε από τα case studies που εξετάστηκαν, από παγκόσμιους βιομηχανικούς οργανισμούς έως φορείς κρίσιμων υποδομών, και η σύνθεση αυτή αποτελεί μια από τις κύριες συνεισφορές της παρούσας εργασίας.

Μια τρίτη, ίσως πιο μακρόπνοη διαπίστωση αφορά τις νέες διαστάσεις που προστίθενται στο τοπίο OT ασφάλειας από την Industry 4.0. Η είσοδος Τεχνητής Νοημοσύνης, Big Data και IIoT δεν αλλάζει απλώς τον αριθμό των endpoints που πρέπει να προστατευθούν — αλλάζει ριζικά τη φύση των απειλών και των αμυντικών δυνατοτήτων ταυτόχρονα. Η ίδια τεχνολογία που επιτρέπει σε έναν defender να εντοπίσει anomaly σε PLC μέσα σε δευτερόλεπτα επιτρέπει σε έναν επιτιθέμενο να σχεδιάσει adversarial attacks που εξαπατούν τα ίδια τα συστήματα ανίχνευσης. Τα Digital Twins μετατρέπουν τον τρόπο με τον οποίο δοκιμάζεται η ασφάλεια, επιτρέποντας πλήρη red team ασκήσεις χωρίς κίνδυνο για παραγωγή. Και η απειλή των κβαντικών υπολογιστών — μέσω της στρατηγικής "Harvest Now, Decrypt Later" — αναδεικνύεται ως ο κίνδυνος με τον μεγαλύτερο

χρονικό ορίζοντα, ο οποίος δεν μπορεί να αντιμετωπιστεί αύριο αλλά μόνο με τεκμηριωμένες και οργανωμένες δράσεις σήμερα. Η κυκλοφορία των NIST FIPS 203, 204 και 205 το 2024 θέτει τώρα τα θεμέλια για μια μετάβαση που πρέπει να ξεκινήσει ως στρατηγική επιλογή για κάθε οργανισμό που λειτουργεί βιομηχανική υποδομή με μακρά ζωή assets.

Κλείνοντας, η εργασία αυτή επιβεβαιώνει ότι η ασφάλεια OT/IT στην εποχή της Industry 4.0 δεν είναι τεχνική παρένθεση στη βιομηχανική στρατηγική, αλλά αναπόσπαστη συνιστώσα της βιωσιμότητας του ίδιου του μοντέλου. Οργανισμοί που αντιμετωπίζουν την OT ασφάλεια ως συμμόρφωση θα βρεθούν διαρκώς πίσω από τις εξελίξεις. Αντίθετα, εκείνοι που την ενσωματώνουν στη λήψη αποφάσεων, στην αρχιτεκτονική τους, στις προμήθειές τους και στη στρατηγική τους για το μέλλον θα είναι σε θέση να αξιοποιήσουν πλήρως τα οφέλη της ψηφιακής μετάβασης, χωρίς να μετατρέπουν κάθε νέα τεχνολογία σε νέο φορέα κινδύνου. Αυτή είναι η ουσία της ασφάλειας ως στρατηγικής λειτουργίας — και αυτό είναι το κεντρικό μήνυμα που η παρούσα εργασία επιδιώκει να αφήσει ως συνεισφορά στην ελληνική ακαδημαϊκή και επαγγελματική κοινότητα.

Παράρτημα Α - Αρχιτεκτονικές Αναφοράς για OT/IT Ασφάλεια

A.1 Το Purdue Enterprise Reference Architecture (PERA) και η εφαρμογή του σε ICS/OT

Το Purdue Enterprise Reference Architecture, γνωστό και ως Purdue Model ή PERA, αποτελεί το πιο ευρέως χρησιμοποιούμενο μοντέλο αναφοράς για την οργάνωση και τμηματοποίηση βιομηχανικών δικτύων. Αναπτύχθηκε από το Purdue Laboratory for Applied Industrial Control και αρχικά υιοθετήθηκε από το πρότυπο ISA-95 και, στη συνέχεια, από το ISA-99/IEC 62443. Ο κεντρικός σκοπός του είναι η λογική διαχωρισμός των λειτουργικών επιπέδων ενός βιομηχανικού οργανισμού σε ιεραρχικά επίπεδα, ώστε να επιτρέπεται η ελεγχόμενη ροή δεδομένων μεταξύ τους χωρίς απευθείας πρόσβαση από τα ανώτερα επίπεδα (IT/enterprise) στα κατώτερα (field devices, process control).

Η δομή του Purdue Model οργανώνεται ως εξής:

Επίπεδο 0 — Field Devices: Αισθητήρες, actuators, μετρητές και κινητήρες που αλληλεπιδρούν άμεσα με τη φυσική διεργασία. Πρόκειται για το πλέον κρίσιμο επίπεδο, καθώς οποιαδήποτε παραβίαση εδώ μπορεί να έχει άμεσες φυσικές επιπτώσεις.

Επίπεδο 1 — Basic Control: PLCs, DCS controllers και RTUs που δέχονται σήματα από το Level 0 και εκδίδουν εντολές ελέγχου. Λειτουργούν σε πραγματικό χρόνο και με εξαιρετικά αυστηρές απαιτήσεις latency και διαθεσιμότητας.

Επίπεδο 2 — Area Supervisory Control: SCADA servers, HMIs και engineering workstations που παρέχουν εποπτεία και διαχείριση των controllers του Level 1. Εδώ βρίσκεται η κύρια διεπαφή ανθρώπου-μηχανής για τους χειριστές.

Επίπεδο 3 — Site Operations: Manufacturing Execution Systems (MES), historians, scheduling και optimization systems. Το Level 3 διαχειρίζεται τη λειτουργία της εγκατάστασης συνολικά, συλλέγει δεδομένα από τα κατώτερα επίπεδα και τα θέτει διαθέσιμα για επιχειρησιακή ανάλυση.

Επίπεδο 3.5 — Industrial DMZ: Η Demilitarized Zone αποτελεί την κεντρική αρχιτεκτονική καινοτομία για την ασφαλή IT/OT σύγκλιση και, αν και δεν ήταν μέρος του αρχικού Purdue Model, θεωρείται σήμερα απαραίτητη. Εδώ βρίσκονται firewalls, historian mirrors, jump servers, patch management servers και remote access gateways. Η κρίσιμη λειτουργία της DMZ είναι να εξασφαλίζει ότι κανένα σύστημα δεν επικοινωνεί απευθείας μεταξύ Level 3 και Level 4 χωρίς να περνά μέσα από αυτήν.

Επίπεδο 4 — Enterprise Network: ERP, CRM, επιχειρηματικές εφαρμογές και εταιρικό δίκτυο. Αποτελεί το επίπεδο IT με τις υψηλότερες κυβερνοαπειλές, καθώς είναι πιο ανοιχτό και εκτεθειμένο σε εξωτερικό internet και email.

Στην πράξη, η ορθή εφαρμογή του Purdue Model σε IEC 62443 ζωνοποίηση σημαίνει ότι: κάθε επίπεδο αντιστοιχεί σε μία ή περισσότερες Security Zones με ορισμένο SL-T, κάθε ροή δεδομένων μεταξύ zones διαμεσολαβείται αποκλειστικά από Conduit (firewall, data diode, VPN gateway), και η DMZ λειτουργεί ως mandatory checkpoint για κάθε επικοινωνία IT↔OT.

A.2 IEC 62443 Ζωνοποίηση: Security Levels και Conduits

Η εφαρμογή ζωνοποίησης κατά IEC 62443-3-2 εκκινεί από τον ορισμό Security Zones — ομαδοποιήσεων assets που μοιράζονται κοινές απαιτήσεις ασφάλειας — και Conduits — ελεγχόμενων διαύλων επικοινωνίας μεταξύ ζωνών. Για κάθε ζώνη ορίζεται ένα Target Security Level (SL-T), που αντιστοιχεί στον βαθμό αντίστασης που πρέπει να προσφέρει η ζώνη έναντι συγκεκριμένου τύπου threat actor (SL-1: απλή προστασία από τυχαία παραβίαση, SL-2: προστασία από εσκεμμένη παραβίαση με χαμηλούς πόρους, SL-3: εξελιγμένος εισβολέας με σημαντικούς πόρους, SL-4: κρατικός ή ισοδύναμης ισχύος actor). Ο ορισμός SL-T προκύπτει από το risk assessment της IEC 62443-3-2 και αντικατοπτρίζει τις αποφάσεις διακυβέρνησης για αποδεκτό επίπεδο κινδύνου.

Το ακόλουθο παράδειγμα τυπικής ζωνοποίησης για βιομηχανική εγκατάσταση μέτριας κριτικότητας δείχνει πώς οι SL-T κατανέμονται ανά ζώνη και πώς διαμορφώνονται τα αντίστοιχα μέτρα:

Ζώνη	Επίπεδο Purdue	SL-T	Τεχνολογία Conduit
Enterprise	4	SL-1	Firewall, NAC
Industrial DMZ	3.5	SL-2	Dual-firewall, IDS/IPS
Site Operations	3	SL-2	Industrial Firewall
Process Control	2	SL-3	Industrial Firewall + IDS
Safety Zone (SIS)	1/2	SL-4	Data Diode (unidirectional)
Field Device Zone	0/1	SL-2	Managed Switch, Port Auth

Κρίσιμη αρχή: ένα Conduit πρέπει να προστατεύεται στο ίδιο ή υψηλότερο SL με τη ζώνη υψηλότερης κρισιμότητας που συνδέει. Αυτό σημαίνει ότι ένα conduit μεταξύ Level 2 (SL-3) και DMZ (SL-2) πρέπει να ικανοποιεί τις απαιτήσεις SL-3, εξασφαλίζοντας ότι η ζώνη υψηλότερης ασφάλειας δεν εξασθενεί λόγω του conduit που τη διασυνδέει με λιγότερο ασφαλή ζώνη.

