ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αξιολόγηση της ασφάλειας και απόδοσης των συστημάτων SCADA με εφαρμογή λογισμικών

ΠΑΠΑΓΕΩΡΓΙΟΥ ΔΗΜΗΤΡΙΟΣ

Επιβλέπων
ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ

Λαμία, 02/03/2017

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

02/03/2017

Ο ΔΗΛΩΝ

Τριμελής Επιτροπή:

ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ

ΤΣΟΥΚΑΛΑΣ ΕΛΕΥΘΕΡΙΟΣ

ΒΑΒΟΥΓΥΙΟΣ ΔΙΟΝΥΣΙΟΣ

Επιστημονικός Σύμβουλος:

Π. ΑΓΓΕΛΗΣ ΕΥΑΓΓΕΛΟΣ ΔΩΡΟΘΕΟΣ

Περιεχόμενα

1.1 Εισαγωγή στα συστήματα SCADA

Ξεκινώντας την περιγραφή των συστημάτων SCADA είναι σκόπιμο να αναφερθεί τι είναι το SCADA. Η λέξη SCADA αποτελεί τα αρχικά των λέξεων Supervisory Control And Data Acquisition System, δηλαδή σύστημα εποπτείας, ελέγχου και συλλογής πληροφοριών. Είναι συνεπώς συστήματα τηλεμετρίας και τηλεχειρισμού, τα οποία συλλέγουν πληροφορίες από διάφορες διεργασίες και χρησιμοποιούνται για τον εποπτικό έλεγχο.

Αρχικά υλοποιήθηκαν στο λειτουργικό σύστημα DOS(VMS) και το Unix αλλά τα τελευταία χρόνια οι προμηθευτές SCADA έχουν κινηθεί προς τα NT και μερικά επίσης προς το λειτουργικό Linux. Τα SCADA βρίσκουν τεράστιες εφαρμογές, τόσο σε βιομηχανικές μονάδες όσο και σε συστήματα μεταφοράς και διανομής ηλεκτρικής ενέργειας. Αυτό γιατί επιτρέπουν την διαχείριση και την εποπτεία ενός συστήματος που μπορεί να βρίσκεται αρκετές εκατοντάδες χιλιόμετρα μακριά από τον χώρο ελέγχου, όπως συνήθως συμβαίνει με τα συστήματα ηλεκτρικής ενέργειας, αλλά και στις μεγάλες βιομηχανικές μονάδες. Το μέγεθος τέτοιας σειράς εγκαταστάσεων εκτείνεται από το 1000 μέχρι 10.000 κανάλια εισόδου-εξόδου (I/0). Παρά όλα αυτά δεν συναντάμε συστήματα SCADA σε μικρομεσαίες βιομηχανικές μονάδες, λόγω του μεγάλου κόστους της υλικοτεχνικής υποδομής (hardware) αλλά και του λογισμικού (software). Ένα σύστημα SCADA είναι υπεύθυνο για την διαχείριση και τον έλεγχο διαφόρων διεργασιών, δηλαδή είναι υπεύθυνο για την παρακολούθηση, την καταγραφή και τον έλεγχο ενός πλήθους βασικών μεταβλητών και παραμέτρων του συστήματος.

Τα συστήματα SCADA παρακολουθούν on-line μέσω μονάδων Προγραμματιζόμενων Λογικών Ελεγκτών και καταγράφουν συνεχώς σε ηλεκτρονικούς υπολογιστές όλες τις κρίσιμες παραμέτρους της παραγωγικής διαδικασίας, για την επίτευξη εποπτείας σε πραγματικό χρόνο. Αυτά τα συστήματα καλύπτουν τη μεταφορά των δεδομένων μεταξύ ενός κεντρικού οικοδεσπότη υπολογιστή SCADA (central host PC) και διάφορες μονάδες απομακρυσμένων τερματικών (RTUs) και προγραμματιζόμενων λογικών ελεγκτών (PLCs), και τα τερματικά χειριστών. Παραδοσιακά, τα συστήματα SCADA έχουν χρησιμοποιηθεί στο δημόσιο δίκτυο μεταβίβασης (PSN) για λόγους ελέγχου. Σήμερα πολλά συστήματα ελέγχονται χρησιμοποιώντας την υποδομή του εταιρικού δικτύου Local Area Network (LAN) / Wide Area Network (WAN).

Οι ασύρματες τεχνολογίες τώρα πλέον ευρέως επεκτείνονται και χρησιμοποιούνται για λόγους του ελέγχου. Οι στόχοι του SCADA αναφέρονται ευθύς αμέσως:

- Η διασφάλιση της ποιότητας του παραγόμενου προϊόντος.
- Η μεγιστοποίηση της παραγωγής με χρήση των ελάχιστων δυνατών (ενεργειακών) πόρων.
- Η βέλτιστη διαχείριση του εξοπλισμού, των υλικών και της ενέργειας της εγκατάστασης.
- Η ασφάλεια του εξοπλισμού και του προσωπικού παρακολούθησης της διεργασίας.

Είναι σημαντικό όλοι οι παραπάνω στόχοι να επιτυγχάνονται παράλληλα. Δεν είναι δυνατό να επιδιώκουμε μεγιστοποίηση της παραγωγής χωρίς πρώτα να έχουμε εξασφαλίσει την βελτιστοποίηση διαχείρισης των διαθέσιμων πόρων και υλικών. Επιπλέον ο έλεγχος των διεργασιών θα πρέπει να είναι εξαιρετικά γρήγορος, ώστε να

έχουμε επίγνωση της κατάστασης των επιτηρούμενων μεγεθών σε πραγματικό χρόνο (real time).

Αυτό γίνεται αμέσως εμφανές αν αναφερθούμε στο θέμα της ασφάλειας. Η επέμβαση στις διεργασίες σε περίπτωση κινδύνου θα πρέπει να είναι άμεση και αποτελεσματική ώστε να αποφεύγουμε μερική ή ολική καταστροφή του εξοπλισμού, ακόμα και ανθρώπινες απώλειες. Εκτός των παραπάνω, ένα σύστημα SCADA μπορεί να επιτηρεί και να χειρίζεται ένα πλήθος μεταβλητών του συστήματος αυτομάτου ελέγχου, αλλά και να διαχειρίζεται και οικονομικά μεγέθη (παραγγελίες – παραδόσεις προϊόντων) σε συνεργασία με οικονομικά πακέτα, προκειμένου να παρέχει στον χειριστή του συνολική εποπτεία της παραγωγικής μονάδας.

Πιο συγκεκριμένα ένα σύστημα SCADA προσφέρει:

- Άμεση πληροφόρηση της κατάστασης της διεργασίας
- Αντιστάθμιση των μεταβλητών ελέγχου της διεργασίας με στόχο τη διατήρηση των δεδομένων ονομαστικών τους τιμών (set points) καθώς και τη διατήρηση των απαιτούμενων επιπέδων παραγωγής
- Έγκαιρη σήμανση των βλαβών και της κακής λειτουργίας του εξοπλισμού στις διάφορες διεργασίες, ώστε να παρέχεται η μέγιστη ασφάλεια του εξοπλισμού και των εργαζομένων
- Πρόγνωση και διάγνωση των βλαβών του εξοπλισμού και έγκαιρο εντοπισμό τους για την μεγιστοποίηση της διαθεσιμότητας του
- Καταγραφή και αποθήκευση πληροφοριών σχετικά με την παραγωγή και τη διαχείριση της
- Καλή λειτουργία του εξοπλισμού με στόχο τη βελτιστοποίηση της χρήσης και επομένως της παραγωγικότητας του.

Τα συστήματα SCADA επίσης αποτελούν εφαρμογή της βιομηχανικής πληροφορικής για την εποπτεία της παραγωγής. Κάθε διεργασία παραγωγής χαρακτηρίζεται από κάποιες κρίσιμες παραμέτρους, οι οποίες παίζουν καθοριστικό ρόλο στην παραγωγική διαδικασία και στην ποιότητα των παραγόμενων προϊόντων.

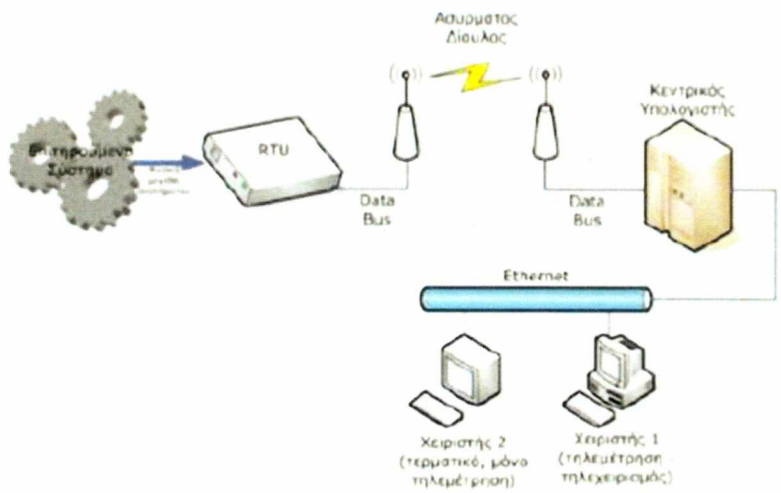
Επίσης ένα σύστημα SCADA περιλαμβάνει απεικόνιση σε μιμικά διαγράμματα όλων των διεργασιών παραγωγής, ενδείξεις των τιμών των μετρούμενων μεγεθών, διαρκή συλλογή και αποθήκευση δεδομένων σε Η/Υ, γνωστοποίηση σφαλμάτων κ.α. Επίσης σημαντική είναι η δυνατότητα παρακολούθησης του συστήματος μέσω κατάλληλα διαμορφωμένων σελίδων του διαδικτύου.

1.2 Αρχή λειτουργίας

Όπως έχουμε ήδη αναφέρει σύστημα SCADA αποτελεί ένα πλήρες σύστημα τηλεμετρίας και τηλεχειρισμού. Έτσι χρησιμοποιείται σε περιπτώσεις όπου το προς διαχείριση σύστημα απέχει αρκετά από το χώρο διαχείρισης. Προκειμένου να υλοποιήσουμε ένα SCADA απαιτούντα, εκτός των άλλων, ένα σύστημα τηλεμετρίας. Το σύστημα αυτό υλοποιείται με τη βοήθεια σταθμών RTU (Remote Telemetry Units), οι οποίοι είναι συνδεδεμένοι με την παραγωγική διαδικασία, διαβάζουν τις τιμές διαφόρων φυσικών μεγεθών που μας ενδιαφέρουν, π.χ. πίεση, θερμοκρασία, συχνότητα, τα μετατρέπουν σε ηλεκτρικά σήματα και τα μεταδίδουν μέσω ενός ενσύρματου ή ασύρματου διαύλου (ανάλογα με τις ανάγκες της εφαρμογής) στον υπολογιστή που φέρει τα λογισμικά SCADA, σε τακτά χρονικά διαστήματα.

Το χρονικό διάστημα που μεσολαβεί ανάμεσα στις διαδοχικές μεταδόσεις εξαρτάται αφενός από την ταχύτητα εξέλιξης της επιτηρούμενης διεργασίας και αφετέρου από την ακρίβεια που επιθυμούμε για το σύστημά μας. Εκτός των RTU, για την υλοποίηση του SCADA, απαιτούνται και ένας κεντρικός υπολογιστής, αρκετά μεγάλης υπολογιστικής ισχύος, που θα φέρει το λογισμικό SCADA και στον οποίο θα καταλήγουν οι μετρήσεις από όλους τους σταθμούς RTU καθώς και οι απαιτούμενες τηλεπικοινωνιακές ζεύξεις ανάμεσα στους σταθμούς RTU και τον κεντρικό υπολογιστή.

Στο σχήμα 1.1 φαίνεται μια συνηθισμένη τοπολογία ενός συστήματος SCADA.



Σχήμα 1.1 Τοπολογία ενός συστήματος SCADA

1.3 Κύριες λειτουργίες συστημάτων SCADA

Οι κύριες λειτουργίες ενός συστήματος SCADA είναι οι ακόλουθες:

- Συλλογή δεδομένων από τα PLC και τις απομακρυσμένες τερματικές μονάδες (Remote Telemetry Unit RTU). Οι RTU εγκαθίστανται σε απομακρυσμένα σημεία με σκοπό την αποστολή και λήψη εντολών. Όλα τα επιθυμητά σήματα μεταδίδονται προς το σύστημα SCADA μέσω του δικτύου βιομηχανικού αυτοματισμού
- Αποθήκευση των πληροφοριών στη βάση δεδομένων και αναπαράσταση τους μέσω γραφημάτων
- Ανάλυση δεδομένων και ειδοποίηση του προσωπικού σε περιπτώσεις σφάλματος. Όταν τα δεδομένα πάρουν τιμές μη κανονικές το σύστημα SCADA ειδοποιεί με οπτική ή ακουστική σήμανση τους χειριστές, ώστε να αποφευχθούν δυσάρεστες επιπτώσεις
- Έλεγχος κλειστού βρόχου διεργασιών. Υπάρχει η δυνατότητα εφαρμογής τεχνικών ελέγχου, αυτόματες ή χειροκίνητες
- Γραφική απεικόνιση των τμημάτων της διεργασίας σε μιμικά διαγράμματα και παρουσιάσεις των δεδομένων σε ενεργά πεδία. Τα μιμικά διαγράμματα

απεικονίζουν ρεαλιστικά τμήματα της διεργασίας με στόχο την ευκολότερη εποπτεία και την κατανόηση των δεδομένων από τους χειριστές του συστήματος

- Καταγραφή όλων των συμβάντων για την δημιουργία ιστορικού αρχείου. Σε κάθε βιομηχανία υπάρχει καταγραφή όλων των κρίσιμων παραμέτρων. Παλιότερα γινόταν με χειρόγραφη καταγραφή, ενώ σήμερα την ευθύνη αυτή έχει αναλάβει η βάση δεδομένων του συστήματος SCADA
- Υποστήριξη διπλού υπολογιστικού συστήματος με αυτόματη εναλλαγή, αν αυτό κρίνεται σκόπιμο βάση της υπό έλεγχο διεργασίας. Σε διεργασίες υψηλής επικινδυνότητας πρέπει να ελαχιστοποιηθεί όσο το δυνατόν περισσότερο η εμφάνιση σφάλματος λόγω βλάβης του εξοπλισμού. Για το λόγο αυτό τα συστήματα SCADA υποστηρίζουν δεύτερο υπολογιστικό σύστημα που αναλαμβάνει σε περίπτωση σφάλματος
- Μεταφορά δεδομένων σε άλλα τμήματα του κεντρικού συστήματος πληροφόρησης και διαχείρισης
- Έλεγχος της πρόσβασης χειριστών στα διάφορα υποσυστήματα του συστήματος SCADA
- Ειδικές εφαρμογές λογισμικού όπως εκτέλεση κώδικα C++ ή ανάπτυξη ευφυών συστημάτων

1.4 Εφαρμογές συστημάτων SCADA

Όπως έχουμε αναφέρει τα συστήματα SCADA έχουν τεράστια εφαρμογή στη βιομηχανία και τα συστήματα ηλεκτρικής ενέργειας. Η πιο ολοκληρωμένη και πιο μεγάλη σε μέγεθος εφαρμογή SCADA στη χώρα μας, έχει γίνει από τη ΔΕΗ για τον έλεγχο και την διαχείριση του δικτύου της. Σε κάθε υποσταθμό (ομάδα ζυγών) υπάρχει εγκατεστημένο ένα RTU, το οποίο καταγράφει την τάση κάθε ζυγού, την ενεργό και άεργο ισχύ που παράγεται ή δαπανάται ανάλογα με το είδος του ζυγού (παραγωγής ή φορτίου αντίστοιχα). Ακόμη λαμβάνονται μετρήσεις στους μετασχηματιστές, όπως τάσεις και ρεύματα σε πρωτεύον και δευτερεύον, θερμοκρασία κλπ.

Όλα αυτά τα δεδομένα αποστέλλονται με τη χρήση ενσύρματων τηλεπικοινωνιακών ζεύξεων, στο Κέντρο Ελέγχου Ενέργειας της ΔΕΗ. Εκεί τα δεδομένα αυτά εισάγονται σε μια βάση δεδομένων πραγματικού χρόνου (real time) και χρησιμοποιούνται από ειδικά προγράμματα, οικονομικής ανάλυσης και εκτίμησης κατάστασης τα οποία χρησιμοποιούν αλγορίθμους βελτιστοποίησης και τεχνητής νοημοσύνης.

Έτσι ελέγχεται αν υπάρχει πτώση τάσης σε κάποιο ζυγό ή αν υπάρχει υπερφόρτιση κάποιας γραμμής. Επίσης δίνονται εντολές για την εκκίνηση ή το σταμάτημα μιας γεννήτριας ενός σταθμού παραγωγής (θερμικού, υδροηλεκτρικού κλπ), Η βάση δεδομένων που αναφέραμε πιο πάνω μεταβάλλεται δυναμικά με την σάρωση των πληροφοριών από τους σταθμούς RTU. Υπάρχει όμως και μια δεύτερη βάση δεδομένων στην οποία αποθηκεύονται οι τιμές των μεταβλητών μιας δεδομένης χρονικής στιγμής. Έτσι είναι δυνατόν αργότερα να μελετηθεί η συμπεριφορά του συστήματος, για παράδειγμα σε ένα βραχυκύκλωμα ή ένα black out και να βρεθεί ο καλύτερος χειρισμός που θα μπορούσε να γίνει σε περίπτωση επανάληψης του φαινομένου αυτού.

Ένα σύστημα εποπτικού ελέγχου και απόκτησης δεδομένων (SCADA) είναι ένα ευρέως διαδεδομένο σύστημα βασισμένο στη χρήση υπολογιστή που

αρχικά χρησιμοποιήθηκε για τον έλεγχο και την παρακολούθηση από απόσταση των συνθηκών λειτουργίας των μερών μία κεντρικής εγκατάστασης.

