Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ανάλυση & Διαχείριση Επικινδυνότητας Βιομηχανικών Συστημάτων σε Εφαρμογές Ενέργειας** **Analysis & Risk Management of Industrial Control Systems in Energy Applications**
Ονοματεπώνυμο Φοιτητή	**Λάμπρος Δαΐκος**
Πατρώνυμο	**Γεώργιος**
Αριθμός Μητρώου	**ΜΠΣΠ/17016**
Επιβλέπων	**Χρήστος Δουληγέρης**

Ημερομηνία Παράδοσης **Ιούλιος 2021**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Δουληγέρης Χρήστος Καθηγητής	Πατσάκης Κωνσταντίνος Αναπληρωτής Καθηγητής	Κοτζανικολάου Παναγιώτης Αναπληρωτής Καθηγητής

Ευχαριστίες

Η παρούσα μεταπτυχιακή διατριβή εκπονήθηκε το διάστημα μεταξύ Οκτωβρίου 2020 και Ιουνίου 2021 στο πλαίσιο του μεταπτυχιακού προγράμματος “Προηγμένα Συστήματα Πληροφορικής” του τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς. Οφείλω να ευχαριστήσω όλους όσους συνέβαλαν στην εκπόνησή της και ιδιαίτερα τον επιβλέποντα καθηγητή μου, κύριο Χρήστο Δουληγέρη, για την πολύτιμη καθοδήγηση και υποστήριξή του, και τον Δρ. Θεόδωρο Ντούσκα για τις παραγωγικές υποδείξεις του. Τέλος, θα ήθελα να ευχαριστήσω όλα τα κοντινά μου πρόσωπα που με στήριξαν όλο αυτό το διάστημα.

Περίληψη

Η παρούσα μεταπτυχιακή διατριβή, έχει ως αντικείμενο την ανάλυση και τη διαχείριση επικινδυνότητας Βιομηχανικών Συστημάτων Ελέγχου (Industrial Control Systems (ICS)) σε εφαρμογές ενέργειας. Σε ένα συνεχώς μεταβαλλόμενο περιβάλλον, οι βιομηχανικές μονάδες θεωρούνται κρίσιμες υποδομές, εξυπηρετώντας τις αναγκαίες λειτουργίες των σύγχρονων κοινωνιών και η προστασία τους από απειλές στον κυβερνοχώρο είναι απαραίτητη. Προκειμένου να κατανοήσουμε τις λύσεις με τις οποίες θα προσφέρουμε τη μέγιστη δυνατή ασφάλεια σε Βιομηχανικά Συστήματα Ελέγχου (ICS), εντοπίστηκαν οι κύριες διαφορές των συστημάτων αυτών από τα παραδοσιακά Συστήματα Πληροφορικής (Information Technology (IT)). Στη συνέχεια, παρουσιάζονται και αναλύονται τα βασικά συστατικά που αποτελούν τα Βιομηχανικά Συστήματα Ελέγχου (ICS) καθώς και ο σχεδιασμός της αρχιτεκτονικής τους. Για να είναι ασφαλή τα συστατικά αυτά από γνωστές επιθέσεις, εντοπίστηκαν οι απειλές από τις οποίες κινδυνεύουν κι οι ευπάθειες που μπορεί να εκμεταλλευθούν οι επιτιθέμενοι, προκειμένου να αποτιμηθούν και να μειωθεί η επικινδυνότητά τους, βελτιώνοντας την επίλυση τυχόν προβλημάτων σε θέματα ασφάλειας μέσα από προτεινόμενα μέτρα, συνεχείς δοκιμές και βέλτιστες πρακτικές.

Abstract

The present master thesis dissertation aims at the analysis and risk management of Industrial Control Systems (ICS) in energy applications. In an ever-changing environment, industrial units are considered critical infrastructures, serving the necessary functions of modern societies, and protecting them from cyber threats. In order to understand the solutions with which we will offer the maximum possible security in Industrial Control Systems (ICS), the main differences of these systems from the traditional Information Technology (IT) systems were identified. Afterwards, the basic components of the Industrial Control Systems (ICS), are presented, and analyzed as well as the design of their architecture. In order to protect these components from known attacks, the threats from which they are endangered and the vulnerabilities that the attackers can exploit were identified, in order to assess and reduce their risk, improving the resolution of any security issues through proposed measures, continuous testing and best practices.

Περιεχόμενα

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

1 Εισαγωγή

Οι οργανισμοί φιλοξενούν στα Πληροφοριακά τους Συστήματα τα πιο κρίσιμα και ευαίσθητα δεδομένα τους. Πιθανή υποβάθμιση, δυσλειτουργία ή διακοπή των Πληροφοριακών Συστημάτων έχει σημαντικές επιπτώσεις στην ασφάλεια, στην απώλεια δεδομένων, στην απώλεια φήμης και στην απώλεια διαθεσιμότητας των υπηρεσιών με αποτέλεσμα η ασφάλεια ενός Πληροφοριακού Συστήματος να είναι ένα από τα πιο σημαντικά θέματα που πρέπει να λάβουν υπόψη τους οι οργανισμοί.

Πέρα όμως από τα Πληροφοριακά Συστήματα, σε πολλές βιομηχανίες όπως σε ηλεκτρικές βιομηχανίες, σε βιομηχανίες νερού, σε βιομηχανίες πετρελαίου και φυσικού αερίου, σε αυτοκινητοβιομηχανίες, καθώς και σε ενεργειακά πάρκα, χρησιμοποιούνται Βιομηχανικά Συστήματα Ελέγχου (Industrial Control Systems (ICS)), τα οποία είναι εξίσου σημαντικά για την ομαλή λειτουργία ενός οργανισμού και η ασφάλειά τους πρέπει να λαμβάνετε υπόψιν.

Οι κρίσιμες υποδομές ICS, έχουν αλλάξει ραγδαία τις τελευταίες δεκαετίες, καθώς εξελίχθηκαν με τη διασύνδεσή τους μέσω διαδικτύου κάνοντας εφικτό τον απομακρυσμένο έλεγχό τους με αυτοματοποιημένο τρόπο και σε πραγματικό χρόνο.

1.1 Αντικείμενο και Στόχος της Διατριβής

Στόχος της παρούσας διατριβής είναι να αναλυθεί η επικινδυνότητα των συστημάτων ICS σε εφαρμογές ενέργειας και να παρουσιαστούν οι βέλτιστες πρακτικές διαχείρισής τους, προκειμένου να μετριαστεί ο κίνδυνος που μπορεί να αντιμετωπίζουν. Για τον λόγο αυτό, παρουσιάζονται και αναλύονται τα βασικά συστατικά που αποτελούν τα συστήματα ICS και προτείνεται ο βέλτιστος τρόπος σχεδιασμού της αρχιτεκτονικής τους.

Για να επιτευχθεί η βέλτιστη ασφάλεια των συστημάτων ICS, πρέπει επιπλέον να αναγνωριστούν οι σημαντικότερες και πιο συχνά εμφανιζόμενες απειλές, οι αδυναμίες που μπορεί να προκύπτουν μέσα από τις απειλές και τα ήδη υπάρχοντα μέτρα ασφαλείας, καθώς και οι επιπτώσεις που μπορεί να έχει ένας οργανισμός αν ένας επιτιθέμενος εκμεταλευτεί τις αδυναμίες αυτές.

Η ανάλυση και η διαχείριση επικινδυνότητας πραγματοποιείται μέσω της χρήσης διάφορων μεθοδολογιών και βέλτιστων πρακτικών από διεθνή πρότυπα και κανονισμούς που θα αναφερθούν στις επόμενες ενότητες, προκειμένου να μειωθεί ο κίνδυνος και να επισημανθούν τα προτεινόμενα μέτρα που πρέπει να λαμβάνουν οι οργανισμοί που χειρίζονται συστήματα ICS για την βέλτιστη προστασία τους.

1.2 Δομή της Διατριβής

Η μεταπτυχιακή διατριβή αποτελείται από δέκα (10) κεφάλαια.

Στο Κεφάλαιο 2 παρουσιάζεται μία εισαγωγή στην Ασφάλεια των Πληροφοριών, γνωστά διεθνή πρότυπα συμμόρφωσης που πρέπει να ακολουθούνται σε ένα επιχειρησιακό περιβάλλον, καθώς και εθνικές κανονιστικές απαιτήσεις ασφάλειας οι οποίες παρέχουν συμβουλές, καθοδήγηση και απαραίτητα μέτρα που πρέπει να τηρούνται για την προστασία των Εθνικών Κρίσιμων Υποδομών.

Στο Κεφάλαιο 3 γίνεται αναφορά και περιγραφή των συστημάτων ICS καθώς και σύγκριση με τα κλασσικά παραδοσιακά Συστήματα Πληροφορικής (IT).

Στο Κεφάλαιο 4 γίνεται αναφορά και ανάλυση των συστατικών που αποτελούν τα συστήματα ICS.

Στο Κεφάλαιο 5 παρουσιάζεται ένα από τα πιο διαδεδομένα μοντέλα αρχιτεκτονικής για συστήματα ICS, το Purdue Model.

Στο Κεφάλαιο 6 παρουσιάζονται οι επιθέσεις και οι απειλές ασφάλειας από τις οποίες κινδυνεύουν τα συστατικά των συστημάτων ICS.

Στο Κεφάλαιο 7 παρουσιάζεται η μελέτη για την Ανάλυση και τη Διαχείριση Επικινδυνότητας σε ένα ενεργειακό πάρκο και τα προτεινόμενα μέτρα ασφαλείας.

Στο Κεφάλαιο 8 παρουσιάζεται η διαδικασία απόκρισης περιστατικών για κυβερνοεπιθέσεις σε συστήματα ICS και τα βήματα που πρέπει να ακολουθούνται.

Στο Κεφάλαιο 9 αναφέρονται τα συμπεράσματα από τις περιπτώσεις που μελετήθηκαν.

Τέλος, στο Παράρτημα του Κεφαλαίου 10 παρουσιάζονται δύο συγκριτικοί πίνακες με τα προτεινόμενα μέτρα του NIST και του NERC-CIP ανά κατηγορία στην οποία ανήκουν.

1.3 Συντομογραφίες

Πίνακας 1: Συντομογραφίες

Συντομογραφία / Λέξη	Ορισμός / Περιγραφή
AD	Active Directory
ARP	Address Resolution Protocol
BACnet	Building Automation and Control Networks
BES	Bulk Electric System(s)
BIA	Business Impact Assessment
CIO	Chief Information Officer
CIP	Common Industrial Protocol
CSET	Cyber Security Evaluation Tool
CSIRT	Cyber Security Incident Response Team
CSSP	Cyber Security Service Provider
DCS	Distributed Control System(s)
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
FTP	File Transfer Protocol
HDLC	High-Level Data Link Control
HMI	Human Machine Interface
IACS	Industrial Automation and Control System(s)
IAS	Industrial Automation System(s)
ICS	Industrial Control System(s)
IDS	Intrusion Detection System(s)
IED	Intelligent Electronic Device
I/O	Input/Output
IP	Internet Protocol
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technology
LAN	Local Area Network
MitM	Man-in-the-Middle
MTU	Master Terminal Unit
NCSC	National Cyber Security Centre
NERC - CIP	North American Electric Reliability Corporation - Critical Infrastructure Protection

NIS	Network and Information Security
NIST	National Institution of Standards and Technology
NTP	Network Time Protocol
OPC	Open Platform Communication
OS	Operating system
OT	Operational Technology
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable Logic Controller
PROFIBUS	Process Field Bus
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
STORM	Secure Tool for Risk Management
SW	Software
XSS	Cross Site Scripting

2 Ασφάλεια Πληροφοριών

2.1 Εισαγωγή στην Ασφάλεια Πληροφοριών

Η διαχείριση της ασφάλειας είναι μια συνεχής και συστηματική διαδικασία προσδιορισμού, ανάλυσης, χειρισμού και παρακολούθησης των επιχειρησιακών κινδύνων ενός οργανισμού. Στόχο έχει την προστασία του Πληροφοριακού Συστήματος από εσωτερικούς και εξωτερικούς κινδύνους που θα μπορούσαν να επηρεάσουν αρνητικά την επίτευξη των επιχειρησιακών στόχων του οργανισμού και την ομαλή λειτουργία του.

Η ασφάλεια πληροφοριών είναι ύψιστης σημασίας για έναν οργανισμό καθώς παρέχει προστασία των πληροφοριών και των πληροφοριακών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση ή καταστροφή προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητά τους [1].

Οι οργανισμοί χρησιμοποιούν σε μεγάλο βαθμό προϊόντα και υπηρεσίες τεχνολογίας πληροφοριών (IT) για να λειτουργήσουν τις καθημερινές τους δραστηριότητες. Τα Πληροφοριακά Συστήματα των οργανισμών καθώς και τα προϊόντα και οι υπηρεσίες που χρησιμοποιούν πρέπει να έχουν ως απαραίτητη προϋπόθεση να διασφαλίζουν την ασφάλεια προκειμένου να είναι επιτυχείς οι οργανισμοί.

Στο παρόν κεφάλαιο γίνεται ανασκόπηση των υπαρχόντων προτύπων διαχείρισης ασφάλειας που ένας οργανισμός πρέπει να ακολουθεί προκειμένου να αποκρίνεται σε περιστατικά στον κυβερνοχώρο.

2.2 Πρότυπα Διαχείρισης Ασφάλειας

Για να είναι επιτυχής η ασφάλεια πληροφοριών σε έναν οργανισμό, υπάρχουν διάφορα διεθνή πρότυπα συμμόρφωσης που πρέπει να ακολουθούνται σε ένα επιχειρησιακό περιβάλλον.

Η εφαρμογή ή ο συνδυασμός εφαρμογής των παρακάτω προτύπων συνεισφέρει στη βέλτιστη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων και στο μετριασμό των κινδύνων που μπορεί να απειλούν έναν οργανισμό.

2.2.1 Το πρότυπο ISO / IEC 27001

Ένα από τα πιο γνωστά πρότυπα διαχείρισης ασφάλειας των Πληροφοριακών Συστημάτων είναι το ISO/IEC 27001: 2013 [2], ένα εμπορικό πρότυπο του Διεθνούς Οργανισμού Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC).

Το διεθνές πρότυπο ISO/IEC 27001 έχει δημιουργηθεί για να παρέχει συγκεκριμένες απαιτήσεις για τη θέσπιση, την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Η εφαρμογή του προτύπου αυτού έχει άμεση σχέση με τις ανάγκες και τους στόχους του οργανισμού, τις απαιτήσεις ασφάλειας που χρειάζονται, τις διαδικασίες και τις υπηρεσίες που χρησιμοποιούνται, καθώς και με το μέγεθος και την υποδομή του κάθε οργανισμού.
Το σύστημα διαχείρισης ασφάλειας πληροφοριών διατηρεί την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών, εφαρμόζοντας μια διαδικασία διαχείρισης επικινδυνότητας και παρέχει εμπιστοσύνη στα ενδιαφερόμενα μέρη.

Το πρότυπο καλύπτει ως επί το πλείστον μεγάλης κλίμακας επιχειρήσεις (π.χ. κυβερνητικές υπηρεσίες και μεγάλες επιχειρήσεις), ενώ θεωρείται «πολύ βαρύ» (πολύπλοκο) για τις πολύ μικρές, μικρές και μεσαίου μεγέθους επιχειρήσεις. Παρόλα αυτά, είναι χρήσιμο και αναγκαίο για οποιασδήποτε φύσης οργανισμό.

Θα πρέπει να σημειωθεί ότι το πρότυπο δίνει μεγάλη έμφαση στον πληροφοριακό κίνδυνο (risk-based) και όλες οι απαιτήσεις και οδηγίες του επικεντρώνονται στον προσδιορισμό, την εκτίμηση και τον μετριασμό των κινδύνων που αντιμετωπίζει ο υπό εξέταση οργανισμός. Μία από τις υποχρεωτικές τεκμηριωμένες διαδικασίες τις οποίες απαιτεί το πρότυπο είναι η χρήση μιας μεθοδολογίας για την ανάλυση και τη διαχείριση επικινδυνότητας, χωρίς όμως να παρέχει μια συγκεκριμένη μέθοδο.

2.2.2 Το πρότυπο ISO / IEC 27002

Το ISO/IEC 27002: 2013 [3] είναι ένα εμπορικό πρότυπο που παρέχει προδιαγραφές με αναλυτικές οδηγίες για την υλοποίηση, την εφαρμογή και τη βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σε έναν οργανισμό. Ως εκ τούτου, το πρότυπο ISO/IEC 27002 θεωρείται ως ο οδηγός που επιτρέπει σε εσωτερικούς και εξωτερικούς αναλυτές, συνήθως με υψηλή τεχνογνωσία και εμπειρία στις Τεχνολογίες Πληροφοριών και Επικοινωνιών, να αξιολογήσει το επίπεδο ασφάλειας ενός οργανισμού και να καθοριστούν τα θέματα που θα βελτιώσουν τη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων του.

Ωστόσο, το πρότυπο ISO/IEC 27002 δεν περιλαμβάνει κάποια συγκεκριμένη μέθοδο για την ανάλυση και τη διαχείριση επικινδυνότητας, αλλά περιλαμβάνει μια λίστα από 10 βασικούς τομείς ελέγχου που αποτελείται από 36 σημεία ελέγχου (control objectives) και 127 ελέγχους (controls) που καθορίζουν τις προϋποθέσεις ότι ένας οργανισμός θα πρέπει να είναι συμβατός με το πρότυπο. Αν και το συγκεκριμένο πρότυπο, δεν αποτελεί μια μέθοδο για την αξιολόγηση και τη διαχείριση κινδύνων, περιλαμβάνει συγκεκριμένες πτυχές χειρισμού του κινδύνου, όπως τον προσδιορισμό των κινδύνων και τη δημιουργία ενός αρχικού σχεδίου αντιμετώπισης του κινδύνου.

Το πρότυπο είναι σε θέση να καλύψει όλα τα είδη των οργανισμών (π.χ. κυβερνητικούς οργανισμούς, μικρής, μεσαίας και μεγάλης κλίμακας επιχειρήσεις). Υπάρχουν διάφορα εργαλεία που υλοποιούν το πρότυπο ISO/IEC 27002.

2.2.3 Το πρότυπο ISO / IEC 27005

Το πρότυπο ISO/IEC 27005:2018 [4] αποτελεί ένα εμπορικό πρότυπο του Διεθνούς Οργανισμού Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC) που ορίζει τις βασικές αρχές, τις πτυχές και τις δραστηριότητες μιας καλά ορισμένης διαδικασίας διαχείρισης επικινδυνότητας. Έτσι, μπορεί να θεωρηθεί ως ένα ελάχιστο πλαίσιο το οποίο περιγράφει τις απαιτήσεις για τη διαδικασία αξιολόγησης του κινδύνου και όχι ως μία ολοκληρωμένη μέθοδο διαχείρισης επικινδυνότητας. Το πρότυπο αυτό υποστηρίζει τις γενικές έννοιες που ορίζει το πρότυπο ISO/IEC 27001: 2013, καθώς και τις κύριες διαδικασίες και τους κανόνες που περιγράφονται στο πρότυπο ISO/IEC 27002: 2013. Έχει εφαρμογή σε όλους τους τύπους των οργανισμών (π.χ. κυβερνητικούς οργανισμούς, μεγάλες εταιρείες, μικρές και μεσαίες επιχειρήσεις) οι οποίοι προτίθενται να διαχειρίζονται τους κινδύνους οι οποίοι θα μπορούσαν να διακυβεύσουν την ομαλή λειτουργία του Πληροφοριακού Σσυστήματος του οργανισμού τους.

Το πρότυπο ISO 27005 προτείνει τη χρήση τόσο ποσοτικής όσο και ποιοτικής μεθοδολογίας για τον υπολογισμό του επιπέδου του κινδύνου, ωστόσο δεν υποστηρίζει καμία συγκεκριμένη τεχνική για το σκοπό αυτό ή οποιαδήποτε υπολογιστική μέθοδο για τη συλλογή και την ανάλυση της απαιτούμενης πληροφορίας για την ανάλυση και τη διαχείριση επικινδυνότητας. Επίσης, η γενική φύση του προτύπου δεν περιλαμβάνει στοιχεία που προωθούν τη συνεργασία μεταξύ των χρηστών.

2.2.4 Το πρότυπο ISO / IEC 27019

Άλλο ένα εξίσου διαδεδομένο πρότυπο ασφάλειας είναι το ISO/IEC 27019: 2017 [5] το οποίο παρέχει αρχές βασισμένες στο ISO/IEC 27002 για διαχείριση της ασφάλειας των πληροφοριών για συστήματα που χρησιμοποιούνται στην βιομηχανία της ενέργειας. Εκτός από τους στόχους και τα μέτρα ασφαλείας που ορίζονται στο ISO/IEC 27002: 2013, τα συστήματα ελέγχου διεργασιών που χρησιμοποιούνται από ενεργειακούς φορείς και προμηθευτές ενέργειας υπόκεινται σε περαιτέρω απαιτήσεις που αναφέρονται στο πρότυπο αυτό.

2.2.5 Τα πρότυπα NIST SP 800-53r5 και NIST SP 800-82r2

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology (NIST)) παρέχει το NIST SP 800-53r5 [31], ένα πρότυπο που καταγράφει ελέγχους για την ασφάλεια και το απόρρητο των πληροφοριακών συστημάτων ενός οργανισμού, προστατεύοντας τις υπηρεσίες, τα αγαθά και τους υπαλλήλους από ένα σύνολο κινδύνων και απειλών. Οι έλεγχοι αυτοί, αντιμετωπίζουν διάφορες

απαιτήσεις που απορρέουν από τον στόχο και τις ανάγκες μιας επιχείρησης, από τους νόμους και τους κανονισμούς της, από τις πολιτικές της, και από άλλα πρότυπα και οδηγίες.

Το πρότυπο NIST SP 800-82r2 [10] παρέχει τα ίδια πεδία ελέγχου με το NIST SP 800-53r5 προσαρμοσμένο στα μοναδικά χαρακτηριστικά των συστημάτων και υποδομών ICS.

2.2.6 Το πρότυπο ISA / IEC 62443

Το πρότυπο ISA/IEC 62443 [6] ασχολείται με την ασφάλεια των συστημάτων ICS, γνωστό ως το Σύστημα Βιομηχανικού Αυτοματισμού και Ελέγχου (Industrial Automation and Control System). Τα συστήματα αυτά χρησιμοποιούνται στις εγκαταστάσεις παραγωγής και επεξεργασίας, όπως σε εγκαταστάσεις ηλεκτρικής ενέργειας, φυσικού αερίου και νερού και είναι αυτοματοποιημένα, τηλεχειριζόμενα ή ελεγχόμενα. Ο στόχος του προτύπου ISA/IEC 62443 είναι να διασφαλίσει ότι ένας προμηθευτής προϊόντος, ένας κατασκευαστής ή ένας ιδιοκτήτης ενός αγαθού ακολουθεί μια ασφαλής διαδικασία με βασικό στόχο την ασφάλεια του προσωπικού και της παραγωγής, τη διαθεσιμότητα, την αποτελεσματικότητα και την ποιότητα της παραγωγής ενός τέτοιου συστήματος, καθώς και την ασφάλεια του περιβάλλοντος.

2.3 Κανονιστικές Απαιτήσεις Ασφάλειας

Υπάρχουν πολλοί τομείς κρίσιμων υποδομών ανά τον κόσμο όπως οι υποδομές ενέργειας, επικοινωνίας, μεταφοράς και οικονομίας, όπου η απώλεια ή ο συμβιβασμός των στοιχείων που τις αποτελούν, θα είχε σοβαρές επιπτώσεις στη διαθεσιμότητα, την παροχή ή την ακεραιότητα των βασικών υπηρεσιών, με αποτέλεσμα να οδηγήσει μια χώρα σε σοβαρές οικονομικές ή κοινωνικές συνέπειες ή σε απώλεια ζωής.

Οι Η.Π.Α, το Ηνωμένο Βασίλειο και η Ευρωπαϊκή Ένωση έχουν την ανάγκη να ακολουθούν συγκεκριμένες εθνικές κανονιστικές απαιτήσεις ασφάλειας οι οποίες παρέχουν συμβουλές, καθοδήγηση και απαραίτητα μέτρα που πρέπει να τηρούνται από όσους ενδιαφέρονται για τις Εθνικές Κρίσιμες Υποδομές.

2.3.1 Η.Π.Α. - NERC CIP

Μία από τις πιο κρίσιμες υποδομές που επιτρέπει σε αρκετές από τις υπόλοιπες να λειτουργούν είναι η υποδομή της ενέργειας. Ο οργανισμός NERC (North American Electric Reliability Corporation) [7] είναι υπεύθυνος για τη διατήρηση της ομαλής λειτουργίας και των διεργασιών του Συστήματος Υψηλής Ισχύος (Bulk Electric System – BES) και γενικότερα όλου του ηλεκτρικού δικτύου στις ΗΠΑ. Το 2008, αναπτύχθηκε το πλαίσιο συμμόρφωσης για την Προστασία Κρίσιμων Υποδομών (Critical Infrastructure Protection – CIP), με στόχο τον μετριασμό των επιθέσεων ασφαλείας στον κυβερνοχώρο ενός BES. Ο κανονισμός NERC CIP, αποτελεί ένα σύνολο απαιτήσεων για τη διασφάλιση των αγαθών που απαιτούνται για την απρόσκοπτη λειτουργία του ηλεκτρικού συστήματος των ΗΠΑ.

2.3.2 Ηνωμένο Βασίλειο - NCSC (National Cyber Security Centre)

Το Εθνικό Κέντρο Ασφάλειας στον κυβερνοχώρο NCSC [8] υποστηρίζει τους πιο κρίσιμους οργανισμούς στο Ηνωμένο Βασίλειο, τον ευρύτερο δημόσιο τομέα, τη βιομηχανία, τις μικρο-μεσαίες επιχειρήσεις καθώς και το ευρύ κοινό. Όταν συμβαίνουν περιστατικά ασφαλείας, παρέχει αποτελεσματική αντίδραση σε περιστατικά για να ελαχιστοποιηθούν οι βλάβες στο Ηνωμένο Βασίλειο, να βοηθήσει στην ανάκαμψη και να μάθει τα διδάγματα για το μέλλον μέσα από προτεινόμενα μέτρα και βέλτιστες πρακτικές.

2.3.3 Ευρωπαϊκή Ένωση - NIS (Network and Information Security)

Στο πλαίσιο της στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο, η Ευρωπαϊκή Επιτροπή πρότεινε την οδηγία της ΕΕ για την ασφάλεια δικτύων και πληροφοριών. Η οδηγία NIS [9] είναι το πρώτο κομμάτι της νομοθεσίας για την ασφάλεια στον κυβερνοχώρο σε ολόκληρη την ΕΕ. Ο στόχος είναι η ενίσχυση της ασφάλειας στον κυβερνοχώρο σε ολόκληρη την ΕΕ.
Η οδηγία NIS αποτελείται από τρία μέρη:

- Τα κράτη μέλη της ΕΕ πρέπει να διαθέτουν ορισμένες εθνικές δυνατότητες ασφάλειας στον κυβερνοχώρο των επιμέρους χωρών της ΕΕ, π.χ. πρέπει να έχουν εθνική Ομάδα Απόκρισης

Περιστατικών Ασφάλειας στον Κυβερνοχώρο (Cyber Security Incident Response Team – CSIRT), να κάνουν ασκήσεις στον κυβερνοχώρο κ.λπ.

- Διασυνοριακή συνεργασία μεταξύ χωρών της ΕΕ, π.χ. το επιχειρησιακό δίκτυο CSIRT της ΕΕ, η στρατηγική ομάδα συνεργασίας NIS κ.λπ.
- Τα κράτη μέλη της ΕΕ πρέπει να εποπτεύουν την κυβερνοασφάλεια των κρίσιμων φορέων της αγοράς στη χώρα σε κρίσιμους τομείς όπως ενέργεια, μεταφορές, νερό, υγεία, ψηφιακή υποδομή και χρηματοοικονομικός τομέας, και σε κρίσιμους παρόχους ψηφιακών υπηρεσιών όπως απευθείας σύνδεση αγορών, υπολογιστική νέφους και διαδικτυακές μηχανές αναζήτησης.

3 Περιγραφή των Συστημάτων ICS

3.1 Εισαγωγή

Τα συστήματα ICS αποτελούν το δομικό συστατικό όλων των βιομηχανικών μονάδων και των κρίσιμων υποδομών παγκοσμίως, εξυπηρετώντας απαραίτητες και αναγκαίες λειτουργίες των σύγχρονων κοινωνιών.

Σε πολλές βιομηχανίες όπως σε ηλεκτρικές βιομηχανίες, σε βιομηχανίες νερού, σε φαρμακευτικές βιομηχανίες, σε βιομηχανίες πετρελαίου και φυσικού αερίου, σε αυτοκινητοβιομηχανίες, καθώς και σε ενεργειακά και φωτοβολταϊκά πάρκα, χρησιμοποιούνται Βιομηχανικά Συστήματα Ελέγχου, τα οποία είναι εξίσου σημαντικά για την ομαλή λειτουργία ενός οργανισμού και η ασφάλεια τους πρέπει να λαμβάνεται υπ'όψιν.

3.2 Ορισμός των Συστημάτων ICS

Τα συστήματα ICS είναι εξειδικευμένα πληροφοριακά συστήματα τα οποία διαφέρουν σημαντικά από τα κλασσικά πληροφοριακά συστήματα. Ο κύριος σκοπός τους είναι η διαχείριση κρίσιμων υποδομών όπως πυρηνικοί σταθμοί, έξυπνα δίκτυα, εγκαταστάσεις πετρελαίου και φυσικού αερίου, και φωτοβολταϊκά και αιολικά πάρκα. Τα συστήματα ICS έχουν κάποια μοναδικά λειτουργικά χαρακτηριστικά, όπως την ανάγκη για απόκριση σε πραγματικό χρόνο, και εξαιρετικά υψηλή διαθεσιμότητα, προβλεψιμότητα και αξιοπιστία.

Ο όρος Industrial Control Systems (ICS) είναι αρκετά ευρύς καθώς περιλαμβάνει διαφόρων ειδών συστήματα, όπως:

- DCS (Distributed Control Systems)
- SCADA (Supervisory Control And Data Acquisition)
- IAS (Industrial Automation System)
- IACS (Industrial Automation and Control Systems)
- PLC (Programmable Logic Controller)

Τα συστήματα που απαρτίζουν το περιβάλλον ICS είναι κρίσιμα για τη λειτουργία των υποδομών που υποστηρίζουν και είναι συνήθως διασυνδεδεμένα σε μεγάλο βαθμό και αμοιβαία αλληλεξαρτώμενα.

3.3 Η Εξέλιξη των Συστημάτων ICS

Πολλά από τα σημερινά συστήματα ICS εξελίχθηκαν από την εισαγωγή δυνατοτήτων πληροφορικής σε υπάρχοντα φυσικά συστήματα, συχνά αντικαθιστώντας ή συμπληρώνοντας μηχανισμούς φυσικού ελέγχου. Για παράδειγμα, τα ενσωματωμένα ψηφιακά χειριστήρια αντικατέστησαν τα αναλογικά μηχανικά χειριστήρια σε περιστρεφόμενες μηχανές και κινητήρες [10].

Η μηχανική των συστημάτων ICS συνεχίζει να εξελίσσεται για να παρέχει νέες δυνατότητες διατηρώντας παράλληλα τους τυπικούς μεγάλους κύκλους ζωής αυτών των συστημάτων. Η εισαγωγή δυνατοτήτων πληροφορικής στα φυσικά συστήματα παρουσιάζει μια αναδυόμενη συμπεριφορά που έχει επιπτώσεις στην ασφάλεια. Μηχανικά μοντέλα και αναλύσεις εξελίσσονται προκειμένου να αντιμετωπίσουν αυτές τις αναδυόμενες ιδιότητες, όπως ασφάλεια, προστασία, προστασία της ιδιωτικής ζωής και αλληλεξάρτηση περιβαλλοντικών επιπτώσεων.

3.4 Σύγκριση ICS με Συστήματα Ασφάλειας IT

Προκειμένου να κατανοήσουμε τις λύσεις με τις οποίες θα προσφέρουμε τη μέγιστη δυνατή ασφάλεια σε συστήματα ICS, πρέπει να αναγνωρίσουμε και να διερευνήσουμε τις κύριες διαφορές των συστημάτων αυτών από τα παραδοσιακά συστήματα IT.

Τα συστήματα ICS έχουν πολλά χαρακτηριστικά που διαφέρουν από τα παραδοσιακά συστήματα πληροφορικής, συμπεριλαμβανομένων διαφορετικών κινδύνων και προτεραιοτήτων. Μερικά από αυτά

περιλαμβάνουν σημαντικό κίνδυνο για την υγεία και την ασφάλεια των ανθρώπινων ζωών, σοβαρές ζημιές στο περιβάλλον και οικονομικά ζητήματα όπως απώλειες παραγωγής και αρνητικές επιπτώσεις στην οικονομία ενός έθνους.

Η βασική διαφορά των ICS και των παραδοσιακών συστημάτων IT είναι ότι τα πρώτα αλληλοεπιδρούν έντονα με το φυσικό περιβάλλον ελέγχοντας τον φυσικό κόσμο ενώ τα συστήματα IT διαχειρίζονται κυρίως δεδομένα. Τα συστήματα ICS είναι συστήματα διασυνδεδεμένα με το διαδίκτυο και κατ' επέκταση ευπαθή σε κυβερνοεπιθέσεις. Η αλληλεπίδραση των συστημάτων αυτών οδηγεί σε αρκετές προκλήσεις αλλά και σε πρωτόγνωρες ευκαιρίες αξιοποίησής τους.

Για τη σωστή διαχείριση της ασφάλειας των συστημάτων ICS, πρέπει να συνυπολογιστούν όλα τα στοιχεία που κάνουν τα δύο είδη συστημάτων να διαφέρουν.

Στον παρακάτω πίνακα παρουσιάζονται οι κύριες διαφορές μεταξύ των συστημάτων IT και ICS [10], [11].