Α.2.1 Data Diodes (Μονόδρομες Πύλες Δεδομένων)

Ορισμός και βασική αρχή λειτουργίας

Ένα data diode (ή αλλιώς “unidirectional gateway”, “μονόδρομη πύλη δικτύου”) είναι μια συσκευή δικτύου η οποία επιτρέπει τη ροή δεδομένων αποκλειστικά προς μία κατεύθυνση, χωρίς καμία φυσική δυνατότητα επιστροφής πληροφορίας. Το NIST (National Institute of Standards and Technology) το ορίζει ως μια συσκευή δικτύου που επιτρέπει τη μεταφορά δεδομένων μόνο προς μία κατεύθυνση, γνωστή επίσης ως unidirectional gateway, deterministic one-way boundary device ή unidirectional network.
Η θεμελιώδης διαφορά από ένα firewall είναι ότι το firewall εφαρμόζει τους κανόνες του σε επίπεδο λογισμικού (software), κάτι που θεωρητικά μπορεί να παρακαμφθεί μέσω κακής διαμόρφωσης, ευπάθειας ή επιτυχημένης επίθεσης. Το data diode αντίθετα επιβάλλει τη μονοκατευθυντικότητα σε επίπεδο υλικού (hardware), δηλαδή με τους νόμους της φυσικής, και όχι με κανόνες λογισμικού που θα μπορούσαν να παρακαμφθούν.

Πώς λειτουργεί τεχνικά

Η πιο κοινή υλοποίηση βασίζεται σε οπτική ίνα (fiber optic):

- Η συσκευή αποτελείται από δύο ξεχωριστά, φυσικά διαχωρισμένα module: έναν πομπό (TX – transmitter), που συνδέεται μόνο στο “προστατευμένο”/εσωτερικό δίκτυο (π.χ. το δίκτυο ελέγχου/OT), και έναν δέκτη (RX – receiver), που συνδέεται μόνο στο εξωτερικό/λιγότερο ασφαλές δίκτυο (π.χ. εταιρικό IT δίκτυο ή internet).
- Ο πομπός διαθέτει μόνο λέιζερ/LED Tx, ο δέκτης μόνο Rx λήψης. Τα δεδομένα μετατρέπονται σε φως και διαβιβάζονται μέσω μιας μονόδρομης σύνδεσης που επιβάλλεται από το ίδιο το υλικό, εξασφαλίζοντας ότι δεν υπάρχει κανένα μονοπάτι επιστροφής.
- Επειδή δεν υπάρχει φυσικά καλώδιο/ίνα επιστροφής, είναι αδύνατη οποιαδήποτε αμφίδρομη επικοινωνία (π.χ. TCP handshake, acknowledgment πακέτα), τα data diodes δεν προωθούν καν πακέτα TCP, καθώς το TCP απαιτεί εξ ορισμού αμφίδρομη επικοινωνία.

Για τον λόγο αυτό, τα κλασικά data diodes υποστηρίζουν μόνο πρωτόκολλα χωρίς σύνδεση (connectionless), όπως broadcast Ethernet ή UDP.

Η εξέλιξη: Unidirectional Security Gateways

Επειδή η αμιγής μονοδρομικότητα δυσχεραίνει τη χρήση σύγχρονων βιομηχανικών πρωτοκόλλων (OPC, βάσεις δεδομένων κ.λπ.), έχει αναπτυχθεί η σύγχρονη εκδοχή του data diode, το Unidirectional Gateway, το οποίο συνδυάζει το μονόδρομο hardware με λογισμικό που αναπαράγει βάσεις δεδομένων και εξομοιώνει servers πρωτοκόλλων. Στην πράξη, το λογισμικό στην πλευρά του πομπού “διαβάζει” δεδομένα (π.χ. από PLC, historian, OPC-server) και τα προωθεί μέσω του οπτικού μονόδρομου συνδέσμου στην άλλη πλευρά, ένα αντίγραφο λογισμικό αναδημιουργεί/εξομοιώνει τον αντίστοιχο server ώστε τα εργαλεία IT να μπορούν να “διαβάσουν” τα δεδομένα σαν να επικοινωνούν κανονικά, χωρίς όμως ποτέ να υπάρχει πραγματικό κανάλι επιστροφής προς το OT δίκτυο.

Πώς μοιάζει η συσκευή στην πράξη

Φυσικά, τα εμπορικά data diodes/unidirectional gateways συνήθως έχουν τη μορφή:

- Rack-mounted appliance (π.χ. 1U διαστάσεων, όπως αναφέρεται χαρακτηριστικά για τη σειρά Owl ReCon), τοποθετούμενο σε server rack.
- Δύο ξεχωριστές φυσικές μονάδες/κάρτες μέσα στο σασί (ή και δύο εντελώς ξεχωριστά κουτιά), μία για TX και μία για RX, συνδεδεμένες μεταξύ τους αποκλειστικά με οπτική ίνα.
- Θύρες δικτύου (Ethernet) σε κάθε πλευρά για τη σύνδεση με τα αντίστοιχα δίκτυα (OT στη μία πλευρά, IT/εξωτερικό στην άλλη).
- Σε ορισμένες περιπτώσεις, ενσωματωμένο λογισμικό διαχείρισης/replication (Unidirectional Gateway software) που τρέχει σε μικρούς embedded servers στη συσκευή.

Α.3 Αρχιτεκτονική Ασφαλούς Απομακρυσμένης Πρόσβασης σε OT

Η ασφαλής απομακρυσμένη πρόσβαση αποτελεί έναν από τους κεντρικούς φορείς παραβίασης σε OT περιβάλλοντα — το 65% των OT περιβαλλόντων το 2024 είχε ανασφαλείς remote access διαδρομές (Dragos Inc., 2025), ενώ το ένα στα τέσσερα penetration tests εντοπίζει default credentials σε βιομηχανικά συστήματα. Η αρχιτεκτονική αναφοράς για ασφαλή remote access σε OT πρέπει να ακολουθεί τα SANS ICS 5 Critical Controls (Control #4) και να ενσωματώνει: Jump Server στη DMZ ως το μοναδικό σημείο εισόδου (Single Point of Entry), MFA για κάθε χρήστη ανεξαρτήτως ρόλου, session recording για audit trail, time-limited access tokens για vendor sessions, και Just-In-Time (JIT) access provisioning ώστε να μην υπάρχουν μόνιμα accounts. Στο μοντέλο αυτό, κανένας εξωτερικός χρήστης δεν έχει απευθείας πρόσβαση στο OT δίκτυο, συνδέεται αποκλειστικά στον Jump Server στη DMZ, και από εκεί εγκαθιδρύεται μια ξεχωριστή, ελεγχόμενη και παρακολουθούμενη σύνδεση στο OT στοιχείο-στόχο.

Παράρτημα Β – Case Studies Πραγματικών Περιστατικών και Εφαρμογών

Β.1 Colonial Pipeline (2021) – Ο κίνδυνος του IT/OT boundary

Η επίθεση DarkSide στο Colonial Pipeline τον Μάιο του 2021 αποτελεί ένα από τα πιο τεκμηριωμένα παραδείγματα IT/OT convergence κινδύνου σε κρίσιμη υποδομή. Οι επιτιθέμενοι απέκτησαν αρχική πρόσβαση μέσω ενός παλαιωμένου λογαριασμού VPN χωρίς MFA — ένα μόνο compromised password έφτανε — και ανέπτυξαν ransomware στο IT δίκτυο, κρυπτογραφώντας περίπου 100 GB δεδομένων. Το OT δίκτυο δεν μολύνθηκε άμεσα, αλλά η Colonial Pipeline αποφάσισε προληπτικά να διακόψει την αυτοματοποιημένη λειτουργία του αγωγού, εκτιμώντας ότι ο κίνδυνος lateral movement από IT σε OT ήταν πραγματικός. Το αποτέλεσμα ήταν η μεγαλύτερη διακοπή λειτουργίας αγωγού καυσίμων στις ΗΠΑ τις τελευταίες δεκαετίες, με άμεσες ελλείψεις καυσίμων στην Ανατολική Ακτή.

Τα βασικά μαθήματα που αναδεικνύονται από αυτό το περιστατικό, σε σχέση με τα πλαίσια και τις αρχιτεκτονικές που αναλύθηκαν σε αυτή την εργασία, είναι σαφή: η απουσία MFA σε κρίσιμα σημεία remote access (παραβίαση SANS Control #4), η ανεπαρκής segmentation μεταξύ IT και OT (παραβίαση IEC 62443-3-2 και NIST CSF Protect), η έλλειψη OT-specific incident response plan που θα επέτρεπε συνέχιση λειτουργίας υπό συνθήκες IT breach (παραβίαση SANS Control #1), και η ανεπαρκής ορατότητα σε πραγματικό χρόνο για εντοπισμό lateral movement (παραβίαση NIST CSF Detect). Μετά την επίθεση, η TSA εξέδωσε υποχρεωτικές κυβερνοασφαλείας οδηγίες για όλους τους operators αγωγών, ενώ η εκτελεστική εντολή Biden για κυβερνοασφάλεια του Μαΐου 2021 επιτάχυνε ριζικά τη θέσπιση υποχρεωτικών απαιτήσεων για κρίσιμες υποδομές.