1.4.1 Τα συστήματα SCADA χρησιμοποιούνται σε:

- Βιομηχανικές διεργασίες, οι οποίες περιλαμβάνουν διεργασίες στον τομέα της κατασκευής, της παραγωγής προϊόντων, της παραγωγής ηλεκτρικής ενέργειας κλπ.
- Διεργασίες υποδομής, οι οποίες μπορεί να είναι δημόσιες ή ιδιωτικές όπως η επεξεργασία νερού και η διανομή του, η συλλογή και επεξεργασία των λυμάτων, η μεταφορά ηλεκτρικής ενάργειας και η διανομή της, τα αιολικά πάρκα και τα μεγάλα επικοινωνιακά συστήματα

- Διεργασίες σε εγκαταστάσεις όπως κτίρια, αεροδρόμια, πλοία και διαστημικούς σταθμούς

1.5 Βασικά μέρη ενός συστήματος SCADA

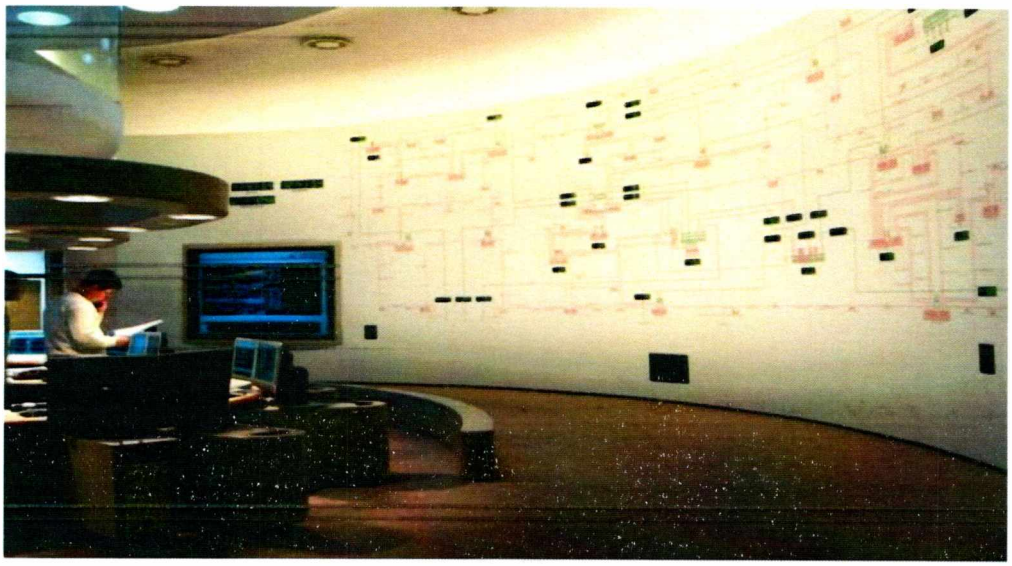
Τα βασικά μέρη ενός συστήματος SCADA είναι:

- Ένα σύνηθες σύστημα SCADA χρησιμοποιεί σαν κεντρικό πυρήνα έναν κεντρικό υπολογιστή, αρκετά μεγάλης υπολογιστικής ισχύος, στον οποίο βρίσκεται το λογισμικό SCADA εγκατεστημένο, όπως και το πρόγραμμα της εκάστοτε εφαρμογής. Η ζητούμενη τηλεμετρία στον επιθυμητό χώρο, επιτυγχάνεται με την εγκατάσταση σταθμών τηλεμετρίας RTU (Remote Telemetry Units)
- Οι σταθμοί αυτοί διαβάζουν τις τιμές διαφόρων μεγεθών που μας ενδιαφέρουν (τάση, πίεση, θερμοκρασία κτλ), τις μετατρέπουν σε ηλεκτρικά σήματα και τα σήματα αυτά τα μεταδίδουν ενσύρματα ή ασύρματα με κατάλληλες τηλεπικοινωνιακές ζεύξεις στον κεντρικό υπολογιστή, ανά τακτά χρονικά διαστήματα
- Από εκεί και πέρα, αρχίζει η παρακολούθηση και επεξεργασία τους από τους χρήστες του κεντρικού υπολογιστή και εξάγονται χρήσιμα συμπεράσματα για τη λειτουργία της εκάστοτε διεργασίας (σχήμα επόμενης διαφάνειας)

1.5.1 Δομικά στοιχεία ενός συστήματος SCADA

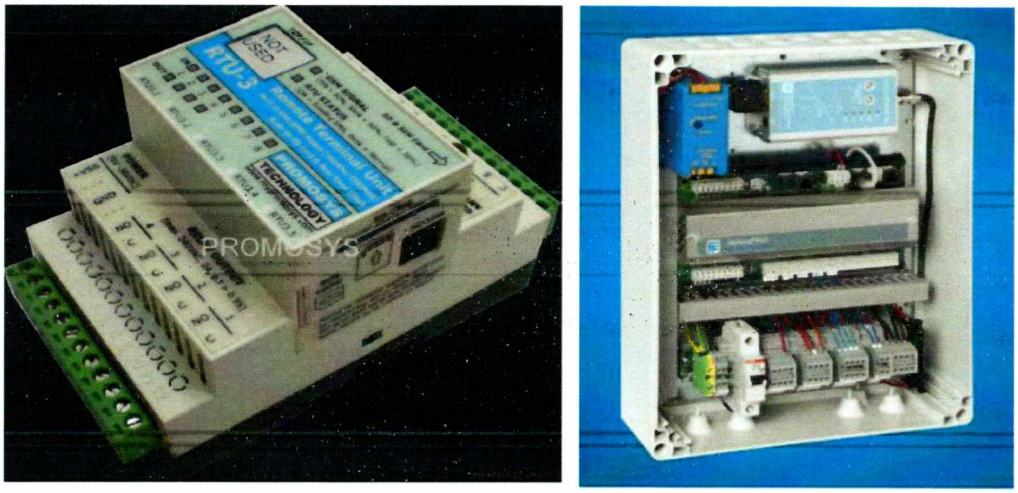
Τα δομικά στοιχεία ενός συστήματος SCADA είναι:

- Ένας κεντρικός υπολογιστικός σταθμός (Master Station Computer -MTU)



Σχήμα 1.2 Κεντρικός υπολογιστικός σταθμός SCADA

- Οι γραμμές επικοινωνίας (radio, καλωδιακή, τηλεφωνική)
- RTU's που κωδικοποιούν και αποκωδικοποιούν σήματα από τον πραγματικό κόσμο



Σχήμα 1.3 RTU συστήματος SCADA

- Το ελεγχόμενο σύστημα (Field Instrumentation)

1.5.2 Υποσυστήματα συστημάτων SCADA

Ένα σύστημα SCADA αποτελείται επίσης από τα ακόλουθα υποσυστήματα:

- Ένα σύστημα ανθρώπινης αλληλεπίδρασης (HMI-Human Machine Interface), που έχει σαν σκοπό να παρουσιάζει τα δεδομένα της γραμμής και ο χρήστης να μπορεί να τα ελέγχει καθ' όλη τη διάρκεια της παραγωγής

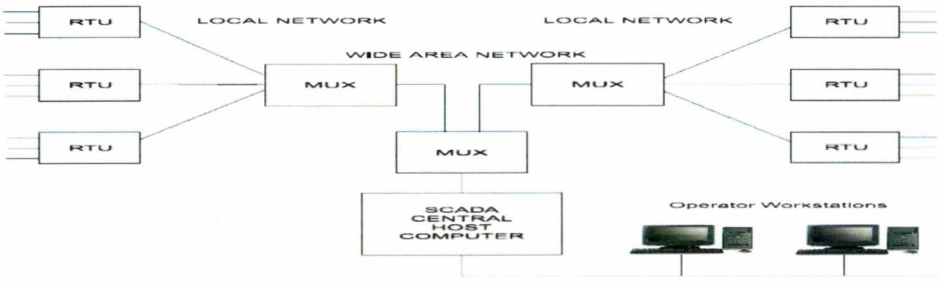
Σχήμα 1.4 Σύστημα ανθρώπινης αλληλεπίδρασης

- Από ένα υπολογιστή ο οποίος συλλέγει όλες τις πληροφορίες και στέλνει την κατάλληλη ανατροφοδότηση
- Τηλεχειριζόμενες τερματικές μονάδες, οι οποίες είναι συνδεδεμένες με αισθητήρες σε όλη τη διαδικασία, εναλλάσσοντας έτσι σήματα από τους αισθητήρες στο συντονιστικό υπολογιστή
- Προγραμματιζόμενους λογικούς ελεγκτές (PLC's)
- Την επικοινωνιακή υποδομή του συστήματος, η οποία συνδέει όλα τα παραπάνω κατάλληλα μεταξύ τους

1.6 Σχηματικές απεικονίσεις

Παρακάτω απεικονίζεται ένα γενικό σύστημα SCADA που επεξεργάζεται κάποια μορφή πολλαπλών δεδομένων μεταξύ του κεντρικού υπολογιστή και των RTU's. Αυτές οι διατάξεις βοηθούν στην δρομολόγηση των δεδομένων από και προς έναν αριθμό RTU σε ένα τοπικό δίκτυο, ενώ χρησιμοποιούνται ένας ή λίγοι φυσικοί σύνδεσμοι σε ένα δίκτυο μίας ευρείας περιοχής (WAN) για να δώσει δεδομένα πίσω στον κεντρικό υπολογιστή.

1.7 Γενικό δίκτυο ενός συστήματος SCADA



Σχήμα 1.5 Γενικό δίκτυο ενός συστήματος SCADA

1.7.1 Συσκευές δεδομένων

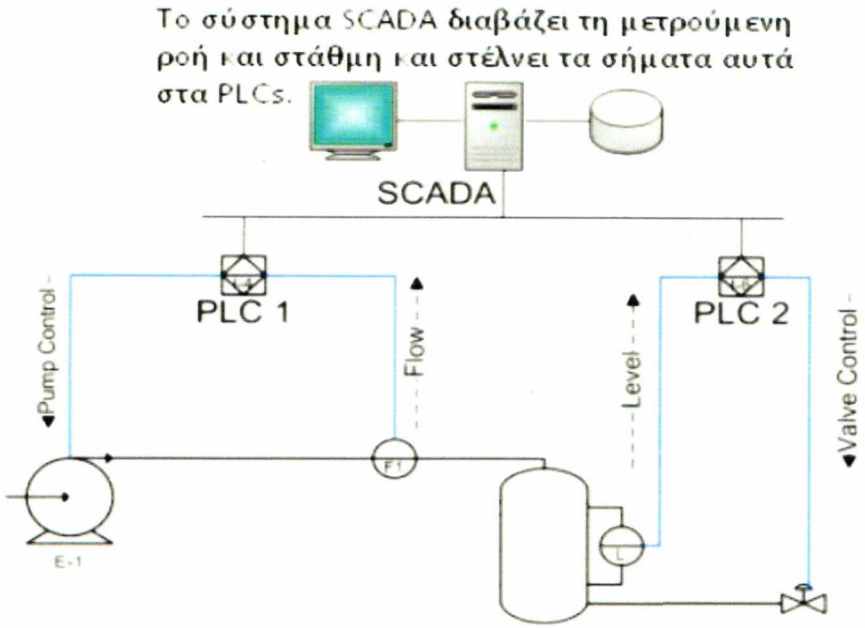
Οι συσκευές δεδομένων διαμορφώνουν τα μάτια και τα αυτιά ενός συστήματος SCADA. Για παράδειγμα ένα σύστημα SCADA το οποίο ελέγχει το δίκτυο νερού χρησιμοποιεί κάποιες συσκευές. Οι συσκευές όπως οι μετρητές του επιπέδου του reservoir, οι μετρητές ροής του νερού, οι μετρητές θερμοκρασίας, οι μετρητές κατανάλωσης ενέργειας και οι μετρητές πίεσης όλοι μαζί παρέχουν πληροφορίες που μπορούν να δώσουν πληροφορία σε έναν χειριστή ως προς το πόσο καλά λειτουργεί ένα σύστημα διανομής νερού. Επιπλέον, ο εξοπλισμός όπως οι ηλεκτρικοί μηχανισμοί κίνησης των βαλβίδων, οι πίνακες ελέγχου του μηχανισμού και οι ηλεκτρονικές εγκαταστάσεις μπορούν να χρησιμοποιηθούν για να διαμορφώσουν τα χέρια του συστήματος SCADA και να βοηθήσουν στην αυτοματοποίηση της διαδικασίας της διανομής του νερού.

Παρόλα αυτά, πριν από κάποια αυτοματοποιημένη ή απομακρυσμένη παρακολούθηση, οι πληροφορίες που περνούν από και προς τις συσκευές δεδομένων θα πρέπει να μετατραπούν σε μία μορφή που είναι συμβατή με την γλώσσα του συστήματος SCADA. Για να επιτευχθεί αυτό, απαιτείται κάποια μορφή ηλεκτρονικών δεδομένων. Τα RTU (Remote Telemetry Units) βασικά χρησιμοποιούνται για να μετατρέπουν τα ηλεκτρονικά σήματα που έρχονται από τις συσκευές σε μία γλώσσα (γνωστή και ως πρωτόκολλο επικοινωνίας) που χρησιμοποιείται για να μετατρέπει τα δεδομένα σε ένα κανάλι επικοινωνίας. Τα RTU εμφανίζονται ως ένα κουτί σε ένα τηλεφωνικό πίνακα με καλώδια ηλεκτρονικού σήματος που τρέχουν μέσα στις συσκευές δεδομένων και καλώδια σύνδεσης στο κανάλι επικοινωνίας.

Οι οδηγίες για τον αυτοματισμό των συσκευών των δεδομένων συνήθως αποθηκεύονται τοπικά. Αυτό οφείλεται σε μεγάλο βαθμό στο συνηθισμένο περιορισμένο εύρος ζώνης των συνδέσμων των επικοινωνιών μεταξύ του κεντρικού υπολογιστή του SCADA και των συσκευών των δεδομένων. Τέτοιες οδηγίες συνήθως κρατούνται μέσα σε τοπικές ηλεκτρονικές συσκευές γνωστές ως Programmable Logic Controllers (PLC), οι οποίες έχουν κατά το παρελθόν διαχωριστεί από τα RTU. Τα PLC συνδέονται άμεσα με τις συσκευές δεδομένων και ενσωματώνουν προγραμματισμένη γνώση σε μορφή λογικών διαδικασιών. Τα PLC συχνά χρησιμοποιούνται σε εργοστάσια με κατασκευαστικές εφαρμογές και σε αυτοκινητόδρομους για τον έλεγχο της κυκλοφορίας. Η ανάγκη ώστε τα PLC να συνδέονται με τα κανάλια επικοινωνίας δεν ήταν αρχικά μεγάλη σε αυτές τις εφαρμογές, καθώς αυτά συχνά απαιτούνταν να αντικαθιστούν τα λογικά συστήματα καθυστέρησης ή τους πνευματικούς ελεγκτές.

Με την πάροδο του χρόνου έγινε επιθυμητό να επηρεάσουν το πρόγραμμα μέσα στο PLC από ένα απομακρυσμένο σταθμό. Αυτό στην πραγματικότητα είναι το μέρος του εποπτικού ελέγχου (Supervisory Control) από το ακρωνύμιο του SCADA. Οι κατασκευαστές των PLC και RTU επομένως ανταγωνίζονται στην ίδια αγορά. Σαν αποτέλεσμα αυτών των εξελίξεων, η γραμμή μεταξύ των PLC και RTU έχει εμφανιστεί και η ορολογία είναι προφανώς εναλλακτική. Για χάρη της απλότητας, ο όρος RTU θα χρησιμοποιείται για να αναφέρει μια απομακρυσμένη συσκευή δεδομένων.

1.8 Σύστημα ελέγχου με SCADA και PLC



Σχήμα 1.6 Συνδεσμολογία PLC με SCADA

Η συλλογή δεδομένων ξεκινά από το RTU ή το PLC και περιλαμβάνει τις ενδείξεις των μετρητικών οργάνων καθώς και τις ενδείξεις κατάστασης (status) του εξοπλισμού. Τα δεδομένα αυτά αποστέλλονται στο SCADA. Τα δεδομένα στη συνέχεια καταρτίζονται και διαμορφώνονται με τέτοιο τρόπο ώστε ο χειριστής στην αίθουσα έλεγχου χρησιμοποιώντας το HMI να μπορεί να πάρει εποπτικές αποφάσεις για να προσαρμόσει ή να παρακάμψει τον κανονικό έλεγχο των RTU's ή PLC's.

Τα δεδομένα μπορούν επίσης να αποθηκευτούν σε μία βάση δεδομένων, στην οποία καταγράφονται διάφορα μεγέθη της εγκατάστασης με το πέρασμα του χρόνου και έτσι προσφέρεται η δυνατότητα στους διαχειριστές του συστήματος να ανατρέξουν σαι παλαιότερες μετρήσεις και να προχωρήσουν σε βελτιώσεις ή προσαρμογές του συστήματος. Για παράδειγμα στο σύστημα flow και level control του συστήματος του ανωτέρω σχήματος το σύστημα SCADA διαβάζει τη μετρούμενη ροή και στάθμη και στέλνει τα σήματα αυτά στα PLC's.

Το PLC1 συγκρίνει τη μετρούμενη ροή με την επιθυμητή και ελέγχει την ταχύτητα της αντλίας όσο χρειάζεται για να ταιριάξει τη ροή με την επιθυμητή και το PLC2 συγκρίνει τη μετρούμενη στάθμη με την επιθυμητή και ελέγχει τη ροή μέσω της βαλβίδας για να ταιριάξει τη στάθμη με την επιθυμητή.

1.8.1 Η έννοια των PLC στα συστήματα SCADA

Τα PLC συχνά χρησιμοποιούνται σε εργοστάσια με κατασκευαστικές εφαρμογές. Η ανάγκη ώστε τα PLC να συνδέονται με τα κανάλια επικοινωνίας δεν ήταν μεγάλη σε αυτές τις εφαρμογές, καθώς αυτά συχνά απαιτούνταν να αντικαθιστούν τα λογικά συστήματα καθυστέρησης ή τους πνευματικούς ελεγκτές. Καθώς τα PLCs χρησιμοποιούνταν πιο συχνά για να αντικαθιστούν τα relay switching control systems, η τηλεμετρία χρησιμοποιούνταν πιο πολύ με τα PLC's σε

απομακρυσμένες εγκαταστάσεις. Έγινε επιθυμητό να επηρεάσουν το πρόγραμμα μέσα στο PLC μέσω της χρήσης ενός απομακρυσμένου σήματος.

Αυτό στη πραγματικότητα είναι το μέρος του εποπτικού ελέγχου (Supervisory Control) από το ακρωνύμιο του SCADA. Όπου απαιτούνταν ένα απλό τοπικό σύστημα ελέγχου, έγινε δυνατό να αποθηκεύεται αυτό το πρόγραμμα μέσα στο RTU και να διεξάγει έλεγχο στην συσκευή. Την ίδια στιγμή, τα παραδοσιακά RTU που περιείχαν υπομονάδες επικοινωνίας που επιτρέπουν τα PLC να παρακολουθούν και να στέλνουν αναφορά της κατάστασης του προγράμματος ελέγχου στον υπολογιστή που συνδέεται στο PLC ή σε έναν απομακρυσμένο υπολογιστή μέσω μία τηλεφωνικής γραμμής. Οι κατασκευαστές των PLC και RTU επομένως ανταγωνίζονται στην ίδια αγορά.

Σαν αποτέλεσμα αυτών των εξελίξεων, η γραμμή μεταξύ των PLC και RTU έχει εξαφανιστεί και η ορολογία είναι προφανώς εναλλακτική. Για χάρη της απλότητας, ο όρος RTU θα χρησιμοποιείται για να αναφέρει μία απομακρυσμένη συσκευή δεδομένων. Παρόλα αυτά, μία τέτοια συσκευή θα μπορούσε να περιλαμβάνει προγραμματισμό αυτοματισμού και θα μπορούσε να χαρακτηριστεί σαν ένα PLC.