Πίνακας 2: Διαφορές μεταξύ συστημάτων IT και ICS

Κατηγορία	IT	ICS
Βασικοί στόχοι ασφάλειας (CIA)	• Κύριος στόχος η προστασία εμπιστευτικότητας δεδομένων	• Κύριος στόχος η προστασία ανθρωπίνων ζωών, περιβάλλοντος και υποδομών, η διαθεσιμότητα των συστατικών του, η ακεραιότητα της διαδικασίας παραγωγής
Απαιτήσεις απόδοσης	• Απαιτούν υψηλό χρόνο απόδοσης αλλά μπορούν να αντέξουν κάποιο επίπεδο καθυστέρησης	• Πολύ κρίσιμα στον χρόνο απόδοσης
Χρόνος απόκρισης	• Ανάλογα με το επίπεδο των παρεχόμενων υπηρεσιών	• Άμεσος, ειδικά για περιστατικά ασφάλειας
Διαχείριση Επικινδυνότητας	• Διαχείριση δεδομένων • Εμπιστευτικότητα κι ακεραιότητα δεδομένων • Ανοχή σε σφάλματα • Η κύρια επίπτωση κινδύνου είναι η καθυστέρηση των επιχειρησιακών λειτουργιών	• Ελέγχος φυσικού κόσμου • Ασφάλεια στην ανθρώπινη ζωή • Απαραίτητη ανοχή σφαλμάτων – μη αποδεκτός ο στιγμαίος χρόνος διακοπής • Οι κύριες επιπτώσεις είναι η μη συμμόρφωση σε κανονισμούς, περιβαλλοντικές επιπτώσεις, απώλεια ζωής, εξοπλισμού ή παραγωγής
Πρόσβαση	• Εκτενής διασύνδεση με το εξωτερικό περιβάλλον	• Περιορισμένη συνδεσιμότητα, υπό σαφής όρους
Δικαιώματα πρόσβασης στα συστήματα	• Σε επίπεδο χρήστη του συστήματος	• Σε επίπεδο ρόλου στην εταιρεία

Κατηγορία	IT	ICS
Πρόσβαση στο Διαδίκτυο	• Διασυνδεδεμένα υποδίκτυα με σύνδεση στο Διαδίκτυο	• Δεν επιτρέπεται η πρόσβαση στο Διαδίκτυο
Επικοινωνία	• Τυπικά πρωτόκολλα επικοινωνίας • Ενσύρματα κι ασύρματα δίκτυα	• Ιδιόκτητα και τυπικά πρωτόκολλα εικοινωνίας • Χρήση ειδικών και ασύρατων καλωδίων • Περίπλοκα δίκτυα με εμπειρία μηχανικών ελέγχου
Λειτουργικά Συστήματα	• Παραδοσιακά Λειτουργικά Συστήματα • Απλές αναβαθμίσεις μέσω εργαλειών αυτόματης ανάπτυξης	• Ειδικά ανεπτυγμένα Λειτουργικά Συστήματα με εξειδικευμένους αλγόριθμους και τροποποιημένο υλικό και λογισμικό • Αλλαγές στο λογισμικό πρέπει να γίνονται προσεκτικά
Αναβαθμίσεις	• Αυτόματες και τακτικές αναβαθμίσεις	• Δυσκολία αναβαθμίσεων λόγω της συνεχούς χρήσης
Χρόνος ζωής συστημάτων	• 3 έως 5 χρόνια	• 10 έως 15 χρόνια
Τοποθεσία συστημάτων	• Τοπικά με εύκολη πρόσβαση	• Απομονωμένα, απομακρυσμένα και με δύσκολη πρόσσβαση

4 Συστατικά των Συστημάτων ICS

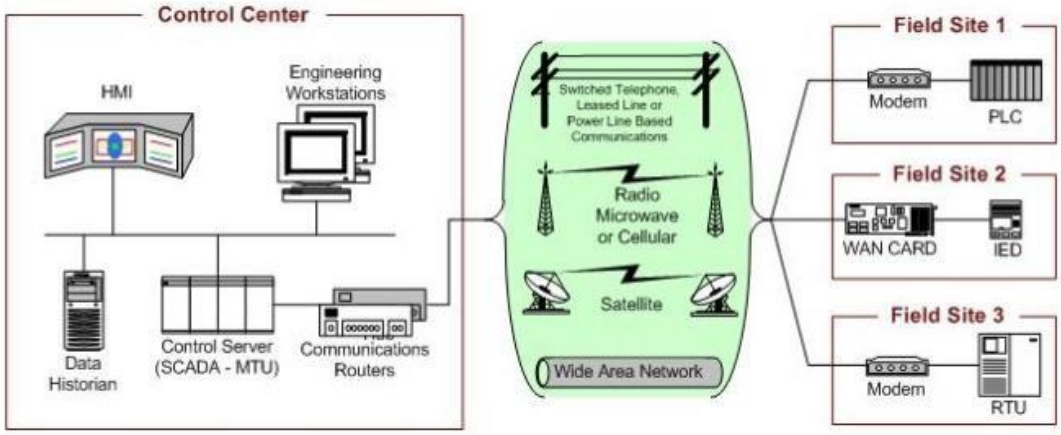
4.1 Διατάξεις Ελέγχου

Supervisory Control And Data Acquisition (SCADA)

Τα συστήματα SCADA χρησιμοποιούνται για τον έλεγχο των αγαθών που μπορεί να είναι τοποθετημένα σε διάφορα σημεία ενός ή περισσοτέρων πεδίων, όπου η απόκτηση δεδομένων είναι εξίσου σημαντική με τον έλεγχο.

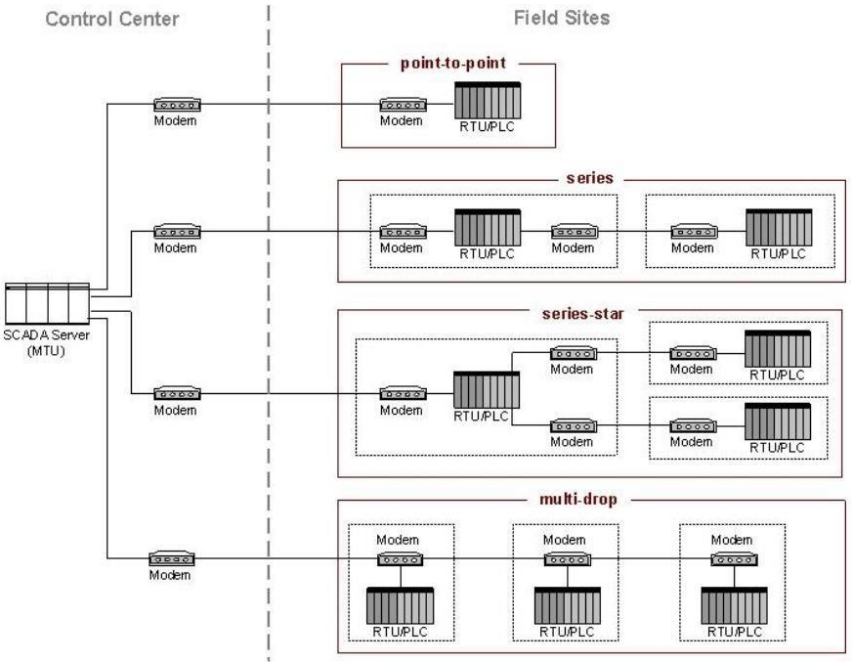
Τα συστήματα SCADA ενσωματώνουν συστήματα απόκτησης δεδομένων με συστήματα μετάδοσης δεδομένων και λογισμικό HMI για να παρέχουν ένα κεντρικό σύστημα παρακολούθησης και ελέγχου για πολλές εισόδους και εξόδους διεργασιών. Τα συστήματα SCADA έχουν σχεδιαστεί για να συλλέγουν πληροφορίες από το πεδίο (sensors, PLCs, IEDs κ.λπ.), να τις μεταφέρουν σε μια κεντρική εγκατάσταση υπολογιστή και να εμφανίζουν τις πληροφορίες στον χειριστή γραφικά ή με κείμενο, επιτρέποντας έτσι στον χειριστή να παρακολουθεί ή να ελέγχει ένα ολόκληρο σύστημα από μια κεντρική τοποθεσία σε σχεδόν πραγματικό χρόνο. Με βάση την πολυπλοκότητα και τη ρύθμιση του μεμονωμένου συστήματος, ο έλεγχος οποιουδήποτε μεμονωμένου συστήματος, λειτουργίας ή εργασίας μπορεί να είναι αυτόματος ή μπορεί να εκτελεστεί με εντολές χειριστή.

Στην Εικόνα 1 φαίνεται η γενική τοπολογία ενός συστήματος SCADA, ο απαραίτητος εξοπλισμός για τον έλεγχο και την επικοινωνία μεταξύ του κέντρου ελέγχου και του πεδίου. Ο εξοπλισμός αυτός μεταξύ άλλων περιλαμβάνει έναν Control Server, εξοπλισμό επικοινωνίας (routers, modems) και RTU (Remote Termina Units) ή/και PLCs (Programmable Logic Controllers), οι οποίοι ελέγχουν ενεργοποιητές ή αισθητήρες παρακολούθησης που βρίσκονται στο πεδίο.



Εικόνα 1: Γενική Τοπολογία συστήματος SCADA, "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82r2

Οι τέσσερις κατηγορίες τοπολογιών επικοινωνίας συστημάτων SCADA είναι οι point-to-point, series, series-star, multi-drop, όπως φαίνονται στην Εικόνα 2.

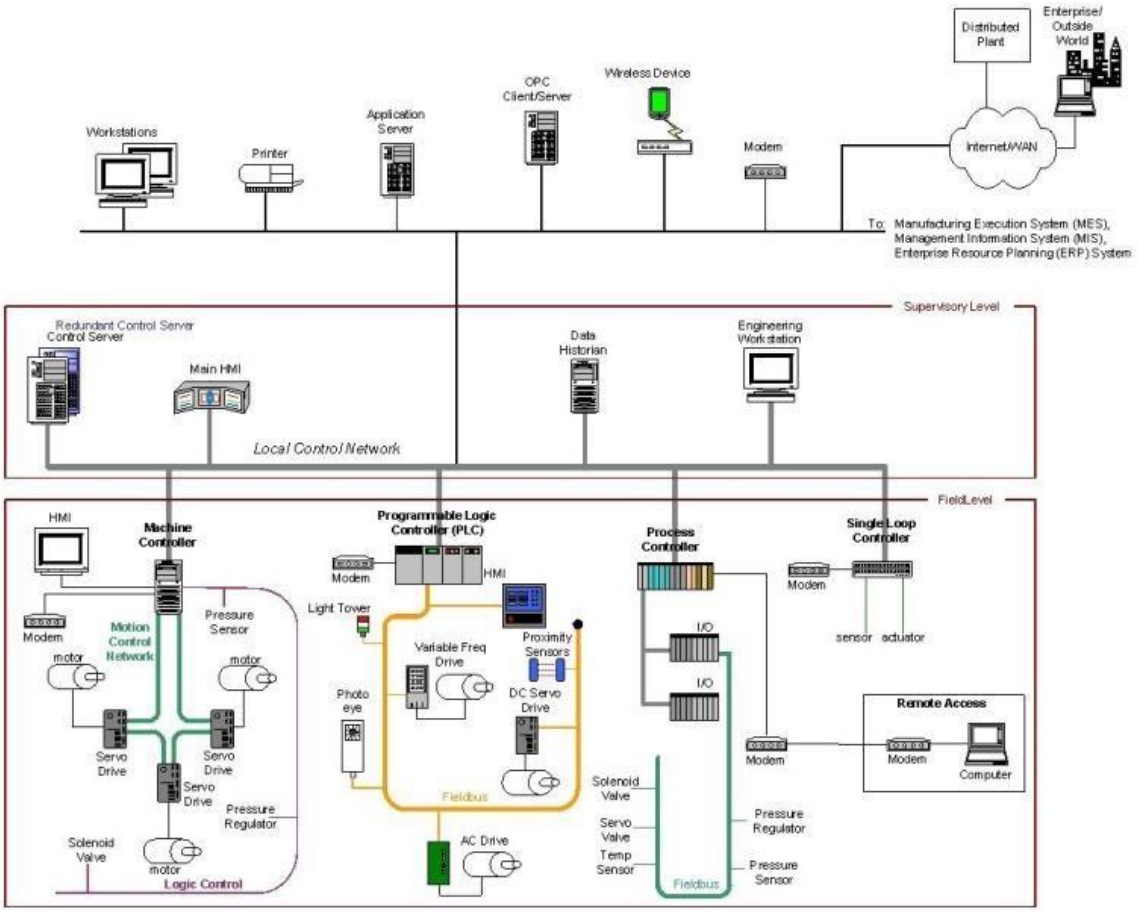


Εικόνα 2: Κατηγορίες Τοπολογιών Επικοινωνίας συστήματος SCADA, "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82r2

Distributed Control Systems (DCS)

Τα Κατανεμημένα Συστήματα Ελέγχου (DCS) [12] είναι συστήματα ελέγχου, ειδικά σχεδιασμένα για τον έλεγχο πολύπλοκων και γεωγραφικά κατανεμημένων εφαρμογών. Τα DCS περιέχουν ένα εποπτικό επίπεδο ελέγχου παρακολουθώντας ταυτόχρονα πολλαπλά υποσυστήματα τα οποία είναι υπεύθυνα να ελέγχουν τις λεπτομέρειες μιας τοπικής διεργασίας. Όπως υποδηλώνει το όνομα, οι ελεγκτές διανέμονται σε ολόκληρη την περιοχή της εγκατάστασης, όπου συνδεόμενοι με διάφορους αισθητήρες ή ενεργοποιητές και με την βοήθεια ειδικών υπολογιστικών συστημάτων όπου επικοινωνούν μέσω ενός δικτύου υψηλής ταχύτητας, μας δίνουν μία ολική εικόνα της παρατηρούμενης βιομηχανικής μονάδος.

Ένα παράδειγμα υλοποίησης φαίνεται στην Εικόνα 3. Αυτό το DCS περιλαμβάνει μια ολόκληρη εγκατάσταση από τις διαδικασίες παραγωγής κατώτατου επιπέδου έως το εταιρικό επίπεδο. Ο Εποπτικός Ελεγκτής (Control Server) επικοινωνεί με τα υποσυστήματα μέσω ενός Δικτύου Ελέγχου (Control Network). Ο επόπτης στέλνει καθορισμένα αιτήματα και ζητά δεδομένα από τον κατανεμημένο ελεγκτή πεδίου. Οι κατανεμημένοι ελεγκτές ελέγχουν τους ενεργοποιητές διεργασίας με βάση τις εντολές του Control Server και της ανατροφοδότησης από τους αισθητήρες διεργασιών [10].

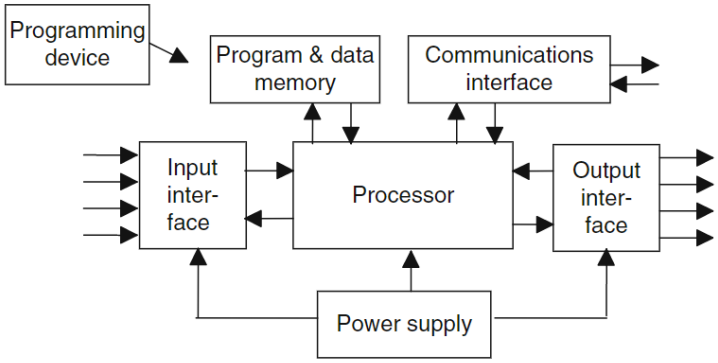


Εικόνα 3: Παράδειγμα υλοποίησης συστήματος DCS, "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82r2

Programmable Logic Controller (PLC)

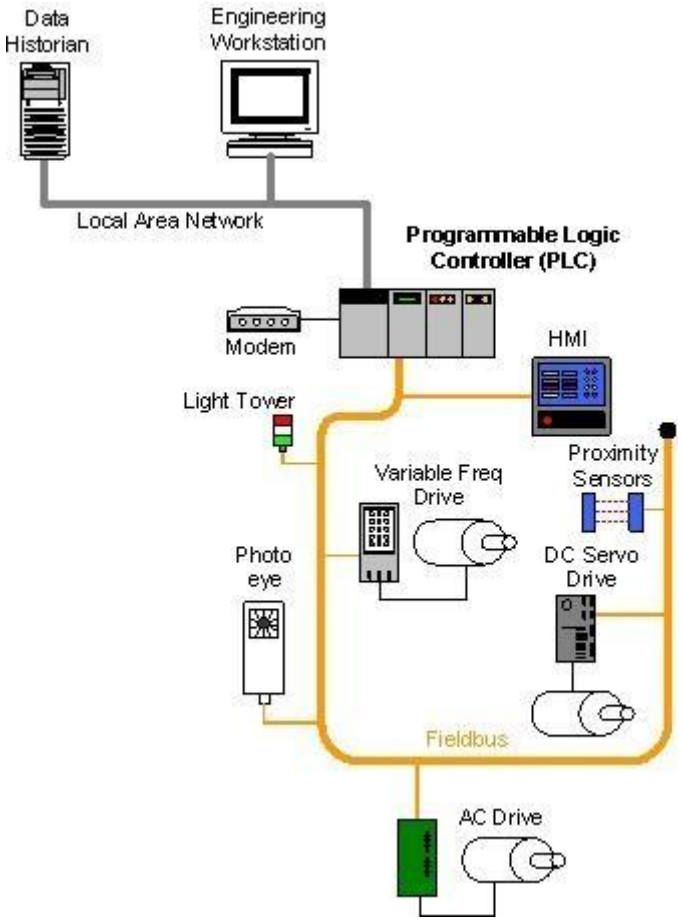
Τα PLCs είναι προγραμματιζόμενοι λογικοί ελεγκτές οι οποίοι έχουν τα χαρακτηριστικά ενός ειδικού τύπου υπολογιστή που χρησιμοποιείται σε βιομηχανικά περιβάλλοντα, τα οποία είναι γνωστά για την αξιοπιστία τους [13]. Πιο συγκεκριμένα, είναι ελεγκτές γενικής χρήσης που χρησιμοποιούν δεδομένα που λαμβάνονται από μια συλλογή εισόδων, τα επεξεργάζονται μέσω μιας σειράς προ-προγραμματισμένης λογικής και στέλνουν μια φυσική έξοδο με βάση τα αποτελέσματα αυτής της λογικής. Κατά συνέπεια, αυτοί οι ελεγκτές μπορούν να αυτοματοποιήσουν τη λειτουργία μιας μηχανής, μιας διαδικασίας ή μιας ολόκληρης γραμμής κατασκευής. Τα PLCs μπορούν να διαβάσουν τις εισόδους που συνδέονται με αυτά και να «αποφασίσουν» τι πρέπει να συμβεί μόλις έχουν προγραμματιστεί σωστά. Βάσει αυτής της απόφασης, χειρίζονται τα σήματα εξόδου. Συνδεδεμένα με αυτά τα σήματα εξόδου είναι τα τμήματα του εξοπλισμού που βρίσκεται στο πεδίο [14].

Τα PLCs παρουσιάζονται σαν τα βασικά δομικά κομμάτια σε συστήματα DCS και SCADA, αλλά μπορούν να χρησιμοποιηθούν και αυτόνομα σε μικρότερες βιομηχανικές μονάδες για τον ρυθμιστικό έλεγχο διακριτών διεργασιών όπως σε γραμμές συναρμολόγησης αυτοκινήτων.



Εικόνα 4: Αρχιτεκτονική συστήματος PLC, https://mec6004suheyb.wordpress.com/2016/03/12/architecture-of-plc/

Στην παρακάτω εικόνα φαίνεται ο έλεγχος μιας διαδικασίας κατασκευής που εκτελείται από ένα PLC μέσω ενός δικτύου Fieldbus.
Το PLC είναι προσβάσιμο μέσω μιας διεπαφής προγραμματισμού που βρίσκεται σε ένα Engineering Workstation και τα δεδομένα είναι αποθηκευμένα στη βαση δεδομένων Data Historian. Όλα είναι συνδεδεμένα σε LAN.



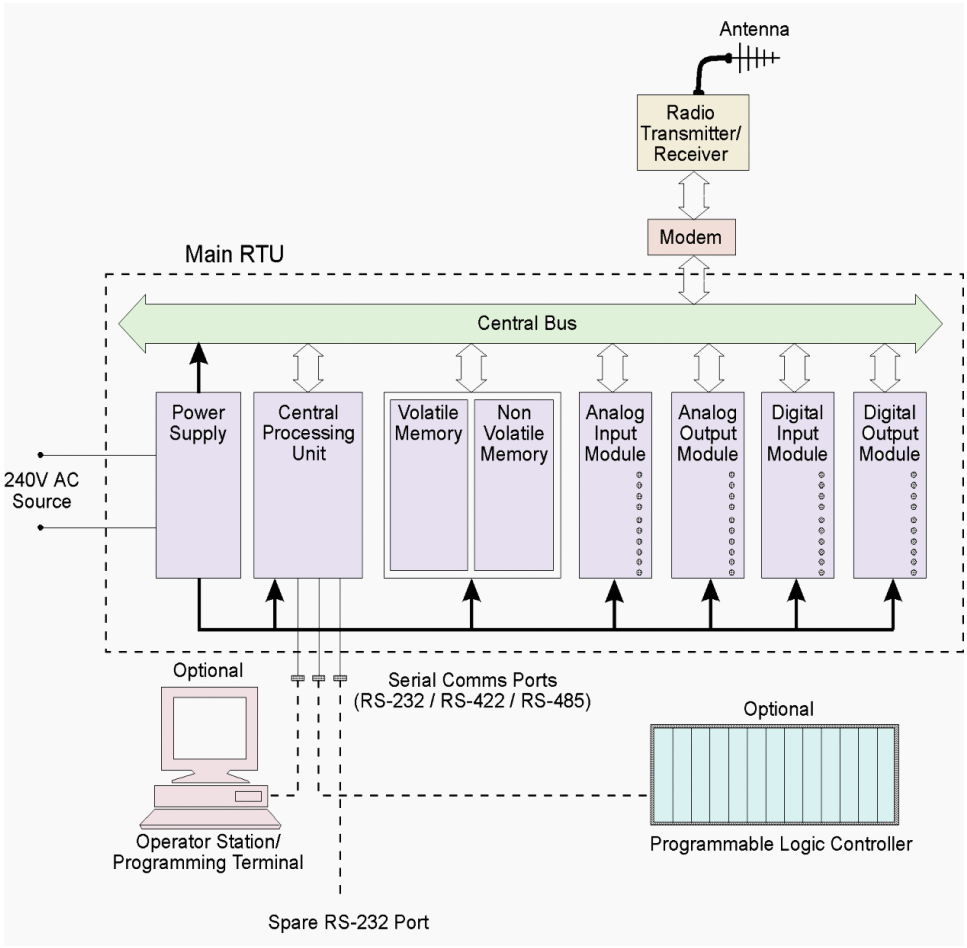
Εικόνα 5: Παράδειγμα υλοποίησης συστήματος PLC, "Guide to Industrial Control", NIST SP 800-82r2

Remote Terminal Unit (RTU)

Ένα RTU είναι μια αυτόνομη μονάδα λήψης δεδομένων και ελέγχου, βασισμένη σε μικροεπεξεργαστή, η οποία παρακολουθεί και ελέγχει τον εξοπλισμό και η οποία συνήθως βρίσκεται σε κάποιον υποσταθμό, κατά μήκος ενός αγωγού ή σε κάποια άλλη απομακρυσμένη τοποθεσία από τον κεντρικό σταθμό. Ο κύριος στόχος ενός RTU είναι να ελέγχει και να αποκτά δεδομένα από τον εξοπλισμό επεξεργασίας στην απομακρυσμένη τοποθεσία και να μεταφέρει αυτά τα δεδομένα πίσω σε έναν κεντρικό σταθμό. Αυτός ο κεντρικός σταθμός μπορεί να είναι ένας MTU (Master Terminal Unit), ένα κεντρικά τοποθετημένο PLC ή κάποιο HMI (Human Machine Interface) [10], [15].

Γενικά, ένα RTU έχει επίσης τη δυνατότητα να λαμβάνει προγράμματα διαμόρφωσης και ελέγχου από κάποιο κεντρικό σταθμό. Επιπλέον έχει τη δυνατότητα να διαμορφώνεται τοπικά από κάποια μονάδα προγραμματισμού RTU. Παρόλο που το RTU επικοινωνεί πίσω σε κάποιο κεντρικό σταθμό, είναι επίσης δυνατό να επικοινωνεί peer-to-peer με άλλους RTU. Το RTU μπορεί επίσης να λειτουργήσει ως σταθμός αναμετάδοσης (μερικές φορές αναφέρεται ως σταθμός αποθήκευσης και προώθησης) σε έναν άλλο RTU, ο οποίος ενδέχεται να μην είναι προσβάσιμος από τον κεντρικό σταθμό.

Τα RTUs για να επιτύχουν αυτή την απομακρυσμένη επικοινωνία συνήθως ενσωματώνουν κάποιο modem, μια σύνδεση μέσω δικτύου κινητής τηλεφωνίας, σύνδεση μέσω ραδιοκυμάτων ή κάποια άλλη επικοινωνία ευρέως φάσματος. Συχνά τοποθετούνται σε μέρη τα οποία μπορεί να μην έχουν σύνδεση με το δίκτυο ενέργειας και να τροφοδοτούνται από κάποιο τοπικό φωτοβολταϊκό στοιχείο ή από μια ανεμογεννήτρια.



Εικόνα 6: Δομή ενός RTU, https://electrical-engineering-portal.com/scada-dcs-plc-rtu-smart-instrument

Master Terminal Unit (MTU)

Το MTU είναι ο SCADA Server και αποτελεί τον πυρήνα σε ένα σύστημα βιομηχανικού ελέγχου SCADA [12]. Το MTU αποτελείται από ένα κεντρικό υπολογιστικό σύστημα, αρκετά μεγάλης ισχύος, στο οποίο βρίσκεται εγκατεστημένο το λογισμικό SCADA, όπως και το πρόγραμμα της εκάστοτε εφαρμογής.
Πρόκειται για ένα υπολογιστικό σύστημα το οποίο λαμβάνει τα δεδομένα που αποστέλλονται από τα διάφορα περιφερειακά συστήματα του ελεγκτικού μηχανισμού (αισθητήρες, IEDs, RTUs), τα επεξεργάζεται και αποστέλλει τα ανάλογα αποτελέσματα για την ορθή και άρτια διαχείριση του συστήματος.

Intelligent Electronic Device (IED)

Το IED είναι μία "έξυπνη" συσκευή με ικανότητα να συλλέγει δεδομένα, να επικοινωνεί με άλλες συσκευές και να πραγματοποιεί τοπικές διεργασίες και ελέγχους. Η χρήση IEDs σε συστήματα ελέγχου SCADA και DCS επιτρέπει σε ελέγχους στο τοπικό επίπεδο να γίνονται αυτόματα. Χρησιμοποιείται κυρίως στον ενεργειακό τομέα για την παρακολούθηση και τον έλεγχο ηλεκτρικών συσκευών όπως διακόπτες κυκλώματος, πυκνωτές και μετασχηματιστές.

Human Machine Interface (HMI)

Το HMI είναι λογισμικό και υλισμικό το οποίο επιτρέπει σε χειριστές να παρακολουθούν την κατάσταση μιας διεργασίας υπό έλεγχο, να τροποποιούν τις ρυθμίσεις του ελέγχου ώστε να μεταβάλλουν το στόχο του και να μπορούν να παρακάμπτουν τον αυτοματοποιημένο έλεγχο των διεργασιών σε περίπτωση έκτακτου περιστατικού. Συνήθως αποτελούνται από μία οπτική απεικόνιση της διεργασίας, πάνω στην οποία εμφανίζονται τιμές μεταβλητών, καταστάσεις και διαγράμματα.
Το HMI επιτρέπει ακόμα σε έναν μηχανικό ή χειριστή ελέγχου, την παραμετροποίηση των σημείων παρακολούθησης και των αλγορίθμων των συσκευών ελέγχου. Τέλος, ένα HMI είναι ικανό να κρατά ιστορικό αναφορών διαθέσιμο για το προσωπικό ελέγχου.

Data Historian Server

Το σύστημα Data Historian είναι μία κεντρική Βάση Δεδομένων η οποία περιέχει όλα τα αρχεία καταγραφής (logs) των διεργασιών ενός ICS. Τα αρχεία αυτά μπορεί να χρησιμοποιηθούν σε ένα ευρύ φάσμα αναλύσεων από το επίπεδο των διεργασιών έως το επιχειρηματικό επίπεδο.

Input/Output (IO) Server

Ο I/O Server είναι υπεύθυνος για την συλλογή και την παροχή πρόσβασης στην επεξεργασία δεδομένων από τα υποσυστήματα ελέγχου όπως είναι τα PLCs, RTUs και τα IEDs. Ο I/O Server μπορεί να βρίσκεται στον Control Server ή σε μία ξεχωριστή υπολογιστική πλατφόρμα.

Αισθητήρες (Sensors / Actuators)

Πρόκειται για συσκευές που δίνουν τη δυνατότητα ανίχνευσης τυχόν αλλαγών και μεταβολών ορισμένων βασικών τιμών που επιθυμούμε να παρακολουθούμε σε ένα βιομηχανικό σύστημα. Δέχονται ως είσοδο τυχόν αλλαγές στην μορφή ή στην ποσότητα του χαρακτηριστικού που έχουμε ορίσει και δίνουν μία αντίστοιχη έξοδο, πολλές φορές είτε ως ηλεκτρικό είτε ως οπτικό σήμα, μαζί με συγκεκριμένα δεδομένα που αφορούν τη μεταβολή αυτή.
Ορισμένα παραδείγματα χρήσης αισθητήρων σε βιομηχανικές μονάδες είναι οι αισθητήρες καπνού, υγρασίας καθώς και αισθητήρες ανίχνευσης της κίνησης.

4.2 Διατάξεις Δικτύου

Fieldbus Network

Χρησιμοποιείται για την σύνδεση αισθητήρων και άλλων συσκευών σε ένα PLC ή σε κάποιον άλλο ελεγκτή. Η χρήση τεχνολογιών Fieldbus εκμηδενίζει την ανάγκη διασύνδεσης point-to-point των συνδεδεμένων μερών και πραγματοποιείται με τη χρήση ειδικού πρωτοκόλλου επικοινωνίας.

Control Network

Συνδέει το εποπτικό επίπεδο (Area Supervisory Level) με τους ελεγκτές χαμηλότερων επιπέδων.

Communications Routers

Ένας δρομολογητής μεταφέρει μηνύματα μεταξύ δύο δικτύων. Παραδείγματα εφαρμογής είναι η σύνδεση ενός LAN δικτύου με ένα WAN, καθώς και η σύνδεση MTUs και RTUs με μέσα που βρίσκονται σε μεγάλη απόσταση για την επικοινωνία μιας διάταξης SCADA.

Firewall

Το Firewall προστατεύει ένα δίκτυο παρακολουθώντας και ελέγχοντας τα πακέτα επικοινωνίας, χρησιμοποιώντας προκαθορισμένες πολιτικές φιλτραρίσματος. Τα Firewalls χρησιμοποιούνται επίσης και για στρατηγικές διαχωρισμού σε ένα δίκτυο ICS.

Modems

Ένα modem είναι μία συσκευή που χρησιμοποιείται για την μετατροπή μεταξύ σειριακών ψηφιακών δεδομένων και ενός κατάλληλου σήματος για μετάδοση μέσω τηλεφωνικής γραμμής που επιτρέπει στις συσκευές να επικοινωνούν. Τα modems χρησιμοποιούνται συχνά στα συστήματα ICS γιατί επιτρέπουν την σειριακή επικοινωνία μεγάλων αποστάσεων μεταξύ MTUs και συσκευών πεδίου.

Remote Access Points

Τα Remote Access Points είναι διακριτές συσκευές, τοποθετημένες σε περιοχές ενός control network που επιτρέπουν την εξ αποστάσεως διαμόρφωση και παραμετροποίηση συστημάτων ελέγχου κι την πρόσβαση στα δεδομένα επεξεργασίας τους. Ένα παράδειγμα είναι η χρησιμοποίηση ενός laptop για την απομακρυσμένη πρόσβαση ενός συστήματος ICS.

5 Αρχιτεκτονική Ασφάλειας σε Συστήματα ICS

5.1 Αρχιτεκτονική – Purdue Model

Προκειμένου να σχεδιαστεί μια αρχιτεκτονική δικτύου για ανάπτυξη συστημάτων ICS σε κρίσιμες υποδομές, ο ασφαλέστερος τρόπος είναι να διαχωριστεί το δίκτυο ICS από το εταιρικό δίκτυο, επειδή η φύση της κυκλοφορίας δικτύου σε αυτά τα δύο δίκτυα είναι διαφορετική.

Η πρόσβαση στο Διαδίκτυο, το FTP, το email και η απομακρυσμένη πρόσβαση συνήθως επιτρέπονται στο εταιρικό δίκτυο, αλλά δεν πρέπει να επιτρέπονται στο δίκτυο ICS. Αυστηρές διαδικασίες ελέγχου αλλαγών για τον εξοπλισμό του δικτύου, η διαμόρφωση και οι αλλαγές λογισμικού ενδέχεται να μην ισχύουν στο εταιρικό δίκτυο. Εάν η κυκλοφορία ενός δικτύου ICS μεταφέρεται στο εταιρικό δίκτυο, θα μπορούσε να υποκλαπεί ή να υποβληθεί σε επιθέσεις Denial of Service (DoS) ή Man-in-the-Middle. Έχοντας ξεχωριστά δίκτυα, οποιοδήποτε πρόβλημα ασφάλειας και απόδοσης του εταιρικού δικτύου δεν θα έχει τη δυνατότητα να επηρεάσει το δίκτυο ICS [10].

Μία από τις πιο διαδεδομένες και ασφαλείς αρχιτεκτονικές για τα συστήματα ICS είναι το Purdue Model. Στη δεκαετία του 1990, ο Theodore J. Williams μαζί με μέλη του Purdue University Consortium for computer integrated manufacturing, ανέπτυξαν το Purdue Enterprise Reference Architecture (PERA) ως μοντέλο για αρχιτεκτονική επιχειρήσεων. Έκτοτε, το μοντέλο αυτό, προτείνεται από τους μεγαλύτερους οργανισμούς όπως οι NIST, ENISA και SANS ως βέλτιστη και πιο ασφαλής πρακτική για την ασφάλεια της αρχιτεκτονικής των συστημάτων και του δικτύου ενός περιβάλλοντος ICS.

Το Purdue Model βοήθησε στην παροχή ασφάλειας βιομηχανικής επικοινωνίας μέσω του διαχωρισμού των στρωμάτων και του ορισμού του τρόπου λειτουργίας και αλληλεπίδρασης μεταξύ των μηχανών ενός πεδίου και των αντίστοιχων διαδικασιών. Με άλλα λόγια, το μοντέλο αυτό παρέχει μια εξαιρετική εικόνα των διαφορετικών επιπέδων που χρησιμοποιούνται στις γραμμές παραγωγής και τον τρόπο διασφάλισής τους, στις κρίσιμες υποδομές. Αν υλοποιηθεί σωστά μπορεί να δημιουργήσει τις απαραίτητες ασφαλιστικές δικλείδες μεταξύ των συστημάτων ICS και των συστημάτων IT [16], [17].

Τα 6 επίπεδα του Purdue Model αναλύονται παρακάτω [18], [19].

Επίπεδο 0: Process (Cell/Area Zone)

Αυτό το επίπεδο περιλαμβάνει τους αισθητήρες και τα στοιχεία των οργάνων που συνδέονται άμεσα και ελέγχουν τη διαδικασία κατασκευής. Αυτές οι συσκευές ελέγχονται από συσκευές που βρίσκονται στο Επίπεδο 1.

Επίπεδο 1: Basic Control (Cell/Area Zone)

Αυτό το επίπεδο περιλαμβάνει τον εξοπλισμό ελέγχου διεργασιών που λαμβάνει είσοδο από αισθητήρες, επεξεργάζεται τα δεδομένα που εισάγονται χρησιμοποιώντας αλγόριθμους ελέγχου και στέλνει τα εξερχόμενα δεδομένα σε ένα τελικό στοιχείο. Οι συσκευές σε αυτό το επίπεδο είναι υπεύθυνες για συνεχή και διακριτό έλεγχο. Ορισμένες συσκευές που υπάρχουν στο επίπεδο είναι προγραμματιζόμενοι λογικοί ελεγκτές (PLCs) και απομακρυσμένες μονάδες τερματικού (RTUs). Αυτές οι συσκευές εκτελούν λειτουργικά συστήματα συγκεκριμένων προμηθευτών και είναι προγραμματισμένες και διαμορφωμένες από τους μηχανολογικούς σταθμούς εργασίας (Engineering Workstations).

Επίπεδο 2: Area Supervisory Control (Cell/Area Zone)

Αυτό το επίπεδο περιλαμβάνει τον κατασκευαστικό εξοπλισμό λειτουργίας για μια μεμονωμένη περιοχή παραγωγής. Το επίπεδο 2 περιλαμβάνει συνήθως:

- Διεπαφές Ανθρώπου Μηχανής (HMI)
- Συστήματα συναγερμών / ειδοποιήσεων (Alarms/Alert systems)
- Σταθμούς Εργασίας Δωματίου Ελέγχου (Control Room Workstations)

Αυτά τα συστήματα ενδέχεται να επικοινωνούν με συστήματα στο Επίπεδο 1. Επιπλέον, μπορούν επίσης να διασυνδέονται με συστήματα στις ζώνες Manufacturing και Enterprise μέσω του DMZ.