Β.2 TRITON/TRISIS (2017) – Στόχος τα Safety Instrumented Systems

Η επίθεση TRITON, που αποκαλύφθηκε το 2017 σε πετροχημική εγκατάσταση της Σαουδικής Αραβίας και αποδίδεται σε ομάδα με ρωσικές συνδέσεις (XENOTIME), αντιπροσωπεύει ένα ποιοτικά νέο είδος ICS attack: ο μόνος της στόχος ήταν να εκμεταλλευτεί τα Safety Instrumented Systems (SIS) των Schneider Electric Triconex controllers, τα οποία υπεύθυνα για την ασφαλή απενεργοποίηση της εγκατάστασης σε περίπτωση επικίνδυνης κατάστασης. Αν η επίθεση είχε επιτύχει πλήρως, θα μπορούσε να είχε οδηγήσει σε πραγματική καταστροφή με ανθρώπινες απώλειες, καθώς η απενεργοποίηση των SIS θα αφαιρούσε την τελευταία γραμμή άμυνας κατά φυσικής ατυχήματος. Ο ιός εντοπίστηκε τυχαία, όταν οι safety controllers εισήλθαν σε fail-safe mode ανιχνεύοντας anomaly — ακριβώς το είδος ανίχνευσης μέσω behavioral baseline που υποστηρίζεται από ML-based OT monitoring.

Τα μαθήματα αυτής της επίθεσης υπογραμμίζουν την κρισιμότητα της απομόνωσης Safety Zones σε ξεχωριστή ζώνη με SL-4 και data diodes, την αναγκαιότητα ελέγχου ακεραιότητας firmware για SIS controllers, την τεκμηρίωση και παρακολούθηση κάθε επικοινωνίας μέσω proprietary protocols (στο TRITON χρησιμοποιήθηκε reverse-engineered TriStation protocol), και τη σύνδεση της OT ασφάλειας με τις functional safety διαδικασίες (IEC 61511) έτσι ώστε κυβερνοαπειλές και physical safety να αντιμετωπίζονται ενιαία. Το 2022, κοινή ανακοίνωση FBI-CISA-NSA προειδοποίησε ότι το TRITON παραμένει ενεργή απειλή για παγκόσμιες κρίσιμες υποδομές.

Β.3 Norsk Hydro (2019) – Υπόδειγμα ανάκαμψης και διαφάνειας

Τον Μάρτιο του 2019, ο παγκόσμιος παραγωγός αλουμινίου Norsk Hydro δέχθηκε επίθεση ransomware LockerGoga που επηρέασε πάνω από 22.000 υπολογιστές σε 170 εγκαταστάσεις σε 40 χώρες. Η εταιρεία αρνήθηκε να πληρώσει λύτρα — ένα σπάνιο παράδειγμα αρχής στη διαχείριση ransomware — και αντέδρασε με πλήρη διαφάνεια απέναντι στο κοινό, οργανώνοντας ημερήσιες ζωντανές ενημερώσεις μέσω web. Η παραγωγή μεταπήδησε σε manual mode, με χαρτί και στυλό, και σε ορισμένες περιπτώσεις κλήθηκαν εργάτες από συνταξιοδότηση για να βοηθήσουν στη λειτουργία εγκαταστάσεων "με τον παλιό τρόπο". Το κόστος ξεπέρασε τα 70 εκατομμύρια δολάρια, αλλά η τιμή της μετοχής παρέμεινε σταθερή — απόδειξη ότι η διαφάνεια και η ανοιχτή επικοινωνία κρίσης έχουν αξία εμπιστοσύνης που αντισταθμίζει το οικονομικό κόστος.

Τα μαθήματα για τα πλαίσια που αναλύθηκαν στην εργασία αφορούν κυρίως τη σημασία: προ-ετοιμότητας για χειροκίνητη λειτουργία (manual fallback procedures, IEC 62443-2-1 απαίτηση), ύπαρξης δοκιμασμένου OT Incident Response Plan, offline backups που πράγματι λειτούργησαν, και καλλιέργειας οργανωσιακής κουλτούρας ετοιμότητας που έδωσε στη Norsk Hydro τη δυνατότητα να αντιδράσει αποτελεσματικά και διαφανώς. Η αντίδρασή της θεωρείται από τη βιομηχανική κυβερνοασφάλεια ως "gold standard" κρίσης διαχείρισης για OT περιστατικά.

B.4 Campari Group – Παγκόσμια εφαρμογή IEC 62443-2-1

Η Campari Group αποτελεί ένα από τα λίγα δημόσια τεκμηριωμένα case studies εφαρμογής IEC 62443-2-1 σε πολυεθνικό βιομηχανικό οργανισμό. Η εταιρεία εφάρμοσε ένα Security Management System για OT σε παγκόσμιο επίπεδο, ξεκινώντας με ένα pilot plant, διενεργώντας risk assessment κατά IEC 62443-3-2 σε συνδυασμό με Business Impact Analysis (ISO 22317) και θεσπίζοντας ένα operating model βασισμένο στις απαιτήσεις της IEC 62443-2-1 με σαφείς ρόλους εταιρικού και εργοστασιακού επιπέδου. Το μοντέλο επεκτάθηκε στη συνέχεια σε εργοστάσια παγκοσμίως, εφαρμόζοντας ομοιόμορφες πολιτικές OT ασφάλειας ανεξαρτήτως τοπικών ιδιαιτεροτήτων.

Το πρωτοποριακό στοιχείο της προσέγγισης της Campari ήταν η υιοθέτηση maturity-based roadmap αντί για εφάπαξ compliance: η εταιρεία χαρτογράφησε το τρέχον επίπεδο ωριμότητας ανά εγκατάσταση, όρισε στόχους βήμα προς βήμα και παρακολούθησε την πρόοδο μέσω KPIs, αποφεύγοντας την παγίδα της "paper compliance" και επιτυγχάνοντας πραγματική βελτίωση ασφάλειας. Αυτό το μοντέλο είναι ιδιαίτερα χρήσιμο για οργανισμούς που διαχειρίζονται μεγάλο αριθμό εγκαταστάσεων με ανομοιογενές επίπεδο ωριμότητας, όπως οι περισσότεροι παγκόσμιοι βιομηχανικοί όμιλοι.

Παράρτημα Γ – Εφαρμογή Αρχιτεκτονικής Ασφάλειας OT/IT σε Γραμμή Παραγωγής Έλασης Αλουμινίου (Γενικευμένη μελέτη περίπτωσης)

Γ1 Σκοπός και μεθοδολογία του παραρτήματος

Το παρόν παράρτημα αναπτύσσει, με μεγαλύτερη τεχνική λεπτομέρεια, την πρόταση αρχιτεκτονικής ασφάλειας OT/IT που παρουσιάστηκε στα προηγούμενα κεφάλαια, εφαρμόζοντάς την σε ένα συγκεκριμένο, αλλά γενικευμένο, βιομηχανικό σενάριο, μια γραμμή παραγωγής έλασης αλουμινίου (foil). Η επιλογή αυτού του σεναρίου δεν αντιστοιχεί σε συγκεκριμένη πραγματική εγκατάσταση πρόκειται για μια συνθετική, ενδεικτική αναπαράσταση, βασισμένη σε δημόσια διαθέσιμη βιομηχανική γνώση για τη διεργασία έλασης αλουμινίου, με στόχο να καταστήσει την προτεινόμενη αρχιτεκτονική απτή και ελέγξιμη.

Η ανάλυση οργανώνεται σε επτά ενότητες (α) περιγραφή της παραγωγικής διαδικασίας και αντιστοίχιση σε τυπικό OT εξοπλισμό, (β) ενδεικτικά σενάρια κυβερνοεπίθεσης ανά στάδιο παραγωγής, (γ) αναλυτική αρχιτεκτονική κατά το μοντέλο Purdue με ζώνες ασφαλείας, (δ) αρχιτεκτονική υπολογιστικών πόρων υψηλής διαθεσιμότητας (HA) και η διασύνδεσή της με το επίπεδο ελέγχου, (ε) μεθοδολογία ποσοτικοποίησης κινδύνου, (στ) μεθοδολογία δοκιμών διείσδυσης σε πραγματικά περιβάλλοντα και σε digital twins, και (ζ) συγκεντρωτική ανάλυση επιφάνειας επίθεσης με κατευθυντήριες γραμμές εφαρμογής.

Γ2 Η παραγωγική διαδικασία και ο αντίστοιχος OT εξοπλισμός

Η παραγωγή foil αλουμινίου ακολουθεί μια αλληλουχία σταδίων μηχανικής και θερμικής επεξεργασίας, από τη χύτευση της πρώτης ύλης έως την τελική κοπή και συσκευασία του προϊόντος. Κάθε στάδιο συνδυάζει φυσική διεργασία με ψηφιακό έλεγχο, και επομένως εισάγει τη δική του κατηγορία λειτουργικού τεχνολογικού (OT) εξοπλισμού.