2.1 Σύστημα επικοινωνιών δεδομένων

Ο τομέας του συστήματος επικοινωνιών δεδομένων τείνει να παρέχει τα μέσα από τα οποία τα δεδομένα μπορούν να μεταφέρονται μεταξύ των servers του κεντρικού υπολογιστή και των RTU.

Μία σημαντική ιδιότητα ενός καναλιού επικοινωνιών είναι η ικανότητά του να φέρει δεδομένα. Ο όρος εύρος ζώνης χρησιμοποιείται για να περιγράψει αυτή την ικανότητα. Γενικά ο όρος εύρος ζώνης χρησιμοποιείται για το εύρος σε Hertz ενός αναλογικού καναλιού. Για παράδειγμα, ένα κανάλι μία τηλεφωνικής γραμμής που χρησιμοποιεί το εύρος 0.3 έως 3.4 kHz έχει ένα εύρος ζώνης των 3.1 kHz και ένα ραδιοφωνικό κανάλι που χρησιμοποιεί ένα φάσμα από 929.88875 έως 929.8875 MHz έχει ένα κανάλι εύρους ζώνης των 12.5 kHz. Με την ψηφιακή μετάδοση, ο όρος εύρος ζώνης έχει διευρυνθεί για να συμπεριλάβει τον ρυθμό μετάδοσης δεδομένων σε bits ανά δευτερόλεπτο (bps) 41.

2.1.1 Διαθεσιμότητα SCADA επικοινωνιών

Η διαθεσιμότητα που υπάρχει στη δομή των επικοινωνιών είναι μία σημαντική πλευρά του SCADA συστήματος. Επειδή τα SCADA συστήματα συνήθως αναπτύσσονται σε μεγάλες γεωγραφικές περιοχές, συνδέσεις των απομακρυσμένων SCADA σταθμών από τον κεντρικό υπολογιστή συνήθως είναι πολυστρωματικές, εννοώντας ότι μπορεί να υπάρχουν μερικά φυσικά και λογικά μονοπάτια μέσω των οποίων τα δεδομένα πρέπει να δρομολογηθούν πριν φτάσουν στον προορισμό τους. Σε αυτές τις συνδέσεις θα πρέπει να δοθεί μεγάλη σημασία από οικονομική πλευράς στον τύπο των συστημάτων επικοινωνιών που θα χρησιμοποιηθούν και στο εύρος ζώνης που θα χρησιμοποιηθεί σε αυτές τις συνδέσεις.

Το πρόβλημα στη διαθεσιμότητα μπορεί να αποδοθεί στο γεγονός ότι οι πολυστρωματικές SCADA συνδέσεις διατρέχουν έναν μεγαλύτερο αριθμό μέσων μετατροπής και θυρών δρομολόγησης δεδομένων συγκριτικά με τις LAN κατασκευές υψηλής ταχύτητας. Επομένως, υπάρχουν πολλά σημεία αποτυχίας σε πολλά δίκτυα επικοινωνιών SCADA. Οι βλάβες στις επικοινωνίες συνήθως προκύπτουν από τον

εξοπλισμό και από τις βλάβες στην παροχή ενέργειας και στην ανθρώπινη παρέμβαση. Καλύτερη διαθεσιμότητα είναι δυνατή μέσω της χρήσης εφεδρικών μονοπατιών επικοινωνίας στους εξωτερικούς σταθμούς. Παρόλα αυτά, τέτοιοι σχεδιασμοί μπορούν να συνεισφέρουν σημαντικά στο κόστος του συστήματος επικοινωνιών και επομένως δεν μπορεί να είναι οικονομικά βιώσιμο αν η σύνδεση των επικοινωνιών δεν είναι σημαντική στην λειτουργική ασφάλεια.

2.2 Πρωτόκολλα επικοινωνίας SCADA

Τα πρωτόκολλα της επικοινωνίας SCADA είναι σχεδιασμένα ειδικά για την μειωμένη αξιοπιστία των συνδέσμων επικοινωνίας που συνήθως χρησιμοποιούνται στα SCADA συστήματα και παρέχουν ασφαλή μεταφορά των δεδομένων, διασφαλίζοντας την αξιόπιστη μεταφορά των δεδομένων στους προορισμούς κάτω από οποιαδήποτε περίπτωση. Τα πρωτόκολλα συμβάλλουν στον εντοπισμό του σφάλματος και στις τεχνικές ανασκόπησης των μηνυμάτων. Παρόλα αυτά, οι παραπάνω πληροφορίες που εισάγονται δημιουργούν πρόβλημα στην μετάδοση των δεδομένων, καταλήγοντας σε προβλήματα μεταξύ της ταχύτητας μετάδοσης των δεδομένων και της αξιοπιστίας του συνδέσμου των επικοινωνιών.

Σαν αποτέλεσμα, η ταχύτητα των επικοινωνιών των δεδομένων που σχετίζονται με το SCADA είναι χαμηλότερη από την συνηθισμένη στις επικοινωνίες που χρησιμοποιούνται σε ένα γραφείο ή σε κάποιον όροφο ενός εργοστασίου. Οι χρήστες των SCADA συστημάτων και τα δεδομένα που προκύπτουν δεν χρειάζονται να είναι ενήμερα των πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται. Παρόλα αυτά, είναι σημαντικό να κατανοηθεί ότι με την χρήση των συνδέσμων επικοινωνίας όπως το ράδιο, υπάρχει μία πιθανότητα αν και μικρή να συμβούν κάποια σφάλματα επικοινωνίας

2.2.1 Πρωτόκολλο επικοινωνίας DNP

Ένα παράδειγμα πρωτοκόλλου SCADA επικοινωνιών είναι το DNP 3.0 (Distributed Network Protocol), ένα ανεξάρτητο πρωτόκολλο που ενσωματώνει πολλαπλά στρώματα εντοπισμού σφαλμάτων και διόρθωσης και επιτρέπει την επιβεβαίωση των εντολών ελέγχου.

Το Modbus (αναλύεται παρακάτω) είναι άλλο ένα ευρέως διαδεδομένο πρωτόκολλο για το SCADA, αλλά δεν προσφέρει το ίδιο επίπεδο ασφάλειας στην μετάδοση δεδομένων όπως το DNP 3.0. Υπάρχει επίσης μία μεγάλη ποικιλία πρωτοκόλλων που προσφέρουν μαζί με τα συστήματα SCADA και προσφέρουν πολλές δυνατότητες όπως τα RP-570, Profibus και Conitel.

2.2.2 Τυποποιημένα πρωτόκολλα

Τα τυποποιημένα πρωτόκολλα είναι τα: IEC 60870-5-101 ή 104, IEC 61850 και DNP3. Αυτά τα πρωτόκολλα επικοινωνίας είναι τυποποιημένα και αναγνωρισμένα από όλους τους μεγάλους προμηθευτές SCADA. Πολλά από αυτά τα πρωτόκολλα περιέχουν πλέον επεκτάσεις ώστε να λειτουργούν σε TCP/IP

Modbus -1

Το Modbus είναι ένα πρωτόκολλο ανταλλαγής μηνυμάτων που αναπτύχθηκε από την Modicon το 1979. Χρησιμοποιείται για την επίτευξη master-slave/client-server επικοινωνίας μεταξύ ευφυών συσκευών. Είναι ένα de facto πρότυπο, πραγματικά ανοιχτό και το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο δικτύου σε περιβάλλον βιομηχανικής παραγωγής. Έχει τεθεί σε εφαρμογή σε χιλιάδες

διαφορετικές συσκευές για τη μεταφορά διακριτών/ αναλογικών I/O και την εγγραφή δεδομένων μεταξύ συσκευών ελέγχου.

Το Modbus χρησιμοποιείται σε πολλαπλές εφαρμογές master-slave:

- Για την παρακολούθηση και προγραμματισμό διαφόρων συσκευών
- Για την επικοινωνία μεταξύ ευφυών συσκευών με αισθητήρες και όργανα
- Για την παρακολούθηση των συσκευών πεδίου χρησιμοποιώντας Η/Υ και HMI's

Modbus -2

- Το Modbus είναι ένα πρωτόκολλο επιπέδου εφαρμογής ανταλλαγής μηνυμάτων που τοποθετείται στο επίπεδο 7 του μοντέλου OSI και παρέχει client / server επικοινωνία μεταξύ συσκευών που συνδέονται με διαφορετικούς τύπους μέσων σύνδεσης και δικτύων. Οι κώδικες λειτουργίας του Modbus είναι στοιχεία του Modbus request/reply PDU's (Protocol Data Unit)
- Το Modbus είναι επίσης ιδανικό πρωτόκολλο για RTU εφαρμογές όπου απαιτείται ασύρματη επικοινωνία. Για αυτό το λόγο, έχει χρησιμοποιηθεί σε αναρίθμητες εφαρμογές σε υποσταθμούς φυσικού αερίου και πετρελαίου
- Δεν είναι μόνο ένα βιομηχανικό πρωτόκολλο. Μπορεί επίσης να χρησιμοποιηθεί σε εφαρμογές κατασκευών, υποδομών, μεταφορών και ενέργειας

Modbus -3

Με απλά λόγια, είναι μια μέθοδος που χρησιμοποιείται για τη διαβίβαση πληροφοριών μέσω σειριακών γραμμών μεταξύ ηλεκτρονικών συσκευών. Η συσκευή που ζητεί τις πληροφορίες ονομάζεται Modbus Master και οι συσκευές που παρέχουν πληροφορίες Modbus Slaves. Σε ένα τυπικό Modbus δίκτυο, υπάρχει ένας Master και μέχρι 247 Slaves, ο καθένας με μια μοναδική Slave διεύθυνση από 1 έως 247. Το Master μπορεί επίσης, να στείλει πληροφορίες στους Slaves.

Διάφοροι τύποι Modbus

Υπάρχουν διάφοροι τύποι του πρωτοκόλλου Modbus. Ο πιο κοινός τύπος είναι το Modbus RTU που βασίζεται σε σειριακή επικοινωνία, όπως RS485 και RS232. Υπάρχει επίσης το πρωτόκολλο Modbus ASCII. Σήμερα το πρωτόκολλο Modbus over Ethernet αυξάνεται σημαντικά. Λέγεται Modbus TCP και είναι βασικά το πρωτόκολλο Modbus RTU με ενσωματωμένα πακέτα TCP/IP. Είναι μια εξαιρετική επιλογή για να συνδέσετε συσκευές που χρησιμοποιούν για την επικοινωνία τους πρωτόκολλο Modbus με συστήματα SCADA ή PLC.

Το πρωτόκολλο Modbus μεταδίδεται μέσω σειριακής γραμμής μεταξύ συσκευών. Η πιο απλή εγκατάσταση θα ήταν ένα σειριακό καλώδιο που συνδέει τις σειριακές θύρες δύο συσκευών, μιας Master και μιας Slave.

Μέσα επικοινωνίας

Τα πιο κοινά μέσα επικοινωνίας μέσα στο οικοσύστημα του scada είναι τα εξής:

- Δημόσια δίκτυα τηλεφώνου
- Ραδιοσύνδεσμοι (UHF και VHF)
- Κινητή τηλεφωνία
- Μικροκύματα
- Δορυφορικοί σύνδεσμοι
- Εταιρικά υπολογιστικά συστήματα επικοινωνιών LAN και WAN
- Δίκτυα οπτικών ινών

Στις περισσότερες περιπτώσεις γίνεται συνδυασμός των παραπάνω μέσων επικοινωνίας ώστε να επιτευχθεί η μέγιστη αξιοποίηση των συστημάτων του Scada. Για την μεγαλύτερη όμως αξιοπιστία και λειτουργικότητα χρησιμοποιούνται τα δύο τελευταία μέσα επικοινωνίας.

3.1 Η κυβερνοασφάλεια Scada των συστημάτων.

Μετά την εισαγωγή και τις βασικές έννοιες λειτουργίας ενός συστήματος Scada,θα εστιάσουμε στον κύριο σκοπό της διπλωματικής αυτής εργασίας που δεν είναι άλλος από την κυβερνοασφάλεια των συστημάτων αυτών.

Τα συστήματα Scada κυρίως βρίσκονται σε οργανισμούς και εταιρείες οι οποίες θεωρούνται ύψιστης σημασίας υποδομές(critical infrastructures) για την καλή λειτουργία ενός κράτος αλλά και της κοινωνίας .Τέτοιες υποδομές είναι οι πάροχοι ενέργειας και καυσίμων ,οι τηλεπικοινωνίες, τα κύρια μέσα μαζικής μεταφοράς , τα νοσοκομεία κ.α.

Παρόλο όμως που τα συστήματα Scada βρίσκονται βαθιά ριζωμένα σε αυτούς του οργανισμούς, παρατηρείται σύμφωνα με πολλές έρευνες ότι η κυβερνοασφάλεια τους είναι μηδαμινή, ακόμη και σε χώρες οι οποίες θεωρούνται υπερδυνάμεις.

Ένας λόγος που η προστασία από ψηφιακές απειλές και επιθέσεις είναι πολυδιάστατη και πολύπλοκή είναι διότι υπάρχουν πολλοί που έχουν όφελος από μια επίθεση και αποτελούν απειλές για μια επίθεση. Θα γίνει παρουσίαση των πιθανών εμπλεκομένων σε μια επίθεση παρακάτω με σειρά προτεραιότητας

3.1.1 Χώρες-Κράτη

Είναι οι πιο σημαντικοί παίχτες στο τοπίο μιας κυβερνοεπίθεσης εναντίον κρίσιμων υποδομών. Η σημαντικότητα τους πηγάζει από το γεγονός ότι στον μοντέρνο κυβερνοπόλεμο οι κρίσιμες υποδομές και τα Scada είναι οι στόχοι με την μεγαλύτερη σημασία. Επιθέσεις από χώρες εναντίον άλλων χωρών είναι άριστα οργανωμένες με άπειρες πηγές πληροφοριών και στοχεύουν σε στόχους οι οποίοι κινούνται σε οικονομικά και πολιτικά πλαίσια. Επίσης στην κατηγορία των επιτιθέμενων ως κράτη λογίζονται και ομάδες κακόβουλων χάκερ οι οποίες χρηματοδοτούνται από κρατικούς προϋπολογισμού

3.1.2 Κυβερνοτρομοκράτες

Είναι επικίνδυνες ομάδες κακόβουλων επιτιθέμενων οι οποίες προσπαθούν να καταλύσουν τις υποδομές μιας χώρας ή ενός οργανισμού. Απαρτίζονται από μέλη άρτια εκπαιδευμένα και οι πηγές χρημάτων και πληροφοριών συνήθως είναι τεράστια για να βγάλουν εις πέρας μια επίθεση.

3.1.3 Χακτιβιστές

Τελευταία έχουν βγει στο προσκήνιο ομάδες ακτιβιστών, οι οποίες εκφράζονται μέσω κακόβουλων επιθέσεων σε κρίσιμες υποδομές και Scada. Οι

τεχνικές τους ικανότητες συνήθως είναι χαμηλού επιπέδου οι οποίες στηρίζονται σε εργαλεία ήδη γνωστά. Σκοπός τους είναι να προκαλέσουν μια μορφή διαμαρτυρίας και όχι ζημιά. Τα κίνητρα τους είναι συνήθως πολιτικά.

3.1.4 Επιτιθέμενοι επιχειρησιακής κατασκοπείας

Ίσως είναι η πιο παραδοσιακή ομάδα που μπορεί να προκαλέσει κακόβουλες επιθέσεις. Συνήθως οι επιθέσεις τους έχουν σκοπό στην δυσλειτουργία των συστημάτων των ανταγωνιστικών επιχειρήσεων τους. Κίνητρο τους είναι η απόκτηση στρατηγικού πλεονεκτήματος στην αγορά εναντίων των ανταγωνιστών τους.

3.1.5 Τυχαίοι μεμονωμένοι επιτιθέμενοι

Συνήθως είναι άτομα ή μικρές ομάδες ατόμων που κάνουν επιθέσεις χαμηλού επιπέδου. Υπάρχει όμως ο κίνδυνος να κάνουν τρομερή και ανεπανόρθωτη ζημιά

3.2 Η ανάγκη για διασφάλιση της ασφαλούς μεταφοράς πληροφοριών

Αρχικά για να προσεγγίσουμε το θέμα θα πρέπει να δώσουνε παραδείγματα που θα ορίσουν την κρίσιμη πληροφορία(critical information).

Η κρίσιμη πληροφορία σαν όρος αναφέρεται στις πληροφορίες που προστατεύουν πολύτιμα στοιχεία όπως κωδικούς συστημάτων πρόσβασης σε ένα κτίριο, χημικές φόρμουλες, επιχειρησιακές στρατηγικές, προσωπικά στοιχεία αλλά ακόμη και σκουπίδια στα οποία ένας κακόβουλος επιτιθέμενος θα μπορέσει να αντλήσει στοιχεία για μια social engineering επίθεση ή μίας phishing επίθεσης.

Στα συστήματα ελέγχου η διαρροή κρίσιμων πληροφοριών μπορεί να έχει σοβαρές οικονομικές επιπτώσεις ή ακόμη και απώλεια ζωής όπως θα δούμε και παρακάτω σε παραδείγματα κυβερνοεπιθέσεων σε Scada συστήματα.

3.2.1 Παραδείγματα κυβερνοεπιθέσεων σε Scada

W32.Stuxnet

Το Stuxnet κοινώς είναι ένα malware που χρησιμοποιήθηκε το 2009 και το 2010 για να εκτελεστεί η μεγαλύτερη έως τώρα κυβερνοεπίθεση σε scada συστήματα. Αυτή η στοχευόμενη επίθεση κέντρισε το ενδιαφέρον των μέσων μαζικής ενημέρωσης αλλά και της ερευνητικής κοινότητας .Ακόμη και μετά από τόσα χρόνια που έχουν περάσει υπάρχουν πολλά αδιευκρίνιστα και σκοτεινά σημεία για αυτήν την επίθεση ,το μόνο σίγουρο είναι όμως ότι το Stuxnet δημιουργήθηκε για να διαδοθεί και να προσβάλει συστήματα Scada τα οποία χρησιμοποιούσαν plc της Siemens. Χάρη σε μια 0-day ευπάθεια, ένα Windows rootkit , ένα PLC rootkit και πολλές υψηλής τεχνολογίας τεχνικές υπεκφυγής και αντιγραφής το Stuxnet κατάφερε να μολύνει πολλές εγκαταστάσεις οι οποίες χρησιμοποιούσαν Scada. Σύμφωνα με κυβερνητικές πηγές και μετά από έρευνες ειδικών, το Stuxnet έκανε την μεγαλύτερη ζημιά στα πυρηνικά εργοστάσια του Ιράν.