Επίπεδο 3 - Site Manufacturing Operations and Control (Manufacturing Zone)

Αυτό το επίπεδο περιλαμβάνει συστήματα που είναι υπεύθυνα για τη διαχείριση των λειτουργιών της μονάδας ελέγχου για την παραγωγή του επιθυμητού τελικού προϊόντος. Οι εφαρμογές, οι υπηρεσίες και τα συστήματα που βρίσκονται σε αυτό το επίπεδο περιλαμβάνουν:

- Βάση Δεδομένων (Data Historian)
- Μηχανολογικοί Σταθμοί Εργασίας (Engineering Workstations)
- Διακομιστές Αρχείων Δικτύου (Network File Servers)
- Υπηρεσίες πληροφορικής όπως DNS, DHCP, Active Directory και NTP
- Υπηρεσίες απομακρυσμένης πρόσβασης (Remote access services)

Τα συστήματα και οι εφαρμογές στο Επίπεδο 3 επικοινωνούν με τα συστήματα στο Enterprise Zone μέσω DMZ. Αποθαρρύνεται η άμεση επικοινωνία μεταξύ συστημάτων στις ζώνες Manufacturing και Enterprise. Επιπλέον, τα συστήματα στο Επίπεδο 3 ενδέχεται να επικοινωνούν με συστήματα στα Επίπεδα 1 και 0.

Επίπεδο 3.5 – Αποστρατικοποιημένη Ζώνη (Demilitarized zone, DMZ)

Η Αποστρατικοποιημένη Ζώνη (DMZ) είναι μια προσθήκη στο μοντέλο που εντοπίζεται την τελευταία κυρίως δεκαετία και περιλαμβάνει συστήματα ασφαλείας, όπως είναι τα Firewalls και οι proxies, που χρησιμοποιούνται για τον διαχωρισμό των συστημάτων IT και των συστημάτων OT. Σε αυτό το επίπεδο/στρώμα είναι που οι δύο “κόσμοι”, IT και OT, συγκλίνουν, αυξάνοντας την ενεργό επιφάνεια για επιθέσεις στα συστήματα OT. Πολλές βιομηχανικές μονάδες είτε δεν διαθέτουν αυτό το στρώμα είτε έχουν πολύ περιορισμένες δυνατότητες. Η άνοδος των αυτοματοποιημένων διεργασιών που οδηγεί σε υψηλότερες αποδόσεις δημιούργησε αυξημένη ανάγκη για αμφίδρομες ροές δεδομένων μεταξύ συστημάτων IT και OT. Αυτή η σύγκλιση συστημάτων IT-OT δημιουργεί τελικά ένα τρομερό ανταγωνιστικό πλεονέκτημα για εταιρείες που επιταχύνουν τον ψηφιακό μετασχηματισμό.

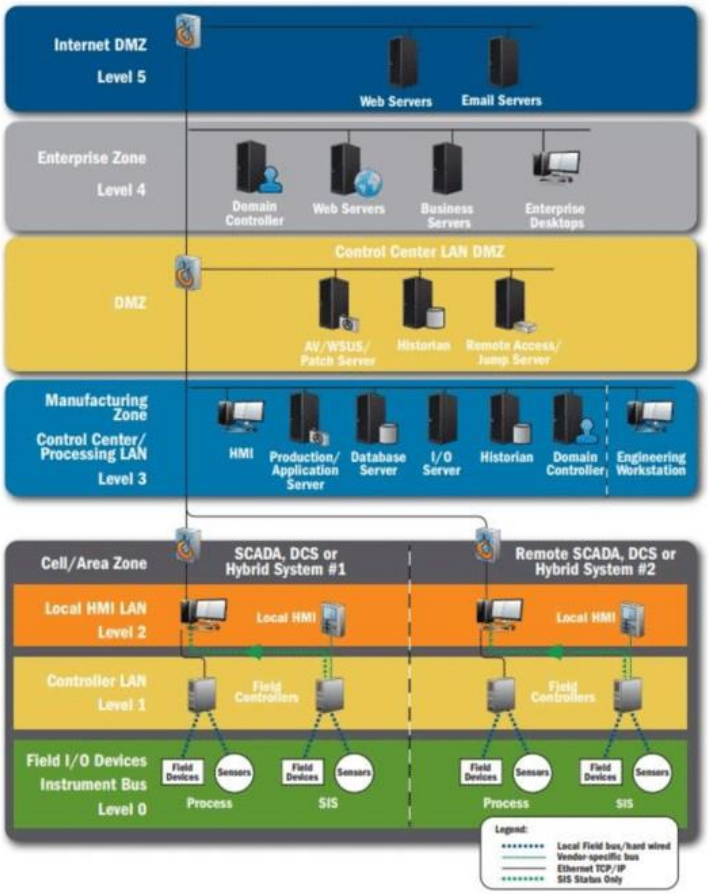
Επίπεδο 4 - Site Business Planning and Logistics (Enterprise Zone)

Αυτό το επίπεδο περιλαμβάνει συστήματα πληροφορικής που ασχολούνται με την αναφορά, τον προγραμματισμό, τη διαχείριση αποθέματος, τον προγραμματισμό χωρητικότητας, τη διαχείριση λειτουργίας και συντήρησης, τις υπηρεσίες ηλεκτρονικού ταχυδρομείου, τηλεφώνου και εκτύπωσης. Οι υπηρεσίες, τα συστήματα και οι εφαρμογές στα Επίπεδα 4 και 5 διαχειρίζονται και λειτουργούν από το Τμήμα Πληροφορικής.

Επίπεδο 5 – Enterprise (Enterprise Zone)

Αυτό το επίπεδο περιλαμβάνει εταιρικά συστήματα και εφαρμογές υποδομής πληροφορικής όπως απομακρυσμένη πρόσβαση VPN και εταιρικές υπηρεσίες πρόσβασης στο Διαδίκτυο. Η απευθείας επικοινωνία μεταξύ συστημάτων στις επιχειρηματικές ζώνες και στο περιβάλλον ICS αποθαρρύνεται συνήθως με βάση το επίπεδο κινδύνου που θα εκθέσει τον οργανισμό. Η πρόσβαση αυτή, γίνεται στο περιβάλλον ICS μέσω μιας αποστρατικοποιημένης ζώνης (DMZ).

Στην Εικόνα 7 διακρίνεται η αρχιτεκτονική Pupdue Model που περιγράφεται παραπάνω.



Εικόνα 7: Αρχιτεκτονική του Purdue Model, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies" 2016

5.2 Πρωτόκολλα Επικοινωνίας

Οι συσκευές των συστημάτων ICS μεταδίδουν πληροφορίες μέσω διαφόρων προτοκόλλων επικοινωνίας. Τα περισσότερα από αυτά, έχουν σχεδιαστεί για συγκεκριμένους σκοπούς, όπως αυτοματοποίηση διεργασιών, αυτοματισμοί κτιρίων, και αυτοματοποίηση συστημάτων ισχύος. Αυτά τα πρωτόκολλα αναπτύχθηκαν επίσης για να διασφαλιστεί η λειτουργικότητα μεταξύ διαφορετικών κατασκευαστών. Ωστόσο, υπάρχουν ορισμένα πρωτόκολλα που λειτουργούν μόνο εάν τα πρωτόκολλα και ο εξοπλισμός προέρχονται από τον ίδιο κατασκευαστή [20], [21], [22]. Τα πιο διαδεδομένα πρωτόκολλα επικοινωνίας για συστήματα ICS αναφέρονται παρακάτω:

Modbus

Το Modbus είναι το πιο παλιό και διαδεδομένο πρωτόκολλο για συστήμεατα ICS και χρησιμοποιείται για την επικοινωνία με τα PLCs. Υπάρχουν δύο τύποι υλοποιήσεων Modbus: Το Serial Modbus το οποίο χρησιμοποιεί το πρότυπο ελέγχου συνδέσεων δεδομένων υψηλού επιπέδου (High-Level Data Link Control - HDLC) για τη μετάδοση δεδομένων και το Modbus-TCP το οποίο χρησιμοποιεί το πρωτόκολλο TCP / IP για τη μετάδοση δεδομένων.

Process Field Bus (PROFIBUS)

Το πρωτόκολλο PROFIBUS χρησιμοποιείται κυρίως για την επικοινωνία μεταξύ ενός RTU και ενός MTU, μεταξύ δύο MTUs ή μεταξύ δύο RTUs που βρίσκονται στο πεδίο.

Distributed Network Protocol (DNP3)

Το πρωτόκολλο DNP3 έχει τρία επίπεδα που λειτουργούν στο επίπεδο σύνδεσης δεδομένων (Data Link Layer), στο επίπεδο εφαρμογής (Application Layer) και στο επίπεδο μεταφοράς (Transport Layer). Αυτό το πρωτόκολλο χρησιμοποιείται κυρίως σε σταθμούς ηλεκτροπαραγωγής και σε εγκαταστάσεις επεξεργασίας νερού και λυμάτων.

Open Platform Communication (OPC)

Το OPC είναι μια σειρά προτύπων και προδιαγραφών για βιομηχανικές επικοινωνίες. Η προδιαγραφή OPC βασίζεται σε τεχνολογίες που αναπτύχθηκαν από τη Microsoft για λειτουργικά συστήματα Windows.

Building Automation and Control Networks (BACnet)

Το BACnet είναι ένα πρωτόκολλο επικοινωνίας που έχει σχεδιαστεί για τον έλεγχο της θέρμανσης, του αερισμού και του κλιματισμού (HVAC).

Common Industrial Protocol (CIP)

Το CIP είναι ένα σύνολο υπηρεσιών και μηνυμάτων για έλεγχο, ασφάλεια, συγχρονισμό, διαμόρφωση, πληροφορία κ.λπ. Το πρωτόκολλο αυτό μπορεί να ενσωματωθεί σε δίκτυα Ethernet και στο Διαδίκτυο. Διαθέτει έναν αριθμό προσαρμογών που παρέχουν ενδοεπικοινωνία και ενοποίηση για διαφορετικούς τύπους δικτύων.

6 Επιθέσεις και Ασφάλεια Συστημάτων ICS

6.1 Ορισμός ενός Περιστατικού Ασφάλειας

Σύμφωνα με τον NIST, ένα περιστατικό ασφάλειας είναι ένα περιστατικό που θέτει σε πραγματικό ή δυνητικό κίνδυνο την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός συστήματος πληροφοριών ή των πληροφοριών που το σύστημα επεξεργάζεται, αποθηκεύει ή μεταδίδει, ή που συνιστά παραβίαση ή επικείμενη απειλή παραβίασης των πολιτικών ασφαλείας, των διαδικασιών ασφαλείας ή των πολιτικών αποδεκτής χρήσης.

Ένα περιστατικό ασφάλειας σε υπολογιστή είναι μια παραβίαση ή επικείμενη απειλή παραβίασης των πολιτικών ασφαλείας του υπολογιστή, των πολιτικών αποδεκτής χρήσης ή των τυπικών πρακτικών ασφαλείας. Αυτό κυμαίνεται από σοβαρές επιθέσεις ασφάλειας στον κυβερνοχώρο σε κρίσιμες εθνικές υποδομές και σε μεγάλο οργανωμένο έγκλημα στον κυβερνοχώρο, μέσω των hackers και βασικών επιθέσεων κακόβουλου λογισμικού, έως εσωτερική κακή χρήση συστημάτων και δυσλειτουργίας λογισμικού. Αυτό περιλαμβάνει επίσης τις λεγόμενες Προηγμένες Επίμονες Απειλές (Advanced Persistent Threats (APT)).

Παραδείγματα από περιστατικά ασφάλειας είναι μεταξύ άλλων τα ακόλουθα:

- Ένας επιτιθέμενος δίνει εντολή σε ένα botnet να στέλνει μεγάλους όγκους αιτημάτων σύνδεσης σε έναν διακομιστή ιστού, προκαλώντας του σφάλμα.
- Ανεπιθύμητη διακοπή ή άρνηση υπηρεσίας (Denial of Service)
- Μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα
- Αλλαγές στα χαρακτηριστικά του υλισμικού ή του λογισμικού ενός συστήματος, χωρίς τη γνώση, την οδηγία ή τη συγκατάθεση του ιδιοκτήτη
- Παρουσία κακόβουλης εφαρμογής, όπως ο ιός
- Παρουσία απροσδόκητων ή ασυνήθιστων προγραμμάτων

6.2 Τύποι Περιστατικών Ασφάλειας

Τα περιστατικά ασφαλείας μπορεί να ομαδοποιηθούν σε διαφορετικές κατηγορίες ανάλογα με τον τύπο του επιτιθέμενου, τον στόχο της επίθεσης, τον σκοπό της επίθεσης και την ικανότητα του επιτιθέμενου. Ο τύπος του επιτιθέμενου μπορεί να μεταβεί από μια μικρή ομάδα εγκληματιών σε εξαιρετικά οργανωμένους και εξαιρετικά εξειδικευμένους επαγγελματίες με διεθνή παρουσία όπως το APT29, ο οποίος είναι γνωστός παράγοντας απειλής από τη Ρωσία που στοχεύει κυβερνήσεις και συναφείς οργανισμούς. Ο στόχος της επίθεσης μπορεί να είναι ένα άτομο ή ένας χρηματοοικονομικός κλάδος ή ακόμα και κυβερνητικές υπηρεσίες. Ο σκοπός της επίθεσης μπορεί να είναι γεωπολιτικός, ιδεολογικός, ικανοποίηση ή κέρδος. Γενικά, οι διάφοροι παράγοντες απειλής στον κυβερνοχώρο έχουν τα δικά τους κίνητρα. Για παράδειγμα, τα κίνητρα για εσωτερικές απειλές σε έναν οργανισμό μπορεί να είναι δυσαρέσκεια, το κίνητρο για εγκληματίες στον κυβερνοχώρο μπορεί να είναι το κέρδος και για τις τρομοκρατικές ομάδες μπορεί να είναι ιδεολογική βία.

6.3 Επιθέσεις

Ενώ οι τακτικές, οι τεχνικές και οι διαδικασίες του εισβολέα ενδέχεται να μην αλλάζουν δραματικά, οι συνολικές τάσεις συνεχίζουν να εξελίσσονται. Στόχος των πεπισσότερων οργανισμών είναι να σχηματίσουν ομάδες ασφαλείας με την απαραίτητη γνώση που πρέπει να υπερασπιστούν έναντι των πιο συχνά χρησιμοποιούμενων επιθέσεων στον κυβερνοχώρο, καθώς και σε λιγότερο εμφανείς και αναδυόμενες απειλές.

Τα στατιστικά στοιχεία που αναφέρονται στο M-Trends 2020 βασίζονται στις έρευνες της FireEye [23] Mandiant για στοχοθετημένη δραστηριότητα επίθεσης που πραγματοποιήθηκε μεταξύ 1ης Οκτωβρίου 2018 και 30 Σεπτεμβρίου 2019.
Όπως απεικονίζεται και στον Πίνακα 3, κατά το έτος αυτό, οι σύμβουλοι της FireEye Mandiant παρατήρησαν μείωση 12% των συμβιβασμών που εντοπίζονται εσωτερικά. Αυτή είναι η μεγαλύτερη μείωση σε αυτήν τη μέτρηση από το 2011.

Πίνακας 3: Ανίχνευση από πηγή

Συμβιβαστικές Ειδοποιήσεις	2011	2012	2013	2014	2015	2016	2017	2018	2019
Εξωτερικά	94%	63%	67%	69%	53%	47%	38%	41%	53%
Εσωτερικά	6%	37%	33%	31%	47%	53%	62%	59%	47%

6.4 Στοχευμένες Επιθέσεις και Επαναπροσδιορισμός

Μερικοί από τους πιο στοχευμένους κλάδους στον χώρο της βιομηχανίας [23] είναι οι παρακάτω:

- Αεροπορία
- Βιοτεχνολογία
- Επιχειρισιακές/Επαγγελματικές υπηρεσίες
- Κατασκευή/Μηχανική
- Εκπαίδευση
- Ενέργεια
- Ψυχαγωγία/ΜΜΕ
- Χρηματοοικονομική
- Κυβέρνηση
- Υγεία
- Μη Κερδοσκοπικές Οργανώσεις
- Τηλεπικοινωνίες
- ΜΜΜ

Οι ειδικοί της Mandiant σε κυβερνοεπιθέσεις αποκρίθηκαν σε αρκετές επιθέσεις τον περασμένο χρόνο παρατηρώντας τα εξής:

- Το 7% προήλθε από ή χρησιμοποίησε παραβιασμένη πρόσβαση τρίτων.
- Το 15% είχε πολλαπλούς εισβολείς.
- Λιγότερο από 1% αφορούσε ένα άτομο.
- Το 22% είχε πιθανή κλοπή δεδομένων για την υποστήριξη της πνευματικής ιδιοκτησίας ή της κατασκοπείας τελικών στόχων.
- Το 29% ήταν πιθανό για άμεσο οικονομικό κέρδος. Αυτό περιλαμβάνει εκβιασμό, λύτρα, κάρτα, κλοπή και παράνομες μεταφορές.
- Το 3% αυτών των στοχευμένων επιθέσεων ήταν για το σκοπό της μεταπώλησης της πρόσβασης που αποκτήθηκε η εισβολή.
- Το 4% πιθανότατα δεν εξυπηρέτησε κάποιον σκοπό, εκτός από τη διευκόλυνση άλλων πιθανών επιθέσεων.

Το 11% από τις αποκρίσεις και αποτιμήσεις σε περιστατικά κυβερνοεπιθέσεων αφορούσαν περιβάλλον υπολογιστικής νέφους. Όσο οι οργανισμοί εξακολουθούν να χρησιμοποιούν έναν υβριδικό περιβαλλοντικό συνδυασμό υπηρεσιών στις εγκαταστάσεις τους αλλά και στην υπολογιστική νέφους, οι επιτιθέμενοι θα έχουν το πλεονέκτημα να επιδιώξουν τους στόχους τους.

6.5 Ζώνες Ασφαλείας των Συστημάτων ICS

Προκειμένου να δημιουργηθεί μια πολυεπίπεδη άμυνα, πρέπει να υφίσταται μια σαφή κατανόηση του πώς όλη η τεχνολογία συνδέεται μεταξύ της και που βρίσκεται όλη η διασυνδεσιμότητα. Διαχωρίζοντας τις αρχιτεκτονικές των συστημάτων ελέγχου σε ζώνες, μπορεί να βοηθήσει τους οργανισμούς να

δημιουργήσουν σαφή όρια προκειμένου να εφαρμόσουν αποτελεσματικά πολλαπλά στρώματα άμυνας. Η κατανόηση του τρόπου τμηματοποίησης του δικτύου είναι ζωτικής σημασίας για τη δημιουργία ζωνών ασφαλείας και για τον καθορισμό των μεθοδολογιών που θα χρησιμοποιηθούν για τον διαχωρισμό των δικτύων εντός και γύρω από τα σύστημα ελέγχου.

Από την σκοπιά της κυβερνοασφάλειας, τα συστήματα ICS μπορεί να κατηγοριοποιηθούν σε τρείς ζώνες [19] όπως φαίνεται και στην Εικόνα 8.

- Enterprise zone
- Manufacturing zone
- Cell zone

Enterprise Zone

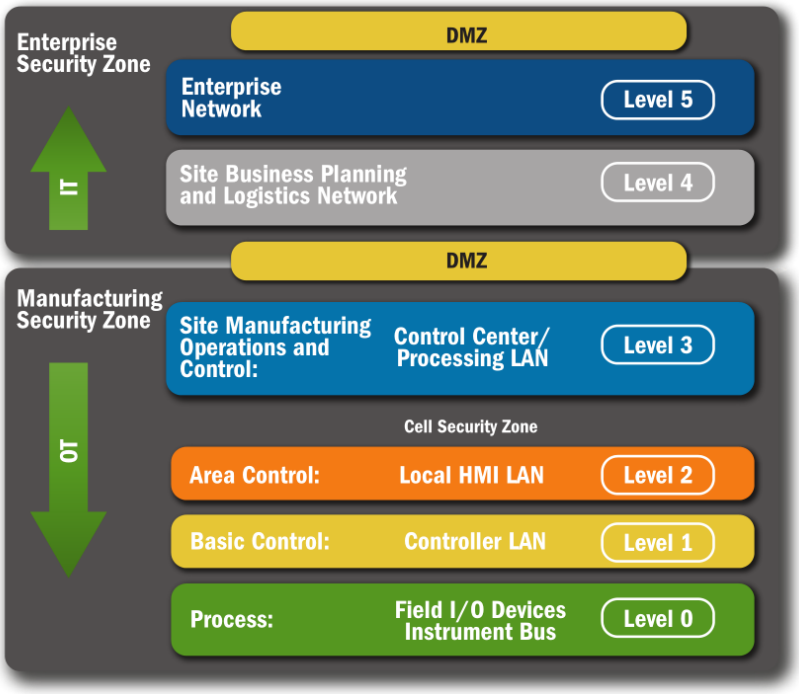
Η Enterprise Zone περιλαμβάνει το Επίπεδο 4 και το Επιπεδο 5 της Αρχιτεκτονικής Purdue. Πιο συγκεκριμένα, περιέχει τα επιχειρηματικά δίκτυα και τα συστήματά τους, τη συνδεσιμότητα στο Διαδίκτυο, εφεδρικές ή απομακρυσμένες εγκαταστάσεις (Σύνδεση εταιρικού δικτύου-Επίπεδο 5) καθώς και τα επιχειρηματικά δίκτυα που περιλαμβάνουν εταιρική επικοινωνία, Email Servers, Domain Name System (DNS) Servers, και επιχειρηματικά συστήματα IT (Επίπεδο 4). Υπάρχει μεγάλη ποικιλία κινδύνων σε αυτήν τη ζώνη λόγω του ποσού των συστημάτων και της συνδεσιμότητας, κι από άποψη ασφάλειας, αυτή η ζώνη θεωρείται αναξιόπιστη.

Manufacturing Zone

Η Manufacturing Zone περιλαμβάνει το Επίπεδο 3 της Αρχιτεκτονική Purdue. Πιο συγκεκριμένα, περιέχει την περιοχή συνδεσιμότητας όπου είναι κατανεμημένα τα στοιχεία παρακολούθησης και ελέγχου σε συστήματα SCADA. Είναι ένας κρίσιμος τομέας για τη διαθεσιμότητα και τη διαχείριση ενός δικτύου ελέγχου. Οι συσκευές επιχειρησιακής υποστήριξης βρίσκονται σε αυτήν τη ζώνη μαζί με τους Data Acquisition Servers και τους Data Historian Servers. Η ζώνη αυτή είναι κεντρική για τη λειτουργία των τελικών συσκευών (end devices) και παρέχει την απαιτούμενη συνδεσιμότητα με την Enterprise Zone. Η προτεραιότητα αυτής της ζώνης είναι υψηλή καθώς υπάρχουν κίνδυνοι που σχετίζονται με την άμεση συνδεσιμότητά τους με οποιαδήποτε εξωτερικά συστήματα ή δίκτυα.

Cell Zone

Η Cell Zone περιλαμβάνει το Επίπεδο 2, το Επίπεδο 1 και το Επίπεδο 0 της Αρχιτεκτονικής Purdue. Πιο συγκεκριμένα, περιέχει τις συσκευές και τα δίκτυα που είναι υπεύθυνα για τον έλεγχο και τους αυτοματισμούς τοπικής ή απομακρυσμένης περιοχής, όπως τα HMIs πεδίου (Επίπεδο 2), τα PLCs και τα στοιχεία ελέγχου τους (Επίπεδο 1) και βασικές συσκευές εισόδου/εξόδου όπως ενεργοποιητές και αισθητήρες (Επίπεδο 0). Η προτεραιότητα αυτών των ζωνών είναι πολύ υψηλή, καθώς αυτές είναι οι περιοχές όπου οι λειτουργίες ελέγχου επηρεάζουν τις φυσικές τελικές συσκευές. Τα δίκτυα επικοινωνίας αυτής της ζώνης έχουν μεγαλύτερο εύρος και συχνά χρησιμοποιούν πρωτόκολλα κάτω από το IP συνδέοντας μεγάλη ποικιλία βιομηχανικών πρωτοκόλλων και φυσικών διεπαφών. Όλες οι συσκευές της ζώνης αυτής, υπόκεινται σε αυστηρές απαιτήσεις όσο αφορά στην ασφάλεια, την αξιοπιστία και τον συγχρονισμό. Λόγω των παραπάνω, ελάχιστες κοινές πρακτικές κυβερνοασφάλειας έχουν εφαρμογή σε αυτή την ζώνη.



Εικόνα 8: Ζώνες Ασφάλειας των συστημάτων ICS, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies" 2016

6.6 Τακτικές και Τεχνικές Επίθεσης σε Συστήματα ICS

Ο οργανισμός MITRE ATT&CK [24] κυκλοφόρησε ένα πλαίσιο σχετικά με τις τακτικές και τις τεχνικές που χρησιμοποιούν οι αντίπαλοι του κυβερνοχώρου όταν επιτίθενται στα συστήματα ICS που λειτουργούν μερικές από τις πιο κρίσιμες υποδομές, συμπεριλαμβανομένων εγκαταστάσεων μεταφοράς και διανομής ενέργειας, διυλιστηρίων πετρελαίου, εγκαταστάσεων επεξεργασίας λυμάτων, και συστημάτων μεταφοράς. Οι επιπτώσεις από αυτές τις επιθέσεις κυμαίνονται από διακοπές στη λειτουργική παραγωγικότητα έως σοβαρές βλάβες στην ανθρώπινη ζωή και στο περιβάλλον.

Η χρήση της σύνδεσης στο Διαδίκτυο, της ασύρματης σύνδεσης, της υπολογιστικής νέφους, καθώς και η "κοινωνική μηχανική" σε δίκτυα SCADA έχουν καταστήσει την αρχιτεκτονική των συστημάτων ICS ευάλωτη. Ένας από τους κύριους λόγους των αδυναμιών σε συστήματα ICS είναι η έλλειψη ισχυρής κρυπτογράφισης καθώς και η ανάγκη για συστηματική παρακολούθηση των συστημάτων σε πραγματικό χρόνο.

Οι επιθέσεις μπορεί να συμβούν σε όλα τα επίπεδα της αρχιτεκτονικής των ICS και μπορεί να κατηγοριοποιηθούν σε επιθέσεις υλισμικού, λογισμικού και σύνδεσης δικτύου [25].

- **Επιθέσεις σε Υλισμικό**: Σε αυτήν την περίπτωση ο εισβολέας αποκτά μη εξουσιοδοτημένη πρόσβαση στις συσκευές και παρεμβαίνει στις λειτουργίες τους, γι' αυτό και ο κύριος στόχος για την ασφάλεια των υλισμικών είναι ο έλεγχος πρόσβασης.
- **Επιθέσεις σε Λογισμικό**: Τα συστήματα SCADA χρησιμοποιούν μια ποικιλία λογισμικού για να βελτιώσουν την αποτελεσματικότητά τους, ικανοποιώντας τις λειτουργικές τους απαιτήσεις. Ωστόσο, λόγω της κακής εφαρμογής, πολλές φορές είναι ευάλωτα σε επιθέσεις SQL Injection, Trojan Horse και Buffer Overflow.
- **Επιθέσεις σε Συνδέσεις Δικτύου**: Οι επιθέσεις στην επικοινωνία μπορεί να πραγματοποιηθούν στο επίπεδο δικτύου, στο επίπεδο μεταφοράς και στο επίπεδο εφαρμογής παραβιάζοντας τους στόχους ασφάλειας, δηλαδή της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της μη-αποποίησης ευθύνης.

Σε αυτήν την ενότητα θα περιγραφούν μερικές από τις πιο διαδεδομένες μεθόδους επίθεσης σε συστήματα ICS. Στην Εικόνα 9 παρουσιάζονται αναλυτικά οι τρόποι επιθέσεων που έχει καταγράψει ο οργανισμός MITRE ATT&CK.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Εικόνα 9: Τακτικές και τεχνικές επίθεσεις σε συστήματα ICS, MITRE, ATT&CK for Industrial Control Systems

SCADA System Compromise

Αυτή η επίθεση καλύπτει μια μόλυνση που έχει σχεδιαστεί για τον έλεγχο ενός ή περισσότερων περιουσιακών στοιχείων SCADA εντός ενός δικτύου προκειμένου να είναι σε θέση ο εισβολέας να τις χειριστεί ή να τις συντρίψει κατά βούληση (π.χ. τροποποίηση τιμών, αλλαγή λειτουργιών ή άρνηση πρόσβασης).

Αυτό μπορεί να προκαλέσει ανεπιθύμητα αποτελέσματα, όπως δυσλειτουργία ή καταστροφή των συστημάτων, φυσική ζημιά, καθώς και κίνδυνο να επεκταθεί και σε άλλα περιουσιακά στοιχεία και συστήματα εντός της υποδομής (ή σε άλλα υποδομές), προκαλώντας δυνητική ζημιά [25], [26].

Insider Threat

Οι εσωτερικοί χρήστες (υπάλληλοι, εργολάβοι, εξωτερικοί συνεργάτες) μπορεί να έχουν άμεση γνώση και εμπειρία στις λεπτομέρειες των εσωτερικών συστημάτων, σε εταιρικά συστήματα, στα δίκτυα SCADA και σε λεπτομέρειες εγκατάστασης.

Επομένως, ένας υπάλληλος μπορεί να εκμεταλλευτεί αυτήν τη γνώση, καθώς και τα δικαιώματα πρόσβασης που έχει στα συστήματα του οργανισμού, για την πραγματοποίηση κακόβουλων δραστηριοτήτων.

Για αυτόν τον λόγο, οι δραστηριότητες και τα δικαιώματα των χρηστών των συστημάτων πρέπει να περιορίζονται στο ελάχιστο και όλες οι ενέργειες πρέπει να παρακολουθούνται και να καταγράφονται κατά την πρόσβαση σε ευαίσθητες πληροφορίες ή κρίσιμα συστήματα [25], [26].

Malware Infection

Το κακόβουλο λογισμικό Malware είναι ένα κακόβουλο λογισμικό ή πρόγραμμα που εισβάλει μέσα σε ένα σύστημα με διάφορους τρόπους προκειμένου να καταστρέψει τα δεδομένα που είναι αποθηκευμένα στον υπολογιστή.

Τα συστήματα ICS χρειάζονται διαρκή συντήρηση, καθώς και αναβαθμίσεις μέσω ενημερώσεων λογισμικού και λειτουργιών προκειμένου να διασφαλίσουν την ασφαλέστερη και πιο αποτελεσματική λειτουργία τους [25], [26].

Unauthorized Access Attacks

Πολλά συστήματα ελέγχου είναι σχεδιασμένα ώστε οι διαχειριστές και οι χρήστες τους να έχουν απομακρυσμένη πρόσβαση. Όταν τα συστήματα αυτά δεν έχουν μέτρα ασφάλειας, ένας επιτιθέμενος, με μικρή προσπάθεια, μπορεί να συνδεθεί απομακρυσμένα με ελάχιστη πιθανότητα ανίχνευσης της

πρόσβασης αν δεν υπάρχουν τα κατάλληλα μέτρα (monitoring, logging). Επιθέσεις όπως Brute-force cracking μπορεί να προκύψουν σε συσκευές που διαθέτουν ασφαλείς μεθόδους login με διαπιστευτήρια χρηστών, αφου δεν διατίθεται από το σύστημα μηχανισμός κλειδώματος της πρόσβασης μετά από αποτυχημένες προσπάθειες.

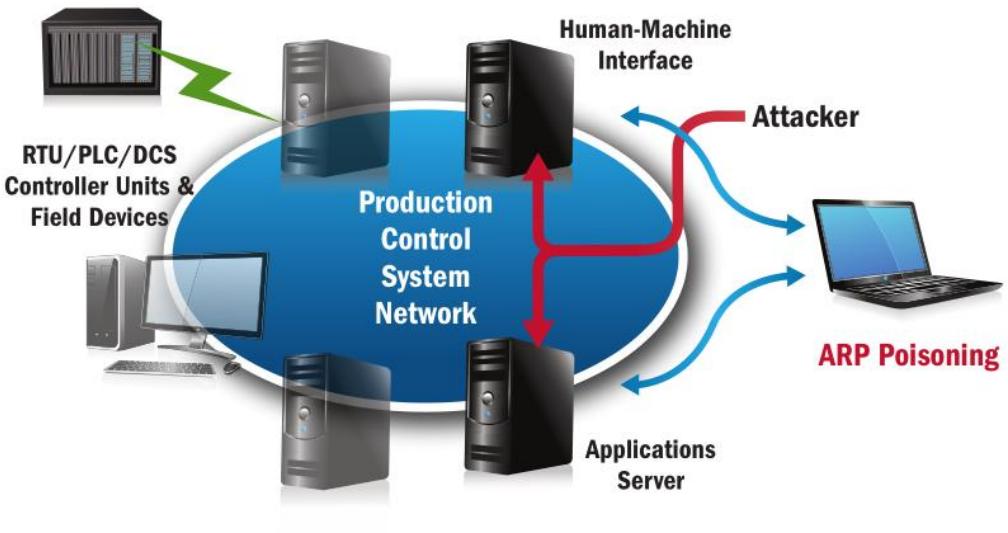
Επιπλέον, οι συσκευές πεδίου είναι μέρος του εσωτερικού και έμπιστου δικτύου, οπότε η πρόσβαση ενός εισβολέα σε μία τέτοια συσκευή μπορεί να δώσει πρόσβαση στην δομή του συστήματος ελέγχου. Χρησιμοποιώντας την πρόσβαση στο εσωτερικό δίκτυο αισθητήρων, ο εισβολέας μπορεί να πραγματοποιήσει μια αντίστροφη σύνδεση tunneling στο δίκτυο του κέντρου ελέγχου. Τέτοιες επιθέσεις αν και θεωρούνται αδύνατες με τη χρήση των σειριακών συνδέσεων, έχουν κεντρίσει την προσοχή των υπεύθυνων ασφαλείας λόγω της χρήσης των “παραδοσιακών” ασύρματων πρωτοκόλλων επικοινωνίας για απομακρυσμένες συσκευές.

Αν ένας εισβολέας αποκτήσει τον έλεγχο μίας συσκευής, τότε μπορεί να εκκινήσει έναν αριθμό διαδικασιών (π.χ. σάρωση για ανίχνευση συσκευών προς το εσωτερικό δίκτυο ελέγχου, παραποίηση των δεδομένων που αποστέλλονται στο κεντρικό σημείο ελέγχου ή αλλαγή στη συμπεριφορά της ίδιας της συσκευής). Εάν ο εισβολέας αποφασίσει να εκτελέσει μία σάρωση για ανίχνευση συσκευών στο δίκτυο ελέγχου, το οποίο αξιοποιεί την εμπιστοσύνη μεταξύ των πόρων του συστήματος, μπορεί να επιτύχει την εκμετάλλευση των πραγματικών πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται σε όλο τον τομέα του συστήματος ελέγχου. Αυτό μπορεί να είναι πλεονέκτημα για τον εισβολέα, καθώς οι διασύνδεσεις στο εσωτερικό των συστημάτων δεν παρακολουθούνται από κάποιο σύστημα παρακολούθησης (monitoring) για κακόβουλη ή ύποπτη κίνηση. Κάποια συστήματα IDS (Intrusion Detection Systems) παρέχουν τη δυνατότητα αναβάθμισης ώστε να μπορούν να ανιχνεύσουν επιθέσεις σε συστήματα ICS. Συνήθως τέτοια συστήματα λειτουργούν με την ανίχνευση κάποιας χαρακτηριστικής υπογραφής (signature) και ενεργοποιούνται όταν εντοπίσουν κάποια “γνώριμη” κακόβουλη κίνηση. Κάποια συστήματα IDS μπορεί επίσης να ενεργοποιηθούν με την ανίχνευση μη προβλεπόμενης κίνησης δεδομένων [19], [27].

Man-in-the-Middle Attacks

Τα παραδοσιακά συστήματα ICS θεωρούνται προστατευμένα συστήματα λόγω της “απομόνωσής” τους από τα παραδοσιακά συστήματα IT. Στα συστήματα ICS οι διαχειριστές, συνήθως, δεν προστατεύουν τις ροές των δεδομένων μεταξύ των servers, των συσκευών και των πόρων, θεωρώντας ότι αυτά βρίσκονται εντός ενός προστατευμένου δικτύου. Με την πάροδο των ετών και με την διασύνδεση όλο και περισσότερων δικτύων ICS με τα επιρρηματικά δίκτυα, έχουν προκύψει αρκετά ζητήματα ασφαλείας με ένα από τα κυριότερα να είναι η δυνατότητα του επιτιθέμενου να επαναδρομολογεί την κίνηση των δεδομένων που μεταφέρονται, να εντοπίζει και να αναλύει τα δεδομένα αυτά, που συνήθως μεταφέρονται σε μορφή απλού κειμένου (plain text) ή ακόμα και η απόκτηση πλήρους ελέγχου σε πρωτόκολλα που χρησιμοποιούνται για τον έλεγχο συσκευών.