Γ2.1 Στάδια παραγωγής

Στάδιο	Περιγραφή
Χύτευση πλακών (DC casting)	Το τηγμένο κράμα χύνεται σε καλούπι και στερεοποιείται σε πλάκες (slabs), υπό ελεγχόμενη ψύξη.
Φρεζάρισμα / scalping	Μηχανική αφαίρεση του εξωτερικού, οξειδωμένου στρώματος της πλάκας πριν τη θερμή έλαση.
Θερμή έλαση	Προοδευτική μείωση πάχους της πλάκας μέσω διαδοχικών περασμάτων σε υψηλή θερμοκρασία, έως τη μορφή coil.
Ψυχρή έλαση (tandem)	Πολλαπλές διαδοχικές έδρες έλασης σε θερμοκρασία περιβάλλοντος, με κρίσιμο σημείο τον έλεγχο δόνησης (chatter).
Ενδιάμεση ανόπτηση & έλαση foil	Θερμική κατεργασία που αποκαθιστά την ολκιμότητα του κράματος, ακολουθούμενη από τελική έλαση έως το ζητούμενο πάχος.
Κοπή (slitting) & οπτικός έλεγχος	Κοπή σε στενότερα ρολά και αυτοματοποιημένος οπτικός έλεγχος ποιότητας επιφάνειας.

Πηγή γενικής βιομηχανικής διεργασίας: δημόσια τεχνική βιβλιογραφία παραγωγής foil αλουμινίου (βλ. ενδεικτικές αναφορές στο Π.9).

Γ2.2 Ενδεικτικός OT εξοπλισμός ανά στάδιο

Στάδιο	Ενδεικτικός ΟΤ εξοπλισμός
Χύτευση πλακών	Θερμοστοιχεία/RTD τήγματος και ψυκτικού, αισθητήρες πίεσης/ροής, PLC ρυθμού χύτευσης, laser/ultrasonic μέτρηση πάχους.
Scalping	Encoders θέσης/βάθους κοπής, load cells δύναμης κοπής, αισθητήρες δόνησης κοπτικού.
Θερμή έλαση	Πυρόμετρα/θερμικές κάμερες, X-ray/isotope πάχους (Automatic Gauge Control), υδραυλικός έλεγχος διάκενου κυλίνδρων, αισθητήρες τάσης λωρίδας.
Ψυχρή έλαση (tandem)	Επιταχυνσιόμετρα δόνησης/chatter (δειγματοληψία έως 4 kHz), flatness meters, αισθητήρες τάσης λωρίδας, θερμοκρασία/ροή λιπαντικού, PLC/drives ανά έδρα με συγχρονισμό ταχύτητας.
Ανόπτηση & έλαση foil	PLC ελέγχου προφίλ θερμοκρασίας/χρόνου φούρνου, πολυζωνικοί αισθητήρες θερμοκρασίας, gauge control υψηλής ευαισθησίας.
Κοπή & οπτικός έλεγχος	Γραμμικές/matrix βιομηχανικές κάμερες, λογισμικό ταξινόμησης ελαττωμάτων, encoders κοπής, αισθητήρες τάνυσης περιέλιξης.

Γ2.3 Ασφάλεια διεργασίας: δόνηση, λιπαντικά, πυρόσβεση, οπτικός έλεγχος

Στην ψυχρή έλαση tandem, η ανεξέλεγκτη ταλάντωση (chatter) αποτελεί κρίσιμο κίνδυνο ποιότητας και εξοπλισμού τυπικά συστήματα παρακολούθησης δόνησης λειτουργούν με δειγματοληψία έως 4 kHz μέσω IEPE επιταχυνσιόμετρων και μειώνουν αυτόματα την ταχύτητα της γραμμής όταν ανιχνεύεται επικίνδυνη ταλάντωση, αποτρέποντας θραύση της λωρίδας. Η χαρακτηριστική ζώνη συχνοτήτων του λεγόμενου "third-octave" chatter σε βιομηχανικές εφαρμογές κινείται περίπου στα 100-120 Hz.

Η διεργασία έλασης χρησιμοποιεί μεγάλες ποσότητες εύφλεκτου λαδιού ψύξης/λίπανσης (rolling oil), γεγονός που καθιστά αναγκαία την ύπαρξη αισθητήρων θερμοκρασίας/ατμού λαδιού και αυτόματων συστημάτων πυρόσβεσης ανά ζώνη, τα οποία ενεργοποιούνται είτε χειροκίνητα είτε μέσω αυτόματης ανίχνευσης, πριν μια υπερθέρμανση εξελιχθεί σε πυρκαγιά.

Στο στάδιο του οπτικού ελέγχου, συστήματα τύπου machine-vision προσφέρουν πλήρη έλεγχο ποιότητας σε κάθε στάδιο παραγωγής αλουμινίου, από τη θερμή έλαση έως τον τελικό έλεγχο foil, συνδυάζοντας αισθητήρες εικόνας με εξειδικευμένη τεχνολογία φωτισμού για τον εντοπισμό ελαττωμάτων επιφάνειας σε πραγματικό χρόνο.

Γ3 Ενδεικτικά σενάρια κυβερνοαπειλών ανά στάδιο παραγωγής

Η ακόλουθη ανάλυση παραμένει σε επίπεδο κατηγορίας απειλής και αναμενόμενου αντίκτυπου, σύμφωνα με τη λογική δημόσιων πλαισίων αναφοράς (π.χ. MITRE ATT&CK for ICS), χωρίς αναφορά σε τεχνικές εκμετάλλευσης συγκεκριμένων ευπαθειών.

Στάδιο	Ενδεικτικό σενάριο	Αναμενόμενος αντίκτυπος
Χύτευση πλακών	Παραποίηση/MITM σε μη αυθεντικοποιημένη επικοινωνία αισθητήρα-PLC (θερμοκρασία ψυκτικού).	Εσφαλμένη στερεοποίηση κράματος, εσωτερικές ρωγμές δυσδιάγνωστες σε επόμενα στάδια, κίνδυνος υπερθέρμανσης.

Στάδιο	Ενδεικτικό σενάριο	Αναμενόμενος αντίκτυπος
Scalping	Compromise PLC βάθους κοπής μέσω μη τμηματοποιημένου δικτύου.	Ανεπαρκής αφαίρεση οξειδίων (ελαττώματα) ή υπερβολική κοπή (ζημιά εργαλείου/πλάκας).
Θερμή/ψυχρή έλαση	Παραποίηση σημάτων gauge/tension control ή εντολών bending.	Ανεξέλεγκτο chatter, θραύση λωρίδας, ανομοιόμορφο πάχος, πιθανή μηχανική ζημιά έδρας.
Ανόπτηση & έλαση foil	Αλλοίωση setpoint θερμοκρασίας/χρόνου φούρνου.	Ανεπαρκές μαλάκωμα κράματος, ενεργειακή σπατάλη, κίνδυνος πυρκαγιάς αν παρακαμφθούν interlocks.
Κοπή & οπτικός έλεγχος	Compromise/τύφλωση συστήματος οπτικού ελέγχου.	Quality escape: ελαττωματικό προϊόν διαφεύγει ανίχνευσης.

Γ3.1 Οριζόντια σενάρια σε επίπεδο εγκατάστασης

- Ransomware σε OT-adjacent servers (historians, HMI servers, engineering stations): διακοπή γραμμής χωρίς ανάγκη εξειδικευμένης γνώσης διεργασίας.
- Κατάχρηση remote access τρίτων (integrators/vendors): χωρίς χρονικά περιορισμένη, καταγεγραμμένη πρόσβαση, ένας compromised λογαριασμός δίνει ουσιαστικά ευρεία πρόσβαση.
- Lateral movement λόγω ανεπαρκούς segmentation: μια αρχική παραβίαση IT μπορεί να εξαπλωθεί σε πολλαπλά στάδια ταυτόχρονα.

Γ3.2 Ιστορικό παράδειγμα αναφοράς

Ένα τεκμηριωμένο, δημόσια αναφερμένο περιστατικό ανάλογης κατηγορίας βαριάς βιομηχανίας είναι η επίθεση σε γερμανικό χαλυβουργείο το 2014, σύμφωνα με έκθεση της γερμανικής ομοσπονδιακής υπηρεσίας πληροφορικής και ασφάλειας (BSI), οι επιτιθέμενοι απέκτησαν πρόσβαση στο δίκτυο γραφείων μέσω spear-phishing και κοινωνικής μηχανικής, και στη συνέχεια κινήθηκαν προς το δίκτυο παραγωγής, όπου η αλλοίωση λειτουργίας συστημάτων ελέγχου οδήγησε σε μη ελεγχόμενο τερματισμό υψικαμίνου και εκτεταμένη υλική ζημιά, χωρίς αναφερθέντες τραυματισμούς. Η έκθεση σημείωνε ότι η τεχνογνωσία των επιτιθέμενων δεν περιοριζόταν στην κλασική ασφάλεια IT, αλλά επεκτεινόταν σε λεπτομερή γνώση βιομηχανικών συστημάτων ελέγχου, μοτίβο άμεσα συναφές με τα οριζόντια σενάρια lateral movement που περιγράφηκαν παραπάνω.

Γ4 Αρχιτεκτονική κατά το μοντέλο Purdue με ζώνες ασφαλείας

Η προτεινόμενη αρχιτεκτονική οργανώνεται σε επτά επίπεδα, από το Level 5 (Enterprise) έως το Level 0 (Field/Process), με ρητά καθορισμένους ελέγχους ασφαλείας σε κάθε ζεύξη μεταξύ επιπέδων. Ο Πίνακας Π.4 συνοψίζει, για κάθε επίπεδο, ενδεικτικό εύρος διευθυνσιοδότησης (subnet), το περιεχόμενό του, και τον έλεγχο ασφαλείας που διαχωρίζει το επίπεδο από το αμέσως ανώτερο.