Ο στόχος του Stuxnet ήταν να τροποποιήσει την λειτουργικότητα των PLC, έτσι ώστε να μετατρέψει την λειτουργία του εξοπλισμού σαμποτάροντας και κάνοντας τεράστια ζημιά στον φυσικό κόσμο όπως εκρήξεις ή έκλυση ραδιενέργειας. Σύμφωνα με την εταιρεία Symantec, προηγούμενες εκδόσεις αυτού του εκλεπτυσμένου κυβερνο όπλου περιείχε κακόβουλου κώδικα ο οποίος είχε συμφώνα με πληροφορίες εξαπολυθεί από τις Ηνωμένες Πολιτείες και το Ισραήλ σε μια προσπάθεια να σαμποτάρουν το πυρηνικό πρόγραμμα του Ιράν. Αυτό υποδεικνύει ότι το Stuxnet ήταν ενεργό περίπου δυο χρόνια πριν γίνει η κύρια επίθεση. Επίσης

υποδεικνύει ότι σε καμία από τις δύο εξορμήσεις του Stuxnet (το 2007 και το 2009-2010) δεν υπήρχε μεγάλο αντίκτυπο στις πυρηνικές εγκαταστάσεις του Ιράν. Συμπερασματικά αν και απέτυχε το Stuxnet παρατηρήσαμε για πρώτη φορά μια προσπάθεια δημιουργίας ενός νέου είδους όπλου το οποίο ήταν προσεχτικά σχεδιασμένο και με άπειρους πόρους.

(http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf)

Η επίθεση στην Aramco

Η επίθεση αυτή έγινε το 2012 σε μια από τις μεγαλύτερες εταιρείες πετρελαίου ,της Aramco που βρίσκεται στην Σαουδική Αραβία. Από διάφορους ερευνητές και εταιρείες που εξειδικεύονται στην κυβερνοασφάλεια, ανακαλύψανε ότι ένα worm ήταν υπεύθυνο, με ονομασίας Shamoon. Το worm ήταν ένα μέρος μιας μεγάλης επιχείρησης που είχε σκοπό την κατασκοπεία και τη δολιοφθορά στην περιοχή της Μέσης Ανατολής. Η λειτουργία του Shamoon ήταν η εξής: αφού το σύστημα είχε μολυνθεί, το Shamoon συγκέντρωνε αρχεία από συγκεκριμένες τοποθεσίες και στη συνέχεια τα έστελνε πίσω άμεσα στον επιτιθέμενο. Τέλος αντικαθιστούσε τα αρχεία του master boot record με μια εικόνα επεξεργασμένη που απεικόνιζε μια σημαία των Η.Π.Α. στις φλόγες. Το Shamoon πρόσβαλε 30.000 υπολογιστές και χρειάστηκε στην εταιρεία μια εβδομάδα να ανακάμψει. Το καλό σε όλη την υπόθεση ήταν ότι δεν υπήρξαν στόχοι τα συστήματα της παραγωγής πετρελαίου διότι σε μια τέτοια περίπτωση θα υπήρχε κίνδυνος για ανθρώπινες ζωές.

3.3 Η ασφάλεια στο δίκτυο του SCADA.

Για να καταφέρει κάποιος να αλλάξει μια εντολή ελέγχου ή την τιμή ενός αισθητήρα, θα πρέπει ο επιτιθέμενος να αποκτήσει πρόσβαση άμεσα στον αισθητήρα/πίνακα ελέγχου, ή να εισβάλει απομακρυσμένα στο δίκτυο επικοινωνίας τους. Τα περισσότερα Scada έχουνε κάποιο επίπεδο ασφάλειας εγκατεστημένο στην περίμετρο συμπεριλαμβανομένου τεχνολογιών firewall και κατάτμησης του δικτύου. Παρακάμπτοντας την περιμετρική άμυνα του συστήματος από την εξωτερική του πλευρά είναι μια δύσκολη διαδικασία, για αυτό το λόγο οι επιτιθέμενοι προσπαθούν να ανακαλύψουν μια εναλλακτική οδό για να διεισδύσουν .Για παράδειγμα βρίσκοντας μιας θύρας που είναι μισάνοιχτη ή πυροδοτώντας ορισμένες λειτουργίες από το εσωτερικό του οργανισμού που ανοίγει ένα κανάλι επικοινωνίας προς τα έξω. Μερικές τεχνικές περιγράφονται από κάτω:

- Χρήση μιας απομακρυσμένης θύρας εισόδου η οποία χρησιμοποιείται από τους τεχνικούς για συντήρηση
- Παίρνοντας υπό τον έλεγχο μια νόμιμη δίοδο μεταξύ των πληροφοριακών συστημάτων και των συστημάτων Scada
- Πείθοντας έναν εσωτερικό χρήστη να κάνει κλικ σε έναν σύνδεσμο URL ή σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από ένα σταθμό εργασίας που συνδέεται τόσο με το δίκτυο Scada όσο και στο Internet
- Μολύνοντας φορητούς υπολογιστές και / ή αφαιρούμενα μέσα εκτός του δικτύου Scada, μολύνοντας αργότερα τα εσωτερικά συστήματα τα οποία είναι συνδεδεμένα με δίκτυα συλλογής πληροφοριών, αισθητήρων και ενημέρωσης λογισμικών.
- Κάνοντας χρήση των λαθών διαμόρφωσης στις συνδεδεμένες συσκευές

Από την στιγμή που εισέλθει κάποιος στο δίκτυο, μπορεί να μοχλεύσει τις πληροφορίες που έχει στην κατοχή του για το δίκτυο ή να κάνει αναγνωριστική επιχείρηση για να μάθει όλο το περιβάλλον.

3.3.1 Η ασφάλεια στα SCADA Protocols

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο τα δίκτυα Scada χρησιμοποιούν συγκεκριμένα και μερικές φορές ιδιόκτητα πρωτόκολλα. Πολλά από αυτά τα πρωτόκολλα έχουν γνωστές αδυναμίες που τα καθιστούν ευπαθή σε επιθέσεις.
Εδώ είναι μερικά χαρακτηριστικά παραδείγματα:

Το MODBUS είναι ένα πρωτόκολλο επικοινωνίας που ανήκει στο επίπεδο (layer) της εφαρμογής. Παρέχει επικοινωνία client-server ανάμεσα σε συσκευές συνδεδεμένες σε διαφορετικούς διόδους ή δίκτυα. Το MODBUS συνήθως χρησιμοποιείται για επίβλεψη και έλεγχο αυτοματισμών και είναι όμως ένα πρωτόκολλο το οποίο δεν προσφέρει προστασία από υποκλοπή δεδομένων ή μη εξουσιοδοτημένης εντολής.
Ένας εισβολέας με συνδεσιμότητα IP και έναν προσομοιωτή client Modbus μπορεί να δημιουργήσει διάφορους τύπους επιθέσεων.

- Εκτελεί μια προσπάθεια αναγνώρισης χρησιμοποιώντας ένα σαρωτή για να προσδιορίσει ποιοι κώδικες λειτουργίας υποστηρίζονται σε ένα διακομιστή Modbus TCP για να βοηθηθεί να σχεδιάσει μια επίθεση
- Εκπέμπει γραπτές αιτήσεις στο PLC πού έχει σαν αποτέλεσμα η συσκευή να καταστραφεί ή να συμπεριφέρεται ανεπιθύμητα.
- Στέλνει FORCE LISTEN MODE εντολές στο PLC καθιστώντας το σε κατάσταση χάους χωρίς να μπορέσει να ανταποκριθεί σε αιτήματα
- Ένας εισβολέας με φυσική ή απομακρυσμένη πρόσβαση σε ένα PLC παρακολουθεί ή μπλοκάρει τα MODBUS requests προς το PLC και απαντά με ένα μήνυμα εξαίρεσης, επιτρέποντας στον επιτιθέμενο επιπλέον χρόνο για να τροποποιήσει το PLC ή άλλα συστήματα του πεδίου και να αποφύγει τον εντοπισμό του

Το DNP3(Πρωτόκολλο κατανεμημένου δικτύου) είναι ένα σύνολο πρωτοκόλλων επικοινωνίας που χρησιμοποιείται μεταξύ των εξαρτημάτων των συστημάτων αυτοματισμού. Η κύρια χρήση του είναι σε επιχειρήσεις κοινής ωφελείας, όπως εταιρείες ηλεκτρισμού και νερού. Αν και το πρωτόκολλο σχεδιάστηκε για να είναι πολύ αξιόπιστο, δεν σχεδιάστηκε για να είναι ασφαλής από επιθέσεις. Τυπικές εφαρμογές του DNP3 δεν περιέχουν κρυπτογράφηση, έλεγχο ταυτότητας ή εξουσιοδότηση χρήσης και οι συσκευές απλά υποθέτουν ότι όλα τα μηνύματα είναι έγκυρα .Οι κοινές επιθέσεις DNP3 βασίζονται στην ικανότητα να υποκλέψει, να τροποποιήσει ή να κατασκευάσει μηνύματα DNP3 κάποιος επιτιθέμενος. Μερικά τυπικά σενάρια περιλαμβάνουν:

- Ένας εισβολέας με πρόσβαση στο δίκτυο συλλαμβάνει και αναλύει τα μηνύματα DNP3 παρέχοντας τον με πληροφορίες σχετικά με την τοπολογία του δικτύου, τη λειτουργικότητα της συσκευής, τις διευθύνσεις μνήμης και άλλα δεδομένα
- Βάσει της γνώσης των προτύπων κυκλοφορίας DNP3, ο εισβολέας μπορεί να προσομοιώσει τις απαντήσεις στην κύρια μονάδα στέλνοντας ταυτόχρονα κατασκευασμένα μηνύματα σε απομακρυσμένες συσκευές

- Ένας εισβολέας μπορεί να εγκαταστήσει μια "man-in-the-middle" συσκευή μεταξύ της κύρια μονάδας και τους εξωτερικούς σταθμούς, που μπορεί να διαβάσει, τροποποιήσει και να κατασκευάσει μηνύματα DNP3 ή / και την κυκλοφορία του δικτύου

Οι επιθέσεις αυτές μπορεί να οδηγήσουν σε Denial of Service ή σε αλλαγές της παραγωγικής διαδικασίας χωρίς την γνώση των χειριστών του συστήματος Scada.

3.3.2 Είδη επιθέσεων σε Scada συστήματα (ATTACK VECTORS)

Οι κυβερνοεπιθέσεις σε Scada συστήματα δρομολογούνται μέσα από συνδέσεις με το διαδίκτυο, τις συνδέσεις μέσα στις επιχειρήσεις και είναι ευάλωτες σε κοινές επιθέσεις όπως κάθε σύστημα που βασίζεται σε TCP/IP. Από τη στιγμή που ένα εταιρικό δίκτυο παραβιαστεί τότε κάθε σύστημα ή υπολογιστής βασιζόμενος σε IP μπορεί να προσεγγιστεί. Έτσι εκμεταλλευόμενοι τα παρακάτω είδη επιθέσεων κάποιος χρήστης μπορεί να δημιουργήσει μεγάλες καταστροφές. Συνεπώς τα πιο κοινά είδη επιθέσεων είναι:

- **Πίσω πόρτες (backdoors) και τρύπες στην περίμετρο του δικτύου.**
  - Τα δίκτυα στα συστήματα ελέγχου συχνά έχουν εγγενείς δυνατότητες οι οποίες αναπτύσσονται χωρίς επαρκή ασφάλεια και μπορούν να δώσουν πρόσβαση σε επιτιθέμενους
  - Τα εξαρτήματα των δικτύων χρησιμοποιούν τεχνολογίες που συχνά περιέχουν firewall, δημόσιες υπηρεσίες και απομακρυσμένη πρόσβαση. Κάθε ένα από αυτά τα εξαρτήματα συχνά συνδέονται με κοινές ευπάθειες ασφάλειας
  - Τα στοιχεία που βρίσκονται σε απομακρυσμένες τοποθεσίες και υπάρχει απομακρυσμένη πρόσβαση που βασίζεται σε κοινά λειτουργικά συστήματα δέχονται επιθέσεις DDOS και επιθέσεις κλιμακωμένων δικαιωμάτων
  - Οι οργανισμοί που χρησιμοποιούν Scada παρέχουν στους πελάτες τους και στους χρήστες τους μέσω δημόσιων υπηρεσιών, δεδομένα τα οποία μπορούν να οδηγήσουν κάποιον επιτιθέμενο σε δεδομένα τα οποία δεν έχουν περιορισμένη πρόσβαση
  - Η σχέση μεταξύ του firewall του οργανισμού και του web server, εάν δεν έχει ρυθμιστεί σωστά επιτρέπει μη εξουσιοδοτημένη πρόσβαση σε εσωτερικά τοπικά δίκτυα
- **Ευπάθειες σε κοινά πρωτόκολλα**
  - Πολύ γνωστό λειτουργικό το οποίο είναι και το πιο σύνηθες να τρέχει Scada συστήματα μετριάζουν θέματα ασφάλειας
  - Τα συστήματα και δίκτυα ελέγχου είναι ήδη ευπαθή εξ 'αρχής και παρόλο που πολλές ευπάθειες έχουν λύση μέσω update, είναι έτσι η αρχιτεκτονική τους που τα κάνει ανέφικτα να διορθωθούν
- **Επιθέσεις σε συσκευές στο πεδίο χρήσης με τρόπο που εκμεταλλεύεται κενά κυβερνοασφάλειας**
  - Οι κατασκευαστές των συστημάτων αυτοματισμού και ελέγχου έχουν την δυνατότητα απομακρυσμένης πρόσβασης για λόγους ελέγχου και συντήρησης των συστημάτων. Αυτό καθιστά τα συστήματα και τις συσκευές ευάλωτες.
  - Ο εξοπλισμός έχει ενσωματωμένους web server και file servers για να διευκολύνουν την εύρωστη επικοινωνία μεταξύ τους. Αυτοί οι server είναι στο οικοσύστημα των εσωτερικών και έμπιστων domain του

οργανισμού. Αυτό δίνει το δικαίωμα σε έναν επιτιθέμενο να εισβάλει σε όλη την αρχιτεκτονική του δικτύου
    - Εάν μια συσκευή δικτύου παραβιαστεί τότε ο επιτιθέμενος μπορεί να μοχλεύσει τον έλεγχο και να αποκτήσει δικαιώματα διαχειριστή στο δίκτυο
- **Επιθέσεις σε βάσεις δεδομένων**
    - Οι βάσεις δεδομένων είναι πίσω από κάθε σύστημα των οργανισμών αλλά οι βάσεις δεδομένων είναι ευάλωτες σε επιθέσεις SQL injection
    - Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί τα κανάλια επικοινωνίας μεταξύ του συστήματος και της βάσης δεδομένων και με αυτόν τον τρόπο να υπερκεράσει την προστασία του περιβάλλοντος ελέγχου του Scada
    - Ένας επιτιθέμενος μπορεί να αλλάξει τα δεδομένα της βάσης δεδομένων που χρησιμοποιεί το Scada με αποτέλεσμα να υπάρχει λανθασμένη λειτουργία του Scada.
- **Εγκατάσταση Trojan και κατάληψη όλου του συστήματος καθώς και "man in the middle attack"**
    - Ένας επιτιθέμενος μπορεί να αναδρομολογήσει τα δεδομένα που εκπέμπουν και μεταφέρονται σε ένα δίκτυο. Με τη μεθόδου του μέσου ανθρώπου ο επιτιθέμενος μπορεί να συλλάβει και να αναλύσει τα πακέτα αυτά τα οποία συνήθως σε Scada συστήματα δεν είναι κρυπτογραφημένα.
    - Με όλα τα παραπάνω μπορεί να παραποιήσει το αυθεντικό μήνυμα και αλλάξει την λειτουργία μιας συσκευής
    - Χρησιμοποιώντας ARP poisoning και συλλέγοντας την κίνηση των δικτύων μπορεί να επιτύχει και να διατηρήσει ένας επιτιθέμενος την επικοινωνία με τις συσκευές του Scada χρησιμοποιώντας αυτές όπως θέλει

4.1 Μεθοδολογία δοκιμής διείσδυσης

Η δοκιμή διείσδυσης (penetration testing) είναι μια δοκιμή η οποία γίνεται από ειδικούς στην κυβερνοασφάλεια με σκοπό να ανακαλύψουν όλες τις ευπάθειες και τα τρωτά σημεία ενός συστήματος ή δικτύου. Ο στόχος είναι ο ερευνητής σε μια τέτοια δοκιμή να σκέφτεται και να ενεργεί σαν ένας κακόβουλος επιτιθέμενος χρήστης. Στο τέλος δημιουργείται μια εκτεταμένη έκθεση με τα ευρήματα του ερευνητή με σκοπό να διορθωθούν είτε από τον ίδιο είτε από κάποιον άλλον ειδικό στο μέλλον.

Η μεθοδολογία της δοκιμής διείσδυσης σε Scada συστήματα δεν διαφέρει από αυτήν που γίνεται και σε οποιοδήποτε άλλο δίκτυο ή σύστημα. Αυτό συμβαίνει γιατί σε ένα σύστημα Scada ο δοκιμαστής έχει να κάνει με συσκευές που έχουν λειτουργικά συστήματα (Windows,Linux) , πρωτόκολλα όπως το TCP , εφαρμογές και βάσεις δεδομένων αλλά και με firewall και συστήματα ελέγχου εισβολής των δικτύων(IDS). Παρακάτω θα αναλυθεί η μεθοδολογία της δοκιμής

4.1.1 Έλεγχος ταυτότητας

Σε αυτό το στάδιο γίνεται έλεγχος σε συσκευές και δίκτυα. Πιο συγκεκριμένα γίνεται έλεγχος σε ρυθμίσεις δρομολογητών , πίνακες δρομολόγησης, πίνακες κατανεμητών, έλεγχος καλωδίων, έλεγχος packet sniffing.Στις εγκατεστημένες υπηρεσίες γίνεται επαλήθευση των τοπικών ports. Όσον αφορά ευπάθειες γίνεται local banner grabbing

4.1.2 Περίμετρος Δικτύου

Γίνεται ταυτοποίηση όλων των εξωτερικών συνδέσεων. Επανεξετάζονται όλοι οι κανόνες του firewall,οι τρόποι απομακρυσμένης σύνδεσης. Επίσης γίνεται έλεγχος για ασύρματα δίκτυα και έλεγχος σε φυσική πρόσβαση.

4.1.3 Υποδομή Δικτύου

Αναθεωρούνται οι ρυθμίσεις των δρομολογητών και οι πίνακες των κατανεμητών, έλεγχος καλωδίων, έλεγχος packet sniffing.