Συνδυάζοντας όλα αυτά, ένας επιτιθέμενος μπορεί να αποκτήσει υψηλά διαβαθμισμένο έλεγχο της κίνησης του δικτύου και να κατευθύνει κατά το δοκούν πραγματικά ή αλλοιωμένα δεδομένα επιτυγχάνοντας το προσδοκώμενο αποτέλεσμα. Για να επιτύχει τους σκοπούς αυτούς ένας επιτιθέμενος εξαπολύει μια επίθεση Man-in-the-Middle (MitM), όπως φαίνεται στην Εικόνα 10.



Εικόνα 10: Man-in-the-Middle attack, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies" 2016

Η διαχείριση των διευθύνσεων ενός δικτύου είναι μία κρίσιμη διαδικασία για την αποδοτική λειτουργία του. Το πρωτόκολλο ARP (Address Resolution Protocol) διατηρεί έναν πίνακα ARP και δρομολογεί την κίνηση συνδέοντας διευθύνσεις IP με τις φυσικές διευθύνσεις MAC των συσκευών. Ο κακόβουλος χειρισμός αυτών των πινάκων δρομολόγησης είναι ο στόχος του επιτιθέμενου, διότι μέσω αυτού μπορεί να επαναδρομολογήσει την κίνηση του δικτύου μέσω του υπολογιστή που έχει αποκτήσει τον έλεγχο. Αυτό αναγκάζει όλες τις συσκευές του δικτύου να επικοινωνούν με την συσκευή που είναι στον έλεγχο του επιτιθέμενού χωρίς να το γνωρίζουν. Επιπλέον, ο επιτιθέμενος μπορεί να εισάγει αλλοιωμένα δεδομένα στο δίκτυο σαν να στέλνονται από μια έμπιστη συσκευή.

Σε κάθε περιβάλλον, και ειδικά σε ένα σύστημα ICS, οι επιθέσεις MitM μπορεί να έχουν καταστροφικά αποτελέσματα. Η χρήση πρωτοκόλλων με αδύναμη ταυτοποίηση ή ο πλημμελής έλεγχος του υποστηριζόμενου firmware των συσκευών μπορεί να χρησιμοποιηθούν για την εκδήλωση μιας τέτοιας επίθεσης [19], [27].

Denial of Service

Μία ακόμα διαδεδομένη επίθεση είναι η επίθεση άρνησης υπηρεσίας Denial of Service, η οποία στοχεύει στην απαίτηση της διαθεσιμότητας ενός δικτύου ή μιας υπηρεσίας. Πρόκειται για έναν τύπο επίθεσης όπου ένας νόμιμος χρήστης δεν έχει πρόσβαση σε έναν συγκεκριμένο πόρο εντός του περιβάλλοντος ICS, π.χ. η μη δυνατή επικοινωνία μεταξύ ενός MTU και ενός RTU στο πεδίο. Αυτό επιτυγχάνεται στέλνοντας μηνύματα στον στόχο παρεμβαίνοντας στη λειτουργία του, και το κάνουν να συντριβεί, να κάνει επανεκκίνηση ή να κάνει μία ανούσια δουλειά. Η επίθεση Denial of Service είναι εύκολη να ξεκινήσει, και δύσκολη να αποφευχθεί [25], [28].

SQL Injection Attacks

Οι Βάσεις Δεδομένων αποτελούν ένα βασικό κομμάτι των συστημάτων ICS. Τα παραδοσιακά μοντέλα ασφαλείας επιχειρούν να ασφαλίσουν τα συστήματα μέσω της απομόνωσης των βασικών μερών που τα αποτελούν συγκεντρώνοντας τις προσπάθειές τους κατά των απειλών στους υπολογιστές ή το λογισμικό και αφήνοντας στο περιθώριο τις Βάσεις Δεδομένων. Οι Βάσεις Δεδομένων στα συστήματα ICS χρησιμοποιούν ανεξάρτητα συστήματα που χρησιμοποιούν το ένα το άλλο για να επιτύχουν την λειτουργικότητα που απαιτείται. Η υψηλή διαλειτουργικότητα μεταξύ των δύο συστημάτων δημιουργεί μεγαλύτερη ενεργό επιφάνεια επίθεσης.

Οι Βάσεις Δεδομένων που χρησιμοποιούνται στα συστήματα ICS συχνά συνδέονται σε υπολογιστές που χρησιμοποιούν εφαρμογές web και βρίσκονται στο επιχειρηματικό δίκτυο του οργανισμού. Κάθε εφαρμογή που χρησιμοποιεί δεδομένα έχει μετατραπεί σε κάποιου είδους Βάση Δεδομένων, με τις περισσότερες να χρησιμοποιούν τη γλώσσα SQL, και διαθέτουν κάποια διεπαφή στο διαδίκτυο που μπορεί να έχει τις τυπικές ευπάθειες του διαδικτύου (XSS ή SQL injection).

Οι πληροφορίες που περιέχονται στις Βάσεις Δεδομένων είναι υψηλής αξίας για κάθε επιτιθέμενο. Σε συστήματα ICS που οι Βάσεις Δεδομένων των συστημάτων ελέγχου συνδέονται σε επιχειρηματικές ή οικονομικές βάσεις ή σε υπολογιστές που χρησιμοποιούν διάφορες εφαρμογές για να προσπελάσουν τα δεδομένα, δίνεται η ευκαιρία σε επιτιθέμενους να παρέμβουν στο κανάλι που χρησιμοποιείται για την μεταφορά των δεδομένων και να αποκτήσουν πρόσβαση στο δίκτυο.

Η εγκατάσταση κακόβουλου κώδικα σε μία Βάση Δεδομένων που περιέχει πολύτιμα δεδομένα μπορεί να έχει εκτεταμένες επιπτώσεις, ιδιαίτερα στο περιβάλλον ελέγχου όπου η ακρίβεια και η ακεραιότητα των δεδομένων είναι κρίσιμη για τη λήψη αποφάσεων τόσο στο επιχειρηματικό πεδίο όσο και στο εκτελεστικό. Η αλλοίωση ή η καταστροφή των δεδομένων σε μια Βάση Δεδομένων, μπορεί να επηρεάσει τους διακομιστές απόκτησης δεδομένων, τους Data Historians ακόμα και την ομαλή λειτουργία της κονσόλας HMI. Τα συστήματα ICS είναι πιο ευπαθή σε επιθέσεις SQL injection από ότι μια κλασσική Βάση Δεδομένων σε ένα σύστημα IT, επειδή βασίζονται άμεσα από τη διαθεσιμότητα και την ακεραιότητα των δεδομένων τους. Επιπλέον, η επιτυχής διείσδυση από κάποιον κακόβουλο ενός τόσο ευαίσθητου αγαθού των συστημάτων ICS, οδηγεί σε πρόσθετους πόρους που μπορεί να χρησιμοποιηθούν από τον κακόβουλο για αναγνώριση ή για εκτέλεση κώδικα [19], [27].

Social Engineering Attacks

Μια από τις πιο γνωστές επιθέσεις Κοινωνικής Μηχανικής είναι οι επιθέσεις Social Engineering. Οι επιθέσεις αυτές στηρίζονται στην εμπιστοσύνη που επιδεικνύουν οι περισσότεροι άνθρωποι προς τον συνάνθρωπό τους. Μέσω της αποστολής κάποιου παραπλανητικού email που περιέχει κάποιο κακόβουλο επισυναπτόμενο αρχείο ή σύνδεσμο, αποκτούν πρόσβαση στο σύστημα.

Οι επιτιθέμενοι όλο και πιο συχνά εξαπολύουν επιθέσεις ψαρέματος (Phishing attacks) σε διαχειριστές συστημάτων και συσκευών με στόχο να εισβάλουν κάποιο κακόβουλο κώδικα μέσα στα συστήματα ICS. Ιδιαίτερα κρίσιμος θεωρείται λοιπόν ο διαχωρισμός και ο έλεγχος οποιασδήποτε διασύνδεσης, από τη φάση της σχεδίασης των συστημάτων, μεταξύ των επιχειρηματικών διαδικασιών και του λειτουργικού τμήματος των συστημάτων ICS. Επιπλέον, σημαντική είναι και η ασφάλεια της φυσικής υποδομής των συστημάτων ICS από τη μη εξουσιοδοτημένη πρόσβαση χωρίς τις απαραίτητες πιστοποιήσεις από το προσωπικό που πρέπει για λόγους συντήρησης ή λειτουργίας να βρίσκεται εντός των χώρων αυτών [19], [27].

7 Μελέτη Περίπτωσης – Ανάλυση και Διαχείριση Επικινδυνότητας Συστημάτων ICS σε Εφαρμογές Ενέργειας

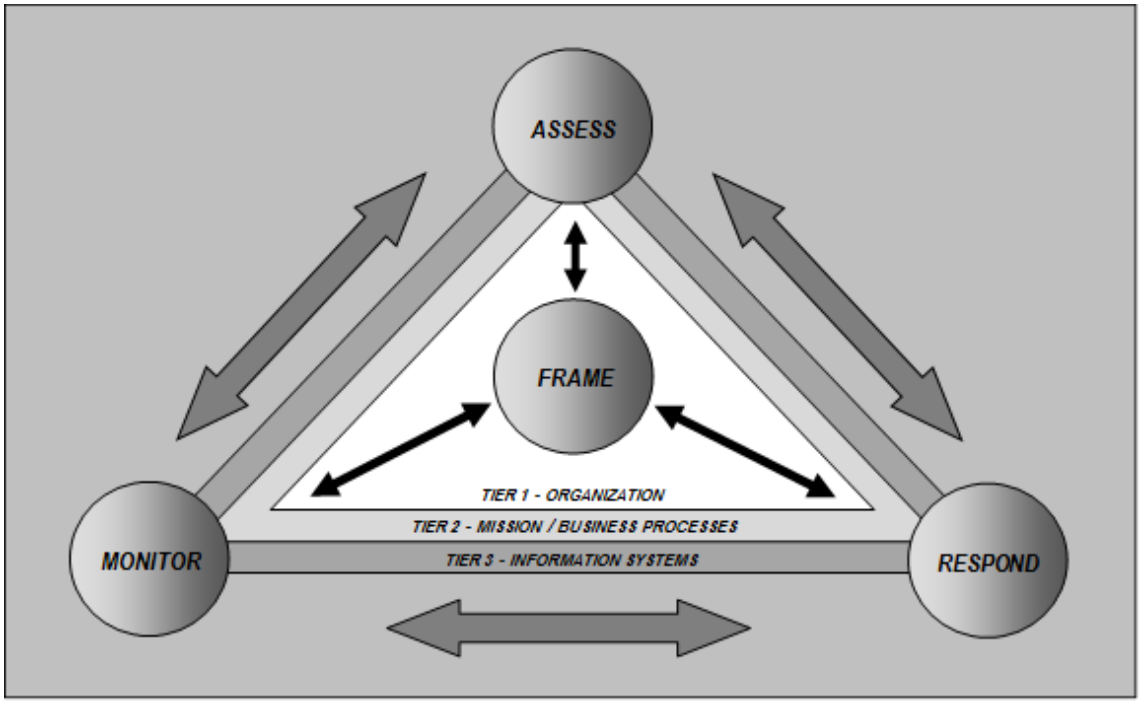
7.1 Εισαγωγή

Οι οργανισμοί διαχειρίζονται τον κίνδυνο κάθε μέρα για την επίτευξη των επιχειρηματικών τους στόχων. Αυτοί οι κίνδυνοι μπορεί να περιλαμβάνουν οικονομικό κίνδυνο, κίνδυνο αστοχίας εξοπλισμού και κίνδυνο ασφάλειας προσωπικού, για να αναφέρουμε μόνο μερικούς. Οι οργανισμοί πρέπει να αναπτύξουν διαδικασίες για να αξιολογήσουν τους κινδύνους που σχετίζονται με την επιχείρησή τους και να αποφασίσουν πώς να αντιμετωπίσουν αυτούς τους κινδύνους με βάση τις οργανωτικές προτεραιότητες και τους εσωτερικούς και εξωτερικούς περιορισμούς. Αυτή η διαχείριση της επικινδυνότητας διεξάγεται ως μια διαδραστική, συνεχής διαδικασία ως μέρος των κανονικών λειτουργιών. Οι οργανισμοί που χρησιμοποιούν συστήματα ICS διαχειρίζονται τον κίνδυνο μέσω καλών πρακτικών ασφαλείας και μηχανικής.

Μια διαδικασία διαχείρισης επικινδυνότητας πρέπει να εφαρμόζεται σε ολόκληρο τον οργανισμό, χρησιμοποιώντας μια προσέγγιση τριών επιπέδων για την αντιμετώπιση του κινδύνου:

- σε επίπεδο οργανισμού
- σε επίπεδο αποστολής / επιχειρηματικής διαδικασίας
- σε επίπεδο συστήματος πληροφοριών (IT και ICS).

Η διαδικασία διαχείρισης επικινδυνότητας πραγματοποιείται απρόσκοπτα στα τρία επίπεδα με τον γενικό στόχο της συνεχούς βελτίωσης των δραστηριοτήτων που σχετίζονται με τον κίνδυνο και της αποτελεσματικής επικοινωνίας μεταξύ των ενδιαφερομένων και ενδοεπιχειρησιακών φορέων που έχουν κοινό ενδιαφέρον για την αποστολή και την επιχειρηματική επιτυχία του οργανισμού.



Εικόνα 11: Διαδικασία διαχείρισης επικινδυνότητας, "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82r2

7.2 Μεθοδολογία Αποτίμησης Επικινδυνότητας

Η μεθοδολογία για τη μελέτη που ακολουθεί πραγματοποιείται για την ανάλυση και τη διαχείριση επικινδυνότητας σε εφαρμογές ενέργειας με πεδίο εφαρμογής ένα ενεργειακό πάρκο που έχει

εγκατεστημένα τα συστήματα ICS ενός οργανισμού. Για την αποτίμηση επικινδυνότητας των αγαθών ICS του ενεργειακού πάρκου, η μεθοδολογία βασίστηκε σε βέλτιστες πρακτικές όπως:

- Το STORM-RM [30], [31] για τη δημιουργία του μοντέλου των αγαθών, και την αναγνώριση απειλών και ευπαθειών.
- Τη μεθοδολογία αξιολόγησης κινδύνου OWASP για την εκτίμηση του επιπέδου απειλής.
- Το πρότυπο ISO/IEC 27005 για τον υπολογισμό της επικινδυνότητας.
- Τον κανονισμό NERC CIP [7], που αποτελεί ένα σύνολο απαιτήσεων για τη διασφάλιση των αγαθών που απαιτούνται για την απρόσκοπτη λειτουργία του ηλεκτρικού συστήματος των ΗΠΑ.
- Τα πρότυπα NIST 800-53 [31], NIST 800-82 [10] για την αναγνώριση απειλών, ευπαθειών, κινδύνων και προτεινόμενων μέτρων.
- Το ENISA, *"Communication network dependencies for ICS/SCADA Systems",* 2016 [26] για την αναγνώριση απειλών, ευπαθειών, κινδύνων και προτεινόμενων μέτρων.

7.2.1 Αναγνώριση Επικινδυνότητας

7.2.1.1 Χαρτογράφηση Αγαθών

Η ομάδα ασφάλειας πληροφοριών πρέπει να ορίσει, να κάνει απογραφή και να κατηγοριοποιήσει τις εφαρμογές και τα συστήματα υπολογιστών εντός ενός περιβάλλοντος ICS, καθώς και τα δίκτυα και τη διασύνδεση με το ICS. Το επίκεντρο θα πρέπει να είναι τα συστήματα και όχι μόνο οι συσκευές και θα πρέπει να περιλαμβάνει τα PLC, RTU, SCADA και τα συστήματα τα βασισμένα σε όργανα που χρησιμοποιούν μια συσκευή παρακολούθησης, όπως ένα HMI. Τα στοιχεία που χρησιμοποιούν ένα δρομολογημένο πρωτόκολλο ή είναι προσβάσιμα μέσω τηλεφώνου πρέπει επίσης να απογραφούν. Η ομάδα θα πρέπει να ελέγχει και να ενημερώνει τη λίστα των αγαθών ICS ετησίως, αλλά και μετά από κάθε προσθήκη ή κατάργηση κάποιου αγαθού.

Η ακόλουθη λίστα των αγαθών που σχετίζονται με στοιχεία ICS πρέπει να λαμβάνεται υπόψιν για την αναγνώρισή τους και την απογραφή τους:

- Φυσικά Αγαθά / Υποδομή: Field, Control Room, Primary Control Center, Backup Control Center

- Υλισμικά Αγαθά: Sensors, Transmitters, Actuators, Valves, Motors, PLC, RTU, IED, Modem, Wireless AP, Local HMI, Engineering Workstations, Switches/ Gateways, Communication Router, HMI, Production / Application Server, Database Server, I/O Server, Data Historian Server, Domain Controller, Antivirus Server, Patch Server, Application Server, Data Historian Server Mirror, Remote Access Server, Corporate Web Server, File Server, DNS Server, AD Server, Corporate Workstations and Laptops, Web Server, Email Server, Smartphones, Tablets, Mobile Devices, Routers, Access Points, Repeaters, etc.

- Λογισμικά Αγαθά: PLC SW, Firewall, Local SCADA Server - MTU OS, Local SCADA Server - MTU SW, Local HMI OS, Local HMI SW, Engineering Workstations OS, Engineering Workstations SW, HMI OS, HMI SW, Production / Application Server OS, Production / Application Server SW, Database Server OS, Database Server SW, I/O Server OS, I/O Server SW, Data Historian Server OS, Data Historian Server SW, Domain Controller OS, Domain Controller SW, Antivirus Server OS, Antivirus Server SW, Patch Server OS, Patch Server SW, Application Server OS, Application Server SW, Remote Access Server OS, Remote Access Server SW, Corporate Web Server OS, Corporate Web Server SW, File Server OS, File Server SW, DNS Server OS, DNS Server SW, AD Server OS, AD Server SW, Corporate Workstations and Laptops OS, Corporate Workstations and Laptops SW, Web Server OS, Web Server SW, Email Server OS, Email Server SW

Πίνακας 4: Χαρτογράφηση Αγαθών

Επίπεδο	#	Όνομα Αγαθού	Περιγραφή	Ρόλος	Κατηγορία	Υποκατηγορία	Τοποθεσία
Level 0: Process (Cell/Area Zone)	A1	Sensors, Transmitters	Ένα ηλεκτρονικό όργανο που μπορεί να μετρήσει τη φυσική ποσότητα και να παράγει διακριτή έξοδο. Αυτές οι έξοδοι των αισθητήρων έχουν συνήθως τη μορφή ηλεκτρικών σημάτων.	Λαμβάνουν πληροφορίες κατάστασης από φυσικά στοιχεία.	Υλισμικό	Συσκευή Πεδίου	Πεδίο (Ενεργειακό Πάρκο)
	A2	Actuators, Valves, Motors	Μια συσκευή που αλλάζει τη φυσική ποσότητα καθώς μπορεί να προκαλέσει την κίνηση ενός μηχανικού εξαρτήματος αφού λάβει κάποια είσοδο από τον αισθητήρα. Με άλλα λόγια, λαμβάνει μια είσοδο ελέγχου (γενικά με τη μορφή του ηλεκτρικού σήματος) και δημιουργεί μια αλλαγή στο φυσικό σύστημα μέσω της παραγωγής ισχύος, θερμότητας, κίνησης κ.λπ.	Αλληλεπιδρούν με φυσικό τρόπο με τα αγαθά.	Υλισμικό	Συσκευή Πεδίου	Πεδίο (Ενεργειακό Πάρκο)
Level 1: Basic Control (Cell/Area Zone)	A3	PLC	Τα PLC χρησιμοποιούνται τόσο στα συστήματα SCADA όσο και στα συστήματα DCS ως συστατικά ελέγχου ενός συνολικού ιεραρχικού συστήματος για την παροχή τοπικής διαχείρισης διαδικασιών μέσω ελέγχου ανατροφοδότησης.	Οι ελεγκτές πεδίου συλλέγουν και επεξεργάζονται δεδομένα εισόδου και εξόδου (I / O). Στέλνουν επίσης τα δεδομένα διεργασίας στο HMI, καθώς και εντολές ελέγχου διεργασίας από το HMI στους ελεγκτές πεδίου.	Υλισμικό	Ελεγκτής Πεδίου	Πεδίο (Ενεργειακό Πάρκο)

	A4	PLC SW	Το λογισμικό PLC χρησιμοποιείται για τη δημιουργία του προγράμματος υπολογιστή που είναι αποθηκευμένο σε ένα PLC για να παρακολουθεί τις εισόδους του και να ελέγχει τις εξόδους από τις συσκευές του πεδίου.	Παρακολουθεί τις εισόδους του και να ελέγχει τις εξόδους από τις συσκευές του πεδίου.	Λογισμικό	Λογισμικό Ελεγκτή Πεδίου	Πεδίο (Ενεργειακό Πάρκο)
	A5	RTU	Ηλεκτρονική συσκευή που ελέγχεται από κάποιον μικροεπεξεργαστή. Είναι διαφορετικό από ένα PLC επειδή θεωρείται πιο κατάλληλο καθώς χρησιμοποιεί ασύρματη επικοινωνία και ταιριάζει σε μια ευρύτερη γεωγραφική τηλεμετρία.	Η κύρια λειτουργία ενός RTU είναι η διασύνδεση του SCADA με τα φυσικά αντικείμενα που υπάρχουν στο πεδίο.	Υλισμικό	Ελεγκτής Πεδίου	Πεδίο (Ενεργειακό Πάρκο)
	A6	IED	Το IED είναι μία “έξυπνη” συσκευή με ικανότητα να συλλέγει δεδομένα, να επικοινωνεί με άλλες συσκευές και να πραγματοποιεί τοπικές διεργασίες και ελέγχους. Η χρήση IEDs σε συστήματα ελέγχου SCADA και DCS επιτρέπει στους ελέγχους στο τοπικό επίπεδο να γίνονται αυτόματα.	Χρησιμοποιείται κυρίως στον ενεργειακό τομέα για την παρακολούθηση και τον έλεγχο ηλεκτρικών συσκευών όπως διακόπτες κυκλώματος, πυκνωτές και μετασχηματιστές.	Υλισμικό	Ελεγκτής Πεδίου	Πεδίο (Ενεργειακό Πάρκο)

	A7	Firewall	Μια συσκευή σε ένα δίκτυο επικοινωνιών που μπορεί να προγραμματιστεί για το φιλτράρισμα πληροφοριών βάσει του περιεχομένου των πληροφοριών, της πηγής ή του προορισμού.	Το Firewall προστατεύει ένα δίκτυο παρακολουθώντας και ελέγχοντας τα πακέτα επικοινωνίας, χρησιμοποιώντας προκαθορισμένες πολιτικές φιλτραρίσματος. Τα Firewalls χρησιμοποιούνται επίσης και για στρατηγικές διαχωρισμού σε ένα δίκτυο ICS.	Λογισμικό	Συσκευή Δικτύου	Πεδίο (Ενεργειακό Πάρκο)
	A8	Modem	Ένα modem είναι μία συσκευή που χρησιμοποιείται για την μετατροπή μεταξύ σειριακών ψηφιακών δεδομένων και ενός κατάλληλου σήματος για μετάδοση μέσω τηλεφωνικής γραμμής που επιτρέπει στις συσκευές να επικοινωνούν.	Τα modems χρησιμοποιούνται συχνά στα συστήματα ICS γιατί επιτρέπουν την σειριακή επικοινωνία μεγάλων αποστάσεων μεταξύ MTUs και συσκευών πεδίου.	Υλισμικό	Συσκευή Δικτύου	Πεδίο (Ενεργειακό Πάρκο)
	A9	Wireless AP	Μια συσκευή που συνδέει μεταξύ τους ασύρματες συσκευές επικοινωνίας για τον σχηματισμό ενός ασύρματου δικτύου. Ο σταθμός βάσης συνήθως συνδέεται με ένα ενσύρματο δίκτυο και μπορεί να μεταφέρει δεδομένα ανάμεσα στις ασύρματες και τις ενσύρματες συσκευές.	Επιτρέπει σε άλλες συσκευές Wi-Fi να συνδεθούν σε ενσύρματο δίκτυο.	Υλισμικό	Συσκευή Δικτύου	Πεδίο (Ενεργειακό Πάρκο)

Level 2: Area Supervisory Control (Cell/Area Zone)	A10	Control Room	Το δωμάτιο εποπτείας που βρίσκονται οι συσκευές και τα συστήματα ελέγχου.	Ο χώρος αυτός προστατεύει τις συσκευές και τα συστήματα ελέγχου από ανεπιθύμητα περιστατικά.	Υποδομή	Δωμάτιο Ελέγχου	Δωμάτιο Ελέγχου
	A11	Local SCADA Server - MTU	Ένας ελεγκτής που λειτουργεί επίσης ως διακομιστής που φιλοξενεί το λογισμικό ελέγχου που επικοινωνεί με συσκευές ελέγχου χαμηλότερου επιπέδου, όπως RTUs και PLCs, μέσω ενός δικτύου ICS. Σε ένα σύστημα SCADA, αυτό συχνά ονομάζεται διακομιστής SCADA, MTU ή εποπτικός ελεγκτής.	Συλλέγει πληροφορίες από το ενεργειακό πάρκο (sensors, PLCs, IEDs κ.λπ.), τις μεταφέρει σε μια κεντρική εγκατάσταση υπολογιστική και εμφανίζει τις πληροφορίες στον χειριστή γραφικά ή με κείμενο, επιτρέποντας έτσι στον χειριστή να παρακολουθεί ή να ελέγχει ένα ολόκληρο σύστημα από μια κεντρική τοποθεσία σε σχεδόν πραγματικό χρόνο.	Υλισμικό	Υπολογιστής Διακομιστή	Δωμάτιο Ελέγχου
	A12	Local SCADA Server - MTU OS	Το λειτουργικό σύστημα του Local SCADA Server – MTU.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Δωμάτιο Ελέγχου
	A13	Local SCADA Server - MTU SW	Το λογισμικό που περιέχει ο Local SCADA Server – MTU.	_	Λογισμικό	Λογισμικό Διακομιστή	Δωμάτιο Ελέγχου

	A14	Local HMI	Το HMI είναι υλισμικό το οποίο περιέχει λογισμικό που επιτρέπει σε χειριστές να παρακολουθούν την κατάσταση μιας διεργασίας υπό έλεγχο, να τροποποιούν τις ρυθμίσεις του ελέγχου ώστε να μεταβάλλουν το στόχο του και να μπορούν να παρακάμπτουν τον αυτοματοποιημένο έλεγχο των διεργασιών σε περίπτωση έκτακτου περιστατικού.	Είναι υπεύθυνο για τον έλεγχο των διαφόρων συστημάτων παραγωγής τα οποία είναι υπό επίβλεψη.	Υλισμικό	Υπολογιστής	Δωμάτιο Ελέγχου
	A15	Local HMI OS	Το λειτουργικό σύστημα του HMI.	_	Λογισμικό	Λειτουργικό Σύστημα Υπολογιστή	Δωμάτιο Ελέγχου
	A16	Local HMI SW	Το λογισμικό που περιέχει το HMI.	_	Λογισμικό	Λογισμικό Υπολογιστή	Δωμάτιο Ελέγχου
	A17	Engineering Workstations	Οι μηχανολογικοί σταθμοί εργασίας είναι αξιόπιστες υπολογιστικές πλατφόρμες υψηλής τεχνολογίας, σχεδιασμένες για τη διαμόρφωση, τη συντήρηση και τη διάγνωση εφαρμογών συστημάτων ελέγχου και άλλου εξοπλισμού.	Το σύστημα αποτελείται συνήθως από πολλούς σκληρούς δίσκους, διασυνδέσεις δικτύων υψηλής ταχύτητας, αξιόπιστες CPU, υλικό γραφικών επιδόσεων και εφαρμογές που παρέχουν εργαλεία διαμόρφωσης και παρακολούθησης για την εκτέλεση της ανάπτυξης εφαρμογών του συστήματος ελέγχου, τη συλλογή και τη διανομή των τροποποιήσεων του συστήματος.	Υλισμικό	Υπολογιστής	Δωμάτιο Ελέγχου
	A18	Engineering Workstations OS	Το λειτουργικό σύστημα των Engineering Workstations.	_	Λογισμικό	Λειτουργικό Σύστημα Υπολογιστή	Δωμάτιο Ελέγχου

	A19	Engineering Workstations SW	Λογισμικά που είναι εγκατεστημένα στους Μηχανολογικούς Σταθμούς Εργασίας.	_	Λογισμικό	Λογισμικό Υπολογιστή	Δωμάτιο Ελέγχου
	A20	Firewall	Μια συσκευή σε ένα δίκτυο επικοινωνιών που μπορεί να προγραμματιστεί για το φιλτράρισμα πληροφοριών βάσει του περιεχομένου των πληροφοριών, της πηγής ή του προορισμού.	Το Firewall προστατεύει ένα δίκτυο παρακολουθώντας και ελέγχοντας τα πακέτα επικοινωνίας, χρησιμοποιώντας προκαθορισμένες πολιτικές φιλτραρίσματος. Τα Firewalls χρησιμοποιούνται επίσης και για στρατηγικές διαχωρισμού σε ένα δίκτυο ICS.	Λογισμικό	Λογισμικό Δικτύου	Δωμάτιο Ελέγχου
	A21	Switches/ Gateways	Συσκευές δικτύου που έχουν σχεδιαστεί για τον έλεγχο και τη διαχείριση των τμημάτων δικτύου όπου βρίσκονται οι εποπτευόμενες διαδικασίες.	Παρέχουν ένα υψηλό επίπεδο ελέγχου και αποτελεσματικότητας εντός του δικτύου, καθώς μπορεί να χρησιμοποιηθούν για την απομόνωση των επικοινωνιών μεταξύ συγκεκριμένων συσκευών και έχουν ρυθμιστεί έτσι ώστε να ρυθμίζουν την κυκλοφορία του δικτύου, διασφαλίζοντας ότι το δίκτυο δεν θα έχει συμφόρηση από πάρα πολλές πληροφορίες.	Υλισμικό	Συσκευή Δικτύου	Δωμάτιο Ελέγχου

	A22	Modem	Ένα modem είναι μία συσκευή που χρησιμοποιείται για την μετατροπή των σειριακών ψηφιακών δεδομένων σε ένα κατάλληλο σήμα για μετάδοση μέσω τηλεφωνικής γραμμής που επιτρέπει στις συσκευές να επικοινωνούν.	Τα modems χρησιμοποιούνται συχνά στα συστήματα ICS γιατί επιτρέπουν την σειριακή επικοινωνία μεγάλων αποστάσεων μεταξύ των MTUs και των συσκευών πεδίου.	Υλισμικό	Συσκευή Δικτύου	Δωμάτιο Ελέγχου
	A23	Communication Router	Παραδείγματα εφαρμογής είναι η σύνδεση ενός δικτύου LAN με ένα WAN, καθώς και η σύνδεση MTUs και RTUs με μέσα που βρίσκονται σε μεγάλη απόσταση για την επικοινωνία μιας διάταξης SCADA.	Ένας δρομολογητής που μεταφέρει μηνύματα μεταξύ δύο δικτύων.	Υλισμικό	Συσκευή Δικτύου	Δωμάτιο Ελέγχου
Level 3 - Site Manufacturing Operations and Control	A24	Primary Control Center	Ο χώρος εποπτείας που βρίσκονται οι συσκευές και τα συστήματα ελέγχου.	Ο χώρος αυτός προστατεύει τις συσκευές και τα συστήματα ελέγχου από ανεπιθύμητα περιστατικά.	Υποδομή	Κέντρο Ελέγχου	Κέντρο Ελέγχου

(Manufacturing Zone)	A25	Backup Control Center	Το εφεδρικό κέντρο ελέγχου είναι ένα πλεονάζον σύστημα ελέγχου που αντικατοπτρίζει το πρωτεύον σύστημα κέντρου ελέγχου.	Το εφεδρικό κέντρο ελέγχου παρέχει παράλληλες επικοινωνίες με τις απομακρυσμένες περιοχές I/O και επιτρέπει την πλήρη μεταφορά ελέγχου από το κύριο σύστημα ελέγχου στο εφεδρικό σύστημα σε περίπτωση έκτακτης ανάγκης ή προγραμματισμένων λειτουργιών χωρίς καμία απώλεια επιχειρησιακού ελέγχου έκτακτης ανάγκης και ικανότητας παρακολούθησης των συστημάτων.	Υποδομή	Κέντρο Ελέγχου	Κέντρο Ελέγχου
	A26	HMI	Το HMI είναι υλισμικό το οποίο περιέχει λογισμικό που επιτρέπει σε χειριστές να παρακολουθούν την κατάσταση μιας διεργασίας υπό έλεγχο, να τροποποιούν τις ρυθμίσεις του ελέγχου ώστε να μεταβάλλουν το στόχο του και να μπορούν να παρακάμπτουν τον αυτοματοποιημένο έλεγχο των διεργασιών σε περίπτωση έκτακτου περιστατικού.	Είναι υπεύθυνο για τον έλεγχο των διαφόρων συστημάτων παραγωγής υπό επίβλεψη.	Υλισμικό	Υπολογιστής	Κέντρο Ελέγχου
	A27	HMI OS	Το λειτουργικό σύστημα του HMI.	_	Λογισμικό	Λειτουργικό Σύστημα Υπολογιστή	Κέντρο Ελέγχου
	A28	HMI SW	Το λογισμικό που περιέχει το HMI.	_	Λογισμικό	Λογισμικό Υπολογιστή	Κέντρο Ελέγχου

	A29	Production / Application Server	Ο διακομιστής εφαρμογών είναι ένας διακομιστής που φιλοξενεί εφαρμογές.	Παρέχει δυνατότητες δημιουργίας web εφαρμογών και περιβάλλοντος διακομιστή για την εκτέλεση τους.	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου
	A30	Production / Application Server OS	Το λειτουργικό σύστημα του Production / Application Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Κέντρο Ελέγχου
	A31	Production / Application Server SW	Το λογισμικό που περιέχει ο Production / Application Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Κέντρο Ελέγχου
	A32	Database Server	Ο διακομιστής βάσης δεδομένων διατηρεί τα δεδομένα σε κεντρική τοποθεσία που μπορεί να δημιουργούν αντίγραφα ασφαλείας τακτικά. Επιτρέπει επίσης στους χρήστες και τις εφαρμογές να έχουν κεντρική πρόσβαση στα δεδομένα στο δίκτυο.	Χρησιμοποιείται για την αποθήκευση και τη διαχείριση των βάσεων δεδομένων που είναι αποθηκευμένες στο διακομιστή και για την παροχή πρόσβασης δεδομένων σε εξουσιοδοτημένους χρήστες.	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου
	A33	Database Server OS	Το λειτουργικό σύστημα του Database Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Κέντρο Ελέγχου
	A34	Database Server SW	Το λογισμικό που περιέχει ο Database Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Κέντρο Ελέγχου

	A35	I/O Server	Ο I/O Server μπορεί να βρίσκεται στον Control Server ή σε μία ξεχωριστή υπολογιστική πλατφόρμα.	Ο I/O Server είναι υπεύθυνος για την συλλογή και την παροχή πρόσβασης στην επεξεργασία δεδομένων από τα υποσυστήματα ελέγχου όπως είναι τα PLCs, τα RTUs και τα IEDs.	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου
	A36	I/O Server OS	Το λειτουργικό σύστημα του I/O Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Κέντρο Ελέγχου
	A37	I/O Server SW	Το λογισμικό που περιέχει ο I/O Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Κέντρο Ελέγχου
	A38	Data Historian Server	Μια κεντρική βάση δεδομένων η οποία περιέχει όλα τα αρχεία καταγραφής (logs) των διεργασιών ενός ICS και βρίσκεται στο LAN του συστήματος ελέγχου που υποστηρίζει την αρχειοθέτηση δεδομένων και την ανάλυση των δεδομένων χρησιμοποιώντας τεχνικές στατιστικής διαδικασίας ελέγχου.	Όλα τα αρχεία καταγραφής (logs) των διεργασιών ενός ICS μπορεί να χρησιμοποιηθούν σε ένα ευρύ φάσμα αναλύσεων από το επίπεδο των διεργασιών έως το επιχειρηματικό επίπεδο.	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου
	A39	Data Historian Server OS	Το λειτουργικό σύστημα του Data Historian Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Κέντρο Ελέγχου
	A40	Data Historian Server SW	Το λογισμικό που περιέχει ο Data Historian Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Κέντρο Ελέγχου