Επίπεδο	Ενδεικτικό subnet	Περιεχόμενο	Έλεγχος ζεύξης προς το ανώτερο επίπεδο
Level 5 - Enterprise	10.10.0.0/16	ERP, email, corporate IT, corporate AD	-

Επίπεδο	Ενδεικτικό subnet	Περιεχόμενο	Έλεγχος ζεύξης προς το ανώτερο επίπεδο
Level 4 - Site business	10.20.0.0/24	MES, προγραμματισμός παραγωγής, reporting	Corporate firewall
Level 3.5 - Industrial DMZ	10.30.0.0/24	Jump host/PAM, historian mirror, patch/AV relay	Firewall + AV/patch relay
Level 3 - Site operations	10.40.0.0/24	SCADA servers, engineering stations, τοπικό AD (χωρίς trust προς Enterprise)	Δύο ανεξάρτητα firewalls (defense-in-depth)
Level 2 - Area supervisory	10.50.x.0/24 ανά κυψέλη	HMI, τοπικό SCADA/DCS, τοπικός historian	Firewall + παθητικό IDS tap
Level 1 - Basic control	10.60.x.0/24, dedicated VLAN	PLC, drive controllers	Managed switch, VLAN segmentation
Level 0 - Field/process	Fieldbus/αναλογικό (όχι IP)	Αισθητήρες, actuators	Fieldbus gateway

Γ4.1 Το Industrial DMZ ως κρίσιμο σημείο αρχιτεκτονικής

Το Level 3.5 λειτουργεί ως ενδιάμεση, ελεγχόμενη ζώνη ανάμεσα στο εταιρικό IT (Level 4) και το επιχειρησιακό OT (Level 3), σύμφωνα με τη λογική άμυνας σε βάθος (defense-in-depth) που περιγράφει η σειρά προτύπων IEC 62443. Φιλοξενεί τρεις κατηγορίες συστημάτων, (α) υποδομή απομακρυσμένης πρόσβασης (jump host/bastion) με MFA και καταγραφή περιόδου σύνδεσης (Privileged Access Management), (β) μηχανισμό αντιγραφής δεδομένων historian προς το IT, τυπικά μονόδρομης ροής, και (γ) relay ενημερώσεων/antivirus, ώστε καμία ενημέρωση να μην κατεβαίνει απευθείας από το Level 4 στο Level 3.

Γ4.2 Πρωτόκολλα σύνδεσης στα επίπεδα 0 έως 2

Η ροή δεδομένων από το πεδίο προς την εποπτεία ακολουθεί τυπικά τρία στρώματα πρωτοκόλλων, στο Level 0, οι αισθητήρες επικοινωνούν μέσω αναλογικού σήματος (4-20 mA), HART, ή IO-Link προς τοπικές μονάδες εισόδου/εξόδου. Στο Level 1, οι μονάδες αυτές τροφοδοτούν το PLC μέσω βιομηχανικού Ethernet (Profinet) ή Modbus/TCP, το δεύτερο ευρέως διαδεδομένο αλλά χωρίς εγγενή μηχανισμό αυθεντικοποίησης, γεγονός που μεταθέτει την ευθύνη προστασίας στο επίπεδο της αρχιτεκτονικής τμηματοποίησης. Στο Level 2, το PLC μεταδίδει δεδομένα προς SCADA/HMI μέσω OPC-UA, πρωτοκόλλου που υποστηρίζει εγγενώς αυθεντικοποίηση και κρυπτογράφηση, σε αντίθεση με το Modbus.

Γ4.3 Απομόνωση δικτύου διαχείρισης cluster από το OT

Ιδιαίτερη προσοχή απαιτεί ο διαχωρισμός ανάμεσα στο δίκτυο παραγωγικής κίνησης (VM/production network) των εικονικών μηχανών εποπτείας, το οποίο συνδέεται νόμιμα με το Level 1 μέσω firewall με κανόνες τύπου allow-list (π.χ. επιτρεπτή μόνο κίνηση OPC-UA σε συγκεκριμένη θύρα, ή Modbus/TCP προς συγκεκριμένα PLC), και το εσωτερικό δίκτυο διαχείρισης/heartbeat του cluster, το οποίο δεν εξυπηρετεί κανέναν λειτουργικό σκοπό ελέγχου διεργασίας και επομένως πρέπει να έχει ρητή πολιτική άρνησης δρομολόγησης (deny-by-default) προς το Level 1. Η απουσία ρητού κανόνα άρνησης, αντί για απλή απουσία κανόνα επιτρεπτικότητας, τεκμηριώνεται και σε ελέγχους συμμόρφωσης.

Γ5 Αρχιτεκτονική υπολογιστικών πόρων υψηλής διαθεσιμότητας

Οι εικονικές μηχανές που φιλοξενούν SCADA/HMI εφαρμογές και τοπικό historian τοποθετούνται σε συστάδα (cluster) τριών κόμβων εικονικοποίησης, σχεδιασμένη ώστε καμία μεμονωμένη αστοχία εξοπλισμού να μην οδηγεί σε απώλεια εποπτείας της παραγωγικής διαδικασίας.

Γ5.1 Επίπεδο υπολογιστικών κόμβων

Ένα cluster τριών κόμβων με ενεργοποιημένες τις λειτουργίες υψηλής διαθεσιμότητας (HA) και ισοκατανομής φόρτου (DRS) προσφέρει πλεονασμό τύπου N+1, σε περίπτωση απώλειας ενός κόμβου, οι εικονικές μηχανές του επανεκκινούνται αυτόματα στους υπόλοιπους δύο. Κάθε φυσικός server διαθέτει τέσσερις δικτυακές κάρτες (NIC) με διακριτό ρόλο η καθεμία, διαχείριση (management), μετακίνηση ζωντανών μηχανών (vMotion), παραγωγική κίνηση (VM/production network), και συγχρονισμό cluster (heartbeat), καθώς και ξεχωριστή οπτική σύνδεση προς το σύστημα αποθήκευσης.

Γ5.2 Επίπεδο δικτύου και πλεονάζοντα switches

Κάθε λειτουργική κάρτα δικτύου συνδέεται ταυτόχρονα σε δύο ανεξάρτητα switches, με σχήμα active/standby ή active/active teaming, ώστε η πλήρης αστοχία ενός switch να μην προκαλεί διακοπή. Προϋπόθεση αποτελεσματικότητας είναι τα δύο switches να μην μοιράζονται κοινή πηγή τροφοδοσίας ή κοινό uplink.

Γ5.3 Επίπεδο αποθήκευσης, dual controller, ALUA, multipathing

Σύμφωνα με τεχνική τεκμηρίωση συστημάτων αποθήκευσης της κατηγορίας, τα συστήματα αυτά συμμορφώνονται με το πρότυπο SCSI-3 για Asymmetric Logical Unit Access (ALUA) τα συστήματα αυτής της κατηγορίας παρέχουν στον host πληροφορία optimal/non-optimal διαδρομής κατά την ανακάλυψη συσκευών, αξιοποιήσιμη μόνο εφόσον οι servers έχουν ρυθμιστεί με multipath I/O (MPIO). Στην πράξη, κάθε server διατηρεί δύο ανεξάρτητες διαδρομές προς το ίδιο λογικό τμήμα αποθήκευσης (LUN) μία ανά ελεγκτή αποθήκευσης, μέσω ξεχωριστού switch η καθεμία ώστε η απώλεια ενός ελεγκτή ή switch να μην διακόπτει τη λειτουργία.

Γ6 Μεθοδολογία ποσοτικοποίησης κινδύνου

Για την ιεράρχηση των ζωνών της αρχιτεκτονικής ως προς την προτεραιότητα εφαρμογής μέτρων ασφαλείας, προτείνεται ένα πενταβάθμιο μοντέλο κινδύνου, το οποίο ενσωματώνει ρητά τον ανθρώπινο και περιβαλλοντικό παράγοντα δίπλα στον καθαρά οικονομικό/λειτουργικό αντίκτυπο, στοιχείο που διαφοροποιεί το OT risk assessment από το αντίστοιχο κλασικό IT.

Γ6.1 Ο τύπος υπολογισμού

- Βήμα 1 - Πιθανότητα (Likelihood, L): L = MO(Threat exposure, Vulnerability exposure), κλίμακα 1-5.
- Βήμα 2 - Σταθμισμένος αντίκτυπος (Weighted Impact, WI): WI = Safety·W1 + Environmental·W2 + Production·W3 + Reputation·W4, όπου τα βάρη αθροίζουν σε 100%.
- Βήμα 3 - Έμφυτο ρίσκο (Inherent Risk): IR = L × WI.
- Βήμα 4 - Αποτελεσματικότητα υφιστάμενων ελέγχων (Control Effectiveness, CE): εκτίμηση 0%-100%.

- Βήμα 5 - Υπολειπόμενο ρίσκο (Residual Risk): RR = IR × (1 − CE), κατηγοριοποιούμενο ως Χαμηλό (≤3) / Μέτριο (3-6) / Υψηλό (6-10) / Κρίσιμο (>10).