4.1.4 Λειτουργικά συστήματα

Αναθεώρηση του επιπέδου διορθώσεων που έχουν γίνει, αναθεώρηση της δυσκολίας των κωδικών, αναθεώρηση των αδειών καταλόγων πρόσβασης και διαμοιρασμού

4.1.5 Εφαρμογές

Γίνεται έλεγχος σε υπηρεσίες και ports που χρησιμοποιεί κάθε εφαρμογή, έλεγχος σε διαπιστευτήρια που έχουν τα λειτουργικά συστήματα, έλεγχος σε απομακρυσμένη λειτουργία.

4.1.6 PLC, αισθητήρες και RTU

Έλεγχος σε κανονισμό update, έλεγχος πολυπλοκότητας κωδικών και έλεγχος σε packet sniffing.

Το penetration testing για να είναι επιτυχημένο πρέπει να ακολουθήσει την ιεραρχία στις μεθόδους και που χρησιμοποιεί με τον ίδιο τρόπο που θα κάνει ένας επιτιθέμενος. Αρχικά ξεκινάει με το στάδιο της σάρωσης και εξερεύνησης του δικτύου .Αυτό μπορεί να γίνει με ειδικά εργαλεία όπως το plcscan και το Modescan που σαρώνει Modbus υπηρεσίες, το nmap και το metasploit. Κατά την σάρωση βρίσκουμε τις συσκευές και τους σταθμούς του Scada με όλες τις πληροφορίες τους όπως IP,ονομασίες και άλλα τα οποία μπορούν να αλλοιωθούν.

Στη συνέχεια γίνεται ανάλυση των πρωτοκόλλων. Γίνεται έλεγχος για το πώς «ζουν» μέσα στο δίκτυο τα πρωτόκολλα, ποια από αυτά μπλοκάρονται από τα firewall, ποια είναι η διαθεσιμότητα με τα τοπικά δίκτυα, πώς γίνεται η μετάβαση από το data link στρώμα στο επίπεδο της εφαρμογής. Επίσης ελέγχεται αν είναι εύκολο να βρεθεί ένα δίκτυο και πόσο εύκολα αναλύεται.

Άρα ανιχνεύονται οι συσκευές και τα πρωτοκολλά τους, παρακολουθούνται οι καταστάσεις του δικτύου, εκτελούνται εντολές, γίνεται αλλαγές στα πακέτα που μεταφέρονται σε πραγματικό χρόνο και τέλος sniffing traffic.Κάποια εργαλεία που χρησιμοποιούνται είναι το Wireshark, το tcpdump και το Hex Viewer.

Στο επόμενο στάδιο γίνεται προσπάθεια χειρισμός των δεδομένων του συστήματος Scada με εργαλεία όπως το Modlib,το OpenDNP3 και το Metasploit. Ελέγχεται επίσης και οποιαδήποτε web εφαρμογή και βάση δεδομένων για επιθέσει SQL Injection και άλλες γνωστές ευπάθειες.

4.2 Κοινές ευπάθειες Scada

Στην κυβερνοασφάλεια, μια ευπάθεια είναι μια αδυναμία που επιτρέπει σε έναν εισβολέα να μειώσει τη διασφάλιση των πληροφοριών ενός συστήματος. Ευπάθεια είναι το σημείο τομής τριών στοιχείων: α) ευαισθησία του συστήματος ή

ελάττωμα, β) η του εισβολέα στο ελάττωμα, και την ικανότητα του εισβολέα να εκμεταλλευτεί το ελάττωμα αυτό.

Για να γίνει πιο κατανοητή η διασφάλιση της κυβερνοασφάλειας ενός Scada συστήματος θα πρέπει να γίνει κατανοητό ότι οι συσκευές ενός Scada δεν έχουν τις ίδιες αρχές λειτουργίας των απλών πληροφορικών συστημάτων. Άλλη μια διαφορά είναι η ιεράρχηση των στόχων της ασφάλειας. Πιο συγκεκριμένα ένα σύστημα Scada πρέπει να οπωσδήποτε να στηρίζεται σε τρείς βασικές αρχές που είναι οι:

1. Εμπιστευτικότητα
2. Ακεραιότητα
3. Διαθεσιμότητα

Είναι το γνωστό στους κύκλους της κυβερνοασφάλειας C(onfidentiality) I(ntergrity) A(vailability).

Στη συνέχεια του κεφαλαίου θα γίνει ανάλυση στις πιο κοινές ευπάθειες των συστημάτων Scada.

4.2.1 Υπερχείλιση buffer (Buffer Overflow)

Η επικύρωση εισόδου χρησιμοποιείται για να διασφαλιστεί ότι το περιεχόμενο που παρέχεται σε μια εφαρμογή δεν παρέχει ακούσια σε έναν εισβολέα πρόσβαση σε λειτουργίες ή σε κλιμάκωση προνομίων. Οι ευπάθειες υπερχείλισης είναι αποτέλεσμα λάθους του προγραμματιστή στον πηγαίο κώδικα. Αυτό συνήθως συμβαίνει επειδή τον προγραμματιστή τον ενδιαφέρει τι μπορεί να γίνει και τι μπορεί να πάει λάθος και δεν εστιάζεται για παράδειγμα σε μια μεταβλητή string που μπορεί να πάρει έως 10000 χαρακτήρες με αποτέλεσμα να προσπαθεί το πρόγραμμα να γράψει περισσότερα δεδομένα σε ένα buffer από το χώρο που διατίθεται στη μνήμη για αυτό. Έτσι υπάρχει ανωμαλία στο σύστημα και αυτό μπορεί να έχει αποτέλεσμα ένας επιτιθέμενος να εισχωρήσει στο σύστημα πηγαίο κώδικα. Επίσης μπορεί να δημιουργήσει μια διαδραστική συνεδρία και να στέλνει εντολές με τα προνόμια που έχει το πρόγραμμα. Επιθέσεις όμως τέτοιου είδους μπορούν να γίνουν και σε ένα δίκτυο μέσω των πακέτων του.

Οι ευπάθειες buffer overflow έχει ανακαλυφθεί ότι είναι οι ποιο κοινές σε προϊόντα που προορίζονται για Scada συστήματα. Παρακάτω είναι μερικά παραδείγματα τρωτών σημείων που εντοπίζονται σε προϊόντα Scada:

- Username και passwords buffer overflows σε προϊόντα HMI (Human-Machine Interface) και πιο συγκεκριμένα στους web servers τους.
- Ευπάθειας υπερχείλισης buffer που προσδιορίζονται σε εφαρμογές PLC
- Πολλαπλές υπερχειλίσεις μνήμης που προσδιορίζονται στο δίκτυο εφαρμογής ανάλυσης πακέτου
- Υπερχειλίσεις μνήμης σε εφαρμογές που δέχονται γραμμή εντολών για τη διαδικασία ελέγχου δικτύου

Για να αποφευχθούν τέτοιες ευπάθειες πρέπει όλος ο κώδικας που γράφεται να κάνει επικύρωση των δεδομένων εισόδου. Οι προγραμματιστές να κάνουν ειδική εκπαίδευση για την ασφαλή γραφή πηγαίου κώδικα.

4.2.2 Η έλλειψη ελέγχου ορίων (Lack of Bounds Checking)

Η έλλειψη επικύρωσης εισόδου για τις τιμές που αναμένεται να είναι σε ένα συγκεκριμένο εύρος, όπως οι δείκτες ενός πίνακα μπορεί να προκαλέσει απροσδόκητη συμπεριφορά και καταστροφή ενός συστήματος. Παράδειγμα εκμετάλευσης μιας τέτοιας ευπάθειας είναι μια επίθεση DoS η οποία έχει σαν αποτέλεσμα την κατάρρευση ενός συστήματος.

4.2.3 Έγχυση εντολών (Command Injection)

Η ευπάθεια command injection επιτρέπει την εκτέλεση σε αυθαίρετες εντολές και κώδικα από τον εισβολέα. Αν ένας κακόβουλος χρήστης εισάγει ένα χαρακτήρα (όπως π.χ. ερωτηματικό) που οριοθετεί το τέλος μιας εντολής και την αρχή μιας άλλης, μπορεί να είναι δυνατόν στη συνέχεια, να τοποθετήσει μια εντελώς νέα και άσχετη εντολή που δεν επρόκειτο να εκτελεστεί. Οι ευπάθειες αυτές συμβαίνουν συνήθως όταν:

- Εισαγωγή δεδομένων από μη αξιόπιστη πηγή
- Τα δεδομένα είναι μέρος μιας συμβολοσειράς που εκτελείται ως μια εντολή από την εφαρμογή.
- Εκτελώντας την εντολή, η εφαρμογή δίνει σε έναν εισβολέα ένα προνόμιο ή μια δυνατότητα που ο εισβολέας δεν θα είχε διαφορετικά.

Για την αποφυγή τέτοιων προβλημάτων καλό είναι να γίνεται σε έναν κώδικα κλήσεις από εσωτερικές βιβλιοθήκες παρά από εξωτερικές διαδικασίες που μπορούν να αναδημιουργήσουν ανεπιθύμητη λειτουργία. Διαφορετικά πρέπει όλες οι εντολές που καλούνται από την εφαρμογή να δημιουργούνται στον κώδικα στατικά.

4.2.4 SQL Injection

Η ευπάθεια αυτή είναι η πιο κοινή σε ιστοσελίδες που έχουν από πίσω τους βάσεις δεδομένων. Το ελάττωμα αυτό ανιχνεύεται εύκολα και εύκολα σημείο εκμετάλλευσης. Έτσι, οποιαδήποτε ιστοσελίδα ή πακέτο λογισμικού με μια ελάχιστη βάση χρηστών είναι πιθανό να υπόκειται σε μια απόπειρα επίθεσης αυτού του είδους.

4.2.5 Cross-Site Scripting (XSS attack)

Επιτρέπει σε επιτιθέμενους να εγχύσει κώδικα σε ιστοσελίδες που είναι σε ευπαθείς web applications. Ο κώδικα επίθεσης εκτελείται στον υπολογιστή του χρήστη-επιτιθέμενου με τα προνόμια ενός web server. Μια τέτοια ευπάθεια έχει την ίδια ρίζα με την ευπάθεια Sql injection δηλαδή εισαγωγή δεδομένων που δεν έχουν φιλτραριστεί σωστά. Ωστόσο, μια cross site scripting επίθεση είναι μοναδική με την έννοια ότι η ίδια web εφαρμογή στέλνει άθελά του κακόβουλου κώδικα στον χρήστη της εφαρμογής. Ένας εισβολέας μπορεί να εισάγει κακόβουλο script σε ένα σύνδεσμο και να έχουν μια ιστοσελίδα η οποία φαίνεται να μην έχει κάτι επιλήψιμο. Το πρόγραμμα περιήγησης του θύματος στη συνέχεια θα τρέξει το κακόβουλο script επειδή ήρθε από τον διακομιστή και θέτει σε κίνδυνο τον υπολογιστή του θύματος χρησιμοποιώντας ένα από τα πολλά exploit του προγράμματος περιήγησης. Οι περισσότερες επιθέσεις XSS βασίζονται στην αλληλεπίδραση του χρήστη και συνήθως έχουν τη μορφή ενός συνδέσμου ο οποίος αποστέλλεται από τον εισβολέα. Οι χρήστες συνήθως κάνουν κλικ σε αυτόν τον σύνδεσμο διότι φαίνεται ότι ο το λίνκ προέρχεται από κάποιον που είναι γνωστός και έχει την εμπιστοσύνη του χρήστη. Η πιο κοινή επίθεση που πραγματοποιείται με cross-site scripting περιλαμβάνει την αποκάλυψη των πληροφοριών που αποθηκεύονται στα cookies του χρήστη .Άλλες επιθέσεις που μπορούν να γίνουν είναι:

1. Γνωστοποιώντας αρχεία στον τελικό χρήστη
2. Εγκατάσταση προγράμματα τύπου Trojan
3. Ανακατεύθυνση του χρήστη σε κάποια άλλη σελίδα ή ιστοσελίδα
4. Τρέχοντας ελέγχους "Active X" από περιοχές που ο χρήστης αντιλαμβάνεται ως αξιόπιστες
5. Τροποποίηση στην παρουσίαση του περιεχομένου.

Οι επιθέσεις XSS αποκαλύπτουν ένα σημείου εισόδου σε ένα δίκτυο Scada έχοντας πρόσβαση σε αυτό. Εκμεταλλεύεται διακομιστές Web που επιστρέφουν δυναμικά παραγόμενες ιστοσελίδες ή επιτρέπουν να δημοσιεύσουν HTML κώδικα ή άλλο ενεργό περιεχόμενο όπως JavaScript, ActiveX, και VBScript σε έναν απομακρυσμένο υπολογιστή.

Αυτό δυνητικά επιτρέπει στον εισβολέα να ανακατευθύνει την σελίδα σε μια κακόβουλη τοποθεσία, να υποκλέψει τις συνεδρίες μεταξύ server-host, να εγκαταστήσει backdoor προγράμματα και να κάνει αναγνώριση όλου του δικτύου. Μερικά παραδείγματα XSS επιθέσεων είναι ευπάθειες σε ιστοσελίδες, σε CGI Scripts σε online βοήθεια.

Ένας άλλο τρόπος επίθεσης είναι το phishing, η οποία εξομοιώνει Scada ιστοσελίδες και ξεγελάει τον χρήστη να εισάγει τους κωδικούς του δίνοντας την δυνατότητα στον εισβολέα να χρησιμοποιήσει με τα προνόμια του χρήστη, τις υπηρεσίες που έχει κάνει login.

Τις περισσότερες φορές ο χρήστης που έχει εξαπατηθεί δεν μπορεί να το καταλάβει ότι έχει δώσει χωρίς την συγκατάθεση του τα στοιχεία του. Για την αντιμετώπιση XSS επιθέσεων πρέπει να γίνουν τα εξής

- Δημιουργία πολιτικής στο Internet από τον οργανισμό
- Εκπαίδευση των χρηστών σε θέματα κυβερνοασφάλειας
- Συνεργασία του IT τμήματος της εταιρείας και των ειδικών ασφαλείας
- Firewall μεταξύ των δικτύων της εταιρείας
- Update σε όλες τις εφαρμογές και firmware συσκευών
- Ασφάλεια σε email και web browsers
- Ασφαλής πηγαίος κώδικας

4.2.6 Path Traversal ευπάθεια

Οι ευπάθειες directory traversal συμβαίνουν όταν οι διαδρομές των αρχείων δεν επικυρώνονται. Επίσης συμβαίνουν όταν το λογισμικό χρησιμοποιεί μια εξωτερική είσοδο για να κατασκευάσει μια διαδρομή που προορίζεται για τον εντοπισμό ενός αρχείου. Ωστόσο, το λογισμικό δεν εξουδετερώνει σωστά πρόσθετα στοιχεία εντός της διαδρομή που μπορεί να προκαλέσει τη πρόσβαση σε μια τοποθεσία η οποία βρίσκεται εξωτερικά της προστατευμένης περιοχής. Έτσι ο εισβολέας είναι σε θέση να διαβάσει, να αντικαταστήσει, ή να δημιουργήσει κρίσιμα αρχεία, όπως προγράμματα, βιβλιοθήκες, ή σημαντικά δεδομένα. Αυτό μπορεί να επιτρέψει σε έναν εισβολέα να:

- Εκτελέσει μη εξουσιοδοτημένο κώδικα ή εντολές
- Διαβάσει ή να τροποποιήσει αρχεία ή καταλόγους
- Να κλείσει ή να επανεκκινήσει κρίσιμα αρχεία ή προγράμματα, προκαλώντας ενδεχομένως μια DoS attack.

Για την αποφυγή αυτής της ευπάθειας είναι απαραίτητη η επικύρωση των δεδομένων εισόδου. Θα γίνει χρήση μιας λίστας με αποδεκτές εισόδους που

συμμορφώνονται απόλυτα με τις πολιτικές του οργανισμού και να απορρίπτει τις εισόδους που δεν είναι σύμφωνες με τις προδιαγραφές αυτές.

4.2.7 Κακή ποιότητα Κώδικα

Η κακή ποιότητα του κώδικα αναφέρεται σε θέματα κώδικα που δεν είναι απαραίτητα τρωτά σημεία, αλλά δείχνουν ότι δεν είχε αναπτυχθεί προσεκτικά μια εφαρμογή. Αυτά τα προϊόντα είναι πιο πιθανό να περιέχουν τρωτά σημεία σε σχέση με ένα προϊόν που έχει αναπτυχθεί χρησιμοποιώντας πρακτικές ασφαλούς προγραμματισμού.

4.2.8 Η χρήση των δυνητικά επικίνδυνων λειτουργιών

Είναι γνωστές σαν ανασφαλείς επικλήσεις συναρτήσεων, όπου η εφαρμογή καλεί μια πιθανώς επικίνδυνη συνάρτηση η οποία μπορεί να οδηγήσει σε μια ευπάθεια. Το πρόβλημα αυτό έγκειται στο ότι ο προγραμματιστής πρέπει να είναι υπεύθυνος για την επικύρωση των δεδομένων εισόδου. Επισφαλής C/C++ συναρτήσεις είναι οι πιο περιβόητες δυνητικά επικίνδυνες συναρτήσεις και αυτές που μπορούν να δημιουργήσουν τα περισσότερα προβλήματα.

Η εκπαίδευση των προγραμματιστών σε δημιουργία ασφαλή κώδικα και πολιτικές ασφαλούς ανάπτυξης λογισμικού είναι το μόνο μέτρο που μπορούν να πάρουν οι εταιρείες και οι οργανισμοί που αναπτύσσουν εφαρμογές.

4.2.9 Ακατάλληλος Έλεγχος Πρόσβασης

Εάν ένα πρόγραμμα αυτοματισμού δεν εκτελεί ή εκτελεί λανθασμένα έλεγχο στην πρόσβαση του οι χρήστες είναι σε θέση να έχουν πρόσβαση σε δεδομένα ή να εκτελέσουν ενέργειες που δεν πρέπει και δεν επιτρέπεται να πραγματοποιούν.

Τα παρακάτω είναι συγκεκριμένες διαπιστώσεις που συνδέονται με τον ακατάλληλο έλεγχο πρόσβασης:

- Η πρόσβαση δεν περιορίζεται μόνο στα αντικείμενα που το απαιτούν.
- Scada πρωτόκολλα επέτρεπαν σε συστήματα Scada να διαβάζουν και να αντικαταστούν αρχεία σε όλο το δίκτυο χωρίς να χρειάζεται logging
- Πληροφορίες ρυθμίσεων και τεχνικών προδιαγραφών είναι ελεύθερα σε οποιονδήποτε
- Έλλειψη role - based ελέγχου ταυτότητας των συσκευών αυτοματισμού
- Ένας απομακρυσμένος χρήστης μπορεί να ανεβάσει ένα αρχείο σε οποιαδήποτε διαδρομή στον υπολογιστή προορισμού.
- Αυθαίρετη λήψη αρχείων επιτρέπεται σε Scada hosts.
- Αυθαίρετη αποστολή αρχείων επιτρέπεται σε Scada hosts.
- Ένας απομακρυσμένος χρήστης μπορεί να εκτελέσει όποια εφαρμογή θέλει
- Επιτρέπεται η ανώνυμη περιήγηση

Για την αποφυγή τέτοιων προβλημάτων πρέπει οι οργανισμοί να σχεδιάσουν την αρχιτεκτονική τους ώστε κάθε χρήστης να έχει μόνο τα επαρκή και τα λιγότερο δυνατόν προνόμια ώστε να κάνουν την δουλειά τους.