	A41	Domain Controller	Ο Domain Controller είναι ένας υπολογιστής διακομιστή που ανταποκρίνεται σε αιτήματα αυθεντικοποίησης ασφαλείας εντός ενός τομέα δικτύου υπολογιστή.	Είναι ένας διακομιστής δικτύου που είναι υπεύθυνος για την πρόσβαση του κεντρικού υπολογιστή στους πόρους ενός τομέα. Ελέγχει την ταυτότητα των χρηστών, αποθηκεύει πληροφορίες λογαριασμού χρήστη και επιβάλλει την πολιτική ασφαλείας για έναν τομέα.	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου
	A42	Domain Controller OS	Το λειτουργικό σύστημα του Domain Controller.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Κέντρο Ελέγχου
	A43	Domain Controller SW	Το λογισμικό που περιέχει ο Domain Controller.	_	Λογισμικό	Λογισμικό Διακομιστή	Κέντρο Ελέγχου
	A44	Engineering Workstations	Οι μηχανολογικοί σταθμοί εργασίας είναι αξιόπιστες πλατφόρμες υπολογιστών υψηλής τεχνολογίας, σχεδιασμένες για διαμόρφωση, συντήρηση και διάγνωση εφαρμογών συστήματος ελέγχου και άλλου εξοπλισμού.	Το σύστημα αποτελείται συνήθως από πολλούς σκληρούς δίσκους, διασύνδεση δικτύου υψηλής ταχύτητας, αξιόπιστες CPU, υλικό γραφικών επιδόσεων και εφαρμογές που παρέχουν εργαλεία διαμόρφωσης και παρακολούθησης για την εκτέλεση της ανάπτυξης των εφαρμογών του συστήματος ελέγχου, και τη συλλογή και τη διανομή των τροποποιήσεων του συστήματος.	Υλισμικό	Υπολογιστής	Κέντρο Ελέγχου

	A45	Engineering Workstations OS	Το λειτουργικό σύστημα των Engineering Workstations.	_	Λογισμικό	Λειτουργικό Σύστημα Υπολογιστή	Κέντρο Ελέγχου
	A46	Engineering Workstations SW	Λογισμικά που είναι εγκατεστημένα στους Μηχανολογικούς Σταθμούς Εργασίας.	_	Λογισμικό	Λογισμικό Υπολογιστή	Κέντρο Ελέγχου
	A47	Firewall	Μια συσκευή σε ένα δίκτυο επικοινωνιών που μπορεί να προγραμματιστεί για το φιλτράρισμα πληροφοριών βάσει του περιεχομένου των πληροφοριών, της πηγής ή του προορισμού.	Το Firewall προστατεύει ένα δίκτυο παρακολουθώντας και ελέγχοντας τα πακέτα επικοινωνίας, χρησιμοποιώντας προκαθορισμένες πολιτικές φιλτραρίσματος. Τα Firewalls χρησιμοποιούνται επίσης και για στρατηγικές διαχωρισμού σε ένα δίκτυο ICS.	Λογισμικό	Λογισμικό Δικτύου	Κέντρο Ελέγχου
Level 3.5 DMZ Zone	A48	Antivirus Server	Χρησιμοποιείται για τη διαχείριση, τον έλεγχο και την παρακολούθηση των διακομιστών που χρειάζονται προστασία.	Προστατεύει τα συστήματα από Ιούς, Worms, Trojans, Spyware και άλλους κινδύνους.	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου
	A49	Antivirus Server OS	Το λειτουργικό σύστημα του Antivirus Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Κέντρο Ελέγχου
	A50	Antivirus Server SW	Το λογισμικό που περιέχει ο Antivirus Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Κέντρο Ελέγχου
	A51	Patch Server	Διακομιστής που ελέγχει ένα πρόγραμμα ή ένα λειτουργικό σύστημα για την επιδιόρθωση ενός εκτεθειμένου ελαττώματος.	Διατηρεί τα συστήματα ενημερωμένα και ασφαλή με ενημερώσεις κώδικα και λογισμικού.	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου

	A52	Patch Server OS	Το λειτουργικό σύστημα του Patch Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Κέντρο Ελέγχου
	A53	Patch Server SW	Το λογισμικό που περιέχει ο Patch Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Κέντρο Ελέγχου
	A54	Application Server	Ο διακομιστής εφαρμογών είναι ένας διακομιστής που φιλοξενεί εφαρμογές.	Παρέχει δυνατότητες δημιουργίας web εφαρμογών και περιβάλλοντος διακομιστή για την εκτέλεση τους.	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου
	A55	Application Server OS	Το λειτουργικό σύστημα του Application Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Κέντρο Ελέγχου
	A56	Application Server SW	Το λογισμικό που περιέχει ο Application Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Κέντρο Ελέγχου
	A57	Data Historian Server Mirror	Επιπλέον προστασία του Data Historian Server μέσα από τη ζώνη DMZ.	_	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου
	A58	Remote Access Server	Ο διακομιστής απομακρυσμένης πρόσβασης είναι ένας τύπος διακομιστή που παρέχει διάφορες υπηρεσίες σε απομακρυσμένους συνδεδεμένους χρήστες μέσω δικτύου ή Διαδικτύου.	Λειτουργεί ως απομακρυσμένη πύλη ή κεντρικός διακομιστής που συνδέει απομακρυσμένους χρήστες με το εσωτερικό τοπικό δίκτυο (LAN) ενός οργανισμού.	Υλισμικό	Υπολογιστής Διακομιστή	Κέντρο Ελέγχου
	A59	Remote Access Server OS	Το λειτουργικό σύστημα του Remote Access Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Κέντρο Ελέγχου
	A60	Remote Access Server SW	Το λογισμικό που περιέχει ο Remote Access Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Κέντρο Ελέγχου

	A61	Firewall	Μια συσκευή σε ένα δίκτυο επικοινωνιών που μπορεί να προγραμματιστεί για το φιλτράρισμα πληροφοριών βάσει του περιεχομένου των πληροφοριών, της πηγής ή του προορισμού.	Το Firewall προστατεύει ένα δίκτυο παρακολουθώντας και ελέγχοντας τα πακέτα επικοινωνίας, χρησιμοποιώντας προκαθορισμένες πολιτικές φιλτραρίσματος. Τα Firewalls χρησιμοποιούνται επίσης και για στρατηγικές διαχωρισμού σε ένα δίκτυο ICS.	Λογισμικό	Λογισμικό Δικτύου	Κέντρο Ελέγχου
Level 4 - Site Business Planning and Logistics (Enterprise Zone)	A62	Corporate Web Server	Ο web server δέχεται αιτήματα μέσω του πρωτοκόλλου δικτύου HTTP ή μέσω της ασφαλής παραλλαγής του HTTPS, για τη διανομή ιστοσελίδων.	Διανομή ιστοσελίδων	Υλισμικό	Υπολογιστής Διακομιστή	Δωμάτιο Διακομιστών
	A63	Corporate Web Server OS	Το λειτουργικό σύστημα του Corporate Web Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Δωμάτιο Διακομιστών
	A64	Corporate Web Server SW	Το λογισμικό που περιέχει ο Corporate Web Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Δωμάτιο Διακομιστών
	A65	File Server	Ο διακομιστής αρχείων είναι ένας κεντρικός διακομιστής σε ένα δίκτυο υπολογιστών που παρέχει συστήματα αρχείων ή τουλάχιστον τμήματα ενός συστήματος αρχείων σε συνδεδεμένους χρήστες και πελάτες.	Προσφέρει στους χρήστες έναν κεντρικό χώρο αποθήκευσης για αρχεία σε εσωτερικά μέσα δεδομένων, τα οποία είναι προσβάσιμα σε όλους τους εξουσιοδοτημένους χρήστες και πελάτες.	Υλισμικό	Υπολογιστής Διακομιστή	Δωμάτιο Διακομιστών

	A66	File Server OS	Το λειτουργικό σύστημα του File Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Δωμάτιο Διακομιστών
	A67	File Server SW	Το λογισμικό που περιέχει ο File Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Δωμάτιο Διακομιστών
	A68	DNS Server	Ο DNS server είναι ένα ιεραρχικό σύστημα ονοματοδοσίας για δίκτυα υπολογιστών που χρησιμοποιούν το πρωτόκολλο IP.	Το σύστημα αυτό μπορεί και αντιστοιχίζει τα ονόματα των υπολογιστών υπηρεσίας σε αριθμητικές διευθύνσεις.	Υλισμικό	Υπολογιστής Διακομιστή	Δωμάτιο Διακομιστών
	A69	DNS Server OS	Το λειτουργικό σύστημα του DNS Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Δωμάτιο Διακομιστών
	A70	DNS Server SW	Το λογισμικό που περιέχει ο DNS Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Δωμάτιο Διακομιστών
	A71	AD Server	Το Active Directory (AD) είναι μια υπηρεσία καταλόγου που αναπτύχθηκε από τη Microsoft για δίκτυα των Windows domain. Περιλαμβάνεται στα περισσότερα λειτουργικά συστήματα Windows Server ως σύνολο διαδικασιών και υπηρεσιών.	Επαληθεύει και εξουσιοδοτεί όλους τους χρήστες και τους υπολογιστές σε ένα δίκτυο τύπου Windows domain.	Υλισμικό	Υπολογιστής Διακομιστή	Δωμάτιο Διακομιστών
	A72	AD Server OS	Το λειτουργικό σύστημα του AD Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Δωμάτιο Διακομιστών
	A73	AD Server SW	Το λογισμικό που περιέχει ο AD Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Δωμάτιο Διακομιστών
	A74	Corporate Workstations and Laptops	Υπολογιστές των υπαλλήλων ενός οργανισμού.	Εκτέλεση καθηκόντων.	Υλισμικό	Υπολογιστής	Κύρια Υποδομή Κτιρίου

	A75	Corporate Workstations and Laptops OS	Το λειτουργικό σύστημα των Workstations και των Laptops.	_	Λογισμικό	Λειτουργικό Σύστημα Υπολογιστή	Κύρια Υποδομή Κτιρίου
	A76	Corporate Workstations and Laptops SW	Το λογισμικό που περιέχουν τα Workstations και των Laptops.	_	Λογισμικό	Αυτόνομη Εφαρμογή	Κύρια Υποδομή Κτιρίου
	A77	Firewall	Μια συσκευή σε ένα δίκτυο επικοινωνιών που μπορεί να προγραμματιστεί για το φιλτράρισμα πληροφοριών βάσει του περιεχομένου των πληροφοριών, της πηγής ή του προορισμού.	Το Firewall προστατεύει ένα δίκτυο παρακολουθώντας και ελέγχοντας τα πακέτα επικοινωνίας, χρησιμοποιώντας προκαθορισμένες πολιτικές φιλτραρίσματος. Τα Firewalls χρησιμοποιούνται επίσης και για στρατηγικές διαχωρισμού σε ένα δίκτυο ICS.	Λογισμικό	Λογισμικό Δικτύου	Δωμάτιο Διακομιστών
Level 5 – Enterprise (Enterprise Zone)	A78	Web Server	Ο web server δέχεται αιτήματα μέσω του πρωτοκόλλου δικτύου HTTP ή μέσω της ασφαλής παραλλαγής του HTTPS, για τη διανομή ιστοσελίδων.	Διανομή ιστοσελίδων.	Υλισμικό	Υπολογιστής Διακομιστή	Δωμάτιο Διακομιστών
	A79	Web Server OS	Το λειτουργικό σύστημα του Web Server.	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Δωμάτιο Διακομιστών
	A80	Web Server SW	Το λογισμικό που περιέχει ο Web Server.	_	Λογισμικό	Λογισμικό Διακομιστή	Δωμάτιο Διακομιστών

	A81	Email Server	Διακομιστής για την ανταλλαγή email	Επικοινωνία μεταξύ των χρηστών	Υλισμικό	Υπολογιστής Διακομιστή	Δωμάτιο Διακομιστών
	A82	Email Server OS	Το λειτουργικό σύστημα του Email Server	_	Λογισμικό	Λειτουργικό Σύστημα Διακομιστή	Δωμάτιο Διακομιστών
	A83	Email Server SW	Το λογισμικό που περιέχει ο Email Server	_	Λογισμικό	Λογισμικό Διακομιστή	Δωμάτιο Διακομιστών
	A84	Smartphones, Tablets, Mobile Devices	Φορητές συσκευές που παρέχονται στους υπαλλήλους ενός οργανισμού	Επικοινωνία μεταξύ των χρηστών	Υλισμικό	Φορητή Συσκευή	Κύρια Υποδομή Κτιρίου
	A85	Modem	Συσκευή που επιτρέπει στους υπολογιστές να επικοινωνούν μέσω τηλεφωνικής γραμμής.	Επικοινωνία μεταξύ των υπολογιστών	Υλισμικό	Συσκευή Δικτύου	Δωμάτιο Διακομιστών
	A86	Routers, Access Points, Repeaters, etc.	Συσκευές επικοινωνίας μεταξύ των δικτύων	Ένας δρομολογητής που μεταφέρει μηνύματα μεταξύ δύο δικτύων.	Υλισμικό	Συσκευή Δικτύου	Δωμάτιο Διακομιστών

7.2.2 Εκτίμηση Επικινδυνότητας

7.2.2.1 Αποτίμηση Επιπτώσεων

Προκειμένου να υπολογιστεί η τιμή αποτίμησης τελικής επίπτωσης, κάθε στοιχείο αξιολογείται για την επίπτωση που προκαλείται λόγω παραβίασης μιας ιδιοκτησίας ασφαλείας (δηλαδή απώλεια διαθεσιμότητας ή / και ακεραιότητας ή / και εμπιστευτικότητας).
Τα σενάρια που εξετάζονται είναι τα εξής:

- Απώλεια διαθεσιμότητας
  - Μη διαθεσιμότητα <2 ώρες
  - Μη διαθεσιμότητα <8 ώρες
  - Μη διαθεσιμότητα <24 ώρες
  - Μη διαθεσιμότητα <1 εβδομάδα (5 εργάσιμες ημέρες)
  - Μη διαθεσιμότητα <10 εργάσιμες ημέρες
  - Μη διαθεσιμότητα <1 μήνα
- Απώλεια ακεραιότητας
  - Μερική απώλεια δεδομένων
  - Συνολική απώλεια δεδομένων (συμπεριλαμβανομένης της δημιουργίας αντιγράφων ασφαλείας)
  - Σκόπιμη τροποποίηση δεδομένων
  - Μη θελημένη αλλαγή δεδομένων
- Απώλεια εμπιστευτικότητας
  - Αποκάλυψη σε υπαλλήλους
  - Αποκάλυψη σε συνεργάτες
  - Αποκάλυψη σε εξωτερικούς

Τιμή αποτίμησης τελικής επίπτωσης

Η τελική τιμή επίπτωσης υπολογίζεται ως το μέγιστο (σενάριο χειρότερης περίπτωσης) από όλες τις τιμές επιπτώσεων για καθένα από τα σενάρια και τις αντίστοιχες συνέπειες. Η κλίμακα επιπτώσεων που χρησιμοποιείται για την αποτίμηση επιπτώσεων παρουσιάζεται στον Πίνακα 5.

Πίνακας 5: Κλίμακα Αποτίμησης Επιπτώσεων

Βαθμός Επίπτωσης	Επίπεδο Επίπτωσης	Περιγραφή
4	Πολύ Υψηλό (ΠΥ)	Η απώλεια διαθεσιμότητας των συστημάτων ICS θα είχε αρνητική και καταστροφική επίπτωση μεγάλης κλίμακας (π.χ. διακοπή ρεύματος σε πόλη > 1.000.000 πληθυσμό) Η τροποποίηση δεδομένων θα είχε καταστροφικό αποτέλεσμα για το ενεργειακό πάρκο.
3	Υψηλό (Υ)	Η απώλεια διαθεσιμότητας των συστημάτων ICS θα είχε σημαντική επίπτωση μεγάλης κλίμακας. Η τροποποίηση δεδομένων θα είχε αρνητικό αποτέλεσμα για το ενεργειακό πάρκο.
2	Μέτριο (Μ)	Η απώλεια διαθεσιμότητας των συστημάτων ICS θα είχε επίπτωση μέτριας κλίμακας. Η αποκάλυψη και τροποποίηση δεδομένων θα είχε αρνητικό

		αποτέλεσμα για το ενεργειακό πάρκο χωρίς να είναι ανεπανόρθωτη η ζημιά.
1	Χαμηλό (Χ)	Η απώλεια διαθεσιμότητας των συστημάτων ICS θα είχε επίπτωση χαμηλής κλίμακας. Η αποκάυψη και τροποποίηση δεδομένων δεν θα είχε αρνητικό αποτέλεσμα για το ενεργειακό πάρκο με αποτέλεσμα να μην επηρεαστεί.
0	Πολύ Χαμηλό (ΠΧ)	Η απώλεια διαθεσιμότητας των συστημάτων ICS δεν θα είχε επίπτωση στο ενεργειακό πάρκο. Η αποκάυψη και τροποποίηση δεδομένων θα ήταν ασήμαντη.

7.2.2.2 Εκτίμηση Πιθανότητας

Στη συνέχεια, η πιθανότητα υπολογίζεται ως ο συνδυασμός του επιπέδου απειλής και του επιπέδου ευπάθειας.

Στον Πίνακα 6 παρουσιάζεται η Κλίμακα Αποτίμησης Απειλής.

Πίνακας 6: Κλίμακα Αποτίμησης Απειλής

Τιμή Απειλής	Επίπεδο Απειλής	Περιγραφή
0	Χαμηλό	Αυτό το επίπεδο απειλής δίνεται σε απειλές που η πιθανότητα εμφάνισής της είναι έως 1 φορά στα 10 χρόνια.
1	Μεσαίο	Αυτό το επίπεδο απειλής δίνεται σε απειλές που η πιθανότητα εμφάνισής της είναι από 1 έως 2 φορές στα 5 χρόνια.
2	Υψηλό	Αυτό το επίπεδο απειλής δίνεται σε απειλές που η πιθανότητα εμφάνισής της είναι πάνω από 3 φορές στα 2 χρόνια.

Στον Πίνακα 7 παρουσιάζεται η Κλίμακα Αποτίμησης Ευπάθειας.

Πίνακας 7: Κλίμακα Αποτίμησης Ευπάθειας

Τιμή Ευπάθειας	Επίπεδο Ευπάθειας	Περιγραφή
0	Χαμηλό	Η επίπτωση είναι χαμηλή και το επίπεδο ευπάθειας είναι χαμηλό Η αδυναμία είναι γνωστή στη διεθνή κοινότητα και απαιτεί εξειδικευμενες τεχνικές γνώσεις εκμετάλλευσής της ή μπορεί να γίνει ανιχνεύσιμη μονο από το εσωτερικό δίκτυο.
1	Μεσαίο	Η επίπτωση είναι μεσαία και το επίπεδο ευπάθειας είναι μεσαίο. Η αδυναμία είναι γνωστή στη διεθνή κοινότητα και απαιτεί προηγμένες τεχνικές γνώσεις εκμετάλλευσής της.

2	Υψηλό	Η επίπτωση είναι υψηλή και το επίπεδο ευπάθειας είναι υψηλό. Η αδυναμία είναι πολύ γνωστή στη διεθνή κοινότητα και απαιτεί ελάχιστη τεχνική γνώση εκμετάλλευσής της.

Προκειμένου να προσδιοριστεί το επίπεδο ευπάθειας κάθε αγαθού έναντι των εξεταζόμενων απειλών, λαμβάνονται υπόψη οι υπάρχοντες έλεγχοι και το επίπεδο αποκαλύπτεται από την κλίμακα αποτίμησης της ευπάθειας της μεθοδολογίας (Πίνακας 7). Μετά τη συλλογή όλων των κατάλληλων τιμών για την επίπτωση, την απειλή και την ευπάθεια, η τιμή επικινδυνότητας υπολογίζεται για κάθε συνδυασμό Αγαθού-Απειλής-Ευπάθειας ως προϊόν:

Πιθανότητα = Τιμή Απειλής + Τιμή Ευπάθειας
Τιμή Επικινδυνότητας (R) = Τιμή Επίπτωσης + Πιθανότητα

Όλες οι πιθανές τιμές κινδύνου φαίνονται στον Πίνακα 8.

Πίνακας 8: Πίνακας Επικινδυνότητας

Τιμή Πιθανότητας		0	1	2	3	4
Επίπεδο Πιθανότητας		Πολύ Απίθανο	Απίθανο	Πιθανό	Πολύ Πιθανό	Συχνά
Ασήμαντη Επίπτωση	0	0	1	2	3	4
Χαμηλή Επίπτωση	1	1	2	3	4	5
Μεσαία Επίπτωση	2	2	3	4	5	6
Σημαντική Επίπτωση	3	3	4	5	6	7
Καταστροφική Επίπτωση	4	4	5	6	7	8

7.2.3 Αξιολόγηση Επικινδυνότητας

Σε αυτό το βήμα οι Τιμές Επικινδυνότητας αποκαλύπτουν το Επίπεδο Επικινδυνότητας με τη χρήση της Κλίμακας Επικινδυνότητας (Πίνακας 9) και όλα τα πιθανά αποτελέσματα εμφανίζονται στον Πίνακα Αξιολόγησης Επικινδυνότητας (Πίνακας 10).

Πίνακας 9: Κλίμακα Επικινδυνότητας

Επίπεδο Επικινδυνότητας	Περιγραφή
Χαμηλό	$0 \leq R < 3$
Μεσαίο	$3 \leq R < 6$
Υψηλό	$6 \leq R \leq 8$

Πίνακας 10: Αξιολόγηση Επικινδυνότητας

Τιμή Πιθανότητας		0	1	2	3	4
Επίπεδο Πιθανότητας		Πολύ Απίθανο	Απίθανο	Πιθανό	Πολύ Πιθανό	Συχνά
Ασήμαντη Επίπτωση	0	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ
Χαμηλή Επίπτωση	1	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ
Μεσαία Επίπτωση	2	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ
Σημαντική Επίπτωση	3	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΥΨΗΛΟ
Καταστροφική Επίπτωση	4	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ

7.2.4 Μετριασμός Επικινδυνότητας

Σε αυτήν τη φάση προτείνονται τα κατάλληλα μέτρα προστασίας για την αντιμετώπιση των εντοπισμένων κινδύνων. Για κάθε αγαθό και για κάθε συνδυασμό αγαθού-απειλής-ευπάθειας, ο εξουσιοδοτημένος χρήστης μπορεί να επιλέξει την κατάλληλη στρατηγική (μείωση, αποδοχή, μεταφορά, αποφυγή) και να συμπληρώσει τις απαραίτητες πληροφορίες σχετικά με το σχέδιο αντιμετώπισης κινδύνων.

- Δράση μετριασμού (στρατηγική): επιλέξτε την κατάλληλη στρατηγική για κάθε προσδιορισμένο κίνδυνο:
  - Μείωση
  - Αποδοχή
  - Μεταφορά
  - Αποφυγή
- Χρόνος υλοποίησης
  - Άμεσα
  - Εντός των επόμενων 6 μηνών
  - Εντός ενός έτους
- Υπεύθυνος για την υλοποίηση
  - Καθορισμός αρμόδιου υπαλλήλου για την υλοποίηση της στρατηγικής

7.3 Αποτελέσματα Αποτίμησης Επικινδυνότητας

Στο κεφάλαιο αυτό παρουσιάζονται αναλυτικά τα αποτελέσματα από την αποτίμηση της επικινδυνότητας, για την αντιμετώπιση των ευπαθειών στα συστήματα ICS αλλά και την επιτυχή πρόληψη επιθέσεων. Οι απειλές , οι ευπάθειες και τα προτεινόμενα μέτρα έχουν συγκεντρωθεί από ευρέως διαδεδομένα και χρησιμοποιούμενα οργανωτικά και τεχνικά πρότυπα ασφαλείας από διάφορους οργανισμούς παγκοσμίως, που βοηθούν τους υπεύθυνους ασφαλείας να λαμβάνουν τα κατάλληλα μέτρα προστασίας. Πιο συγκεκριμένα, έχουν χρησιμοποιηθεί πρότυπα ασφαλείας που έχουν εκπονηθεί από τον NIST [10], [31], τον NERC [7], τον ENISA [26], το U.S. Department of Homeland Security [32], αλλά και η μεθοδολογία αποτίμησης επικινδυνότητας STORM-RM [30],[31].

Αποτίμηση Επικινδυνότητας σε Συστήματα ICS								**Διαχείριση Κινδύνου**		
Αποτίμηση Απειλών		**Αποτίμηση Ευπαθειών**	**Επηρεαζόμενα Αγαθά**	**Επίπεδο Επίπτωσης**	**Επίπεδο Απειλής**	**Επίπεδο Ευπάθειας**	**Επίπεδο Επικινδυνότητας**	**Μέτρα Προστασίας**	**Ομάδες Μέτρων από Διεθνή Πρότυπα**	
Απειλή	**Περιγραφή**	**Ευπάθεια**	**Αγαθά ICS**					**Προτεινόμενο Μέτρο**	**NIST 800-53**	**NERC-CIP**
Περιβαλλοντική καταστροφή στο Κέντρο ελέγχου: - Φυσική ή ανθρωπογενής καταστροφή - Φωτιά - Πλημμύρα / Τσουνάμι - Καταιγίδα / ανεμοστρόβιλος - Τυφώνας - Σεισμός - Αποτυχία / διακοπή υποδομής	Φυσικές καταστροφές και αποτυχίες κρίσιμων υποδομών στις οποίες εξαρτάται ο οργανισμός, αλλά που βρίσκονται εκτός του ελέγχου του οργανισμού.	**Οι κτιριακές υποδομές δεν παρέχουν προστασία σε περίπτωση επίθεσης με φυσικά μέσα (αναγκαστική επίθεση)**	Primary Control Center, Backup Control Center, Control Room	ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Εγκατάσταση 24ωρων συστημάτων ανίχνευσης εισβολής για τον εντοπισμό εξωτερικών και εσωτερικών παραβιάσεων φυσικής ασφάλειας. Αυτό πρέπει να συνδεθεί με αριθμούς κινητών τηλεφώνων για την αποστολή ειδοποιήσεων σε εξουσιοδοτημένο προσωπικό όποτε εντοπίζεται κάποιο περιστατικό. Αυτό θα βοηθήσει στην προστασία της υποδομής των ICS από φυσικές επιθέσεις και βανδαλισμούς. Παραδείγματα περιλαμβάνουν συστήματα ανίχνευσης εισβολής όπως περιμετρική περίφραξη και συναγερμοί, φράχτες, πόρτες, αισθητήρες ανίχνευσης κίνησης, ανιχνευτές σημείου πρόσβασης, κάμερες CCTV κ.λπ.	PE-1 Physical and Environmental Protection Policy and Procedures, PE-2 Physical Access Authorizations, PE-3 Physical Access Control, PE-6	CIP 004-6 (R4, R5), CIP 006-6 (R1, R2, R3), CIP 014-2 (R5)

- Τηλεπικοι-νωνίες - Ηλεκτρική ισχύς		**Οι πόρτες δεν είναι ανθεκτικές στην επίθεση / δεν προστατεύο-νται**		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Οι πόρτες πρέπει να είναι ανθεκτικές σε φυσικές καταστροφές.	Monito-ring Physical Access, PE-8 Visitor Access Records, PE-9 Power Equip-ment and Cabling	
		Ανεπαρκής παρακολούθη-ση των εγκαταστάσεων της κρίσιμης υποδομής		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Πρέπει να υπάρχουν κατάλληλοι έλεγχοι για την παρακολούθηση των εγκαταστάσεων της κρίσιμης υποδομής (π.χ. CCTV, σύστημα ελέγχου πρόσβασης)		
		Ανεπαρκής φωτισμός της ασφαλούς περιμέτρου		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Ο φωτισμός πρέπει να είναι τοποθετημένος σε όλη την έκταση της ασφαλούς περιμέτρου.		
		Δεν υπάρχει σαφώς καθορισμένη ασφαλής περίμετρος κτιρίων / περιοχών που φιλοξενούν συστήματα ICS		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Η ασφαλής περίμετρος των κτιρίων και των περιοχών που φιλοξενούν κρίσιμες υποδομές ICS θα πρέπει να οριστεί, να είναι σαφώς καθορισμένη και να παρακολουθείται επαρκώς.		
		Έλλειψη ευαισθητοποί-ησης και εκπαιδευτικού προγράμματος σχετικά με τη φυσική ασφάλεια		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Πρέπει να εφαρμόζονται αποτελεσματικά προγράμματα ευαισθητοποίησης και κατάρτισης σχετικά με τη φυσική ασφάλεια για όλους τους υπαλλήλους.		

Περιβαλλοντική καταστροφή σε κρίσιμο εξοπλισμό και συστήματα ICS: **- Φυσική ή ανθρωπογενής καταστροφή** **- Φωτιά** **- Πλημμύρα / Τσουνάμι** **- Καταιγίδα / ανεμοστρόβιλος** **- Τυφώνας** **- Σεισμός** **- Αποτυχία / διακοπή υποδομής** **-Τηλεπικοινωνίες** **- Ηλεκτρική ισχύς**	Φυσικές καταστροφές και αποτυχίες κρίσιμων υποδομών στις οποίες ο οργανισμός εξαρτάται, αλλά που βρίσκονται εκτός του ελέγχου του οργανισμού.	**Χωρίς ειδικό σχέδιο έκτακτης ανάγκης για ICS**	PLC, RTU, DCS, Local SCADA Server-MTU, Sensors, Transmitters, Actuators, Valves, Motors	ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Πρέπει να ετοιμαστεί ένα σχέδιο έκτακτης ανάγκης, να δοκιμαστεί και να είναι διαθέσιμο σε περίπτωση σοβαρής αποτυχίας υλισμικού, λογισμικού ή καταστροφής των εγκαταστάσεων. Η έλλειψη σχεδίου έκτακτης ανάγκης για συστήματα ICS θα μπορούσε να οδηγήσει σε παρατεταμένους χρόνους διακοπής λειτουργίας και απώλεια παραγωγής.	PE-1 Physical and Environmental Protection Policy and Procedures, PE-2 Physical Access Authorizations, PE-3 Physical Access Control, PE-6 Monitoring Physical Access, PE-8 Visitor Access Records, PE-9 Power Equipment and Cabling	CIP 004-6 (R4, R5), CIP 006-6 (R1, R2, R3), CIP 014-2 (R5)
		Έλλειψη επαρκούς πολιτικής ελέγχου πρόσβασης		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Η επιβολή ελέγχου πρόσβασης εξαρτάται από την πολιτική που διαμορφώνει σωστά τους ρόλους, τις ευθύνες και τις εξουσιοδοτήσεις.		
		Ανεπαρκής πολιτική ασφάλειας για συστήματα ICS		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Κάθε αντίμετρο πρέπει να είναι ανιχνεύσιμο σε μια πολιτική. Αυτό εξασφαλίζει ομοιομορφία και υπευθυνότητα. Η πολιτική πρέπει να περιλαμβάνει φορητές και κινητές συσκευές που χρησιμοποιούνται σε συστήματα ICS.		
		Απουσία ή ανεπαρκής οδηγίες εφαρμογής του εξοπλισμού των συστημάτων ICS		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Οι οδηγίες εφαρμογής του εξοπλισμού των ICS πρέπει να είναι ενημερωμένες και άμεσα διαθέσιμες. Αυτές οι οδηγίες αποτελούν αναπόσπαστο μέρος των διαδικασιών ασφαλείας σε περίπτωση δυσλειτουργίας των συστημάτων ICS.		
		Μη εξουσιοδοτημένο προσωπικό έχει φυσική		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Πρέπει να εφαρμόζονται πολιτικές και διαδικασίες σχετικά με την πρόσβαση στον εξοπλισμό και στις κρίσιμες υποδομές.		

		πρόσβαση σε εξοπλισμό								
		Ραδιοσυχνότητα, ηλεκτρομαγνητικός παλμός (Electromagnetic Pulse - EMP), στατική εκφόρτιση και αιχμές τάσης		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Συνιστάται η σωστή θωράκιση, γείωση και η ρύθμιση ισχύος.		
		Έλλειψη εφεδρικής ισχύος		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Πρέπει να υπάρχει εφεδρική ισχύς για όλα τα κρίσιμα αγαθά.		
		Απώλεια περιβαλλοντικού ελέγχου		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Πρέπει να υπάρχει σωστός περιβαλλοντικός έλεγχος για την αποφυγή ζημιών στον εξοπλισμό.		
		Μη ασφαλείς φυσικές θύρες		ΠΟΛΥ ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Οι θύρες USB και PS/2 πρέπει να ασφαλίζονται σωστά.		
Τρομοκρατική Επίθεση	Μια τρομοκρατική επίθεση μπορεί να προκαλέσει μεγάλη οικονομική καταστροφή στις εγκαταστάσεις ενός	**Δεν υπάρχει προστασία για την κύρια υποδομή**	Primary Control Center, Backup Control Center, Control Room	ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗΛΟ	ΥΨΗΛΟ	Η υποδομή του κτιρίου πρέπει να παρέχει προστασία σε περίπτωση επίθεσης με φυσικά μέσα (αναγκαστική επίθεση).	PE-1 Physical and Environmental Protection Policy and Proce-	CIP 004-6 (R4, R5), CIP 006-6 (R1, R2, R3), CIP 014-2 (R5)
		Οι πόρτες δεν είναι ανθεκτικές στην επίθεση / δεν προστατεύονται		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗΛΟ	ΥΨΗΛΟ	Οι πόρτες πρέπει να είναι ανθεκτικές σε τέτοιου είδους επιθέσεις.		

	ενεργειακού πάρκου που βρίσκεται το Κέντρο ελέγχου των συστημάτων ICS.	**Έλλειψη ελέγχων για παρακολούθη-ση**		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΥΨΗΛΟ	Πρέπει να υπάρχουν κατάλληλοι έλεγχοι για την παρακολούθηση των εγκαταστάσεων του οργανισμού (π.χ. CCTV, σύστημα ελέγχου πρόσβασης, βιβλίο καταγραφής επισκεπτών).	dures, PE-2 Physical Access Authori-zations, PE-3 Physical Access Control, PE-6 Monito-ring Physical Access, PE-8 Visitor Access Records, PE-9 Power Equip-ment and Cabling, CM-1	
		Δεν υπάρχει περίμετρος ασφαλείας		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΥΨΗΛΟ	Η περίμετρος ασφαλείας πρέπει να είναι επαρκώς φωτισμένη.		
		Οι θέσεις στάθμευσης βρίσκονται εντός της ασφαλούς περιμέτρου		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΥΨΗΛΟ	Οι θέσεις στάθμευσης πρέπει να βρίσκονται έξω από την ασφαλή περίμετρο.		
		Οι περιοχές παράδοσης και φόρτωσης βρίσκονται στην ίδια τοποθεσία		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΥΨΗΛΟ	Τα σημεία πρόσβασης, όπως οι περιοχές παράδοσης και φόρτωσης και άλλα σημεία όπου μπορούν να εισέλθουν μη εξουσιοδοτημένα άτομα στις εγκαταστάσεις, πρέπει να ελέγχονται και, εάν είναι δυνατόν, να απομονώνονται από εγκαταστάσεις επεξεργασίας πληροφοριών για την αποφυγή μη εξουσιοδοτημένης πρόσβασης.		
		Έλλειψη διαδικασιών διαχείρισης αλλαγών		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΥΨΗΛΟ	Πρέπει να υπάρχουν διαδικασίες διαχείρισης αλλαγών και να καταγράφεται οποιαδήποτε αλλαγή στην υποδομή.		
		Έλλειψη πολιτικών και διαδικασιών φυσικής πρόσβασης		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΥΨΗΛΟ	Πρέπει να εφαρμόζονται πολιτικές και διαδικασίες σχετικά με την πρόσβαση στις υποδομές.		