Γ6.2 Ενδεικτική εφαρμογή στην αρχιτεκτονική

Ο Πίνακας Π.6 παρουσιάζει ενδεικτικά αποτελέσματα εφαρμογής του μοντέλου στις κύριες ζώνες της αρχιτεκτονικής, με βάρη Safety 35%, Environmental 15%, Production 30%, Reputation/Compliance 20%. Οι τιμές εισόδου (threat/vulnerability exposure, τέσσερις διαστάσεις αντικτύπου, αποτελεσματικότητα ελέγχων) είναι ενδεικτικές παραδείγματα προς επίδειξη της μεθοδολογίας.

Ζώνη	Purdue level	Έμφυτο ρίσκο (IR)	Υπολειπόμενο ρίσκο (RR)	Κατηγορία
Χύτευση πλακών	0/1	7.88	3.15	Μέτριο
Scalping	0/1	6.25	2.81	Χαμηλό
Θερμή έλαση	1	9.90	4.46	Μέτριο
Ψυχρή έλαση (tandem)	1	12.78	6.39	Υψηλό
Ανόπτηση & έλαση foil	1	8.85	3.98	Μέτριο
Κοπή & οπτικός έλεγχος	2	5.50	2.75	Χαμηλό
HA cluster (SCADA/HMI VMs)	2/3	8.25	2.48	Χαμηλό
Industrial DMZ	3.5	7.95	1.99	Χαμηλό
Site business / MES	4	6.00	2.40	Χαμηλό
APS/SCM scheduling	4	6.30	2.52	Χαμηλό
Enterprise / IT	5	6.30	2.52	Χαμηλό

Παρατηρείται ότι η ψυχρή έλαση (tandem) εμφανίζει το υψηλότερο υπολειπόμενο ρίσκο, λόγω συνδυασμού υψηλού αντικτύπου στην παραγωγή και μέτριας έκθεσης ευπάθειας. Αντίθετα, το Industrial DMZ, παρότι εμφανίζει την υψηλότερη πιθανότητα στόχευσης σε όλη την αρχιτεκτονική, καταλήγει σε χαμηλό υπολειπόμενο ρίσκο λόγω της υψηλής αποτελεσματικότητας των ελέγχων που προβλέπονται εκεί (75%), εύρημα που τεκμηριώνει εμπειρικά την αποτελεσματικότητα της αρχής άμυνας σε βάθος.

Γ7 Μεθοδολογία δοκιμών διείσδυσης (penetration testing) σε OT περιβάλλοντα

Γ7.1 Δοκιμές σε πραγματικά περιβάλλοντα

Η θεμελιώδης διαφορά ανάμεσα σε OT και IT penetration testing δεν έγκειται στο αντικείμενο αλλά στη μέθοδο, η ενεργή εκμετάλλευση ευπάθειας σε ζωντανό OT σύστημα μπορεί να προκαλέσει πραγματική διακοπή παραγωγής ή σε ακραίες περιπτώσεις, κίνδυνο ασφάλειας προσωπικού, κάτι

που δεν ισχύει με την ίδια βαρύτητα σε τυπικά IT περιβάλλοντα. Για τον λόγο αυτό, οι σύγχρονες μεθοδολογίες OT penetration testing βασίζονται σε τεχνικές συλλογής πληροφορίας που δεν αποστέλλουν δυνητικά διασπαστική κίνηση προς συστήματα εποπτικού ελέγχου, παθητική παρακολούθηση δικτύου, ανάλυση καταγεγραμμένης κίνησης, εξέταση αρχείων παραμετροποίησης αντί για ενεργό probing σε ζωντανά συστήματα.

Μια δομημένη διαδικασία OT pentest απαιτεί, σε αντίθεση με το IT όπου οι δοκιμαστές συχνά εργάζονται ανεξάρτητα, συνεχή συνεργασία με ομάδες operations που γνωρίζουν το πρόγραμμα παραγωγής, μηχανικούς ελέγχου που γνωρίζουν τις εξαρτήσεις συστημάτων, υπεύθυνους ασφαλείας (safety officers) ικανούς να αναγνωρίσουν σενάρια κινδύνου, και προσωπικό συντήρησης έτοιμο να ανταποκριθεί σε απρόβλεπτα προβλήματα. Κάθε ενεργή δοκιμή που ενδέχεται να επηρεάσει controllers ή κρίσιμα δίκτυα πρέπει είτε να πραγματοποιείται σε απομονωμένο εργαστήριο, είτε με αυστηρό change control και παρουσία προσωπικού operations/safety.

Πλαίσια αναφοράς

- NIST SP 800-82r3 - καθοδήγηση ασφάλειας ειδικά για OT, με ενότητα assessment προσαρμοσμένη στους περιορισμούς διαθεσιμότητας.
- MITRE ATT&CK for ICS - ταξινομικό πλαίσιο τεχνικών επίθεσης σε βιομηχανικά περιβάλλοντα.
- IEC 62443-3-3 - τεχνικές απαιτήσεις ασφάλειας ανά security level, βάση ελέγχου συμμόρφωσης.

Γ7.2 Δοκιμές μέσω digital twin

Η χρήση digital twin, ενός εικονικού αντιγράφου του OT περιβάλλοντος με επαρκή πιστότητα ως προς τη συμπεριφορά του πραγματικού συστήματος, επιτρέπει επιθετικές δοκιμές χωρίς κανένα ρίσκο για τα πραγματικά συστήματα παραγωγής, ενώ η ζημιά στο twin δεν επηρεάζει τη λειτουργία, αφού το twin μπορεί εύκολα να επαναφερθεί σε αρχική κατάσταση. Δεν απαιτείται η ίδια πιστότητα προσομοίωσης σε όλα τα τμήματα ενός σύνθετου συστήματος, τα στοιχεία που αποτελούν τον στόχο της δοκιμής (π.χ. συγκεκριμένα PLC) χρειάζονται πολύ πιστό twin (emulation/virtualization), ενώ ο περιβάλλων εξοπλισμός μπορεί να αναπαρίσταται με απλούστερο μοντέλο.

Ακαδημαϊκή ανασκόπηση για την εφαρμογή digital twins σε κυβερνοασφάλεια αναφέρει ότι η χρήση τους σε penetration testing προσφέρει διττό όφελος, εκτενέστερη αξιολόγηση κινδύνου και μηδενικό χρόνο διακοπής (zero downtime), σε αντίθεση με δοκιμές σε ζωντανά συστήματα όπου συγκεκριμένες διαδρομές, τεχνικές ή εργαλεία αποφεύγονται λόγω δυνητικής επίδρασης στη διαθεσιμότητα.

Ενδεικτικά PoC και επιχειρηματικές περιπτώσεις

Το ερευνητικό ινστιτούτο Fraunhofer AISEC (Γερμανία) διατηρεί πραγματικό testbed πάνω σε OT εξοπλισμό εγκατεστημένο σε πραγματική γραμμή παραγωγής του ιδρύματος, χρησιμοποιώντας digital twins συγκεκριμένων PLCs για penetration testing, με διαφοροποιημένο επίπεδο πιστότητας ανά στοιχείο του συστήματος.

Στον εμπορικό χώρο, η General Electric αναφέρεται να χρησιμοποιεί digital twins μηχανημάτων για ανίχνευση ανωμαλιών συμπεριφοράς μέσω συστήματος που ονομάζει «Digital Ghost», το οποίο

υποστηρίζει ανίχνευση, εντοπισμό, πρόβλεψη και εξουδετέρωση κακόβουλης δραστηριότητας,ενώ αναφέρεται ότι και η Siemens αναπτύσσει ανάλογες δυνατότητες ανίχνευσης κυβερνοεπιθέσεων μέσω digital twins.

Σε ακαδημαϊκό επίπεδο, δημοσιευμένη έρευνα (Sensors, 2025) παρουσιάζει πλαίσιο Digital Twin-driven Intrusion Detection (DT-ID) για SCADA βιομηχανίας επεξεργασίας νερού, το οποίο ενσωματώνει προσομοίωση διεργασίας υψηλής πιστότητας, μοντελοποίηση αισθητήρων σε πραγματικό χρόνο, και επιθέσεων false data injection, denial-of-service, εντολές έγχυσης. Το σύστημα πέτυχε F1-score ανίχνευσης 96,3% με μέσο χρόνο ανίχνευσης κάτω από 500 ms, επίδοση σαφώς ανώτερη από συμβατικά IDS βασισμένα σε κανόνες ή αποκλειστικά σε φυσικό μοντέλο.

Γ8 Ανάλυση επιφάνειας επίθεσης και κατευθυντήριες γραμμές

Εξετάζοντας συνολικά την αρχιτεκτονική (παραγωγικά στάδια, cluster υψηλής διαθεσιμότητας, Industrial DMZ, λογισμικό προγραμματισμού παραγωγής), προκύπτουν τρία συμπεράσματα άμεσα σχετικά με τον σχεδιασμό αρχιτεκτονικών ασφάλειας OT/IT:

- Το ρίσκο δεν κατανέμεται ομοιόμορφα κατά μήκος της αρχιτεκτονικής, συγκεντρώνεται εκεί όπου ο συνδυασμός φυσικού/παραγωγικού αντικτύπου είναι υψηλότερος (Γ6.2: ψυχρή έλαση tandem), όχι απαραίτητα εκεί όπου η δικτυακή έκθεση είναι μεγαλύτερη.
- Ζώνες υψηλής έκθεσης (π.χ. Industrial DMZ) μπορούν να καταλήξουν σε χαμηλό υπολειπόμενο ρίσκο, εφόσον συνοδεύονται από ανάλογα υψηλή αποτελεσματικότητα ελέγχων, εμπειρική επιβεβαίωση της αρχής άμυνας σε βάθος.
- Ο σχεδιασμός πλεονασμού (redundancy) στο επίπεδο υπολογιστικών πόρων λειτουργεί και ως έλεγχος ασφαλείας καθαυτός, όχι μόνο ως μέτρο διαθεσιμότητας, μειώνοντας τον υπολειπόμενο κίνδυνο ζωνών που φιλοξενούν κρίσιμα φορτία εργασίας.