4.2.10 Εκτέλεση με περιττά προνόμια

Οι υπηρεσίες περιορίζονται στα δικαιώματα των χρηστών που χορηγούνται μέσω του λογαριασμού χρήστη που σχετίζεται με αυτούς. Η εκμετάλλευση κάθε υπηρεσίας θα μπορούσε να επιτρέψει σε έναν εισβολέας μια θέση στο δίκτυο του

Scada με τα δικαιώματα της υπηρεσίας αυτής. Η κλιμάκωση των δικαιωμάτων μπορεί να επιτευχθεί με την αξιοποίηση μιας ευάλωτης υπηρεσίας που τρέχει με περισσότερα προνόμια από ό, τι ο εισβολέας έχει αποκτήσει έως εκείνη την στιγμή. Αυτή η ευπάθεια είναι πολύ συχνή και παρακάτω είναι μερικά συγκεκριμένα ευρήματα που σχετίζονται με αυτό το θέμα ευπάθειας:

- Κατάχρηση του λογαριασμού των διαχειριστών
- Απομακρυσμένη εκμετάλλευση των Scada εφαρμογών που επιτρέπει root level πρόσβαση στο Scada
- Η υπηρεσία βάσης δεδομένων τρέχει σαν διαχειριστής.

Από προεπιλογή Από προεπιλογή, μερικές Scada εγκαταστάσεις ξεκινούν τις υπηρεσίες ως root χρήστης και root ομάδα. Αυτό δεν είναι αναγκαίο διότι υπάρχει μεγαλύτερο φάσμα επιθέσεων σε έναν κακόβουλο χρήστη. Ουσιαστικά, μια συνιστώμενη πρακτική είναι η υπηρεσία να λειτουργεί με ελάχιστα προνόμια έτσι ώστε σε περίπτωση σφάλματος, να μην εκμεταλλεύονται από κακόβουλους χρήστες.

4.2.11 Θέματα Παράκαμψης Πιστοποίησης

Όταν Το λογισμικό δεν εκτελεί σωστά τον έλεγχο ταυτότητας, επιτρέπει να παρακάμπτει την πιστοποίηση με διάφορες μεθόδους. Οι διαδικτυακές υπηρεσίες που αναπτύχθηκαν για Scada τείνουν να είναι ευάλωτες σε επιθέσεις που μπορεί να εκμεταλλευτεί ένας εισβολέας για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.

Συχνά οι κατασκευαστές δικτύων χρησιμοποιούν σαν αρχιτεκτονική DMZ δίκτυα για να προστατέψουν κρίσιμα συστήματα και για να περιορίσουν την έκθεση σε συσκευές δικτύου. Θέματα ευπάθειας στο DMZ Scada Web servers παρέχουν το πρώτο βήμα στον επιτιθέμενο επιτρέποντας την πρόσβαση στο εσωτερικό του εξωτερικού Scada συνόρου.

4.2.12 Man in the Middle επίθεση και οι ευπάθειες της

Οι εντολές από της HMI συσκευές προκαλούν συγκεκριμένες ενέργειες στον αυτοματισμό του Scada. Στη συνέχεια alarms στέλνονται στον χρήστη ο οποίος ειδοποιείται για τις ενέργειες που έχουν γίνει. Η ακεραιότητα και ο χρόνος που παραδίδονται τα alarms και οι εντολές είναι κρίσιμης σημασίας σε Scada συστήματα.

Για να καθοριστεί η ασφαλής επικοινωνία μεταξύ δύο πλευρών, είναι σημαντικό να λαμβάνονται επαρκώς και να επαληθεύεται η ταυτότητα των οντοτήτων σε κάθε άκρο του καναλιού επικοινωνίας. Ανεπαρκή ή ασυνεπής επαλήθευση μπορεί να οδηγήσει σε ανεπαρκή ή εσφαλμένη ταυτοποίηση των οντοτήτων που επικοινωνούν. Ένας εισβολέας μπορεί να το αξιοποιήσει αυτό παρεμβάλλοντας στην μεταξύ τους επικοινωνία των οντοτήτων και μεταμφιέζεται ως την αρχική αυθεντική οντότητα. Επίσης ο εισβολέας είναι σε θέση να στείλει μη έγκυρα δεδομένα να εμφανίζονται στους χρήστες που επικοινωνούν .

Μερικά συμπεράσματα για τις επιθέσεις **man in the middle** είναι τα εξής:

- Οι επιθέσεις γίνονται στην επικοινωνία μεταξύ του εξοπλισμού στο πεδίο και του χειριστή του Scada
- Γίνεται μετάδοση στους κωδικούς πρόσβασης σε μορφή απλού κειμένου, η οποία επιτρέπει την απομακρυσμένη υποκλοπή των κωδικών
- Έλλειψη ακεραιότητας ελέγχου πακέτων.

Η λύση για να μην υπάρξει πρόβλημα με επιθέσεις man in the middle είναι οι σχεδιαστές των συστημάτων Scada να πιστοποιούν πλήρως και τις δύο πλευρές που επικοινωνούν και αν υπάρχει η δυνατότητα να κρυπτογραφηθεί το κανάλι επικοινωνίας.

4.2.13 Ελλιπής κρυπτογράφηση ευαίσθητων δεδομένων

Τα διαπιστευτήρια που αποστέλλονται μέσω του δικτύου σε απλό κείμενο αφήνουν το σύστημα ευπαθές σε μη εξουσιοδοτημένο χρήστη. Αν οι επιτιθέμενοι είναι σε θέση να υποκλέψει ονόματα χρήστη και κωδικούς πρόσβασης, θα είναι σε θέση να συνδεθεί στο σύστημα με τα προνόμια του εν λόγω χρήστη. Ένα από τα μεγαλύτερα ζητήματα ασφάλειας είναι η ευρεία χρήση μη κρυπτογραφημένων δικτύων επικοινωνίας. Πολλές εφαρμογές και υπηρεσίες χρησιμοποιούν πρωτόκολλα που περιλαμβάνουν χαρακτήρες που είναι αναγνώσιμα από τους χρήστες. Εργαλεία που κυκλοφορούν ελεύθερα στο διαδίκτυο και είναι ικανά να υποκλέψουν την κίνηση του δικτύου, μπορούν εύκολα να πάρουν τους χαρακτήρες αυτούς και να τους διαβάσουν, να τους αλλάξουν και να τους χειριστούν όπως θέλουν. Η λύση σε αυτό το σενάριο είναι να υπάρχει παντού σωστή κρυπτογράφηση.

4.2.14 Χρήση επικίνδυνων αλγόριθμων κρυπτογράφησης

Μερικά τυπικά πρωτόκολλα κρυπτογράφησης πληροφορικής που χρησιμοποιούνται έχουν αξιοποιηθεί κακόβουλα λόγω αδυναμιών κρυπτογράφησης. Για την καλύτερη κατανόηση της ευπάθειας των πρωτοκόλλων θα αναφερθούν τα παρακάτω:

- Η κρυπτογράφηση απομακρυσμένης απεικόνισης μπορεί να «σπάσει»
- Κωδικοί διαχειριστών δικτύων βρίσκονται σε hashes στο δίκτυο του Scada
- Αλγόριθμοι με αδύναμη κρυπτογράφηση χρησιμοποιούνται για την είσοδο σε συστήματα
- Ευπαθείς SSL βιβλιοθήκες χρησιμοποιούνται σε ασύρματες συσκευές.

Η λύση στην χρήση επικίνδυνων αλγορίθμων είναι οι διαχειριστές να εκτελέσουν τις απαραίτητες έρευνες πριν να επιλέξουν της ενσωμάτωση ενός αλγορίθμου κρυπτογράφησης. Θα πρέπει επίσης να είναι όλα τα συστήματα ενημερωμένα με τα τελευταία update.

4.2.15 Αδύναμοι ή μη χρήση κωδικών εισόδου

Μετά από έρευνες έχουν διαπιστωθεί πολλές εφαρμογές που δεν χρησιμοποιούν κωδικό εισόδου, που σημαίνει ότι ο καθένας μπορεί να τις χρησιμοποιήσει .Παρακάτω είναι μερικά παραδείγματα Scada που δεν χρησιμοποιούν κωδικούς εισόδου:

- Οι υπηρεσίες βάσης δεδομένων έχει ρυθμιστεί ώστε να μην χρειάζεται κωδικό εισόδου κατά την είσοδο
- NULL συνδέσεις επιτρέπουν την απομακρυσμένη διαχείριση του συστήματος με ερωτήματα που δεν χρειάζονται έλεγχο ταυτότητας

- Το μήκος του κωδικού πρόσβασης μπορεί να είναι μηδέν χαρακτήρες. Κάθε χρήστης του συστήματος μπορεί να έχει ένα κενό κωδικό.

Οποιαδήποτε κακή επιλογή σε κωδικούς πρόσβασης μπορούν εύκολα να ανακαλυφθούν από τον άνθρωπο ή από αλγόριθμους έτσι ώστε ένας εισβολέας να αποκτήσει μη εξουσιοδοτημένη πρόσβαση. Για αυτό το λόγο όσο πιο μεγάλος και σύνθετος είναι ένας κωδικός εισόδου, τόσο πιο δύσκολα μπορεί να ανακαλυφθεί.

Επίσης προεπιλεγμένοι κωδικοί είναι πλέον γνωστοί σε όλον τον κόσμο. Παρακάτω θα παρατεθούν συγκεκριμένα παραδείγματα αδύναμων κωδικών:

- Μερικοί Scada hosts είχαν σαν κωδικό διαχειριστή με τρεις χαρακτήρες.
- Οι αδύναμοι κωδικοί που υποκλέπτονται δίνουν πρόσβαση διαχειριστή
- Η προεπιλεγμένη SNMP συμβολοσειρά χρησιμοποιούνταν σε πολλούς hosts
- Βρέθηκαν αρκετά εύκολους κωδικούς.
- Ο εργοστασιακός κωδικός δεν είχε αλλάξει
- Συσκευές Scada έχουν πρόσβαση από το διαδίκτυο με τους εργοστασιακούς κωδικούς

Για αυτό το λόγο είναι πολύ σημαντικό σε κάθε οργανισμό να υπάρχει αυστηρή και συγκεκριμένη αυτόματη πολιτική για τους κωδικούς εισόδου. Χωρίς τις πολιτικές αυτές δεν μπορούν να ελεγχθούν οι αμέτρητοι κωδικοί που βρίσκονται στο οικοσύστημα ενός Scada.

Μέσα στην πολιτική αυτή θα πρέπει οπωσδήποτε να υπάρχει όριο λήξης των κωδικών, να υπάρχει χρήση κλειδώματος του λογαριασμού σε περίπτωση πολλαπλών λανθασμένων προσπαθειών και να μην υπάρχει ιστορικό κωδικών αποθηκευμένο.

Βήματα για τη βελτίωση της κυβερνοασφάλειας των δικτύων Scada:

1. **Αναγνώριση και ταυτοποίηση όλων των συνδέσεων στα δίκτυα SCADA:**

Διεξαγωγή μίας διεξοδικής ανάλυσης δικτύου για την αξιολόγηση κινδύνου και την αναγκαιότητα της κάθε σύνδεσης στο δίκτυο SCADA.
Ανάπτυξη μίας ολοκληρωμένης κατανόησης όλων των συνδέσεων με το δίκτυο Scada και πόσο καλά είναι προστατευμένες. Ταυτοποίηση και αξιολόγηση των παρακάτω τύπων συνδέσεων:
• Εσωτερικά τοπικά δίκτυα και δίκτυα ευρείας περιοχής, συμπεριλαμβανομένων των εταιρικών δικτύων
• Το Internet
• Συσκευές Wireless δικτύων, συμπεριλαμβανομένων των δορυφορικών ανοδικών ζεύξεων
• Modem ή dial-up συνδέσεις
• Συνδέσεις με επιχειρηματικούς συνεργάτες, προμηθευτές ή ρυθμιστικούς οργανισμούς

2. **Αποσύνδεση μη απαραίτητων συνδέσεων με το δίκτυο Scada:**

Για να εξασφαλιστεί ο υψηλότερος βαθμός ασφάλειας των συστημάτων Scada, απομονώνεται το δίκτυο Scada από τα άλλα δίκτυα στο μέγιστο βαθμό που είναι δυνατό. Οποιαδήποτε σύνδεση με άλλο δίκτυο προαναγγέλλει κινδύνους ασφάλειας, ειδικότερα αν η σύνδεση δημιουργεί μονοπάτι από ή στο Internet. Αν και οι απευθείας συνδέσεις με άλλα δίκτυα πιθανόν επιτρέπουν σημαντικές πληροφορίες να διαβιβαστούν αποδοτικά και άνετα, μη ασφαλείς συνδέσεις απλά

δεν αξίζουν το κόπο. Η απομόνωση των δικτύων SCADA πρέπει να είναι πρωταρχικός σκοπός για να επιτευχθεί η απαιτούμενη προστασία.

Στρατηγικές όπως η χρήση των «demilitarized zones» (DMZs-αποστρατικοποιημένες ζώνες) και η αποθήκευση δεδομένων μπορούν να επιτύχουν την ασφάλεια μεταφοράς των δεδομένων από δίκτυο Scada σε επιχειρηματικά δίκτυα. Ωστόσο, πρέπει να σχεδιαστούν και να υλοποιηθούν κατάλληλα προκειμένου να αποφευχθεί η είσοδος επιπλέον κινδύνων μέσω ακατάλληλης διαμόρφωσης.

3. Αξιολόγηση και ενδυνάμωση της ασφάλειας των εναπομείναν συνδέσεων στο δίκτυο Scada:

Διεξαγωγή penetration testing ή ανάλυση ευπαθειών των εναπομεινάντων συνδέσεων στο δίκτυο SCADA για να αξιολογηθεί η προστασία που συνδέεται με αυτά τα μονοπάτια. Χρήση αυτών των πληροφοριών σε συνδυασμό με τις διαδικασίες διαχείρισης για την ανάπτυξη μίας εύρωστης στρατηγικής προστασίας για οποιοδήποτε μονοπάτι στο δίκτυο SCADA. Επειδή το δίκτυο SCADA είναι τόσο ασφαλή όσο το πιο αδύναμο σημείο σύνδεσης του, είναι απαραίτητη η εφαρμογή firewall, συστήματα ανίχνευσης διεισδύσεων (intrusion detection systems - IDSs) , και άλλα κατάλληλα μέτρα ασφαλείας σε κάθε σημείο εισόδου. Διαμόρφωση κανόνων firewall για να την απαγόρευση της πρόσβασης από και προς το δίκτυο SCADA, και να είναι όσο το δυνατόν συγκεκριμένοι όταν επιτρέπονται οι εγκριμένες συνδέσεις. Για παράδειγμα, ένα Independent System Operator (ISO) δεν πρέπει να χορηγείται τυφλά στη πρόσβαση συστήματος απλά επειδή υπάρχει η ανάγκη για σύνδεση σε ορισμένα πεδία του συστήματος SCADA.

Στρατηγική τοποθέτηση IDSs σε κάθε σημείο εισόδου για την προειδοποίηση του προσωπικού ασφαλείας σε ενδεχόμενες παραβιάσεις των δικτύων ασφαλείας. Οι διαχειριστές των οργανισμών πρέπει να καταλάβουν και να αποδεχθούν τις ευθύνες τους για τους κινδύνους που συνδέονται με οποιαδήποτε σύνδεση σε δίκτυο SCADA.

4. Ενδυνάμωση των δικτύων Scada με την αφαίρεση και απενεργοποίηση των περιττών υπηρεσιών

Οι διακομιστές ελέγχου SCADA (server) χτίζονται σε εμπορικά ή open-source λειτουργικά συστήματα που μπορούν να εκτεθούν σε επιθέσεις μέσω προεπιλεγμένων δικτυακών υπηρεσιών. Στο μέγιστο δυνατό βαθμό, η αφαίρεση ή απενεργοποίηση υπηρεσιών που δεν χρησιμοποιούνται μπορούν να ελαττώσουν των κίνδυνο μίας απευθείας επίθεσης. Αυτό είναι ιδιαίτερα σημαντικό όταν τα δίκτυα SCADA είναι διασυνδεδεμένα με άλλα δίκτυα. Να μην επιτρέπεται μία υπηρεσία ή ένα χαρακτηριστικό σε ένα δίκτυο SCADA αν δεν έχει πραγματοποιηθεί αξιολόγηση κινδύνου (risk assessment) των επιπτώσεων της πρόσβασης της υπηρεσίας/ή του χαρακτηριστικού που να δείχνουν ότι τα οφέλη αυτής της υπηρεσίας/χαρακτηριστικού υπερβαίνουν κατά πολύ μία ενδεχόμενη εκμετάλλευσης της ευπάθειας.

Παραδείγματα υπηρεσιών για αφαίρεση από τα δίκτυα SCADA αποτελούν τα δίκτυα αυτοματοποιημένων μέτρων ανάγνωσης, απομακρυσμένα συστήματα τιμολόγησης, υπηρεσίες email και πρόσβαση στο Internet. Ένα παράδειγμα ενός χαρακτηριστικού για απενεργοποίηση είναι η απομακρυσμένη συντήρηση. Πολυάριθμες κατευθυντήριες γραμμές για την ασφαλή διαμόρφωση τόσο για εμπορικές όσο και ανοικτού κώδικα λειτουργικά συστήματα είναι στο δημόσιο τομέα, όπως οι οδηγίες ασφαλείας του Εθνικού Οργανισμού Ασφάλειας (National Security Agency) . Επιπροσθέτως, η στενή συνεργασία με τους κατασκευαστές SCADA για

τον εντοπισμό ασφαλών διαμορφώσεων και τον συντονισμό όλων των αλλαγών στα λειτουργικά συστήματα ούτως ώστε να εξασφαλιστεί ότι αυτή η κατάργηση ή απενεργοποίηση αυτών των υπηρεσιών δεν προκαλούν downtime, διακοπή της υπηρεσίας ή απώλεια υποστήριξης.

5. **Μην βασίζεστε σε ιδιόκτητα πρωτόκολλα για την προστασία του συστήματός σας.**

Μερικά συστήματα SCADA χρησιμοποιούν μοναδικά, ιδιόκτητα πρωτόκολλα για την επικοινωνία μεταξύ των συσκευών πεδίου και των servers. Συχνά, η ασφάλεια των συστημάτων SCADA βασίζεται αποκλειστικά στο απόρρητο των πρωτοκόλλων αυτών. Δυστυχώς, ασαφή πρωτόκολλα παρέχουν πολύ λίγη "πραγματική" ασφάλεια.