Εσωτερική απειλή από υπάλληλο	Ένας υπάλληλος ή εξωτερικός συνεργάτης που έχει πρόσβαση σε περιορισμένα εσωτερικά συστήματα χρησιμοποιεί αυτό το πλεονέκτημα για κλοπή, τροποποίηση ή πρόσβαση χωρίς άδεια σε αυτά τα συστήματα ή σε άλλα που είναι προσβάσιμα μέσω αυτών.	**Η αυθεντικοποίηση χρηστών, δεδομένων ή συσκευών είναι ελάχιστη ή ανύπαρκτη**	PLC, RTU, DCS, Local SCADA Server-MTU, Local HMI-Central HMI, Sensors, Transmitters, Actuators, Valves, Motors, Data Historian Server	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Πρέπει να υπάρχουν μέθοδοι αυθεντικοποίησης (πολυπλοκότητα κωδικού πρόσβασης, κρυπτογράφηση, έλεγχοι πρόσβασης, έξυπνες κάρτες).	IA-2 Identification and Authentication (Organizational Users), IA-3 Authenticator Management, AC-1 Access Control Policy and Procedures, AC-2 Account Management, AC-3 Access Enforcement	CIP-004-6 (R3, R4, R5), CIP 005-6 (R2), CIP 007-6 (R5)
Μη εξουσιοδοτημένη πρόσβαση	Ένας υπάλληλος ή εξωτερικός συνεργάτης που έχει πρόσβαση σε περιορισμένα εσωτερικά συστήματα χρησιμοποιεί αυτό το	**Υπάρχουν γραπτές σημειώσεις που παρέχουν κωδικούς πρόσβασης**	PLC, RTU, DCS, Local SCADA Server-MTU, Local HMI, Central HMI Sensors, Transmitters, Actuators,	ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Δεν πρέπει να υπάρχουν γραπτές σημειώσεις με κωδικούς πρόσβασης. Οι κωδικοί πρόσβασης πρέπει να είναι κρυπτογραφημένοι.	AC-2 Account Management, AC-3 Access Enforcement, AC-7 Unsuccessful Login Attempts,	CIP 004-6 (R4, R5), CIP 005-6 (R2), CIP 007-6 (R5), CIP 010-3 (R3)
		Υπάρχει ελεύθερη πρόσβαση στο σύστημα		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Η πρόσβαση στο σύστημα πρέπει να απαιτεί κωδικό ασφαλείας ή / και έξυπνη κάρτα ή / και βιομετρικό έλεγχο.		

	πλεονέκτημα για κλοπή, τροποποίηση ή πρόσβαση χωρίς άδεια σε αυτά τα συστήματα ή σε άλλα που είναι προσβάσιμα μέσω αυτών.	**Δεν υπάρχει πολιτική κωδικού πρόσβασης**	Valves, Motors, Data Historian Server	ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Πρέπει να υπάρχει κατάλληλη πολιτική κωδικών πρόσβασης και να την εφαρμόζουν όλοι οι χρήστες.	AC-12 Session Termination, AC-17 Remote Access, IA-2 Identification and Authentication (Organizational Users), RA-5 Vulnerability Monitoring and Scanning	
		Δεν υπάρχει πολυπλοκότητα κωδικού πρόσβασης		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Η πολυπλοκότητα των κωδικών πρόσβασης (π.χ. χρήση τουλάχιστον ενός ειδικού χαρακτήρα, ενός αριθμού, ενός κεφαλαίου κ.λπ.) πρέπει να ενεργοποιείται στην πολιτική κωδικών πρόσβασης. Ο κωδικός πρόσβασης με μήκος μικρότερο από 8 χαρακτήρες πρέπει να απορρίπτεται από την πολιτική.		
		Υπάρχουν κοινόχρηστοι / ομαδοποιημένοι λογαριασμοί		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Οι ομαδοποιημένοι και οι κοινόχρηστοι κωδικοί πρόσβασης δεν πρέπει να επιτρέπονται από την πολιτική.		
		Το προσωπικό έχει απομακρυσμένη πρόσβαση στα συστήματα ICS - Ελλιπής έλεγχοι απομακρυσμένης πρόσβασης		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Οι δυνατότητες απομακρυσμένης πρόσβασης δεν θα πρέπει να επιτρέπονται ή θα πρέπει να ελέγχονται επαρκώς για να αποτρέπεται η πρόσβαση μη εξουσιοδοτημένων ατόμων στα συστήματα ICS.		
		Έλλειψη πολιτικής αποσύνδεσης από λογαριασμούς		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Η πολιτική αποσύνδεσης (π.χ. μετά από 10 λεπτά αδράνειας) πρέπει να ενεργοποιείται και να εφαρμόζεται σε όλους τους σταθμούς εργασίας.		
		Τα αρχεία καταγραφής ελέγχου δεν εκτελούνται σε		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Τα αρχεία καταγραφής ελέγχου πρέπει να παρακολουθούνται και να ελέγχονται σε τακτά χρονικά διαστήματα.		

		τακτά χρονικά διαστήματα								
		Η τεχνική αξιολόγησης ευπαθειών δεν πραγματοποιεί-ται σε τακτά χρονικά διαστήματα		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Οι τεχνικές αξιολογήσεις ευπαθειών πρέπει να διενεργούνται σε τακτά χρονικά διαστήματα (τουλάχιστον μία φορά το χρόνο εξαρτώντας από την κρισιμότητα του συστήματος).		
		Ο έλεγχος πρόσβασης δεν πραγματοποιεί-ται σε τακτά χρονικά διαστήματα προκειμένου να διασφαλιστεί ότι τηρείται πάντα η αρχή "ανάγκης γνώσης"		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Η αρχή "ανάγκης γνώσης" πρέπει να λαμβάνεται υπόψη κατά την εφαρμογή της πολιτικής ελέγχου πρόσβασης.		
Μη έγκαιρη ανάκτηση βιομηχανικών συστημάτων ελέγχου ICS	Η μη έγκαιρη ανάκτηση των ICS μπορεί να προκαλέσει ανεπανόρθωτη ζημιά στα συστήματα και να έχει σοβαρές οικονομικές επιπτώσεις στον οργανισμό.	**Έλλειψη Σχεδίου Ανάκτησης Καταστροφών (DRP)**	PLC, RTU, DCS, Local SCADA Server-MTU, Local HMI, Central HMI, Data Historian Server	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Ένα Σχέδιο Ανάκτησης Καταστροφών πρέπει να είναι σε ισχύ με όλες τις κατάλληλες διαδικασίες αποκατάστασης.	CP-1 Contin-gency Planning Policy and Proce-dures, CP-2 Contin-gency Plan, CP-3 Contin-	CIP-004-6 (R2), CIP 009-6 (R1, R2, R3), CIP 008-6 (R1, R2, R3)
		Το DRP δεν ελέγχεται ποτέ		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Το Σχέδιο Ανάκτησης Καταστροφών πρέπει να ελέγχεται σε τακτά χρονικά διαστήματα (τουλάχιστον μία φορά το χρόνο).		
		Δεν υπάρχουν επαφές έκτακτης ανάγκης		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Πρέπει να είναι διαθέσιμη σε όλους τους υπαλλήλους μια λίστα επαφών έκτακτης ανάγκης (π.χ. τηλέφωνα αστυνομίας, τηλέφωνα		

								νοσοκομείου, τηλέφωνα πυροσβεστικής).	gency Training, CP-4 Contin-gency Plan Testing, CP-9 System Backup, CP-10 System Recovery and Reconsti-tution, IR-1 Incident Response Policy and Proce-dures	
		Έλλειψη διαχειριστικών ευθυνών		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Οι ευθύνες και οι διαδικασίες διαχείρισης πρέπει να καθορίζονται για να διασφαλίζεται η γρήγορη, αποτελεσματική και ομαλή ανταπόκριση σε περιστατικά ασφάλειας πληροφοριών.		
		Δεν υπάρχει διαδικασία απόκρισης περιστατικών ασφαλείας πληροφοριών		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Τα περιστατικά ασφάλειας πληροφοριών αποκρίνονται σύμφωνα με τις τεκμηριωμένες διαδικασίες.		
		Δεν υπάρχει τεκμηρίωση για αδυναμίες του συστήματος		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Οι εργαζόμενοι και οι εργολάβοι που χρησιμοποιούν τα συστήματα ICS και τις υπηρεσίες πληροφοριών του οργανισμού πρέπει να σημειώνουν και να αναφέρουν τυχόν παρατηρούμενες ή ύποπτες αδυναμίες ασφάλειας πληροφοριών σε συστήματα ή υπηρεσίες ICS.		
Άρνηση Ενέργειας Ελέγχου (Denial of Control Action)	Η λειτουργία των συστημάτων ελέγχου διακόπτεται καθυστερώντας ή παρεμποδίζο-ντας τη ροή πληροφοριών, αρνούμενη έτσι τη	**Το προσωπικό δεν έχει εμπειρία στον κυβερνοχώρο σε θέματα σχετικά με την ασφάλεια**	PLC, RTU, DCS, Local SCADA Server-MTU, IED, Local HMI, Central HMI	ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Πρέπει να υπάρχουν πολιτικές και προγράμματα κατάρτισης σχετικά με θέματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο και τις κρίσιμες υποδομές.	At-1 Security Aware-ness and Training Policy and Proce-dures, AC-17 Remote	CIP 003-8 (R2, R4), CIP 004-6 (R1, R2), CIP 005-6 (R2)
		Έλλειψη γνώσεων		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Θα πρέπει να διασφαλιστεί η μεταφορά γνώσεων σχετικά με τη		

	διαθεσιμότητα των δικτύων για τον έλεγχο των διαχειριστών συστημάτων ή προκαλώντας σημεία συμφόρησης μεταφοράς ή άρνηση υπηρεσίας από υπηρεσίες IT (όπως DNS).	**σχετικά με τις συσκευές**						λειτουργία και τη συντήρηση των παλιών συσκευών.	Access, AC-18 Wireless Access, CA-6 Authori-zation	
		Ύπαρξη ασύρματων συνδέσεων		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Συνιστάται ενισχυμένη ασφάλεια για τα συστήματα σε αποστρατικοποιημένες ζώνες (DMZs) καθώς και για το εσωτερικό δίκτυο.		
		Επίβλεψη απομακρυσμέ-νης πρόσβασης		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Εκτός από εργαλεία ακεραιότητας διακομιστών, η ασφάλεια χρειάζεται ενίσχυση, χρησιμοποιώντας εικονικά ιδιωτικά δίκτυα (VPN).		
		Μη εξουσιοδοτημέ-νες δικτυακές συνδέσεις PLC / RTU		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Θα πρέπει να παρέχονται από τους προμηθευτές μέτρα ασφαλείας με τη μορφή ενημερώσεων κώδικα και αναβαθμίσεων για συστήματα SCADA προκειμένου να προστατεύονται οι μη εξουσιοδοτημένες συνδέσεις δικτύου PLC / RTU.		
Επιθέσεις Άρνησης Υπηρεσίας (Denial of Service)	Αυτή η επίθεση αποτελείται από πολλαπλά συστήματα που “επιτίθενται” σε έναν μόνο στόχο για να τον κάνουν να κορεστεί και να τον κάνουν να καταρρεύσει. Αυτό μπορεί να γίνει απλά	**Δεν έχει εγκατασταθεί το λογισμικό των Συστημάτων Ανίχνευσης /Πρόληψης Εισβολής (IDS/IPS)**	RTU, Local SCADA Server-MTU, Local HMI, Central HMI	ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Το λογισμικό των IDS / IPS πρέπει να δοκιμάζεται πριν από την ανάπτυξη για να διαπιστωθεί ότι δεν θέτει σε κίνδυνο την κανονική λειτουργία των συστημάτων ICS.	CM-7 Least Functio-nality, IR-1 Incident Response Policy and Proce-dures, SC-5 Denial-of-Service Protec-	CIP 008-6 (R1, R2, R3), CIP 005-6 (R1), CIP 007-6 (R1, R4)
		Δεν υπάρχει διαδικασία παρακολούθη-σης δικτύου		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Η κυκλοφορία του δικτύου πρέπει να παρακολουθείται επαρκώς.		

	προσπαθώντας να κάνει πάρα πολλές συνδέσεις, να κάνει flooding ενός καναλιού επικοινωνίας ή να επαναλαμβάνει τις ίδιες επικοινωνίες ξανά και ξανά. Έχει μεγάλη σημασία εάν οι συσκευές SCADA επηρεάζονται από αυτήν την επίθεση και η οποία ενδέχεται να προκαλέσει παύση λειτουργιών.	**Έλλειψη διαδικασίας απόκρισης περιστατικών**		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Τα περιστατικά ασφάλειας πληροφοριών αποκρίνονται σύμφωνα με τις τεκμηριωμένες διαδικασίες.	tion, SI-4 System Monito-ring	
		Δεν υπάρχει συγκεκριμένη διαδικασία για επιθέσεις DoS		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Πρέπει να υπάρχει μια προπληρωμένη υπηρεσία ISP για ειδοποίηση επίθεσης DoS.		
		Το σύστημα δεν αξιολογήθηκε ποτέ		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Θα πρέπει να πραγματοποιούνται τακτικοί έλεγχοι για τον εντοπισμό ανεπιθύμητων υπηρεσιών ή ανοιχτών θυρών.		
Κακόβουλο λογισμικό (Virus, Trojan, Worm)	Προγράμματα λογισμικού που έχουν σχεδιαστεί για την εκτέλεση ανεπιθύμητων και μη εξουσιοδοτημέ-νων ενεργειών σε ένα σύστημα χωρίς τη συγκατάθεση του χρήστη, με	**Η προστασία από κακόβουλο λογισμικό δεν έχει εγκατασταθεί ή δεν είναι ενημερωμένη**	PLC, RTU, DCS, Local SCADA Server-MTU, Local HMI, Central HMI, Data Historian Server, Engineering Workstations,	ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Το λογισμικό προστασίας από κακόβουλα προγράμματα, όπως το λογισμικό προστασίας από ιούς, πρέπει να διατηρείται ενημερωμένο σε ένα πολύ δυναμικό περιβάλλον.	SI-3 Malicious Code Protec-tion	CIP 007-6 (R3)

	αποτέλεσμα ζημιά, καταστροφή ή κλοπή πληροφοριών. Οι συνέπειες μπορεί να είναι σοβαρές. Έχει παρατηρηθεί ότι το κακόβουλο λογισμικό μπορεί να είναι κοινό ή προσαρμοσμέ-νο. Αυτός ο τύπος επιθέσεων, επηρεάζει ένα ευρύ φάσμα περιουσιακών στοιχείων, από συστήματα SCADA έως τυποποιημένα συστήματα.	**Η προστασία από κακόβουλο λογισμικό εφαρμόστηκε χωρίς επαρκή έλεγχο**	Application Server	ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Το λογισμικό προστασίας από κακόβουλο λογισμικό, όπως το λογισμικό προστασίας από ιούς, πρέπει να αναπτύσεται με επαρκή έλεγχο πριν από την εγκατάσταση.		
Έλεγχος λογικής χειραγώγησης (Control Logic Manipulation)	Το λογισμικό συστήματος ελέγχου ή οι ρυθμίσεις διαμόρφωσης τροποποιήθη-καν, παράγοντας	**Μη αποτελεσματι-κή διαμόρφωση των συστημάτων (insufficient system hardening)**	PLC, RTU, DCS, Local SCADA Server-MTU, Local HMI, Central HMI, Data Historian Server,	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Πρέπει να εξετάζονται όλες οι ρυθμίσεις διαμόρφωσης.	CM-2 Baseline Configu-ration, CM-3 Configu-ration Change Control,	CIP 010-3 (R1, R2)

	απρόβλεπτα αποτελέσματα	**Οι κρίσιμες διαμορφώσεις δεν είναι αποθηκευμένες ή δεν διατηρείται αντίγραφο ασφαλείας**	Engineering Workstations, Application Server	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	1. Πρέπει να υπάρχουν διαθέσιμες διαδικασίες για την επαναφορά των ρυθμίσεων διαμόρφωσης των συστημάτων ICS σε περίπτωση τυχαίων αλλαγών διαμόρφωσης ή αλλαγών διαμόρφωσης που ξεκινάει ο επιτιθέμενος για τη διατήρηση της διαθεσιμότητας του συστήματος και την αποφυγή απώλειας δεδομένων. 2. Πρέπει να αναπτυχθούν τεκμηριωμένες διαδικασίες για τη διατήρηση των ρυθμίσεων διαμόρφωσης ICS.	CM-6 Configuration Settings	
		Αργές ενημερώσεις ή έλλειψη ενημερώσεων		ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Πρέπει να εφαρμόζονται σε τακτά χρονικά διαστήματα γρήγορες ενημερώσεις λογισμικού.		
		Έλλειψη γνώσης των δυνατοτήτων του λογισμικού των συστημάτων SCADA		ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Οι χειριστές θα πρέπει να γνωρίζουν την ανάγκη ενεργοποίησης των δυνατοτήτων του λογισμικού των συστημάτων SCADA.		
Τροποποιημένα συστήματα ασφαλείας	Η λειτουργία των συστημάτων ασφαλείας τροποποιείται έτσι ώστε είτε να μην λειτουργούν όταν χρειάζεται είτε να εκτελούν	**Έλλειψη επαρκούς πολιτικής αυθεντικοποίησης χρήστη**	PLC, RTU, DCS, Local SCADA Server-MTU, Sensors, Transmitters, Actuators, Valves, Motors	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	Οι πολιτικές αυθεντικοποίησης χρηστών πρέπει να αναπτυχθούν ως μέρος ενός συνολικού προγράμματος ασφάλειας των ICS συστημάτων λαμβάνοντας υπόψη τις δυνατότητες των ICS και του προσωπικού ώστε να χειρίζονται πιο περίπλοκους κωδικούς πρόσβασης και άλλους μηχανισμούς.	IA-2 Identification and Authentication (Organizational Users), IA-3	CIP-004-6 (R3), CIP 005-6 (R2), CIP 007-6 (R5)

	εσφαλμένες ενέργειες ελέγχου που καταστρέφουν τα συστήματα ICS.	**Η αυθεντικοποί-ηση χρηστών, δεδομένων ή συσκευών είναι ανύπαρκτη**	PLC, RTU, DCS, Local SCADA Server-MTU, Sensors, Transmit-ters, Actuators, Valves, Motors	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Πρέπει να υπάρχουν μέθοδοι αυθεντικοποίησης (πολυπλοκότητα κωδικού πρόσβασης, κρυπτογράφηση, έλεγχοι πρόσβασης, έξυπνες κάρτες).	Device Identifi-cation and Authenti-cation, IA-5 Authenti-cator Manage-ment	
Επίθεση XXS (XXS Attack)	Οι επιθέσεις Cross-Site Scripting (XSS) είναι ένας τύπος εισβολής, στον οποίο κακόβουλοι κώδικες εισάγονται σε αξιόπιστους ιστότοπους. Οι επιθέσεις XSS συμβαίνουν όταν ένας εισβολέας χρησιμοποιεί μια εφαρμογή ιστού για να στείλει κακόβουλο κώδικα, με τη μορφή script, σε διαφορετικό τελικό χρήστη.	**Έλλειψη επικύρωσης δεδομένων για τη βάση δεδομένων**	Local SCADA Server-MTU	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	Η επικύρωση της εισαγωγής δεδομένων πρέπει να πραγματοποιείται προκειμένου να επικυρώνονται τα δεδομένα που μεταφέρονται στη βάση δεδομένων.	SI-3 Malicious Code Protec-tion, SI-2 Flaw Remedia-tion	CIP 007-6 (R3)
		Δεν υπάρχει ειδική χρήση χαρακτήρων για εφαρμογές web		ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	Οι εφαρμογές web πρέπει να χρησιμοποιούν ειδικές λειτουργίες μετασχηματισμού χαρακτήρων.		
		Η HTML παρέχει κοινά χαρακτηριστικά (π.χ. όνομα, πλάτος κ.λπ.)		ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	Πρέπει να αποφεύγονται τα χαρακτηριστικά της HTML πριν από την εισαγωγή μη αξιόπιστων δεδομένων σε κοινά χαρακτηριστικά HTML.		
		Ο διακομιστής Ιστού επιτρέπει τη δυναμική δημιουργία JavaScript		ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	Πρέπει να αποφεύγεται η JavaScript πριν από την εισαγωγή μη αξιόπιστων δεδομένων σε τιμές δεδομένων JavaScript.		
		Ο πηγαίος κώδικας δεν έχει ελεγχθεί ποτέ		ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	Πρέπει να πραγματοποιούνται έλεγχοι του πηγαίου κώδικα για όλες τις κρίσιμες εφαρμογές.		

		Το σύστημα επιτρέπει την τοποθέτηση κακόβουλου κώδικα απευθείας σε παραμέτρους αιτήματος GET		ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	Πρέπει να αποφεύγεται το URL πριν από την εισαγωγή μη αξιόπιστων δεδομένων σε τιμές παραμέτρων διεύθυνσης HTML URL.		
Προχωρημέ-νες Επίμονες Απειλές (Advanced Persistent Threats - APTs)	Οι επιθέσεις αυτές είναι επιθέσεις που έχουν σχεδιαστεί για έναν συγκεκριμένο στόχο που συμβαίνει για μεγάλο χρονικό διάστημα και συνήθως πραγματοποι-ούνται σε πολλαπλά στάδια. Ο κύριος στόχος του επιτιθέμενου είναι να παραμείνει κρυμμένος και να αποκτήσει όσες περισσότερες πληροφορίες,	**Απουσία ή ανεπαρκής οδηγίες εφαρμογής για εξοπλισμό και συστήματα ICS**	PLC, Local HMI, Central HMI, Local SCADA Server-MTU, Sensors, Transmit-ters, Actuators, Valves, Motors	ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Οι οδηγίες εφαρμογής του εξοπλισμού των ICS πρέπει να είναι ενημερωμένες και άμεσα διαθέσιμες. Αυτές οι οδηγίες αποτελούν αναπόσπαστο μέρος των διαδικασιών ασφαλείας σε περίπτωση δυσλειτουργίας των συστημάτων ICS.	AT-1 Security Aware-ness and Training Policy and Proce-dures, AC-17 Remote Access	CIP 003-8 (R2), CIP 004-6 (R1, R2), CIP 005-6 (R2)
		Έλλειψη γνώσεων σχετικά με τις συσκευές		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Θα πρέπει να διασφαλίζεται η μεταφορά γνώσης σχετικά με τη λειτουργία και τη συντήρηση των παλιών συσκευών.		
		Ελλιπής έλεγχοι απομακρυσμέ-νης πρόσβασης		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Οι δυνατότητες απομακρυσμένης πρόσβασης πρέπει να ελέγχονται επαρκώς για να αποτρέπεται η πρόσβαση μη εξουσιοδοτημένων ατόμων στα συστήματα ICS.		
		Ανεπαρκής πολιτική ασφάλειας για συστήματα ICS		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Σε μια πολιτική κάθε αντίμετρο πρέπει να είναι ανιχνεύσιμο. Αυτό εξασφαλίζει ομοιομορφία και υπευθυνότητα. Η πολιτική πρέπει να περιλαμβάνει φορητές και κινητές συσκευές που χρησιμοποιούνται σε συστήματα ICS.		

	ευαίσθητα δεδομένα ή έλεγχο μπορεί, προκειμένου να επιτύχει τον στόχο της επίθεσης.	**Ανύπαρκτη διαδικασία παρακολούθησης ύποπτης δραστηριότητας, εντοπισμός πιθανών απειλών και γρήγορη αντίδραση σε κυβερνοεπιθέσεις.**		ΠΟΛΥ ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Μπορεί να αντιμετωπιστεί εν μέρει με την εφαρμογή συστημάτων ανίχνευσης ανωμαλιών. Τα τείχη προστασίας και τα προγράμματα προστασίας από ιούς είναι πιο κοινά, αλλά δεν αποτελούν μια καθολική λύση και δεν καλύπτουν όλους τους κινδύνους.		
Eavesdropping, (Man-in-the-Middle, SCADA communication hijacking)	Μη εξουσιοδοτημένη παρακολούθηση σε πραγματικό χρόνο μιας ιδιωτικής επικοινωνίας, όπως τηλεφωνική κλήση, συνεδρία ανταλλαγής άμεσων μηνυμάτων, τηλεδιάσκεψη ή επικοινωνίες μέσω email. Σε αυτό το περιβάλλον, μπορεί επίσης να περιλαμβάνει την παρακολούθη-	**Η σύνδεση HMI μεταδίδει κωδικούς πρόσβασης σε καθαρό κείμενο, που επιτρέπει στους απομακρυσμένους εισβολείς να πάρουν τον κωδικό πρόσβασης του χειριστή.**	Local HMI, Central HMI, Local SCADA Server-MTU, Switches, Gateways, Modem, Communication Router	ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Πρέπει να κρυπτογραφούνται όλοι οι σύνδεσμοι επικοινωνίας και όλα τα δεδομένα που σχετίζονται με τα συστήματα SCADA, προκειμένου να προστατεύονται τα δεδομένα από την υποκλοπή από έναν hacker ή από το κακόβουλο λογισμικό.	SC-13 Cryptographic Protection, SC-28 Protection of Information at Rest	CIP 011-2 (R1)
		Έλλειψη χρήσης VPN		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Πρέπει να ενίσχυεται η ασφάλεια των απομακρυσμένων επικοινωνιών χρησιμοποιώντας VPN για τη δημιουργία επικοινωνιών.		

	ση των επικοινωνιών των συστημάτων SCADA (π.χ. ελέγχουν τις εντολές και ακόμη και την τροποποίησή τους για μη εξουσιοδοτημένους σκοπούς).									
Διαρροή ευαίσθητων δεδομένων / πληροφοριών	Ευαίσθητα δεδομένα αποκαλύπτονται, εκ προθέσεως ή όχι, σε μη εξουσιοδοτημένα μέρη. Η σημασία αυτής της απειλής μπορεί να διαφέρει σημαντικά, ανάλογα με το είδος των δεδομένων που διαρρέουν.	**Ακατάλληλη σύνδεση δεδομένων**	Data Historian Server, Local SCADA Server-MTU, Local HMI, Central HMI	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Η σύνδεση δεδομένων πρέπει να διαμορφώνεται σωστά.	CA-3 Information Exchange, CP-9 System Backup, MP-1 Media Protection Policy and Procedures, MP-4 Media Storage, MP-5 Media Transport, MP-6 Media Sanitization	CIP 009-6 (R1), CIP 011-2 (R1, R2)
		Δημιουργία, χρήση και προστασία των κωδικών πρόσβασης δεν τηρείται σύμφωνα με την πολιτική		ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Η πολιτική και η διαδικασία κωδικού πρόσβασης πρέπει να ακολουθούνται για να είναι αποτελεσματικές.		
		Τα αρχεία καταγραφής δεν διατηρούνται		ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Πρέπει να διατηρούνται σωστά και ακριβή αρχεία καταγραφής.		
		Τα δεδομένα δεν προστατεύονται σε φορητές συσκευές		ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Πρέπει να ακολουθούνται πολιτικές, διαδικασίες και μηχανισμοί για την προστασία δεδομένων σε φορητές συσκευές.		

									MP-7 Media Use, SC-28 Protec-tion of Informa-tion at Rest	
Εισβολή SQL (SQL Injection)	Η εγκατάσταση κακόβουλου κώδικα σε μία Βάση Δεδομένων που περιέχει πολύτιμα δεδομένα μπορεί να έχει εκτεταμένες επιπτώσεις, ιδιαίτερα στο περιβάλλον ελέγχου, όπου η ακρίβεια και η ακεραιότητα των δεδομένων είναι κρίσιμη για τη λήψη αποφάσεων τόσο στο επιχειρηματικό όσο και στο εκτελεστικό πεδίο. Η αλλοίωση ή η καταστροφή των δεδομένων σε μια Βάση	**Δεν υπάρχει επικύρωση εισαγωγής δεδομένων**	Data Historian Server, Local HMI, Central HMI	ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Η επικύρωση εισαγωγής δεδομένων θα πρέπει να εκτελείται για την επικύρωση των ερωτημάτων SQL στη βάση δεδομένων.	AC-6 Least Privilege, SI-11 Error Handling, CP-9 System Backup, MP-1 Media Protec-tion Policy and Proce-dures MP-4 Media Storage, SC-28 Protec-tion of Informa-tion at Rest	CIP 007-6 (R5), CIP 011-2 (R1)
		Υπάρχουν λεπτομερή σφάλματα βάσης δεδομένων		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Πρέπει να εφαρμόζεται η κατάλληλη διαμόρφωση για να μην επιστρέφονται λεπτομερή μηνύματα σφάλματος βάσης δεδομένων (χρήση προσαρμοσμένων μηνυμάτων σφάλματος).		
		Έλλειψη δικαιωμάτων πρόσβασης στην υπηρεσία βάσης δεδομένων		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Οι λογαριασμοί των χρηστών της βάσης δεδομένων πρέπει να έχουν ελάχιστα δικαιώματα πρόσβασης.		
		Το σύστημα επιτρέπει ειδικούς χαρακτήρες		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Πρέπει να αποφεύγονται οι ειδικοί χαρακτήρες χρησιμοποιώντας τη συγκεκριμένη σύνταξη αποφυγής. (https://www.owasp.org/index.php/ESAPI)		
		Δεν υπάρχει ειδική τοποθεσία για διακομιστές ιστού και διακομιστές		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Οι διακομιστές ιστού και οι διακομιστές βάσεων δεδομένων πρέπει να είναι απομονωμένοι.		

	Δεδομένων, μπορεί να επηρεάσει τους διακομιστές απόκτησης δεδομένων, τους Data Historians ακόμα και την ομαλή λειτουργία της κονσόλας HMI.	**βάσης δεδομένων**								
		Η αναθεώρηση του πηγαίου κώδικα δεν πραγματοποιείται σε τακτά χρονικά διαστήματα		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Η αναθεώρηση του πηγαίου κώδικα πρέπει να πραγματοποιείται για όλες τις κρίσιμες εφαρμογές σε τακτά χρονικά διαστήματα.		
Μη εξουσιοδοτη-μένη πρόσβαση στο δίκτυο	Ένας υπάλληλος ή ένας εξωτερικός συνεργάτης που έχει πρόσβαση σε περιορισμένα εσωτερικά συστήματα χρησιμοποιεί αυτό το πλεονέκτημα για κλοπή, τροποποίηση ή πρόσβαση χωρίς άδεια σε αυτά τα συστήματα ή σε άλλα που είναι προσβάσιμα μέσω αυτών.	**Τα πρωτόκολλα επικοινωνίας χρησιμοποιού-νται σε απλό κείμενο**	SCADA Protocols (DNP3, ICCP-IEC 60870, Modbus, OPC), Switches, Gateways, Modem, Communica-tion Router	ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Τα πρωτόκολλα επικοινωνίας όπως το Modbus και το DNP3 πρέπει να είναι σε ισχύ.	CA-6 Authori-zation, SC-8 Transmis-sion Confiden-tiality and Integrity	CIP 003-8 (R3, R4)
		Χρήση μη ασφαλών πρωτοκόλλων ICS σε ολόκληρη τη βιομηχανία		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Τα πρωτόκολλα επικοινωνίας όπως το Modbus και το DNP3 πρέπει να είναι σε ισχύ.		
		Έλλειψη ελέγχου ακεραιότητας για επικοινωνίες		ΥΨΗΛΟ	ΥΨΗΛΟ	ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	Οι έλεγχοι ακεραιότητας πρέπει να ενσωματώνονται σε πρωτόκολλα ICS. Για να διασφαλιστεί η ακεραιότητα, το ICS μπορεί να χρησιμοποιεί πρωτόκολλα χαμηλότερου επιπέδου (π.χ. IPsec) που προσφέρουν προστασία ακεραιότητας δεδομένων.		

Μεταφορά περιττών δεδομένων μεταξύ δικτύων	Η έλλειψη σωστά διαμορφωμέ-νων Firewalls θα μπορούσε να επιτρέψει τη μεταφορά περιττών δεδομένων μεταξύ δικτύων, όπως τα δίκτυα ελέγχου και εταιρικών δικτύων, επιτρέποντας την εξάπλωση επιθέσεων και κακόβουλου λογισμικού μεταξύ των δικτύων,	**Ανεπαρκή αρχεία καταγραφής των Firewalls και των Routers**	Firewalls, Switches, Gateways, Modem, Communica-tion Router, Remote Access Server	ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Τα αρχεία καταγραφής των Firewall και των Router πρέπει να παρακολουθούνται και να ελέγχονται σε τακτά χρονικά διαστήματα.	SC-13 Crypto-graphic Protec-tion, SI-4 System Monito-ring	CIP 005-6 (R1), CIP 007-6 (R4)
		Δεν υπάρχουν Firewalls ή δεν έχουν ρυθμιστεί σωστά.		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Πρέπει να ελαχιστοποιούνται οι διαδρομές πρόσβασης στο εσωτερικό δίκτυο και να αυξάνονται τα μέτρα παρακολούθησης.		
		Αδύναμοι κανόνες Firewall - Η πρόσβαση σε συγκεκριμένες θύρες στον κεντρικό υπολογιστή δεν περιορίζεται σε απαιτούμενες IP διευθύνσεις.		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Η χρήση τμηματοποίησης της ζώνης ασφαλείας στο δίκτυο SCADA και η χρήση κατανεμημένου Firewall εντός του περιβάλλοντος SCADA μπορεί να προστατεύσουν τις τελικές συσκευές.		