Γ8.1 Ιδιαιτερότητες OT και κατευθυντήριες γραμμές εφαρμογής (baseline)

Η ενότητα αυτή συνοψίζει τις πρακτικές αρχές που θα πρέπει να λάβει υπόψη κάθε μελλοντικός αναγνώστης/εφαρμοστής αντίστοιχης αρχιτεκτονικής, οργανωμένες ως σειρά ιδιαιτεροτήτων του OT σε σχέση με το κλασικό IT.

Αρχή	Πρακτική συνέπεια
Διαθεσιμότητα πριν από εμπιστευτικότητα	Κάθε μέτρο ασφαλείας αξιολογείται πρώτα ως προς την επίδρασή του στη συνέχεια της διεργασίας.
Segmentation ως θεμέλιο, όχι πρόσθετο μέτρο	Τα όρια Purdue σχεδιάζονται πρώτα, όχι ως ύστερη προσθήκη.
Patching ως ρίσκο-έναντι-ρίσκου	Κάθε ενημέρωση δοκιμάζεται σε lab/digital twin πριν την ανάπτυξη, με προβλεπόμενο σχέδιο rollback.
Αντιστάθμιση, όχι διόρθωση, legacy πρωτοκόλλων	Το Modbus δεν αποκτά αυθεντικοποίηση ο κίνδυνος περιορίζεται αρχιτεκτονικά (ζώνες, conduits, whitelisting).
Διαχείριση πρόσβασης τρίτων	Remote access integrators/vendors χρονικά περιορισμένη, με MFA, μέσω PAM/jump host.
Παθητική, όχι ενεργή, παρακολούθηση σε ζωντανά συστήματα	Ενεργές δοκιμές μόνο σε digital twin ή προγραμματισμένο maintenance window.

Αρχή	Πρακτική συνέπεια
Φυσική ασφάλεια Level 0/1	Κανένα δικτυακό μέτρο δεν αντικαθιστά τον έλεγχο φυσικής πρόσβασης στον εξοπλισμό πεδίου.
Πλεονασμός ως έλεγχος ασφαλείας	Ο σχεδιασμός redundancy μειώνει το blast radius μιας παραβίασης, όχι μόνο τον χρόνο διακοπής.
Incident response με συμμετοχή safety officer	Η απόφαση ανάμεσα σε γρήγορη επαναφορά και ελεγχόμενη υποβάθμιση λειτουργίας δεν είναι αμιγώς τεχνική απόφαση.
Πλήρης απογραφή assets ως προϋπόθεση	Καμία τμηματοποίηση, έλεγχος ή παρακολούθηση δεν είναι ουσιαστική χωρίς πλήρη γνώση των υφιστάμενων assets.

Βιβλιογραφία

1. ACET Solutions. (2026, March). *ISA/IEC 62443: Why Implementation Fails and What OT Leaders Need to Know*. https://www.acetsolutions.com/isa-iec-62443-implementation-failures-ot-leaders/

2. Cybersecurity and Infrastructure Security Agency. (2024). *Post-Quantum Cryptography for Operational Technology: Key Takeaways and Next Steps*. CISA. https://postquantum.com/quantum-policy/dhs-cisa-pqc-ot/

3. Cybersecurity and Infrastructure Security Agency. (2025). *Secure Integration of Artificial Intelligence in Operational Technology Environments: Principles and Guidance for Critical Infrastructure*. CISA. https://industrialcyber.co/download/secure-integration-of-ai-in-ot-principles-and-guidance-for-critical-infrastructure-cisa/

4. Cybersecurity and Infrastructure Security Agency. (2026). *Zero Trust Roadmap for OT Environments Facing Legacy Constraints*. CISA. https://industrialcyber.co/zero-trust/new-cisa-guidance-outlines-zero-trust-roadmap-for-ot-environments-facing-legacy-constraints/

5. CyTAL. (2026, March). *IEC 62443 vs NIST: How the Two Frameworks Compare and When to Use Each*. https://cytal.co.uk/blog/iec-62443-vs-nist-how-the-two-frameworks-compare-and-when-to-use-each/

6. Dragos Inc. (2022). *Improving ICS/OT Security Perimeters with Network Segmentation*. https://www.dragos.com/blog/improving-ics-ot-security-perimeters-with-network-segmentation

7. Dragos Inc. (2024). *The SANS ICS Five Critical Controls: A Practical Framework for OT Cybersecurity*. Dragos Inc. https://www.dragos.com/blog/the-sans-ics-five-critical-controls-a-practical-framework-for-ot-cybersecurity/

8. Dragos Inc. (2025). *2025 OT/ICS Cybersecurity Report: A Year in Review*. Dragos Inc. https://www.dragos.com/dragos-2025-ot-cybersecurity-report-a-year-in-review

9. European Parliament and Council of the European Union. (2022, December). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

10. European Union Agency for Cybersecurity. (2019). *Industry 4.0 – Cybersecurity Challenges and Recommendations*. ENISA. https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

11. European Union Agency for Cybersecurity. (2023). *Zoning and Conduits for Railways – Security Architecture*. ENISA. https://www.enisa.europa.eu/sites/default/files/publications/Zoning_and_Conduits_Railways.pdf

12. FBI, CISA, & NSA. (2022). *TRITON Malware Remains Threat to Global Critical Infrastructure* (Joint Cybersecurity Advisory). U.S. Government. https://www.ic3.gov/CSA/2022/220325.pdf

13. Frenos. (2025, July). *Why Simulated OT Pen Tests Beat Traditional Ones: The Digital Twin Advantage*. https://frenos.io/blog/why-your-next-ot-penetration-test-should-be-simulated-the-digital-twin-advantage

14. Hyperproof. (2024, March). *NIST CSF 2.0: Everything You Need to Know About the Update*. https://hyperproof.io/resource/nistcsf2-0-update/

15. IIoT World. (2026, April). *Top 7 ICS/OT Cybersecurity Trends and Frameworks for 2026*. https://www.iiot-world.com/ics-security/ics-ot-cybersecurity-trends-2026/

16. Industrial Cyber. (2025, April). *Integrating AI and ML Technologies Across OT, ICS Environments to Enhance Anomaly Detection*. https://industrialcyber.co/features/integrating-ai-and-ml-technologies-across-ot-ics-environments-to-enhance-anomaly-detection-and-incident-response/

17. Industrial Cyber. (2026, April). *Industrial Systems Face Structural Gap as Quantum Risks Drive Urgency for Crypto-Agility*. https://industrialcyber.co/features/industrial-systems-face-structural-gap-as-quantum-risks-drive-urgency-for-crypto-agility-and-pqc-migration/

18. INL CyOTE Program. (2025). *DarkSide Ransomware Attack on Colonial Pipeline: Case Study*. Idaho National Laboratory. https://cyote.inl.gov/content/uploads/24/2025/12/CyOTE-Case-Study_Colonial-Pipeline.pdf

19. International Electrotechnical Commission. (2013). *IEC 62443-3-3:2013 – Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels* [International Standard]. IEC.

20. International Electrotechnical Commission. (2018). *IEC 62443-4-1:2018 – Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements* [International Standard]. IEC.

21. International Electrotechnical Commission. (2019). *IEC 62443-4-2:2019 – Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components* [International Standard]. IEC.

22. International Electrotechnical Commission. (2020). *IEC 62443-3-2:2020 – Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design* [International Standard]. IEC.

23. International Electrotechnical Commission. (2024). *IEC 62443-2-1:2024 – Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners* [International Standard]. IEC.