Μην βασίζεστε σε ιδιόκτητα πρωτόκολλα ή εργοστασιακά προεπιλεγμένες ρυθμίσεις για την προστασία του συστήματός σας. Επιπλέον, απαιτείστε ότι οι κατασκευαστές αποκαλύπτουν οποιεσδήποτε πίσω πόρτες ή διασυνδέσεις κατασκευαστών στα συστήματα SCADA σας, και την προσδοκία από αυτούς ότι θα μας παρέχουν συστήματα που είναι ικανά να ασφαλίζονται.

6. **Εφαρμογή των χαρακτηριστικών ασφαλείας που παρέχονται από τη συσκευή και το σύστημα κατασκευαστών.**

Τα περισσότερα παλιά συστήματα SCADA (περισσότερα συστήματα σε χρήση) δεν έχουν απόλυτα χαρακτηριστικά ασφαλείας . Οι ιδιοκτήτες συστημάτων SCADA πρέπει να επιμείνουν ότι τα συστήματα κατασκευαστών εφαρμόζουν τα χαρακτηριστικά ασφαλείας με τη μορφή ενημερωμένων εκδόσεων κώδικα προϊόντος ή αναβαθμίσεων. Ορισμένες νεότερες συσκευές SCADA αποστέλλονται με βασικά χαρακτηριστικά ασφαλείας, αλλά αυτά συνήθως απενεργοποιούνται για να εξασφαλιστεί η ευκολία εγκατάστασης τους.

Αναλύστε κάθε συσκευή SCADA για να διαπιστωθεί αν τα χαρακτηριστικά ασφαλείας είναι ενεργά. Επιπλέον, προεπιλεγμένες εργοστασιακές ρυθμίσεις ασφαλείας (όπως firewalls δίκτυο υπολογιστών) συχνά παρέχουν τη μέγιστη χρηστικότητα, αλλά ελάχιστη ασφάλεια. Ρυθμίστε όλα τα χαρακτηριστικά ασφαλείας για να παρέχουν το μέγιστο επίπεδο (ασφάλειας). Επιτρέψτε ρυθμίσεις υπό τη μέγιστη ασφάλεια μόνο μετά από ενδελεχή αξιολόγηση του κινδύνου για τις συνέπειες της μείωσης του επιπέδου ασφαλείας.

7. **Καθιέρωση αυστηρών ελέγχων σε οποιοδήποτε μέσο που χρησιμοποιείται ως «πίσω πόρτα» στο SCADA δίκτυο.**

Όπου υπάρχουν «πίσω πόρτες» ή συνδέσεις κατασκευαστών στα συστήματα SCADA, πρέπει να εφαρμοστεί ισχυρή ταυτοποίηση για να εξασφαλιστούν ασφαλείς οι επικοινωνίες. Μόντεμ, ασύρματα και ενσύρματα δίκτυα που χρησιμοποιούνται για τις επικοινωνίες και τις συντηρήσεις αντιπροσωπεύουν μια σημαντική ευπάθεια των δικτύων SCADA και των απομακρυσμένων περιοχών. Επιτυχείς επιθέσεις “war dialing” ή “war driving” θα μπορούσαν να επιτρέψουν σε έναν εισβολέα να παρακάμψει όλους τους άλλους ελέγχους και να έχει άμεση πρόσβαση σε ένα δίκτυο SCADA ή τους πόρους του. Για την ελαχιστοποίηση του κινδύνου αυτού, πρέπει να απενεργοποιήσετε την εισερχόμενη πρόσβαση και να την αντικαταστήσετε με κάποιο είδος συστήματος επανάκλησης.

8. **Εφαρμογή εσωτερικών και εξωτερικών συστημάτων ανίχνευσης εισβολής και τη θέσπιση 24-ωρης παρακολούθησης περιστατικών.**

Για να είσαι σε θέση να ανταποκριθείς αποτελεσματικά στις επιθέσεις στον κυβερνοχώρο, θα πρέπει να καταρτιστεί μια στρατηγική ανίχνευσης εισβολής που περιλαμβάνει την προειδοποίηση διαχειριστών της κακόβουλης δραστηριότητας του δικτύου που προέρχονται από εσωτερικές ή εξωτερικές πηγές. Παρακολούθηση εισχωρήσεων με σύστημα ανίχνευσης είναι απαραίτητη 24 ώρες την ημέρα. Αυτή η δυνατότητα μπορεί εύκολα να δημιουργηθεί μέσα από ένα σύστημα ειδοποίησης.

Επιπλέον, οι διαδικασίες αντιμετώπισης περιστατικών πρέπει να είναι σε θέση να επιτρέπουν μια αποτελεσματική άμυνα σε οποιαδήποτε επίθεση. Για να συμπληρωθεί η παρακολούθηση του δικτύου, θα πρέπει να επιτρέπεται η σύνδεση με όλα τα συστήματα και τα αρχεία καταγραφής του συστήματος ελέγχου καθημερινά για τον εντοπισμό ύποπτων δραστηριοτήτων, το συντομότερο δυνατό (log files).

9. Εκτέλεση τεχνικών ελέγχων των συσκευών και δικτύων SCADA, καθώς και κάθε άλλου συνδεδεμένου δικτύου, για τον εντοπισμό ζητημάτων ασφάλειας.

Η διενέργεια τεχνικών ελέγχων των συσκευών και των δικτύων SCADA είναι ζωτικής σημασίας για την συνεχιζόμενη αποτελεσματικότητα της ασφάλειας. Πολλά εμπορικά και ανοικτού πηγαίου κώδικα εργαλεία για την ασφάλεια είναι διαθέσιμα επιτρέποντας στους διαχειριστές του συστήματος να διεξάγουν τους ελέγχους των συστημάτων / δικτύων για τον εντοπισμό ενεργών υπηρεσιών και κοινών τρωτών σημείων. Η χρήση αυτών των εργαλείων δεν μπορεί να λύσει συστημικά προβλήματα, αλλά θα εξαλείψει τα «μονοπάτια της ελάχιστης αντίστασης» που ένας εισβολέας θα μπορούσε να εκμεταλλευτεί.

Αναλύστε τις προσδιορισμένες ευπάθειες για να καθοριστεί η σημασία τους, και να λάβετε διορθωτικές ενέργειες, κατά περίπτωση. Επιπλέον, επανεξετάστε τα συστήματα μετά από τις διορθωτικές ενέργειες για να διασφαλιστεί ότι τα θέματα ευπάθειας έχουν πράγματι εξαλειφθεί. Κάντε επίσης ενεργή σάρωση των μη-παραγωγικών περιβαλλόντων για τον εντοπισμό και την αντιμετώπιση πιθανών προβλημάτων.

10. Διεξαγωγή φυσικών ερευνών της ασφάλειας και να αξιολογηθούν όλες οι απομακρυσμένες τοποθεσίες που συνδέονται με το SCADA δίκτυο για την αξιολόγηση της ασφάλειάς τους.

Κάθε τοποθεσία που έχει μια σύνδεση με το δίκτυο SCADA είναι ένας στόχος, ειδικά οι μη επανδρωμένες ή αφύλακτες απομακρυσμένες περιοχές. Η διεξαγωγή μίας φυσικής έρευνας ασφαλείας και η πρόσβαση σημείων απογραφής σε κάθε εγκατάσταση που διαθέτει σύνδεση με το σύστημα SCADA πρέπει να γίνει οπωσδήποτε. Επίσης να γίνει εντοπισμός και αξιολόγηση οποιαδήποτε πηγής πληροφοριών συμπεριλαμβανομένης της εξ αποστάσεως:

- τηλεφωνικό δίκτυο / υπολογιστής /καλώδια οπτικών ινών, που θα μπορούσαν να αξιοποιηθούν,
- συνδέσεις ραδιοφωνικές και μικροκυματικές που είναι εκμεταλλεύσιμες, τερματικά υπολογιστών που θα μπορούσαν να έχουν πρόσβαση,
- και ασύρματα τοπικά σημεία πρόσβασης στο δίκτυο περιοχής.

Να γίνει εντοπισμός και εξάλειψη των ενιαίων σημείων της αποτυχίας σύνδεσης.

Η ασφάλεια του χώρου πρέπει να είναι επαρκής για την ανίχνευση ή την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Αποτροπή απομακρυσμένων «ζωντανών» σημείων πρόσβασης δικτύου και αφύλακτων σημείων απλά και μόνο για ευκολία.

11. Καθιέρωση SCADA « Red Teams» για τον εντοπισμό και την αξιολόγηση πιθανών σεναρίων επίθεσης.

Καθιερώστε μια "Red Team" για τον εντοπισμό πιθανών σεναρίων επίθεσης και αξιολόγηση των πιθανών τρωτών σημείων του συστήματος. Χρησιμοποιήστε μία ποικιλία ανθρώπων που μπορούν να παρέχουν πληροφορίες για τις αδυναμίες του συνολικού δικτύου, των συστημάτων SCADA, των φυσικών συστημάτων και των ελέγχων ασφαλείας. Οι άνθρωποι που εργάζονται στο σύστημα κάθε μέρα έχουν μεγάλη γνώση των θεμάτων ευπάθειας του δικτύου SCADA και θα πρέπει να ζητείται η γνώμη κατά τον προσδιορισμό των πιθανών σεναρίων επίθεσης και των πιθανών συνεπειών.

Επίσης, βεβαιωθείτε ότι ο κίνδυνος από κακόβουλες εμπιστευτικές πληροφορίες έχουν αξιολογηθεί πλήρως, δεδομένου ότι αυτό αποτελεί ένα από τις μεγαλύτερες απειλές για έναν οργανισμό. Καλλιεργήστε πληροφορίες που προκύπτουν από την αξιολόγηση της διαδικασίας διαχείρισης κίνδυνου από την "Red Team" , για να αξιολογηθούν οι πληροφορίες και να δημιουργηθούν οι κατάλληλες στρατηγικές προστασίας.

Τα ακόλουθα βήματα επικεντρώνονται σε δράσεις διαχείρισης για τη δημιουργία ενός αποδοτικού προγράμματος κυβερνόασφάλειας.

1) **Σαφής καθορισμός των ρόλων κυβερνοασφάλειας, των ευθυνών και των αρχών για τους διαχειριστές του συστήματος αλλά και των χρηστών.**

Το προσωπικό ενός οργανισμού πρέπει να κατανοήσει τις συγκεκριμένες προσδοκίες και τις ανάγκες που συνδέονται με την προστασία των πληροφοριών τεχνολογικών πόρων μέσω του προσδιορισμού σαφών και λογικών ρόλων και ευθυνών. Επιπλέον, βασικό κλειδί για την επιτυχία πρέπει να είναι η επαρκής διάθεση της εξουσίας του οργανισμού για να εκτελεστούν οι ανατεθειμένες ευθύνες τους.

Πολύ συχνά, η καλή κυβερνοασφάλεια επαφίεται στην πρωτοβουλία του ατόμου, η οποία συνήθως οδηγεί σε ασυνεπείς εφαρμογές και αναποτελεσματική ασφάλεια.

Να δημιουργηθεί μια οργανωτική διάρθρωση κυβερνοασφάλειας, που να καθορίζει τους ρόλους και τις ευθύνες και να προσδιορίζει με σαφήνεια το πώς τα θέματα κυβερνοασφάλειας κλιμακώνονται και πως κοινοποιούνται σε περίπτωση έκτακτης ανάγκης.

2) **Η αρχιτεκτονική του δικτύου εγγράφων και ο εντοπισμός στα συστήματα που εξυπηρετούν κρίσιμες λειτουργίες ή περιέχουν ευαίσθητες πληροφορίες που απαιτούν πρόσθετα επίπεδα προστασίας.**

Αναπτύξτε και τεκμηριώστε μιας ισχυρή αρχιτεκτονική ασφάλειας πληροφοριών ως μέρος μιας διαδικασίας για τη δημιουργία μίας αποτελεσματικής στρατηγικής προστασίας. Είναι σημαντικό οι οργανισμοί να σχεδιάζουν τα δίκτυά τους με γνώμονα την ασφάλεια και να έχουν μια ισχυρή κατανόηση της αρχιτεκτονικής του δικτύου τους σε όλη την διάρκεια της ζωής του. Ιδιαίτερης σημασίας είναι μια σε βάθος κατανόηση των λειτουργιών που επιτελούν τα συστήματα και η ευαισθησία των αποθηκευμένων πληροφοριών. Χωρίς αυτή την κατανόηση, ο κίνδυνος αυτός δεν μπορεί να εκτιμηθεί σωστά και οι στρατηγικές προστασίας ενδέχεται να μην επαρκούν.

Η τεκμηρίωση της αρχιτεκτονικής της ασφάλειας των πληροφοριών και των συστατικών τους είναι κρίσιμη όσον αφορά τη κατανόηση της συνολικής στρατηγικής για την προστασία και τον εντοπισμό αποτυχημένων ενιαίων σημείων.

3) Εφαρμογή αυστηρής, σε εξέλιξη διαδικασίας διαχείρισης των κινδύνων.

Μια λεπτομερής κατανόηση των κινδύνων στο δίκτυο υπολογιστικών πόρων από denial-of-service επιθέσεις και ο συμβιβασμός της ευπάθειας των ευαίσθητων πληροφοριών είναι απαραίτητα για ένα αποτελεσματικό πρόγραμμα κυβερνο-ασφάλειας.

Οι αξιολογήσεις κινδύνου αποτελούν την τεχνική βάση της κατανόησης και είναι ζωτικής σημασίας για τη διαμόρφωση αποτελεσματικών στρατηγικών για τον μετριασμό των θεμάτων ευπάθειας και τη διατήρηση της ακεραιότητας των υπολογιστικών πόρων. Αρχικά, εκτελείται βασική ανάλυση κινδύνου η οποία βασίζεται σε μια τρέχουσα αξιολόγηση της απειλής που θα χρησιμοποιηθεί για την ανάπτυξη μιας στρατηγικής για την προστασία του δικτύου. Λόγω της ραγδαίας αλλαγής της τεχνολογίας και την εμφάνιση νέων απειλών σε καθημερινή βάση, μια συνεχής διαδικασία αξιολόγησης των κινδύνων είναι απαραίτητη.
Επίσης, χρειάζεται αλλαγές ρουτίνας έτσι ώστε η στρατηγική προστασίας να βεβαιωθείτε ότι παραμένει αποτελεσματικό.
Θεμελιώδους σημασίας για τη διαχείριση των κινδύνων είναι ο προσδιορισμός του υπολειπόμενου κινδύνου με μια στρατηγική προστασίας του δικτύου που είναι σε ισχύ και η αποδοχή του κινδύνου αυτού από τη διοίκηση.

4) Καθιέρωση μιας στρατηγικής για την προστασία του δικτύου με βάση την αρχή της άμυνας σε βάθος.

Μια θεμελιώδης αρχή που πρέπει να είναι μέρος οποιασδήποτε στρατηγικής για την προστασία του δικτύου είναι η άμυνα σε βάθος. Η άμυνα σε βάθος πρέπει να εξεταστεί νωρίς, στη φάση του σχεδιασμού της αναπτυξιακής διαδικασίας, και πρέπει να αποτελεί αναπόσπαστη διαδικασία σε όλες τις τεχνικές λήψης αποφάσεων που σχετίζονται με το δίκτυο. Η χρησιμοποίηση τεχνικών και διοικητικών ελέγχων για τον περιορισμό των απειλών που προέρχονται από συγκεκριμένους κινδύνους στο μέγιστο δυνατό σε όλα τα επίπεδα του δικτύου, είναι απαραίτητη. Πρέπει να αποφεύγονται τα ενιαία σημεία αποτυχίας.

Η άμυνα της κυβερνοασφάλειας πρέπει να είναι πολυεπίπεδη για τον περιορισμό και των επιπτώσεων τυχόν συμβάντων ασφάλειας. Επιπλέον, κάθε στιβάδα πρέπει να προστατεύεται έναντι άλλων συστημάτων. Για παράδειγμα, για την προστασία ενάντια στην απειλή εμπιστευτικών πληροφοριών, ο περιορισμός των χρηστών να έχουν πρόσβαση μόνο στα απαραίτητα για την εκτέλεση των πόρων καθήκοντά τους, προτείνεται ως κύριο μέτρο.

5) Σαφής προσδιορισμός των απαιτήσεων της κυβερνο-ασφάλειας.

Οι οργανισμοί και οι εταιρείες χρειάζονται δομημένα προγράμματα ασφάλειας με ανατεθειμένες απαιτήσεις για τη δημιουργία προσδοκιών επιτρέποντας να είναι προσωπικά υπεύθυνοι οι ίδιες. Οι τυποποιημένες πολιτικές και διαδικασίες χρησιμοποιούνται συνήθως για την καθιέρωση και θεσμοθέτηση ενός προγράμματος κυβερνοασφάλειας. Ένα επίσημο πρόγραμμα είναι απαραίτητο για τη δημιουργία μίας συνεπούς, βασισμένη σε πρότυπα προσέγγισης για την κυβερνοασφάλεια η οποία να εξαλείφει την αποκλειστική εξάρτηση από την ατομική πρωτοβουλία.

Επίσης, πολιτικές και διαδικασίες πρέπει να ενημερώνουν τους υπαλλήλους για τις συγκεκριμένες ευθύνες τους στην κυβερνοασφάλεια αλλά και τις συνέπειες

της μη τήρησης των εν λόγω αρμοδιοτήτων τους. Μπορούν επίσης αυτές οι διαδικασίες να παρέχουν καθοδήγηση σχετικά με τις ενέργειες που λαμβάνονται κατά τη διάρκεια ενός περιστατικού κυβερνοασφάλειας και την προώθηση αποδοτικών και αποτελεσματικών δράσεων κατά τη διάρκεια του χρόνου της κρίσης. Ως μέρος προσδιορισμού των απαιτήσεων της κυβερνοασφάλειας, περιλαμβάνονται συμφωνίες χρήστη και σημεία προειδοποιήσεων.

Πρέπει να θεσπιστούν απαιτήσεις προκειμένου να ελαχιστοποιηθεί η απειλή από κακόβουλες εμπιστευτικές πληροφορίες, συμπεριλαμβανομένης της ανάγκης για τη διεξαγωγή στους ελέγχους και τον περιορισμό των προνομίων του δικτύου στα απολύτως απαραίτητα.

6) Αποτελεσματική θέσπιση διαδικασιών διαχείρισης διαμόρφωσης.