	καθιστώντας ευαίσθητα δεδομένα εκτεθειμένα στην παρακολούθη-ση / υποκλοπή και παρέχοντας στα άτομα μη εξουσιοδοτημέ-νη πρόσβαση σε συστήματα.	**Έλλειψη λειτουργικών DMZ**		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Τα Firewalls πρέπει να χρησιμοποιούνται για τη δημιουργία DMZ για την προστασία του δικτύου ICS. Τα περισσότερα τείχη προστασίας επιτρέπουν πολλαπλά DMZ και μπορούν να καθορίσουν τι είδους κίνηση μπορεί να προωθηθεί μεταξύ ζωνών. Θα πρέπει να δημιουργηθούν διαφορετικά DMZ για ξεχωριστές λειτουργίες / προνόμια πρόσβασης, όπως μια ομότιμη σύνδεση όπως ο διακομιστής ICCP σε συστήματα SCADA, ο Data Historian, οι διακομιστές ασφαλείας, οι αναπαραγόμενοι διακομιστές και οι διακομιστές ανάπτυξης.		
		Ανεπαρκής κατανόηση περιεχομένου κίνησης		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Οι διευθυντές πρέπει να γνωρίζουν τι είδους κίνηση περνά μέσα από τα δίκτυά τους, προκειμένου να είναι σε θέση να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τον τρόπο απόκρισης σε πιθανές απειλές και ποια είδη κυκλοφορίας να επιτρέπουν και ποια να φιλτράρουν. Αυτό βοηθά επίσης στη δημιουργία του κατάλληλου διαχωρισμού και τμηματοποίησης του δικτύου.		
		Ανεπαρκής προστασία δεδομένων μεταξύ ασύρματων clients και σημείων πρόσβασης		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Τα ευαίσθητα δεδομένα μεταξύ ασύρματων clients και σημείων πρόσβασης πρέπει να προστατεύονται χρησιμοποιώντας ισχυρή κρυπτογράφηση για να διασφαλιστεί ότι οι αντίπαλοι δεν μπορούν να αποκτήσουν μη		

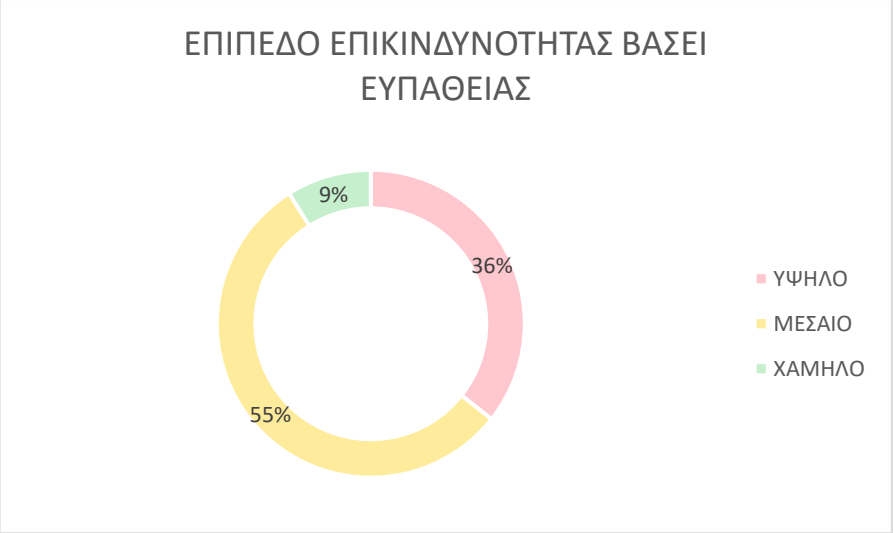
								εξουσιοδοτημένη πρόσβαση στα μη κρυπτογραφημένα δεδομένα.		
		Ανεπαρκής αυθεντικοποί-ηση μεταξύ ασύρματων clients και σημείων πρόσβασης		ΥΨΗΛΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΥΨΗΛΟ	Απαιτείται ισχυρή κοινή αυθεντικοποίηση μεταξύ ασύρματων clients και σημείων πρόσβασης για να διασφαλιστεί ότι οι πελάτες δεν συνδέονται σε ένα κακόβουλο σημείο πρόσβασης που έχει αναπτυχθεί από έναν αντίπαλο, καθώς και για να διασφαλιστεί ότι οι αντίπαλοι δεν θα συνδεθούν σε κανένα από τα ασύρματα δίκτυα των συστημάτων ICS.		
Διακοπή Συστημάτων Επικοινωνίας (Δίκτυο)	Διακοπή ή αποτυχία στην παροχή δικτύου, είτε εκ προθέσεως είτε τυχαία. Ανάλογα με το τμήμα δικτύου που επηρεάζεται και τον χρόνο που απαιτείται για την ανάκτηση των επικοινωνιών, η σημασία αυτής	**Επίβλεψη απομακρυσμέ-νης πρόσβασης**	Firewalls, Switches, Gateways, Modem, Communica-tion Router, Remote Access Server	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΜΕΣΑΙΟ	Αυτά τα σενάρια πρέπει να ελέγχονται και να παρακολουθούνται και πρέπει να περιλαμβάνουν τουλάχιστον τα ίδια μέτρα ασφαλείας με τις εσωτερικές συνδέσεις.	AC-17 Remote Access, CM-6 Configu-ration Settings, CM-7 Least Functio-nality, CP-9 System Backup	CIP 005-6 (R2), CIP 007-6 (R1), CIP 009-6 (R1), CIP 010-3 (R1, R2)
		Οι συσκευές δικτύου πιθανώς δεν έχουν διαμορφωθεί		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Οι συσκευές δικτύου θα πρέπει να διαμορφώνονται κατάλληλα.		
		Η ασφάλεια των θυρών δεν εφαρμόζεται σε εξοπλισμό δικτύου		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΜΕΣΑΙΟ	Οι θύρες του εξοπλισμού δικτύου θα πρέπει να ασφαλίζονται σωστά.		

	της απειλής μπορεί να κυμαίνεται από υψηλή έως κρίσιμη.	**Δεν υπάρχει αντίγραφο ασφαλείας των Firewalls**		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	Όλα τα Firewalls πρέπει να δημιουργούν αντίγραφα ασφαλείας.		
Εκμετάλλευση Kits και Rootkits	Ένα exploit είναι ένας ειδικά κατασκευασμένος κώδικας που έχει σχεδιαστεί για να εκμεταλλευτεί μια ευπάθεια προκειμένου να αποκτήσει πρόσβαση σε ένα σύστημα. Είναι μια από τις σημαντικότερες απειλές για τα δίκτυα ICS / SCADA, καθώς μπορεί να χρησιμοποιηθεί και από επιτιθέμενους με χαμηλή εξειδίκευση, και είναι δύσκολο να εντοπιστούν.	**Τα πρωτόκολλα επικοινωνίας χρησιμοποιούνται σε απλό κείμενο**	SCADA Protocols (DNP3, ICCP-IEC 60870, Modbus, OPC), Switches, Gateways, Modem, Communication Router	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΜΕΣΑΙΟ	Τα πρωτόκολλα επικοινωνίας όπως το Modbus και το DNP3 πρέπει να είναι σε ισχύ.	SC-1 System and Communications Protection Policy and Procedures, SC-3 Security Function Isolation, SC-8 Transmission Confidentiality and Integrity	
		Χρήση μη ασφαλών πρωτοκόλλων ICS σε ολόκληρη τη βιομηχανία		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΜΕΣΑΙΟ	Τα πρωτόκολλα επικοινωνίας όπως το Modbus και το DNP3 πρέπει να είναι σε ισχύ.		
		Έλλειψη ελέγχου ακεραιότητας για επικοινωνίες		ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	ΥΨΗΛΟ	ΜΕΣΑΙΟ	Οι έλεγχοι ακεραιότητας πρέπει να ενσωματώνονται σε πρωτόκολλα ICS. Για να διασφαλιστεί η ακεραιότητα, το ICS μπορεί να χρησιμοποιεί πρωτόκολλα χαμηλότερου επιπέδου (π.χ. IPsec) που προσφέρουν προστασία ακεραιότητας δεδομένων.		
Τεχνικά σφάλματα και αστοχίες	Τεχνικά σφάλματα και αστοχίες στο δρομολογητή μπορεί να προκαλέσουν	**Αποτυχία των διαδικασιών λειτουργίας και συντήρησης, όπως καθορίζεται**	Modem, Communication Router	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	Οι προδιαγραφές του κατασκευαστή πρέπει να τηρούνται κατά την εγκατάσταση, τη λειτουργία και τη συντήρηση των δρομολογητών.	CM-3 Configuration Change Control, CM-6	CIP-010-3 (R1)

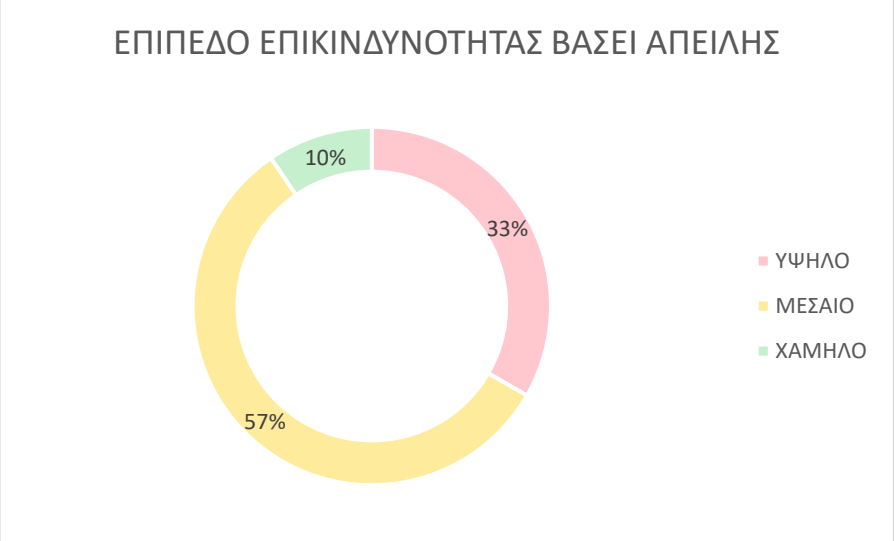
	διακοπή σύνδεσης και επικοινωνίας.	**από τον κατασκευαστή**							Configu-ration Settings, CM-7 Least Functio-nality	
		Ύπαρξη παλιού δρομολογητή		ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	Ο δρομολογητής συνιστάται να είναι μικρότερος των 3 ετών.		
		Ο δρομολογητής λειτουργεί σε ακραίες συνθήκες φόρτωσης		ΧΑΜΗ-ΛΟ	ΜΕΣΑΙΟ	ΧΑΜΗ-ΛΟ	ΧΑΜΗ-ΛΟ	Θα πρέπει να αποφεύγετε η χρήση των δρομολογητών στις πλήρεις δυνατότητές τους, όσον αφορά τη χωρητικότητα, το φορτίο κ.λπ.		

7.4 Συνολικά Στατιστικά Αποτίμησης Επικινδυνότητας

Στις Εικόνες 12 και 13 παρουσιάζονται τα στατιστικά της αποτίμησης επικινδυνότητας τα οποία προέκυψαν από την μελέτη με βάση τις ευπάθειες και τις απειλές αντίστοιχα.



Εικόνα 12: Στατιστικά επικινδυνότητας βάσει ευπάθειας



Εικόνα 13: Στατιστικά επικινδυνότητας βασει απειλής

Στον Πίνακα 11 παρουσιάζονται οι απειλές με υψηλό επίπεδο επικινδυνότητας, τα πιο κρίσιμα αγαθά ενός ενεργειακού πάρκου, οι επιπτώσεις που θα έχουν στα αγαθά αυτά, καθώς και τα προτεινόμενα μέτρα για την πρόληψη και την αντιμετώπιση των πιθανών απειλών.

Πίνακας 11: Αποτίμηση Επικινδυνότητας Υψηλού Επιπέδου

Απειλή	Επίπεδο Επικινδυνό-τητας	Επηρεαζόμενα αγαθά του ενεργειακού πάρκου	Επίπτωση στα αγαθά του ενεργειακού πάρκου	Προτεινόμενα μέτρα
Τρομοκρατική Επίθεση	ΥΨΗΛΟ	Primary Control Center, Backup Control Center, Control Room	• Τρομοκρατική επίθεση με αποτέλεσμα μια μεγάλη καταστροφή της υποδομής του ενεργειακού πάρκου που έχει εγκατεστημένα τα συστήματα ICS.	• Η υποδομή του κτιρίου πρέπει να παρέχει προστασία σε περίπτωση επίθεσης με φυσικά μέσα (αναγκαστική επίθεση). • Οι πόρτες πρέπει να είναι ανθεκτικές σε τέτοιου είδους επιθέσεις. • Πρέπει να υπάρχουν κατάλληλοι έλεγχοι για την παρακολούθηση των εγκαταστάσεων του οργανισμού (π.χ. CCTV) • Η περίμετρος ασφαλείας πρέπει να είναι επαρκώς φωτισμένη. • Πρέπει να εφαρμόζονται πολιτικές και διαδικασίες σχετικά με την πρόσβαση στις υποδομές.
Άρνηση Ενέργειας Ελέγχου (Denial of Control Action)	ΥΨΗΛΟ	PLC, RTU, DCS, Local SCADA Server-MTU, IED, Local HMI, Central HMI	• Καθυστέρηση ή παρεμπόδιση της ροής πληροφοριών, αρνούμενη έτσι τη διαθεσιμό-τητα των δικτύων για τον έλεγχο των	• Πρέπει να υπάρχουν πολιτικές και προγράμματα κατάρτισης σχετικά με θέματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο και

Απειλή	Επίπεδο Επικινδυνό-τητας	Επηρεαζόμενα αγαθά του ενεργειακού πάρκου	Επίπτωση στα αγαθά του ενεργειακού πάρκου	Προτεινόμενα μέτρα
			διαχειριστών συστημάτων ή προκαλώντας σημεία συμφόρησης μεταφοράς ή άρνηση υπηρεσίας από IT υπηρεσίες (όπως DNS).	τις κρίσιμες υποδομές. • Συνιστάται ενισχυμένη ασφάλεια για τα συστήματα που ανήκουν σε αποστρατικοποιημένες ζώνες (DMZs) καθώς και για το εσωτερικό δίκτυο. • Εκτός από τα εργαλεία ακεραιότητας διακομιστών, η ασφάλεια χρειάζεται ενίσχυση, χρησιμοποιώντας εικονικά ιδιωτικά δίκτυα (VPN). • Θα πρέπει να παρέχονται από τους προμηθευτές μέτρα ασφαλείας με τη μορφή ενημερώσεων κώδικα και αναβαθμίσεων για συστήματα SCADA προκειμένου να προστατεύονται οι μη εξουσιοδοτημένες συνδέσεις δικτύου PLC / RTU.
Επιθέσεις Άρνησης Υπηρεσίας (Denial of Service)	ΥΨΗΛΟ	RTU, Local SCADA Server-MTU, Local HMI, Central HMI	• Παύση λειτουργιών με αποτέλεσμα την τροποποίηση στις μεταβλητές των συστημάτων ελέγχου του ενεργειακού πάρκου. • Μη διαθεσιμότητα των συστηματων ελέγχου.	• Το λογισμικό των IDS / IPS πρέπει να δοκιμάζεται πριν από την ανάπτυξη για να διαπιστωθεί ότι δεν θέτει σε κίνδυνο την κανονική λειτουργία των συστημάτων ICS. • Η κυκλοφορία του δικτύου πρέπει να παρακολουθείται επαρκώς.

Απειλή	Επίπεδο Επικινδυνό-τητας	Επηρεαζόμενα αγαθά του ενεργειακού πάρκου	Επίπτωση στα αγαθά του ενεργειακού πάρκου	Προτεινόμενα μέτρα
				• Τα περιστατικά ασφάλειας πληροφοριών αποκρίνονται σύμφωνα με τις τεκμηριωμένες διαδικασίες. • Πρέπει να υπάρχει μια προπληρωμένη υπηρεσία ISP για ειδοποίηση επίθεσης DoS. • Θα πρέπει να πραγματοποιούνται τακτικοί έλεγχοι για τον εντοπισμό ανεπιθύμητων υπηρεσιών ή ανοιχτών θυρών.
Κακόβουλο λογισμικό (Virus, Trojan, Worm)	ΥΨΗΛΟ	PLC, RTU, DCS, Local SCADA Server-MTU, Local HMI, Central HMI, Data Historian Server, Engineering Workstations, Application Server	• Ζημιά, καταστροφή ή κλοπή πληροφοριών και λογισμικού συστημάτων ICS.	• Το λογισμικό προστασίας από κακόβουλα προγράμματα, όπως το λογισμικό προστασίας από ιούς, πρέπει να διατηρείται ενημερωμένο σε ένα πολύ δυναμικό περιβάλλον. • Το λογισμικό προστασίας από κακόβουλο λογισμικό, όπως το λογισμικό προστασίας από ιούς, πρέπει να αναπτύσεται με επαρκή έλεγχο πριν από την εγκατάσταση.
Έλεγχος λογικής χειραγώγησης (Control Logic Manipulation)	ΥΨΗΛΟ	PLC, RTU, DCS, Local SCADA Server-MTU, Local HMI, Central HMI, Data Historian Server,	• Το λογισμικό των συστημάτων ελέγχου ή οι ρυθμίσεις διαμόρφωσης εάν τροποποιηθούν,	• Πρέπει να εξετάζονται όλες οι ρυθμίσεις διαμόρφωσης. • Πρέπει να υπάρχουν διαθέσιμες

Απειλή	Επίπεδο Επικινδυνό-τητας	Επηρεαζόμενα αγαθά του ενεργειακού πάρκου	Επίπτωση στα αγαθά του ενεργειακού πάρκου	Προτεινόμενα μέτρα
		Engineering Workstations, Application Server	μπορεί να παράγουν απρόβλεπτα αποτελέσματα με επίπτωση ανακριβείς μετρήσεις και δεδομένα.	διαδικασίες για την επαναφορά των ρυθμίσεων διαμόρφωσης των συστημάτων ICS • Πρέπει να εφαρμόζονται σε τακτά χρονικά διαστήματα γρήγορες ενημερώσεις λογισμικού • Οι χειριστές θα πρέπει να γνωρίζουν την ανάγκη ενεργοποίησης των δυνατοτήτων του λογισμικού των συστημάτων SCADA.
Προχωρημένες Επίμονες Απειλές (Advanced Persistent Threats - APTs)	ΥΨΗΛΟ	PLC, Local HMI, Central HMI, Local SCADA Server-MTU, Sensors, Transmitters, Actuators, Valves, Motors	• Παραμονή στο δίκτυο για μεγάλο χρονικό διάστημα με αποτέλεσμα την πρόσβαση σε πολύτιμες πληροφορίες και μακροπρόθεσμο έλεγχο της υποδομής.	• Οι οδηγίες εφαρμογής του εξοπλισμού των ICS πρέπει να είναι ενημερωμένες και άμεσα διαθέσιμες. Αυτές οι οδηγίες αποτελούν αναπόσπαστο μέρος των διαδικασιών ασφαλείας σε περίπτωση δυσλειτουργίας των συστημάτων ICS. • Οι δυνατότητες απομακρυσμένης πρόσβασης πρέπει να ελέγχονται επαρκώς για να αποτρέπεται η πρόσβαση μη εξουσιοδοτημένων ατόμων στα συστήματα ICS. • Σε μια πολιτική κάθε αντίμετρο πρέπει να είναι

Απειλή	Επίπεδο Επικινδυνό-τητας	Επηρεαζόμενα αγαθά του ενεργειακού πάρκου	Επίπτωση στα αγαθά του ενεργειακού πάρκου	Προτεινόμενα μέτρα
				ανιχνεύσιμο. Αυτό εξασφαλίζει ομοιομορφία και υπευθυνότητα. Η πολιτική πρέπει να περιλαμβάνει φορητές και κινητές συσκευές που χρησιμοποιούνται σε συστήματα ICS. • Μπορεί να αντιμετωπιστεί εν μέρει με την εφαρμογή συστημάτων ανίχνευσης ανωμαλιών. Τα τείχη προστασίας και τα προγράμματα προστασίας από ιούς είναι πιο κοινά, αλλά δεν αποτελούν μια καθολική λύση και δεν καλύπτουν όλους τους κινδύνους.
Μεταφορά περιττών δεδομένων μεταξύ δικτύων	ΥΨΗΛΟ	Firewalls, Switches, Gateways, Modem, Communication Router, Remote Access Server	• Παροχή μη εξουσιοδοτημε-νης πρόσβασης στα συστήματα ICS με αποτέλεσμα ευαίσθητα δεδομένα να είναι εκτεθιμένα στην παρακολούθηση και την υποκλοπή.	• Τα αρχεία καταγραφής των Firewall και των Router πρέπει να παρακολουθού-νται και να ελέγχονται σε τακτά χρονικά διαστήματα. • Πρέπει να ελαχιστοποιούνται οι διαδρομές πρόσβασης στο εσωτερικό δίκτυο και να αυξάνονται τα μέτρα παρακολούθησης. • Η χρήση της τμηματοποίησης της ζώνης ασφαλείας στο

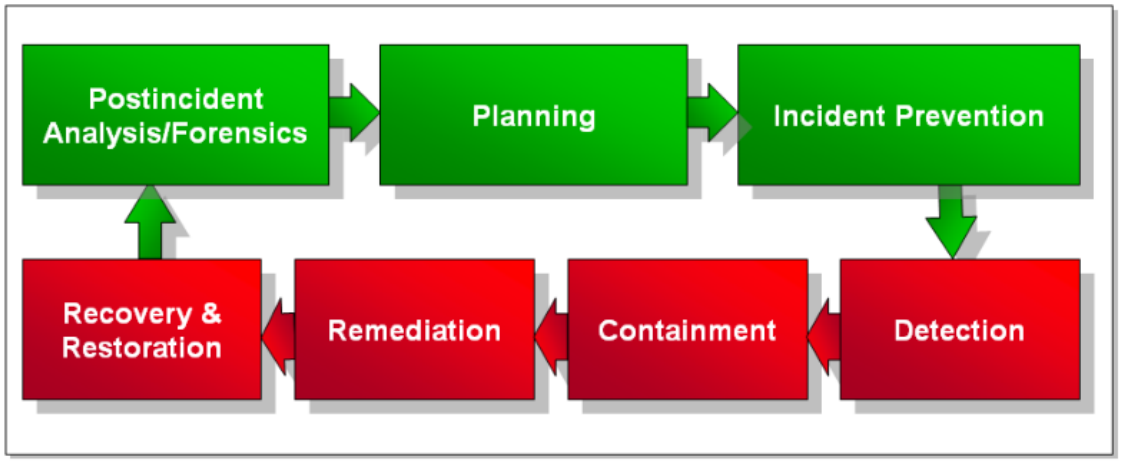
Απειλή	Επίπεδο Επικινδυνό-τητας	Επηρεαζόμενα αγαθά του ενεργειακού πάρκου	Επίπτωση στα αγαθά του ενεργειακού πάρκου	Προτεινόμενα μέτρα
				δίκτυο SCADA και η χρήση ενός κατανεμημένου Firewall εντός του περιβάλλοντος SCADA μπορούν να προστατεύσουν τις τελικές συσκευές • Τα Firewalls πρέπει να χρησιμοποιούνται για τη δημιουργία DMZ για την προστασία του δικτύου ICS.

8 Διαδικασία Απόκρισης Περιστατικών σε Συστήματα ICS

Στην προηγούμενη ενότητα πραγματοποιήθηκε η αποτίμηση και η διαχείριση επικινδυνότητας ενός οργανισμού που έχει εγκατεστημένα συστήματα ICS σε ένα ενεργειακό πάρκο. Είναι σημαντικό να επισημάνουμε ότι κάθε οργανισμός που χρησιμοποιεί συστήματα ICS, προκειμένου να αποτρέψει τον κίνδυνο από τις απειλές που αναλύθηκαν, πρέπει να έχει καταγεγραμμένη μια διαδικασία απόκρισης περιστατικών και να ακολουθούνται τα βήματά της.

Οι θεμελιώδεις αρχές είναι οι ίδιες στην απόκριση σε περιστατικά στον κυβερνοχώρο, συμπεριλαμβανομένων της πρόληψης, της προετοιμασίας, του σχεδιασμού, της διαχείρισης περιστατικών, της ανάκαμψης, του μετριασμού, της αποκατάστασης, της ανάλυσης μετά από περιστατικά και των διδαγμάτων. Στην απόκριση περιστατικών στον κυβερνοχώρο, η εστίαση κατευθύνεται σε αρνητικά περιστατικά που προκαλούνται ειδικά από κακόβουλα μέρη που χρησιμοποιούν υπολογιστές και σχετικές τεχνολογίες.

Η ικανότητα απόκρισης σε περιστατικά στον κυβερνοχώρο πρέπει να περιλαμβάνει αρκετά στοιχεία που έχουν προληπτικό χαρακτήρα για να αποτρέψουν ένα περιστατικό ή να επιτρέπουν στον οργανισμό να ανταποκρίνεται πιο αποτελεσματικά όταν συμβαίνει ένα. Όπως φαίνεται στην Εικόνα 14, αυτά τα στοιχεία είναι πράσινα και περιλαμβάνουν το σχεδιασμό, την πρόληψη και την ανάλυση μετά το περιστατικό. Τα υπόλοιπα στοιχεία της διαδικασίας που είναι κόκκινα επικεντρώνονται στην ανίχνευση, τον περιορισμό, την αποκατάσταση και την ανάκτηση [33].



Εικόνα 14: Φάσεις Δαδικασίας Απόκρισης Περιστατικών, "Recommended Practice: Developing and Industrial Control systems Cybersecurity Incident Response Capability" 2009

8.1 Σχεδιασμός Απόκρισης Περιστατικών

Το σημείο εκκίνησης για τη δημιουργία μιας διαδικασίας απόκρισης σε περιστατικά στον κυβερνοχώρο είναι η φάση σχεδιασμού και προετοιμασίας. Το πρώτο βήμα για την ανάπτυξη μιας διαδικασίας αντιμετώπισης περιστατικών είναι η οργάνωση της ομάδας CSIRT (Cyber Security Incident Response Team).

Αρχικά θα πρέπει να προσδιοριστούν οι βασικοί ρόλοι και οι αρμοδιότητες της ομάδας απόκρισης περιστατικών CSIRT.

- **Διαχειριστής ομάδας**: Είναι απαραίτητο να ανατεθεί σε ένα άτομο η ευθύνη να δει ότι η ομάδα είναι οργανωμένη και επιτυγχάνει τους στόχους της.
- **Μηχανικός Συστημάτων Διαδικασίας ή Ελέγχου**: Αυτό το άτομο θα πρέπει να είναι ειδικός στον έλεγχο της αρχιτεκτονικής του συστήματος και πρέπει να γνωρίζει και να κατανοεί τα συστατικά στοιχεία και τα προϊόντα του συστήματος που παράγονται ή υποστηρίζονται από τα συστήματα ICS.

- **Διαχειριστής δικτύου**: Παρέχει βασικό ρόλο εάν το περιστατικό περιλαμβάνει επίθεση στον κυβερνοχώρο που προέρχεται από το δίκτυο υπολογιστών. Αυτό το άτομο πρέπει συνήθως να έχει γνώση της πρόσβασης στο δίκτυο, συμπεριλαμβανομένων των ευάλωτων σημείων ασφαλείας, της επιδιόρθωσης, του εντοπισμού εισβολών και της παρακολούθησης συστήματος.
- **Διαχειριστής συστήματος**: Ο διαχειριστής συστήματος πρέπει να είναι ενημερωμένος για τα δικαιώματα πρόσβασης και τα αρχεία καταγραφής λειτουργίας του συστήματος στους διακομεστές ICS που επηρεάζονται.
- **Διαχειριστής εγκατάστασης (συμπεριλαμβανομένων των διαχειριστών ICS και Control Center)**: Παρόλο που αυτό το άτομο ενδέχεται να μην εμπλέκεται σε πολλές από τις λεπτομέρειες του σχεδίου απόκρισης περιστατικών, πρέπει να συμμετέχει στην ανάθεση διάφορων αρχών για τη διακοπή των λειτουργίων, ως μέρος της διαδικασίας αποτίμησης επικινδυνότητας όταν εντοπίζεται ένα περιστατικό.
- **Διευθυντής IT ή CIO**: Αυτός ο ρόλος είναι παρόμοιος με τον διαχειριστή της εγκατάστασης όσον αφορά στις ευθύνες. Αυτές οι δύο διευθυντικές θέσεις είναι απαραίτητες και πρέπει να επικοινωνούν και να συντονίζονται και αποφασίζουν ποιοι πόροι μπορούν και θα εφαρμοστούν σε ένα περιστατικό. Ένα σύγχρονο σύστημα ελέγχου είναι συνήθως ενσωματωμένο σε υπάρχοντα δίκτυα πληροφορικής, σε επιχειρηματικά συστήματα και σε εξοπλισμό επικοινωνίας.
- **Εμπειρογνώμονες ασφαλείας**: Αυτά τα άτομα παρέχουν γνώση σχετικά με τις ευπάθειες, το πως μπορεί κάποιος να τις εκμεταλλευτεί, τις τεχνικές και τους τρόπους πρόληψης από περιστατικά, και την ανάκτηση εάν συμβούν.

Ενώ ο πρωταρχικός στόχος της ομάδας αυτής είναι ο χειρισμός περιστατικών που σχετίζονται με τον κυβερνοχώρο, θα μπορούσε να υπάρχει ξεχωριστή ομάδα απόκρισης για περιστατικά εκτός του κυβερνοχώρου, όπως μια διακοπή του συστήματος ICS ή SCADA, μια καταστροφική αποτυχία εξοπλισμού ή φυσικές καταστροφές όπως πλημμύρες ή τυφώνες.

Έπειτα από τη δημιουργία της ομάδας και την ανάθεση των ρόλων και των αρμοδιοτήτων, το επόμενο βήμα είναι ο σχεδιασμός των πολιτικής, της διαδικασίας και του σχεδίου-πλάνου.

Η πολιτική αντιμετώπισης περιστατικών πρέπει να κατευθύνει τη δημιουργία της ομάδας CSIRT και να θέσει τους κανόνες, τα θεμέλια και τα βήματα που ορίζονται στη διαδικασία και στο σχέδιο απόκρισης περιστατικών. Το σχέδιο απόκρισης περιστατικών στον κυβερνοχώρο καθορίζει και τεκμηριώνει τις διαδικασίες και τις ενέργειες που εφαρμόζουν την πολιτική απόκρισης περιστατικών για τα συστήματα ICS. Καθορίζει το περιστατικό ασφαλείας και περιγράφει τα λεπτομερή βήματα που θα πρέπει να ακολουθηθούν για την αντιμετώπιση του περιστατικού και τον περιορισμό της ζημιάς στον οργανισμό.

Στη συνέχεια, το σχέδιο απόκρισης περιστατικών στον κυβερνοχώρο θα πρέπει να δοκιμαστεί ώστε ο οργανισμός να λάβει τα κατάλληλα μέτρα σε περίπτωση που η εφαρμογή του έχει ελλείψεις ή αποκλίσεις.

Τέλος, θα πρέπει να πραγματοποιηθεί η αναφορά κατάστασης των συστημάτων που δοκιμάστηκαν. Η ενεργοποίηση της αναφοράς κατάστασης για την περιγραφή του ενός συστήματος αναφέρεται στη σύνδεση αυτοματοποιημένων μηχανισμών με το υλισμικό ή το λογισμικό που αναφέρουν πληροφορίες σχετικά με το σύστημα, συμπεριλαμβανομένης της μη φυσιολογικής συμπεριφοράς, της απόπειρας εισβολής ή άλλων δεδομένων που θα ήταν χρήσιμα για τον εντοπισμό ενός περιστατικού, την κατανόηση της επίπτωσης και τη γρήγορη υποστήριξη της επίλυσης.

8.2 Πρόληψη Περιστατικών

Η πρόληψη ενός περιστατικού στον κυβερνοχώρο αποκτά μια εντελώς νέα διάσταση στο περιβάλλον ICS σε σύγκριση με το περιβάλλον IT. Αυτό συμβαίνει επειδή, πέρα από το δίκτυο υπάρχουν πολύ λιγότερες και, σε ορισμένες περιπτώσεις, δεν διατίθενται δυνατότητες ανίχνευσης στις συσκευές συστημάτων IT. Επιπλέον, τα λειτουργικά στοιχεία ενδέχεται να έχουν ευπάθειες που δεν μπορεί να διορθωθούν ποτέ και τα αποτελέσματα των πιο σοβαρών επιθέσεων θα μπορούσαν να περιλαμβάνουν τραυματισμό, απώλεια ζωής ή σοβαρή οικονομική απώλεια.

Υπάρχουν διάφορα διαδεδομένα πρότυπα που αναφέρονται στο Κεφάλαιο 2 και τα οποία αντιπροσωπεύουν ένα σύνολο γενικών οδηγιών για την ασφάλεια στον κυβερνοχώρο που καλύπτει το ευρύτερο φάσμα των τομέων που ισχύουν για τα συστήματα ICS.

Επιπλέον διατίθενται αυτοματοποιημένα εργαλεία για να βοηθήσουν έναν οργανισμό να αξιολογήσει την ασφάλεια ενός περιβάλλοντος ICS. Τα εργαλεία αυτά μπορεί να έχουν τη μορφή αυτόνομων προγραμμάτων λογισμικού που προσφέρονται από εμπορικούς προμηθευτές ή να παρέχονται προϊόντα σε συνδυασμό με αξιολόγηση που προσφέρονται από μια εταιρεία συμβούλων.

Παράδειγμα ενός τέτοιου αυτοματοποιημένου εργαλείου που αναπτύχθηκε υπό την καθοδήγηση του DHS των Ηνωμένων Πολιτειών της Αμερικής μέσω του πιστοποιητικού CSSP είναι το Cyber Security Evaluation Tool (CSET). Αυτό το εργαλείο αξιολόγησης βασίζεται στα βιομηχανικά πρότυπα που βρίσκονται σε συστήματα IT και ICS. Αξιολογεί τη στάση ασφαλείας ενός πεδίου βασιζόμενο στις απαντήσεις από μια σειρά ερωτήσεων που αναπτύχθηκαν με βάση τα πρότυπα. Το CSET παρέχει επίσης έναν τρόπο εισαγωγής ενός διαγράμματος των συστημάτων ICS με ερωτήσεις που αντιστοιχούν σε κάθε στοιχείο του διαγράμματος. Τέλος, το εργαλείο CSET παρέχει αναφορές που υποδεικνύουν περιοχές όπου μια εγκατάσταση μπορεί να βελτιωθεί και περιοχές που θα πρέπει να αντιμετωπιστούν πρώτα.

8.3 Ανίχνευση Περιστατικών

Η έγκαιρη ανίχνευση ενός περιστατικού βοηθάει στον περιορισμό ή ακόμη και στην πρόληψη πιθανών ζημιών στο περιβάλλον ICS και μειώνει τις προσπάθειες για περιορισμό, εξάλειψη, ανάκτηση και αποκατάσταση των επηρεαζόμενων συστημάτων.

Παρακάτω αναφέρονται οι βασικές μέθοδοι ανίχνευσης περιστατικών ασφάλειας στον κυβερνοχώρο.

- Αναφορά και συντονισμός ύποπτων και γνωστών περιστατικών, ώστε οι εμπειρογνώμονες να κατανοήσουν και να βρουν λύσεις για το περιστατικό εγκαίρως.
- Ανίχνευση με παρατήρηση του χρήστη για μη φυσιολογική συμπεριφορά του συστήματος ή των συστατικών των ICS.
- Ατόματη ανίχνευση μέσω εφαρμογών ή ρουτίνων, όπως οθόνες δικτύου, εφαρμογές ανάλυσης κίνησης δικτύου, IDS και προγράμματα προστασίας από ιούς που μπορούν να εντοπίσουν και να επισημάνουν κακόβουλα προγράμματα, απόπειρες εισβολής, παραβιάσεις πολιτικής και εκμεταλλεύσεις, καθώς και αποτυχία των συστατικών των ICS.
- Οι αυτοματοποιημένες μέθοδοι εντοπισμού περιστατικών είναι χρήσιμες για την αποτροπή εκμεταλλεύσεων των ευπαθειών που έχουν τα συστήματα ICS. Τα περισσότερα δικτυακά ICS έχουν κάποιο είδος αυτοματοποιημένης ικανότητας ανίχνευσης. Αυτό μπορεί να περιλαμβάνει είτε εξελιγμένα IDS που συνδέονται με τα δίκτυα ICS ή μια απλή καταγραφή Firewall. Ο αυτοματοποιημένος εντοπισμός περιστατικών θα πρέπει να είναι σωστα διαμορφωμένος στις εφαρμογές αυτές.
- Εργαλεία απόκρισης περιστατικών χρήσιμα για την παρακολούθηση, καταγραφή και ανάλυση πιο συγκεκριμένων και λεπτομερών δεδομένων όπως Netflow Capture and Analysis, Network Performance Monitors, Application Monitors, Packet and Traffic Reconstructors, Protocol Analyzer και Trace Route / Whois tools.
- Μόλις προσδιοριστεί το περιστατικό, η επίθεση στον κυβερνοχώρο πρέπει να κατηγοριοποιηθεί και να δοθεί προτεραιότητα στην απόκριση βάσει αυτής της κατηγοριοποίησης. Η κατηγοριοποίηση πρέπει να βασίζεται στον τύπο του περιστατικκού και την πιθανή ζημιά στο σύτσημα ICS σύμφωνα με τα βήματα του Σχεδιού Απόκρισης Περιστατικών.

8.4 Περιορισμός Περιστατικών

Ενώ ο περιορισμός εστιάζει συχνά στην πρόληψη της διάδοσης και των επιπτώσεων που μπορεί να έχει ένα κακόβουλο λογισμικό μέσω της εγκατάστασης ενός λογισμικού προστασίας από ιούς, υπάρχουν περιστατικά που περιορίζονται με άλλες ενέργειες. Ένα παράδειγμα θα ήταν ένας υπάλληλος που αποκτά πρόσβαση σε μη εξουσιοδοτημένες πληροφορίες μέσω του λογαριασμού και του κωδικού ενός

άλλου χρήστη. Ο περιορισμός της κατάστασης θα απαιτούσε τη διαγραφή πρόσβασης του χρήστη και, στη συνέχεια, την επιβολή πειθαρχικών μέτρων, όπως προβλέπεται. Για έναν εισβολέα που δεν άφησε κακόβουλο λογισμικό στο σύστημα, αλλά είχε άμεση πρόσβαση στα συστήματα ICS, ο περιορισμός θα περιλάμβανε τον αποκλεισμό του εισβολέα, την αποκατάσταση του εξοπλισμού, εάν επηρεαστεί, και στη συνέχεια την εφαρμογή προστατευτικών βημάτων.