24. ISACA. (2025). *IT/OT Convergence: An Era of Interconnected Risk and Reward*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/an-era-of-interconnected-risk-and-reward

25. ISAGCA & Hexagon/Iotatec. (2024). *Campari Group Case Study: Applying ISA/IEC 62443 to Operating Technology Security Management Systems*. ISASecure. https://www.isasecure.org/hubfs/ISAGCA%20Campari%20Group%20H-ON%20%2016%20May%202024-1.pdf

26. Jaatun, M. G. & others. (2024). Implementation of Zones and Conduits in Industrial Control and Automation Systems. *Proceedings of ICS Security Research*. https://jaatun.no/papers/2024/Zones-and-Conduits.pdf

27. KPMG Germany. (2025). *IT-OT Cyber Security Convergence Framework*. KPMG. https://assets.kpmg.com/content/dam/kpmg/de/pdf/Themen/2025/04/kpmg-it-ot-cyber-convergence-framework.pdf

28. Liu, Y. & others. (2025). Application of Big Data Technology in Enterprise Information Security Risk Assessment. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-85403-6

29. Marsh. (2018). *Triton – The Deadly New Industrial Cyberweapon*. Marsh. https://www.marsh.com/content/dam/marsh/Documents/PDF/en_au/triton-deadly-new-industrial-cyberweapon.pdf

30. Microsoft. (2023). *Hackers Hit Norsk Hydro with Ransomware. The Company Responded with Transparency*. https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

31. National Cyber Security Centre (NCSC-UK). (2025). *Timelines for Migration to Post-Quantum Cryptography*. NCSC. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

32. National Institute of Standards and Technology. (2023a). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework

33. National Institute of Standards and Technology. (2023b). *Guide to Operational Technology (OT) Security* (NIST SP 800-82 Rev. 3). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-82r3

34. National Institute of Standards and Technology. (2024a). *Module-Lattice-Based Digital Signature Standard* (FIPS 204). U.S. Department of Commerce. https://csrc.nist.gov/pubs/fips/204/final

35. National Institute of Standards and Technology. (2024b). *Module-Lattice-Based Key-Encapsulation Mechanism Standard* (FIPS 203). U.S. Department of Commerce. https://csrc.nist.gov/pubs/fips/203/final

36. National Institute of Standards and Technology. (2024c). *NIST IR 8547 Initial Public Draft: Transition to Post-Quantum Cryptography Standards* (NIST IR 8547 ipd). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

37. National Institute of Standards and Technology. (2024d). *Stateless Hash-Based Digital Signature Standard* (FIPS 205). U.S. Department of Commerce. https://csrc.nist.gov/pubs/fips/205/final

38. National Institute of Standards and Technology. (2024e). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

39. National Institute of Standards and Technology. (2025). *Security and Trust Considerations for Digital Twin Technology* (NIST IR 8356). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8356.pdf

40. NexusConnect. (2026, January). *5 Trends Driving OT Security in 2026: From State-Sponsored Attacks to AI-Powered Threats*. https://nexusconnect.io/articles/5-trends-driving-ot-security-in-2026-from-state-sponsored-attacks-to-ai-powered-threats

41. NSA, CISA, & ASD's ACSC. (2025). *Principles for the Secure Integration of Artificial Intelligence in Critical Infrastructure*. NSA. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4347041/

42. OneKey. (2026). *Tackling Software Supply Chain Risks with IEC 62443 and SBOM*. OneKey. https://www.onekey.com/resource/tackling-software-supply-chain-risks-with-iec-62443-and-sbom

43. OTbase. (2025). *Why IEC 62443 Demands an OT Asset Inventory*. OTbase. https://otbase.com/wp-content/uploads/2025/10/Why-IEC-62443-Demands-an-OT-Asset-Inventory.pdf

44. OTNexus. (2025a, July). *NIST CSF for OT Environments: A Practical Breakdown*. https://otnexus.com/nist-csf-for-ot-environments-a-practical-breakdown/

45. OTNexus. (2025b, August). *OT Compliance in 2025: Where Do Most Organizations Fall Short?* https://otnexus.com/ot-compliance-in-2025-where-do-most-organizations-fall-short/

46. Palo Alto Networks. (2024a). *State of OT Security Report 2024*. Palo Alto Networks. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/state-of-ot-security-report-2024.pdf

47. Palo Alto Networks. (2024b). *What Is the Purdue Model for ICS Security?* https://www.paloaltonetworks.com/cyberpedia/what-is-the-purdue-model-for-ics-security

48. PricewaterhouseCoopers. (2026). *Geopolitical Shifts Amplify OT Security Risks*. PwC. https://www.pwc.com/gx/en/issues/cybersecurity/geopolitical-shifts-amplify-ot-risks.html

49. SANS Institute. (2024). *State of ICS/OT Cybersecurity 2024*. SANS Institute. https://info.opswat.com/hubfs/FY24%20OT-IND%20Assets/Survey_2024-ICS-OT-Cybersecurity_Opswat.pdf

50. Shieldworkz. (2026, April). *How to Align OT Security with NIST CSF and IEC 62443*. https://shieldworkz.com/blogs/how-to-align-ot-security-with-nist-csf-and-iec-62443

51. Technische Universiteit Eindhoven. (2025). *A Digital Twin Framework for Cybersecurity Testing of OT Networks*. Eindhoven University of Technology. https://research.tue.nl/en/publications/a-digital-twin-framework-for-cybersecurity-testing-of-ot-networks/

52. Telstra International & Omdia Research. (2024). *Secure Manufacturing: The Challenges of IT/OT Convergence*. Telstra International. https://www.telstrainternational.com/content/dam/shared-component-assets/telstra-international/global/news-research/research/secure-manufacturing.pdf

53. TXOne Networks. (2022). *Securing Digital Manufacturing: The Essence of ISA/IEC 62443 Implementation*. TXOne Networks. https://itsocial.fr/wp-content/uploads/2023/09/Securing-Digital-Manufacturing-The-Essence-of-ISA-IEC-62443-Implementation-TXOne.pdf

54. TXOne Networks. (2026). *2026 Annual OT/ICS Cybersecurity Report*. TXOne Networks. https://www.txone.com/security-reports/annual-ot-ics-cybersecurity-report-2026/

55. Various Authors. (2021). IT/OT Convergence and Cybersecurity. *Computer & Security*. https://www.sciencedirect.com/science/article/abs/pii/S1361372321001299

56. Various Authors. (2022). Analysis of 2019 LockerGoga Cyber-Attack to Norsk Hydro Multinational Company. *European Journal of Mathematics and Computer Science*. https://geniusjournals.org/index.php/ejmc/article/download/2132/1858/2158

57. Various Authors. (2024a). A Real-Time Network Based Anomaly Detection in Industrial Control Systems. *Digital Communications and Networks*. https://www.sciencedirect.com/science/article/abs/pii/S1874548224000179

58. Various Authors. (2024b). Colonial Pipeline Cyberattack Drives Urgent Reforms in Critical Infrastructure Protection. *Oil, Gas & Coal Engineering*, *12*(5). https://www.sciencepublishinggroup.com/article/10.11648/j.ogce.20241205.11

59. Various Authors. (2025a). *Cyber Security of OT Networks: A Tutorial and Survey*. https://arxiv.org/html/2502.14017v2

60. Various Authors. (2025b). *On the Practical Feasibility of Harvest-Now, Decrypt-Later Attacks on Industrial Systems*. https://arxiv.org/html/2603.01091v1

61. WaterISAC. (2025, December). *CISA and Partners Publish Guidance on the Principles for the Secure Integration of Artificial Intelligence in OT*. https://www.waterisac.org/tlpclear-cisa-and-partners-publish-guidance-on-the-principles-for-the-secure-integration-of-artificial-intelligence

62. Wiseplant. (2025). *IEC Publishes IEC 62443-2-1:2024, Setting Security Standards for Industrial Automation and Control Systems*. https://wiseplant.com/iec-publishes-iec-62443-2-12024-setting-security-standards-for-industrial-automation-and-control-systems/

63. Brooks, C. J. (n.d.). *Practical Industrial Cybersecurity*.

64. Bryant, T. (2020). *PTFM: Purple Team Field Manual*. Verlag nicht ermittelbar.

65. Candell Jr., R., Zimmerman, T. A., & Stouffer, K. A. (2015). *An Industrial Control System Cybersecurity Performance Testbed* (NIST IR 8089; p. NIST IR 8089). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8089

66. European Union Agency for Cybersecurity. (2023). *Good practices for supply chain cybersecurity.* Publications Office. https://doi.org/10.2824/805268

67. Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Knopf Doubleday Publishing Group.

68. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). *Cyber-Physical Systems Security—A Survey* (arXiv:1701.04525). arXiv. https://doi.org/10.48550/arXiv.1701.04525

69. Joint Task Force Interagency Working Group. (2020). *Security and Privacy Controls for Information Systems and Organizations* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

70. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

71. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to Operational Technology (OT) security* (NIST SP 800-82r3; p. NIST SP 800-82r3). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-82r3

72. Teumim, D. J. (2010). *Industrial network security* (2nd ed). ISA. https://doi.org/10.1002/9781394442348

73. Aluminum foil manufacturing process (γενική περιγραφή διεργασίας) https://www.aluminium-foil.org/aluminium-foil-manufacturing-process/
74. Chatter Block Controller — vibration monitoring for cold rolling mills https://www.primetals.com/en/portfolio/solutions/cold-rolling/chatter-block-controller/
75. ISRA PARSYTEC — surface inspection for aluminum production https://aluminium-usa.german-pavilion.com/en/sites/exhibitors/118912
76. BSI (Γερμανία) — Throwback: cyberattack causes physical damage at German steel mill

https://www.controleng.com/throwback-attack-a-cyberattack-causes-physical-damage-at-a-german-steel-mill/
77. Dell EMC PowerVault ME4 Series Storage System Best Practices (ALUA, MPIO)
https://www.dell.com/support
78. OT Penetration Testing for ICS & SCADA μεθοδολογία και digital twin testing
https://frenos.io/ot-penetration-testing
79. Digital Twins in Security Operations: State of the Art and Future Perspectives (ACM Computing Surveys)
https://dl.acm.org/doi/10.1145/3746279
80. Digital Twin-Driven Intrusion Detection for Industrial SCADA: A Cyber-Physical Case Study (Sensors, 2025)
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12390215/
81. ENISA Good Practices for Supply Chain Cybersecurity, June 2023
https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
82. Fortinet, Inc. (2026). 2026 State of Operational Technology and Cybersecurity Report. Fortinet.
https://www.fortinet.com/resources/reports/state-ot-cybersecurity
83. Bitsight. (2025). The Unforgivable Exposure of ICS/OT. Bitsight.