Ο περιορισμός του κακόβουλου λογισμικού δεν ακολουθεί μια τυπική προσέγγιση για κάθε οργανισμό. Ποικίλλει ανάλογα με τον τύπο του κακόβουλου λογισμικού, την κρισιμότητα του επηρεαζόμενου συστήματος καθώς και το αποδεκτό επίπεδο κινδύνου.

Υπάρχουν διάφορες μέθοδοι διαθέσιμες για τον περιορισμό ένος περιστατικού και κάθε οργανισμός πρέπει να καθορίζει τις κατάλληλες ενέργειες περιορισμού βάσει των απαιτήσεων των συστημάτων ICS που διαθέτουν. Μερικές από αυτές είναι οι αυτοματοποιημένες τεχνολογίες, όπως τα προγράμματα απομάκρυνσης ιών για την εξάλειψη του προβλήματος και την αποκατάσταση των λειτουργιών του συστήματος, η διακοπή των υπηρεσιών ενώ αντιμετωπίζεται το περιστατικό και η απόκλιση ορισμένων τύπων συνδεσιμότητας δικτύου χρησιμοποιώντας μια διαδικασία φιλτραρίσματος μέσω Firewall.

8.5 Αποκατάσταση

Πριν από την πλήρη ανάκτηση του συστήματος, θα πρέπει να γίνουν προσπάθειες αποκατάστασης για να διορθωθεί η πηγή του προβλήματος. Αυτό μπορεί να περιλαμβάνει την εξάλειψη τυχόν κακόβουλου λογισμικού που έχει παραμείνει στο σύστημα, την αφαίρεση ή αντικατάσταση ευάλωτου εξοπλισμού, την αναδιάρθρωση και την επιδιόρθωση εξοπλισμού ή λογισμικού και πιθανή ακύρωση πρόσβασης για συγκεκριμένο προσωπικό.

Η πιο συνηθισμένη μέθοδος είναι η χρήση αυτοματοποιημένων εργαλείων εξάλειψης, όπως ενός λογισμικού προστασίας από ιούς, βοηθητικά προγράμματα εντοπισμού και αφαίρεσης spyware και λογισμικό διαχείρισης ενημερώσεων κώδικα. Άλλες επιλογές περιλαμβάνουν την επαναφορά ενός συστήματος σε ένα καθορισμένο σημείο πριν από τη μόλυνση ή την επαναφόρτωση των βασικών αρχείων συστήματος.

Όταν ολοκληρωθούν οι προσπάθειες εξάλειψης, συνιστάται ιδιαίτερα να πραγματοποιούνται δοκιμές για να επαληθευτεί ότι το συγκεκριμένο σύστημα ICS λειτουργεί όπως προορίζεται. Αυτό περιλαμβάνει τη συνεχή παρατήρηση αλλά και την εξέταση τυχόν πληροφοριών ανίχνευσης περιστατικών για την αναζήτηση συγκεκριμένων σημείων υπολειπόμενου κώδικα των εισβολέων.

8.6 Ανάκτηση

Το περιβάλλον ICS έχει πολυπλοκότητες που σχετίζονται με την ανάκτηση και την αποκατάσταση των συστημάτων που δεν θα βρεθούν σε τυπικά συστήματα πληροφορικής. Ωστόσο, ορισμένες ομοιότητες με τα παραδοσιακά IT συστήματα είναι η αφαίρεση κακόβουλου λογισμικού, η επαναφορά αντιγράφων ασφαλείας δεδομένων σε βάσεις δεδομένων, η κατάργηση συστηματικών προσωρινών ενεργειών περιορισμού και η επανεκκίνηση όλων των λειτουργικών συστημάτων και εφαρμογών.

Κατά τη διάρκεια της απόκρισης σε περιστατικά οι υπηρεσίες των συστημάτων ICS δεν πρέπει να σταματήσουν τη λειτουργία τους και αυτό πολλές φορές είναι πολύπλοκο. Ορισμένες προσεγγίσεις στο πρόβλημα αυτό θα μπορούσε να είναι η εναλλαγή των λειτουργιών ελέγχου σε συστήματα αποτυχίας, η μετάβαση σε εφεδρικό εξοπλισμό που είναι προσωρινός ή έχει περιορισμένες δυνατότητες, ή η απομόνωση των στοιχείων του συστήματος από την πρόσβαση στο δίκτυο. Σε αυτές τις καταστάσεις, ο κρίσιμος εξοπλισμός και οι διαδικασίες συνεχίζουν να λειτουργούν, αλλά σε προσωρινή κατάσταση με περιορισμένη ενσωμάτωση και λειτουργικότητα. Αυτό όμως φέρει υψηλό κίνδυνο για έναν οργανισμό καθώς τα συστήματα ICS πρέπει να είναι σε συνεχή λειτουργία.

Συνεπώς, θα πρέπει να είναι διαθέσιμα και τεκτμηριωμένα λεπτομερή Σχέδια Επιχειρισιακής Συνέχειας και θα πρέπει να δοκιμάζονται με όλα τα πιθανά σενάρια διακοπής των υπηρεσιών και λειτουργιών των

συστημάτων ICS, προκειμένου να πραγματοποιείται γρήγορη ανάκτηση και αποκατάσταση, προτού γίνει ανεπανόρθωτη ζημιά.

8.7 Ανάλυση μετά από Περιστατικά

Η ανάλυση και η εγκληματολογία μετά το περιστατικό περιλαμβάνουν τρεις θεματικούς τομείς. Ο πρώτος τομέας είναι τα διδάγματα που αντλήθηκαν όπου γίνεται μια προσπάθεια ανάλυσης του περιστατικού, της απόκρισης και της επίπτωσης ώστε να ανακαλυφθεί και να τεκμηριωθεί τι θα μπορούσε να είχε γίνει διαφορετικά για τη βελτίωση της απόκρισης. Ο δεύτερος τομέας είναι η πρόληψη υποτροπών ή η εφαρμογή όσων μάθαμε για την αποκατάσταση των ευπαθειών που εντοπίστηκαν στο πρόγραμμα ασφαλείας στον κυβερνοχώρο, συμπεριλαμβανομένης της πρόληψης παρόμοιου περιστατικού. Τέλος, ο τρίτος τομέας είναι η εγκληματολογία, η οποία περιλαμβάνει τη σύλληψη και την προστασία δεδομένων ως απόδειξη σε μια πιθανή νομική δράση.

9 Συμπεράσματα

Καθώς τα ICS αναπτύσσονται σε πολυπλοκότητα και συνδέονται με επιχειρηματικά και εξωτερικά δίκτυα, αυξάνεται επίσης ο αριθμός των πιθανών ζητημάτων ασφάλειας και των σχετικών κινδύνων. Η μεγάλη ποικιλία επιθέσεων που στοχεύουν πολλαπλούς πόρους σε συστήματα ελέγχου μπορεί να προκαλέσει ασύγχρονες επιθέσεις για μεγάλο χρονικό διάστημα και θα μπορούσε να στοχεύσει πολλαπλές αδυναμίες σε ένα περιβάλλον συστήματος ελέγχου. Οι οργανισμοί δεν μπορούν να βασίζονται σε ένα μόνο αντίμετρο για τον μετριασμό όλων των ζητημάτων ασφαλείας. Προκειμένου να προστατεύσουν αποτελεσματικά τα ICS από επιθέσεις που βασίζονται στον κυβερνοχώρο, οι οργανισμοί πρέπει να εφαρμόσουν πολλαπλά αντίμετρα - μειώνοντας έτσι τον κίνδυνο χρησιμοποιώντας ένα σύνολο τεχνικών μετριασμού της ασφάλειας. Πρέπει να σημειωθεί ότι τα προτεινόμενα μέτρα δεν προστατεύουν και δεν μπορούν να προστατεύσουν όλες τις ευπάθειες και τις αδυναμίες σε ένα περιβάλλον ICS. Εφαρμόζονται, κυρίως, για να επιβραδύνουν έναν εισβολέα ώστε να επιτρέπουν στο προσωπικό της πληροφορικής του IT και του OT να εντοπίζει και να αποκρίνεται σε συνεχιζόμενες απειλές, ή να κάνει την προσπάθεια, από την πλευρά του εισβολέα πιο δισκίνητη και δύσκολη.

Προκειμένου να βελτιωθεί το επίπεδο ασφάλειας, η ανθεκτικότητα των συστημάτων ICS και οι λειτουργίες του δικτύου επικοινωνίας, παρακάτω παρουσιάζονται τα πιο βασικά συμπεράσματα από την μελέτη.

- Η ασφάλεια πρέπει να συμπεριλαμβάνεται ως κύριο μέλημα κατά τη φάση σχεδιασμού των συστημάτων ICS.
- Πρέπει να καθορίζονται οι ρόλοι και οι αρμοδιότητες των ατόμων που λειτουργούν τα συστήματα ICS.
- Οι τεχνολογίες και η αρχιτεκτονική του δικτύου πρέπει να σχεδιάζονται μέσα από το ασφαλέστερο και πιο διαδεδομένο μοντέλο αρχιτεκτονικής για συστήματα ICS, το Purdue Model.
- Ο εξοπλισμός και τα συστήματα ICS, πρέπει να προστατεύονται από φυσική πρόσβαση και να παρακολουθούνται διαρκώς.
- Πρέπει να δημιουργούνται κανάλια ανταλλαγής ιδεών και επικοινωνίας για τους διάφορους συμμετέχοντες στον κύκλο ζωής των συσκευών για την ανταλλαγή αναγκών και λύσεων.
- Πρέπει να υπάρχει διαδικασία περιοδικής ενημέρωσης των συσκευών, η οποία να αποτελεί μέρος των κύριων λειτουργιών των συστημάτων.
- Πρέπει να υπάρχει και να ακολουθείται η διαδικασία απόκρισης περιστατικών.
- Πρέπει να υπάρχει συνεχής εκπαίδευση και ευαισθητοποίηση για τα συστήματα και το περιβάλλον ICS εντός του οργανισμού.
- Πρέπει να προωθείται η αυξημένη συνεργασία μεταξύ των υπευθύνων λήψης αποφάσεων, των κατασκευαστών και των φορέων εκμετάλλευσης.
- Πρέπει να καθιερώνονται κατευθυντήριες γραμμές για τη θέσπιση αξιόπιστων και κατάλληλων απαιτήσεων ασφάλειας στον κυβερνοχώρο.

10 Παράρτημα Ι – Συγκριτικοί Πίνακες Προτεινόμενων Μέτρων NIST και NERC-CIP

Στο παράρτημα αυτό, παρουσιάζονται δύο πίνακες σε αντιστοιχία με τα προτεινόμενα μέτρα του προτύπου NIST 800-53 και του κανονισμού NERC-CIP. Ο πρώτος πίνακας αντιστοιχεί τις κατηγορίες των προτεινόμενων μέτρων του NERC-CIP με τα προτεινόμενα μέτρα του NIST και ο δεύτερος πίνακας αντιστοιχεί τις κατηγορίες των προτεινόμενων μέτρων του NIST με τα προτεινόμενα μέτρα του NERC-CIP.

Στον παρακάτω πίνακα εμφανίζονται τα προτεινόμενα μέτρα κατά NERC-CIP σε αντιστοιχία με τα προτεινόμενα μέτρα του NIST ανά κατηγορία στην οποία ανήκουν.

NERC-CIP Control Requirements	NIST 800-53
Standard CIP-002-5.1a – Cyber Security – BES Cyber System Categorization	
R1. Asset Inventory	
R2. Asset Inventory	
Standard CIP-003-8 – Cyber Security – Security Management Controls	
R1. Cyber Security Policies	
R2. Cyber Security Plan(s)	PL-2 System Security and Privacy Plans AT-1 Security Awareness and Training Policy and Procedures SC-7 Boundary Protection IR-1 Incident Response Policy and Procedures
R3. Identify CIP Senior Manager	CA-6 Authorization
R4. Authority Delegation	CA-6 Authorization
Standard CIP-004-6 Cyber Security – Personnel & Training	
R1. Security Awareness Program	AT-1 Security Awareness and Training Policy and Procedures AT-2 Literacy Training and Awareness
R2. Cyber Security Training Program	AT-1 Security Awareness and Training Policy and Procedures AT-2 Literacy Training and Awareness AT-3 Role-Based Training AT-4 Training Records CP-3 Contingency Training IR-2 Incident Response Training
R3. Personnel Risk Assessment Program	IA-5 Authenticator Management PS-2 Position Risk Designation PS-3 Personnel Screening
R4. Access Management Program	AC-2 Account Management AC-3 Access Enforcement PE-2 Physical Access Authorization
R5. Access Revocation	PS-4 Personnel Termination AC-2 Account Management PE-2 Physical Access Authorizations
Standard CIP-005-6 – Cyber Security – Electronic Security Perimeter(s)	
R1. Electronic Security Perimeter	SC-7 Boundary Protection

	SI-4 System Monitoring AU-2 Event Logging AU-13 Monitoring for Information Disclosure
R2. Interactive Remote Access	AC-3 Access Enforcement AC-17 Remote Access IA-2 Identification and Authentication (Organizational Users)
Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems	
R1. Physical Security Plan	PE-1 Physical and Environmental Protection Policy and Procedures PE-3 Physical Access Control PE-6 Monitoring Physical Access AU-11 Audit Record Retention PE-9 Power Equipment and Cabling
R2. Visitor Control Program	PE-1 Physical and Environmental Protection Policy and Procedures PE-3 Physical Access Control PE-8 Visitor Access Records AU-11 Audit Record Retention
R3. Physical Access Control System Maintenance and Testing Program	PE-3 Physical Access Control
Standard CIP-007-6 – Cyber Security – System Security Management	
R1. Ports and Services	CM-7 Least Functionality SC-7 Boundary Protection CM-8 System Component Inventory
R2. Security Patch Management	SI-2 Flaw Remediation CA-5 Plan of Action and Milestones
R3. Malicious Code Prevention	SI-3 Malicious Code Protection SI-2 Flaw Remediation
R4. Security Event Monitoring	SI-4 System Monitoring AU-2 Event Logging AU-4 Audit Log Storage Capacity AU-6 Audit Record Review, Analysis, and Reporting AU-11 Audit Record Retention
R5. System Access Control	IA-2 Identification and Authentication (Organizational Users) IA-5 Authenticator Management AC-6 Least Privilege AC-7 Unsuccessful Logon Attempts
Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning	
R1. Cyber Security Incident Response Plan Specifications	IR-1 Incident Response Policy and Procedures IR-4 Incident Handling IR-6 Incident Reporting IR-8 Incident Response Plan
R2. Cyber Security Incident Response Plan Implementation and Testing	IR-1 Incident Response Policy and Procedures IR-3 Incident Response Testing IR-8 Incident Response Plan

R3. Cyber Security Incident Response Plan Implementation and Testing	IR-1 Incident Response Policy and Procedures IR-8 Incident Response Plan
Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems	
R1. Recovery Plan Specifications	CP-1 Contingency Planning Policy and Procedures CP-2 Contingency Plan CP-9 System Backup CP-10 System Recovery and Reconstitution AU-9 Protection of Audit Information
R2. Recovery Plan Implementation and Testing	CP-4 Contingency Plan Testing
R3. Recovery Plan Review, Update and Communication	CP-4 Contingency Plan Testing
Standard CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments	
R1. Configuration Change Management	CM-2 Baseline Configuration CM-3 Configuration Change Control CM-4 Impact Analysis CM-6 Configuration Settings
R2. Configuration Monitoring	CM-2 Baseline Configuration CM-3 Configuration Change Control CM-5 Access Restrictions for Change CM-6 Configuration Settings
R3. Vulnerability Assessment	CA-7 Continuous Monitoring CA-8 Penetration Testing RA-5 Vulnerability Monitoring and Scanning CM-4 Impact Analysis CA-5 Plan of Action and Milestones
R4. Transient Cyber Assets and Removable Media	AC-19 Access Control for Mobile Devices MP-4 Media Storage MP-7 Media Use
Standard CIP-011-2 – Cyber Security – Information Protection	
R1. Information Protection	MP-1 Media Protection Policy and Procedures MP-4 Media Storage MP-5 Media Transport MP-7 Media Use SC-28 Protection of Information at Rest
R2. Information Protection	MP-6 Media Sanitization
Standard CIP-013-1 – Cyber Security – Supply Chain Risk Management	
R1. Supply Chain Cyber Security Risk Management Plan	SR-2 Supply Chain Risk Management Plan SR-3 Supply Chain Controls and Processes
R2. Supply Chain Cyber Security Risk Management Plan Implementation	SR-2 Supply Chain Risk Management Plan SR-3 Supply Chain Controls and Processes
R3. Senior Manager Approval	--
Standard CIP-014-2 – Physical Security	
R1. Risk Assessment	--
R2. Third Party Verification	--
R3. Assessment Completion Notification	--

R4. Potential Threat and Vulnerability evaluation	AU-6 Audit Record Review, Analysis, and Reporting
R5. Physical Security Plan	PE-1 Physical and Environmental Protection Policy and Procedures
R6. Third Party Evaluation	--

Στον παρακάτω πίνακα είναι ομαδοποιημένα τα προτεινόμενα μέτρα κατά NIST σε αντιστοιχία με τα προτεινόμενα μέτρα του NERC-CIP ανά κατηγορία στην οποία ανήκουν.

Control Number	NIST SP 800-53 r5	NERC CIP
ACCESS CONTROL		
AC-1	Access Control Policy and Procedures	
AC-2	Account Management	CIP 004-6 (R4, R5)
AC-3	Access Enforcement	CIP 004-6 (R4), CIP 005-6 (R2)
AC-4	Information FXAMHΛO Enforcement	
AC-5	Separation of Duties	
AC-6	Least Privilege	CIP 007-6 (R5)
AC-7	Unsuccessful Login Attempts	CIP 007-6 (R5)
AC-8	System Use Notification	
AC-9	Previous Logon Notification	
AC-10	Concurrent Session Control	
AC-11	Device Lock	
AC-12	Session Termination	
AC-14	Permitted Actions without Identification or Authentication	
AC-16	Security and Privacy Attributes	
AC-17	Remote Access	CIP 005-6 (R2)
AC-18	Wireless Access	
AC-19	Access Control for Mobile Devices	CIP 010-3 (R4)
AC-20	Use of External Systems	
AC-21	Information Sharing	
AC-22	Publicly Accessible Content	
AC-23	Data Mining Protection	
AC-24	Access Control Decisions	
AC-25	Reference Monitor	
AWARENESS AND TRAINING		
AT-1	Security Awareness and Training Policy and Procedures	CIP 003-8 (R2), CIP 004-6 (R1, R2)
AT-2	Literacy Training and Awareness	CIP 004-6 (R1)
AT-3	Role-Based Training	CIP 004-6 (R2)
AT-4	Training Records	CIP 004-6 (R2)

AT-6	Training Feedback	
AUDIT AND ACCOUNTABILITY		
AU-1	Audit and Accountability Policy and Procedures	
AU-2	Event Logging	CIP 005-5 (R1), CIP 007-6 (R4)
AU-3	Content of Audit Records	CIP 007-3 (R5.1.2)
AU-4	Audit Log Storage Capacity	CIP 007-6 (R4)
AU-5	Response to Audit Logging Processing Failures	
AU-6	Audit Record Review, Analysis, and Reporting	CIP 007-6 (R4), CIP 014-2 (R4)
AU-7	Audit Record Reduction and Report Generation	
AU-8	Time Stamps	
AU-9	Protection of Audit Information	CIP 009-6 (R1)
AU-10	Non-repudiation	
AU-11	Audit Record Retention	CIP 006-6 (R1, R2), CIP 007-6 (R4)
AU-12	Audit Record Generation	
AU-13	Monitoring for Information Disclosure	CIP 005-6 (R1)
AU-14	Session Audit	
AU-16	Cross-Organizational Audit Logging	
ASSESSMENT, AUTHORIZATION, AND MONITORING		
CA-1	Assessment, Authorization and Monitoring Policies and Procedures	
CA-2	Control Assessments	
CA-3	Information Exchange	
CA-5	Plan of Action and Milestones	CIP 010-3 (R3)
CA-6	Authorization	CIP 003-8 (R3, R4)
CA-7	Continuous Monitoring	CIP 010-3 (R3)
CA-8	Penetration Testing	CIP 010-3 (R3)
CA-9	Internal System Connections	
CONFIGURATION MANAGEMENT		
CM-1	Configuration Management Policy and Procedures	
CM-2	Baseline Configuration	CIP 010-3 (R1, R2)
CM-3	Configuration Change Control	CIP 010-3 (R1, R2)
CM-4	Impact Analysis	CIP 010-3 (R1, R3)
CM-5	Access Restrictions for Change	CIP 010-3 (R2)
CM-6	Configuration Settings	CIP 010-3 (R1, R2)
CM-7	Least Functionality	CIP 007-6 (R1)
CM-8	System Component Inventory	CIP 007-6 (R1)

CM-9	Configuration Management Plan	
CM-10	Software Usage Restrictions	
CM-11	User-Installed Software	
CM-12	Information Location	
CM-13	Data Action Mapping	
CM-14	Signed Components	
CONTINGENCY PLANNING		
CP-1	Contingency Planning Policy and Procedures	CIP 009-6 (R1)
CP-2	Contingency Plan	CIP 009-6 (R1)
CP-3	Contingency Training	CIP-004-6 (R2)
CP-4	Contingency Plan Testing	CIP 009-6 (R2, R3)
CP-6	Alternate Storage Sites	
CP-7	Alternate Processing Site	
CP-8	Telecommunications Services	
CP-9	System Backup	CIP 009-6 (R1)
CP-10	System Recovery and Reconstitution	CIP 009-6 (R1)
CP-11	Alternate Communications Protocols	
CP-12	Safe Mode	
CP-13	Alternative Security Mechanisms	
IDENTIFICATION AND AUTHENTICATION		
IA-1	Identification and Authentication Policy and Procedures	
IA-2	Identification and Authentication (Organizational Users)	CIP 005-6 (R2), CIP 007-6 (R5)
IA-3	Device Identification and Authentication	
IA-4	Identifier Management	
IA-5	Authenticator Management	CIP-004-6 (R3), CIP 007-6 (R5)
IA-6	Authentication Feedback	
IA-7	Cryptographic Module Authentication	
IA-8	Identification and Authentication (Non-Organizational Users)	
IA-9	Service Identification and Authentication	
IA-10	Adaptive Authentication	
IA-11	Re-authentication	
IA-12	Identity Proofing	
INCIDENT RESPONSE		
IR-1	Incident Response Policy and Procedures	CIP 008-6 (R1, R2, R3)
IR-2	Incident Response Training	CIP-004-6 (R2)
IR-3	Incident Response Testing	CIP 008-6 (R2)
IR-4	Incident Handling	CIP 008-6 (R1)

IR-5	Incident Monitoring	
IR-6	Incident Reporting	CIP 008-6 (R1)
IR-7	Incident Response Assistance	
IR-8	Incident Response Plan	CIP 008-6 (R1, R2, R3)
IR-9	Information Spillage Response	
MAINTENANCE		
MA-1	Maintenance Policy and Procedures	
MA-2	Controlled Maintenance	
MA-3	Maintenance Tools	
MA-4	Nonlocal Maintenance	
MA-5	Maintenance Personnel	
MA-6	Timely Maintenance	
MA-7	Field Maintenance	
MEDIA PROTECTION		
MP-1	Media Protection Policy and Procedures	CIP 011-2 (R1)
MP-2	Media Access	
MP-3	Media Marking	
MP-4	Media Storage	CIP 010-3 (R4), CIP 011-2 (R1)
MP-5	Media Transport	CIP 011-2 (R1)
MP-6	Media Sanitization	CIP 011-2 (R2)
MP-7	Media Use	CIP 010-3 (R4), CIP 011-2 (R1)
MP-8	Media Downgrading	
PHYSICAL AND ENVIRONMENTAL PROTECTION		
PE-1	Physical and Environmental Protection Policy and Procedures	CIP 006-6 (R1, R2), CIP 014-2 (R5)
PE-2	Physical Access Authorizations	CIP 004-6 (R4, R5)
PE-3	Physical Access Control	CIP 006-6 (R1, R2, R3)
PE-4	Access Control for Transmission	
PE-5	Access Control for Output Devices	
PE-6	Monitoring Physical Access	CIP 006-6 (R1)
PE-8	Visitor Access Records	CIP 006-6 (R2)
PE-9	Power Equipment and Cabling	CIP 006-6 (R1)
PE-10	Emergency Shutoff	
PE-11	Emergency Power	
PE-12	Emergency Lighting	
PE-13	Fire Protection	
PE-14	Environmental Controls	
PE-15	Water Damage Protection	
PE-16	Delivery and Removal	
PE-17	Alternate Work Site	

PE-18	Location of System Components	
PE-19	Information Leakage	
PE-20	Asset Monitoring and Tracking	
PE-21	Electromagnetic Pulse Protection	
PE-22	Component Marking	
PE-23	Facility Location	
PLANNING		
PL-1	Planning and Procedures	
PL-2	System Security and Privacy Plans	CIP 003-8 (R2)
PL-4	Rules of Behavior	
PL-7	Concept of Operations	
PL-8	Security and Privacy Architectures	
PL-9	Central Management	
PL-10	Baseline Selection	
PL-11	Baseline Tailoring	
PROGRAM MANAGEMENT		
PM-1	Information Security Program Plan	
PM-2	Information Security Program Leadership Role	
PM-3	Information Security and Privacy Resources	
PM-4	Plan of Action and Milestones Process	
PM-5	System Inventory	
PM-6	Measures of Performance	
PM-7	Enterprise Architecture	
PM-8	Critical Infrastructure Plan	
PM-9	Risk Management Strategy	
PM-10	Authorization Process	
PM-11	Mission and Business Process Definition	
PM-12	Insider Threat Program	
PM-13	Security and Privacy Workforce	
PM-14	Testing, Training, and Monitoring	
PM-15	Security and Privacy Groups and Associations	
PM-16	Threat Awareness Program	
PM-17	Protecting Controlled Unclassified Information on External Systems	
PM-18	Privacy Program Plan	
PM-19	Privacy Program Leadership Role	
PM-20	Dissemination of Privacy Program Information	
PM-21	Accounting of Disclosures	

PM-22	Personally Identifiable Information Quality Management	
PM-23	Data Governance Body	
PM-24	Data Integrity Board	
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	
PM-26	Complaint Management	
PM-27	Privacy Reporting	
PM-28	Risk Framing	
PM-29	Risk Management Program Leadership Roles	
PM-30	Supply Chain Risk Management Strategy	
PM-31	Continuous Monitoring Strategy	
PM-32	Purposing	
PERSONNEL SECURITY		
PS-1	Personnel Security Policy and Procedures	
PS-2	Position Risk Designation	CIP 004-6 (R3)
PS-3	Personnel Screening	CIP 004-6 (R3)
PS-4	Personnel Termination	CIP 004-6 (R5)
PS-5	Personnel Transfer	
PS-6	Access Agreements	
PS-7	External Personnel Security	
PS-8	Personnel Sanctions	
PS-9	Position Descriptions	
PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY		
PT-1	PII Processing and Transparency Policy and Procedures	
PT-2	Authority to Process Personally Identifiable Information	
PT-3	Personally Identifiable Information Processing Purposes	
PT-4	Consent	
PT-5	Privacy Notice	
PT-6	System of Records Notice	
PT-7	Specific Categories of Personally Identifiable Information	
PT-8	Computer Matching Requirements	
RISK ASSESSMENT		
RA-1	Risk Assessment Policy and Procedures	
RA-2	Security Categorization	
RA-3	Risk Assessment	

RA-5	Vulnerability Monitoring and Scanning	CIP 010-3 (R3)
RA-6	Technical Surveillance Countermeasures Survey	
RA-7	Risk Response	
RA-8	Privacy Impact Assessments	
RA-9	Criticality Analysis	
RA-10	Threat Hunting	
SYSTEM AND SERVICES ACQUISITION		
SA-1	System and Services Acquisition Policy and Procedures	
SA-2	Allocation of Resources	
SA-3	System Development Life Cycle	
SA-4	Acquisition Process	
SA-5	System Documentation	
SA-8	Security and Privacy Engineering Principles	
SA-9	External System Services	
SA-10	Developer Configuration Management	
SA-11	Developer Testing and Evaluation	
SA-15	Development Process, Standards, and Tools	
SA-16	Developer-Provided Training	
SA-17	Developer Security and Privacy Architecture and Design	
SA-20	Customized Development of Critical Components	
SA-21	Developer Screening	
SA-22	Unsupported System Components	
SA-23	Specialization	
SYSTEM AND COMMUNICATIONS PROTECTION		
SC-1	System and Communications Protection Policy and Procedures	
SC-2	Separation of System and User Functionality	
SC-3	Security Function Isolation	
SC-4	Information in Shared System Resources	
SC-5	Denial-of-Service Protection	
SC-6	Resource Availability	
SC-7	Boundary Protection	CIP 003-8 (R2), CIP 005-6 (R1), CIP 007-6 (R1)
SC-8	Transmission Confidentiality and Integrity	
SC-10	Network Disconnect	
SC-11	Trusted Path	

SC-12	Cryptographic Key Establishment and Management	
SC-13	Cryptographic Protection	
SC-15	Collaborative Computing Devices and Applications	
SC-16	Transmission of Security and Privacy Attributes	
SC-17	Public Key Infrastructure Certificates	
SC-18	Mobile Code	
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	
SC-22	Architecture and Provisioning for Name/Address Resolution Service	
SC-23	Session Authenticity	
SC-24	Fail in Known State	
SC-25	Thin Nodes	
SC-26	Decoys	
SC-27	Platform-Independent Applications	
SC-28	Protection of Information at Rest	CIP 011-2 (R1)
SC-29	Heterogeneity	
SC-30	Concealment and Misdirection	
SC-31	Covert Channel Analysis	
SC-32	System Partitioning	
SC-34	Non-Modifiable Executable Programs	
SC-35	External Malicious Code Identification	
SC-36	Distributed Processing and Storage	
SC-37	Out-of-Band Channels	
SC-38	Operations Security	
SC-39	Process Isolation	
SC-40	Wireless Link Protection	
SC-41	Port and I/O Device Access	
SC-42	Sensor Capability and Data	
SC-43	Usage Restrictions	
SC-44	Detonation Chambers	
SC-45	System Time Synchronization	
SC-46	Cross Domain Policy Enforcement	
SC-47	Alternate Communications Paths	
SC-48	Sensor Relocation	

SC-49	Hardware-Enforced Separation and Policy Enforcement	
SC-50	Software-Enforced Separation and Policy Enforcement	
SC-51	Hardware-Based Protection	
SYSTEM AND INFORMATION INTEGRITY		
SI-1	System and Information Integrity Policy and Procedures	
SI-2	Flaw Remediation	CIP 007-6 (R2, R3)
SI-3	Malicious Code Protection	CIP 007-6 (R3)
SI-4	System Monitoring	CIP 005-6 (R1), CIP 007-6 (R4)
SI-5	Security Alerts, Advisories, and Directives	
SI-6	Security and Privacy Functionality Verification	
SI-7	Software, Firmware, and Information Integrity	
SI-8	Spam Protection	
SI-10	Information Input Validation	
SI-11	Error Handling	
SI-12	Information Management and Retention	
SI-13	Predictable Failure Prevention	
SI-14	Non-Persistence	
SI-15	Information Output Filtering	
SI-16	Memory Protection	
SI-17	Fail-Safe Procedures	
SI-18	Personally Identifiable Information Quality Operations	
SI-19	De-Identification	
SI-20	Tainting	
SI-21	Information Refresh	
SI-22	Information Diversity	
SI-23	Information Fragmentation	
SUPPLY CHAIN RISK MANAGEMENT		
SR-1	Supply Chain Risk Management Policy and Procedures	
SR-2	Supply Chain Risk Management Plan	CIP 013-1 (R1, R2)
SR-3	Supply Chain Controls and Processes	CIP 013-1 (R1, R2)
SR-4	Provenance	
SR-5	Acquisition Strategies, Tools, and Methods	
SR-6	Supplier Assessments and Reviews	
SR-7	Supply Chain Operations Security	

SR-8	Notification Agreements	
SR-9	Tamper Resistance and Detection	
SR-10	Inspection of Systems or Components	
SR-11	Component Authenticity	
SR-12	Component Disposal	

Βιβλιογραφία

[1] Michael Nieles, Kelley Dempsey, Victoria Pillitteri, *"NIST SP 800-12 REV. 1 - An Introduction to Information Security*", 2017
[2] "*ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements",* 2013
[3] "*ISO/IEC 27002: 2013, Information technology - Security techniques - Code of practice for information security controls",* 2013
[4] *"ISO/IEC 27005:2018, Information Technology - Security Techniques - Information Security Risk Management"*, 2018
[5] *"ISO/IEC 27019:2017, Information technology - Security techniques - Information security controls for the energy utility industry",* 2017
[6] Michelle Michael, *"TUV-IT Whitepaper - Industrial Security based on IEC 62443 Version 1"*
[7] https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[8] https://www.ncsc.gov.uk/
[9] https://www.enisa.europa.eu/topics/nis-directive
[10] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn *"NIST 800-82r2 - Guide to Industrial Control Systems (ICS) Security"*, 2015
[11] https://blog.isa.org/top-10-differences-ics-cybersecurity
[12] Στασινός Συμεών, Αλεξίου Παναγιώτης "*Βιομηχανικά Συστήματα Ελέγχου SCADA & Προγραμματισμός με το SIMATIC WinCC 7.2*", 2016
[13] https://www.controlsystemsandautomation.com/learn/plc/plc-programming-basics-i/
[14] https://mec6004suheyb.wordpress.com/2016/03/12/architecture-of-plc/
[15] https://electrical-engineering-portal.com/scada-dcs-plc-rtu-smart-instrument
[16] https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant
[17] https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security
[18] Luciana Obregon, *"SANS – Secure Architecture Industrial Control Systems-36327"*, 2015
[19] Homeland Security, *"Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies",* 2016
[20] https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system/
[21] https://resources.infosecinstitute.com/topic/ics-protocols/
[22] Protocols and Network Security in ICS Infrastructures, May 2015, Spanish National Cybersecurity Institute
[23] https://www.fireeye.com/
[24] MITRE ATT&CK for Industrial Control Systems, https://collaborate.mitre.org/attackics/index.php/Main_Page
[25] Sagarika Ghosh, Srinivas Sampalli, *"IEEE Access - A Survey of Security in SCADA Networks: Current Issues and Future Challenges",* 2019
[26] ENISA, *"Communication network dependencies for ICS/SCADA Systems",* 2016
[27] Andrew Ginter, "*The Top 20 Cyberattacks on Industrial Control Systems, VP Industrial Security, Waterfall Security Solutions Version 1.1"*, 2018
[28] Rajesh Kalluri, Lagineni Mahendra, R.K. Senthil Kumar, G.L. Ganga Prasad, *"Simulation and Impact Analysis of Denial-of-Service Attacks on Power SCADA"*
[29] Ntouskas, T. and Polemi, N. (2012) "*STORM-RM: a collaborative and multicriteria risk management methodology*", Int. J. Multicriteria Decision Making, Vol. 2, No. 2, pp.159–177.
[30] T. Ntouskas, G. Pentafronimos, and S. Papastergiou: *STORM - Collaborative Security Management Environment*, C.A. Ardagna and J. Zhou (Eds.): WISTP 2011, LNCS 6633, pp. 320–335, 2011.
[31] NIST 800-53 revision 5, *"Security and Privacy Controls for Information Systems and Organizations"*
[32] Homeland Security, *"Common Cybersecurity Vulnerabilities in Industrial Control Systems"*, 2011
[33] Homeland Security, "*Recommended Practice: Developing and Industrial Control systems Cybersecurity Incident Response Capability*", 2009