Μια θεμελιώδης διαδικασία διαχείρισης που απαιτείται για τη διατήρηση ενός ασφαλούς δικτύου είναι η διαχείριση διαμόρφωσης. Η διαχείρισης της διαμόρφωσης πρέπει να καλύπτει και τις διαμορφώσεις υλικού και τις διαμορφώσεις λογισμικού. Αλλαγές στο υλικό ή το λογισμικό μπορεί να εισάγουν εύκολα θέματα ευπάθειας που υπονομεύουν την ασφάλεια του δικτύου. Οι διαδικασίες αυτές απαιτούνται για την αξιολόγηση και τον έλεγχο οποιαδήποτε αλλαγής, για να εξασφαλιστεί ότι το δίκτυο παραμένει ασφαλές. Η διαχείριση της διαμόρφωσης ξεκινά με μια καλά δοκιμασμένη και τεκμηριωμένη βάση ασφαλείας για τα διάφορα συστήματα σας.

7) Διεξαγωγή ρουτίνας αυτοαξιολόγησης.

Οι ισχυρής απόδοσης διαδικασίες αξιολόγησης είναι αναγκαίες για να παρέχουν οι οργανισμοί ανατροφοδότηση στην αποδοτικότητα της κυβερνοασφάλειας και στην τεχνική εφαρμογή αυτών. Ένα δείγμα ωριμότητας ενός οργανισμού είναι η ικανότητα αυτό-προσδιορισμού των ζητημάτων του, την διεξαγωγή ανάλυσης της ρίζας της αιτίας και η εφαρμογή αποδοτικών δράσεων διόρθωσης που εντοπίζονται στα υποψήφια και συστημικά προβλήματα. Οι διαδικασίες αυτό-αξιολόγησης είναι φυσιολογικά κομμάτια ενός αποδοτικού προγράμματος κυβερνοασφάλειας συμπεριλαμβανομένων των σαρώσεων ρουτίνας για ευπάθειες του αυτοματοποιημένου ελέγχου του δικτύου και την αυτό αξιολόγηση του οργανισμού της ατομικής απόδοσης.

8) Καθιέρωση αντιγράφων ασφαλείας του συστήματος και σχεδίων αποκατάστασης καταστροφών.

Η θέσπιση ενός σχεδίου αποκατάστασης καταστροφών που επιτρέπει την ταχεία ανάκαμψη από κάθε έκτακτης ανάγκης (συμπεριλαμβανομένης μιας επίθεσης στην κυβερνο-ασφάλεια) είναι ζωτικής σημασίας .

Τα αντίγραφα ασφαλείας του συστήματος αποτελούν ουσιαστικό μέρος οποιουδήποτε σχεδίου και επιτρέπει την ταχεία ανασυγκρότηση του δικτύου μετά από μια επίθεση. Σχεδιάστε ασκήσεις ρουτίνας αποκατάστασης καταστροφών γιανα εξασφαλιστεί ότι η λειτουργία και το προσωπικό είναι εξοικειωμένοι με αυτά. Επίσης πρέπει να γίνεται η εφαρμογή και η πραγματοποίηση των κατάλληλων αλλαγών στα σχέδια αποκατάστασης καταστροφών με βάση τα διδάγματα από τις ασκήσεις που διενεργήθηκαν.

9) Η ανώτερη οργανωτική ηγεσία θα πρέπει να καθορίσει τις προσδοκίες για την κυβερνοασφάλεια, τις επιδόσεις και την αναμονή ατόμων υπόλογων για τις επιδόσεις τους.

Η αποτελεσματική απόδοση της κυβερνοασφάλειας απαιτεί τη δέσμευση από την ηγεσία και από τα ανώτερα διευθυντικά στελέχη της οργάνωσης. Είναι σημαντικό τα ανώτερα διευθυντικά στελέχη να δημιουργήσουν την προσδοκία για ισχυρή κυβερνοασφάλεια και να επικοινωνούν με τους υπόλοιπους διαχειριστές σε όλη την οργάνωση. Είναι επίσης σημαντικό η ανώτερη οργανωτική ηγεσία να δημιουργεί μια δομή για την υλοποίηση ενός προγράμματος κυβερνοασφάλειας. Η δομή αυτή θα προωθήσει τη συνεπή εφαρμογή και την ικανότητα να διατηρηθεί ένα ισχυρό πρόγραμμα κυβερνοασφάλειας. Πολύ σημαντικό είναι επίσης τα άτομα να λογοδοτούν για τις επιδόσεις και τις πράξεις τους που σχετίζονται με την κυβερνοασφάλεια. Αυτό ο έλεγχος πρέπει να περιλαμβάνει τους διευθυντές , τους διαχειριστές των συστημάτων, τους τεχνικούς και τους χρήστες.

10) Καθιέρωση πολιτικών και τη διενέργεια εκπαίδευσης για ελαχιστοποίηση της πιθανότητας ότι το προσωπικό θα αποκαλύψει κατά λάθος ευαίσθητες πληροφορίες σχετικά με το σύστημα SCADA, το σχεδιασμό, τη λειτουργία ή την ασφάλεια ελέγχου.

Η απελευθέρωση των δεδομένων που σχετίζονται με το δίκτυο SCADA πρέπει να γίνεται μόνο σε αυστηρή, αναγκαία γνώριμη βάση, και μόνο σε πρόσωπα ρητά εξουσιοδοτημένα να λαμβάνουν τις πληροφορίες αυτές. Η «Κοινωνική μηχανική» (social engineering) ,είναι η συλλογή πληροφοριών για έναν υπολογιστή ή ένα δίκτυο υπολογιστών μέσω ερωτημάτων σε αφελείς χρήστες ,και είναι συχνά το πρώτο βήμα για μια κακόβουλη επίθεση σε δίκτυα υπολογιστών.

Όσο περισσότερες πληροφορίες αποκαλύπτονται για έναν υπολογιστή ή ένα δίκτυο υπολογιστών, τόσο πιο ευάλωτο ο υπολογιστής/δίκτυο είναι. Ποτέ μην αποκαλύπτεται τα στοιχεία που σχετίζονται με δίκτυο SCADA, συμπεριλαμβανομένων των ονομάτων και στοιχείων επικοινωνίας σχετικά με το σύστημα / διαχειριστές, λειτουργικά συστήματα υπολογιστών, ή / και φυσική και λογική θέση των ηλεκτρονικών υπολογιστών και των συστημάτων του δικτύου σε τηλέφωνα ή στο προσωπικό, εκτός αν εγκριθεί ρητά να λαμβάνουν τις πληροφορίες αυτές κάποια άτομα. Οι αιτήσεις για πληροφορίες από αγνώστους πρέπει να αποστέλλονται σε ένα κεντρικό δίκτυο τοποθεσίας ασφαλείας για την επαλήθευση και την εκπλήρωση τους από ειδικούς. Συχνά οι άνθρωποι είναι ο αδύναμος κρίκος σε ένα κατά τα άλλα ασφαλές δίκτυο .Η Διεξαγωγή εκστρατειών εκπαίδευσης και ευαισθητοποίησης προκειμένου να εξασφαλίζεται ότι το προσωπικό παραμένει επιμελές στη φύλαξη ευαίσθητων πληροφοριών του δικτύου, ιδιαίτερα των κωδικών τους είναι αναγκαία από κάθε οργανισμό.

5.2 Στατιστικά δεδομένα κυβερνοασφάλειας Scada

Η έρευνα βασίστηκε διαφορετικές πηγές μεταξύ τους όπως βάσεις δεδομένων ευπαθειών, πακέτα exploit , επιστημονικά συνέδρια και εξειδικευμένα άρθρα και εκδόθηκε το 2012. Είναι σίγουρο ότι από τότε έως τώρα τα στοιχεία είναι διαφορετικά, μπορούμε όμως να βγάλουμε ασφαλή συμπεράσματα για την πορεία της κυβερνοασφάλειας στα συστήματα Scada.

Οι κύριες πηγές που βασίστηκε η έρευνα είναι:

Βάσεις δεδομένων ευπαθειών

- ICS-CERT
- NVD
- CVE
- Bugtraq

- OSVDB
- Mitre Oval Repositories
- exploit-db
- Siemens Product CERT

Exploit packs

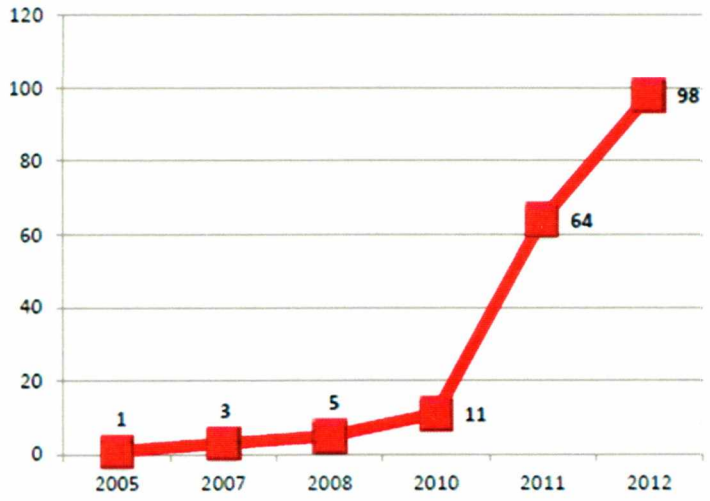
- SAINTexploit
- Metasploit Framework
- Immunity Canvas
    - Agora Pack
    - Agora SCADA+
    - D2 Exploit Pack
    - White Phosphorus exploit pack
    - VulnDisco Exploit Pack

Η δυναμική της ανακάλυψης ευπαθειών

Οι ειδικοί στην ασφάλεια των πληροφοριακών συστημάτων ανακάλυψαν μόνο εννιά ευπάθειες από το 2005 έως το 2010. Από την στιγμή που βρέθηκε το Stuxnet δόθηκε μεγαλύτερη σημασία στην ασφάλεια των Scada με αποτέλεσμα το 2011 να έχουν ανακαλυφθεί 64 ευπάθειες. Επιπλέον τους πρώτους μήνες το 2012 βρέθηκαν 98 ευπάθειες.

Σύνολο Ευπαθειών	Έτος
1	2005
3	2007
5	2008
11	2010
64	2011
98	2012

Πίνακας 1

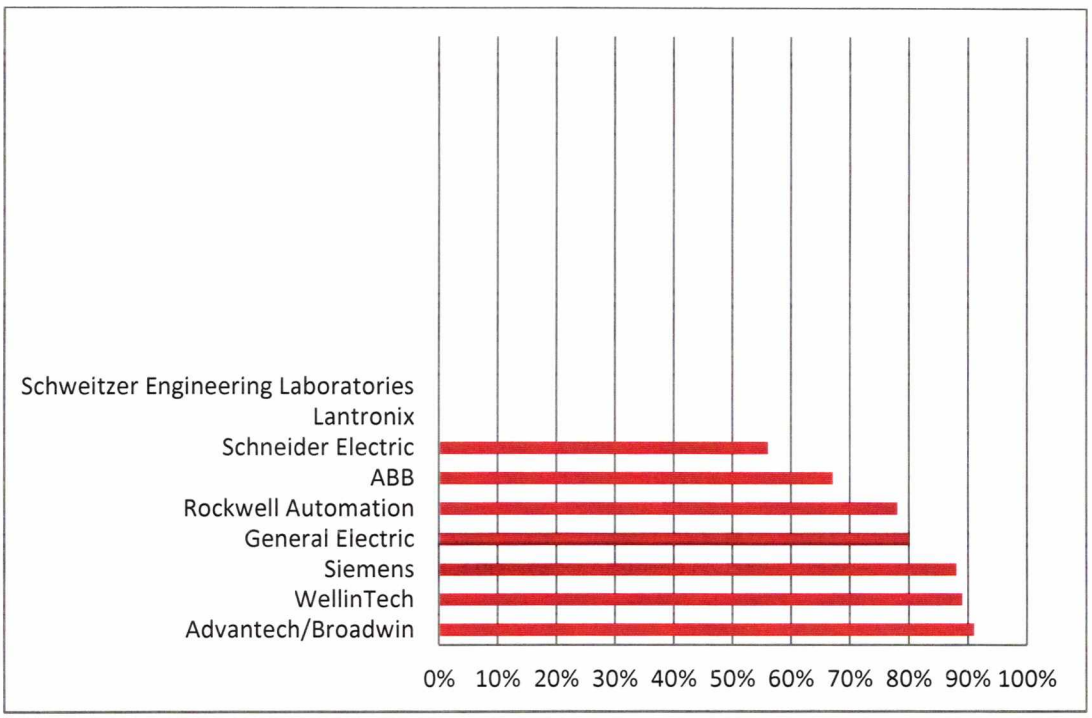


Γράφημα 1

Αριθμός ευπαθειών ανά κατασκευαστών

Automated Solutions	2
Schweitzer Engineering Laboratories	2
RuggedCom	2
Lantronix	3
Progea	3
ABB	3
Sielco Sistemi	3
Iconics	5
Measuresoft	6
Ecava	5
Emerson	6
WellinTech	9
7-Technologies	12
General Electric	15
Invensys Wonderware	15
Schneider Electric	18
Advantech/Broadwin	22
Siemens	42
Emerson	6
Rockwell Automation	9

Πίνακας 2



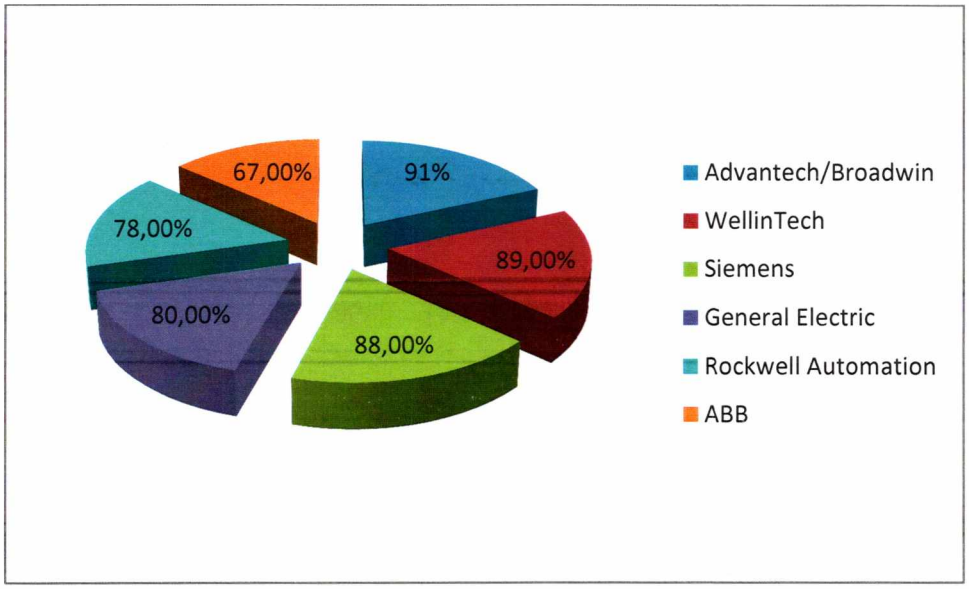
Γράφημα 2

Ο μεγαλύτερος αριθμός των τρωτών σημείων σε Scada εμφανίστηκε στα πιο κοινά εξαρτήματα. Για αυτό το λόγο πολλοί κατασκευαστές άλλαξαν την αντιμετώπιση με μια πιο ενεργή προσέγγιση. Για παράδειγμα η Siemens έφτιαξε ειδική ομάδα που ασχολείται αποκλειστικά με την κυβερνοασφάλεια.

Ευπάθειες σε σχέση με το που βρίσκονται στο σύστημα αυτοματισμού

SCADA	87
HMI	49
PLC	20
Hardware	11
Software	7
Interface/Protocol	1

Πίνακας 3



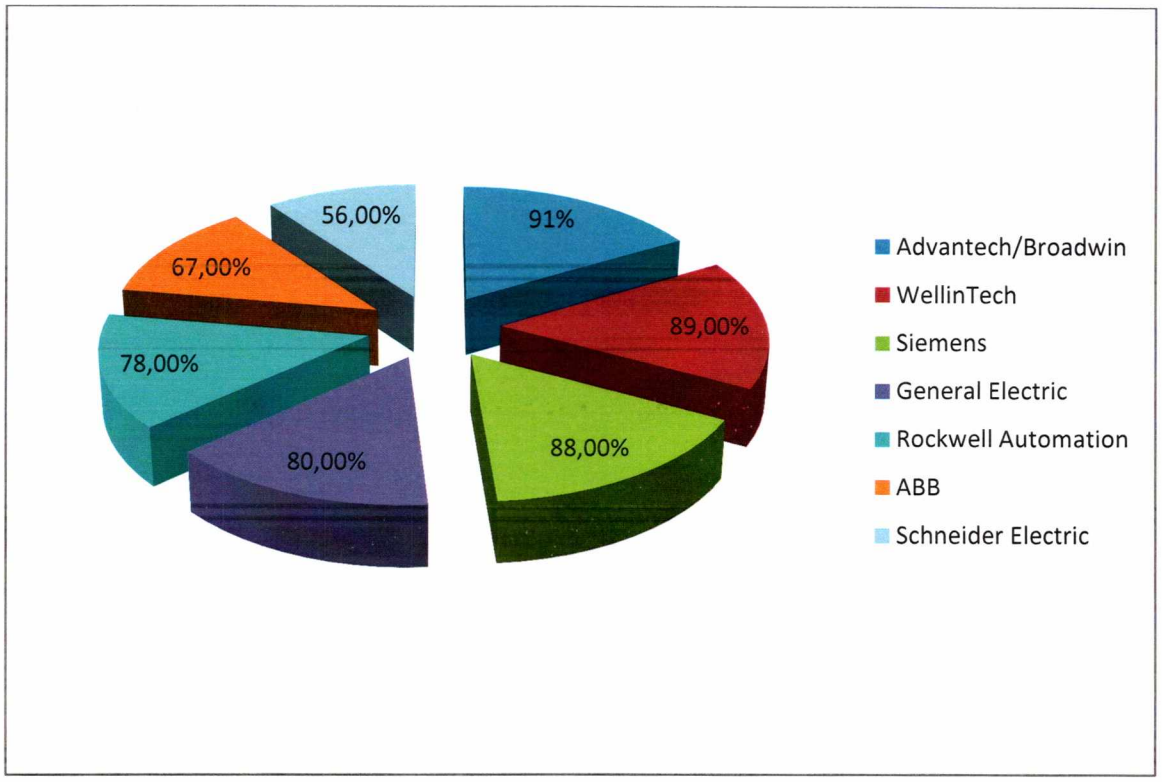
Γράφημα 3

Κατάταξη ευπαθειών σε σχέση με τον τύπο τους και τις πιθανές συνέπειες τους.

Πάνω από το ένα τρίτο σχετίζονται με buffer overflow, όπως αναφέραμε και πιο πάνω μια ανωμαλία πουθενά πρόγραμμα υπερβαίνει τα όρια του buffer γράφοντας δεδομένα

Τύπος ευπάθειας	Ποσοστό
Buffer Overflow	36%
Remote Code Execution	13,14%
Web(client-side)	9,14%
Web(server-side)	10,86%
Local Privilege Escalation	2,29%
DoS/Data Integrity	5,71%
Authentication/Key Management	22,86%

Πίνακας 4



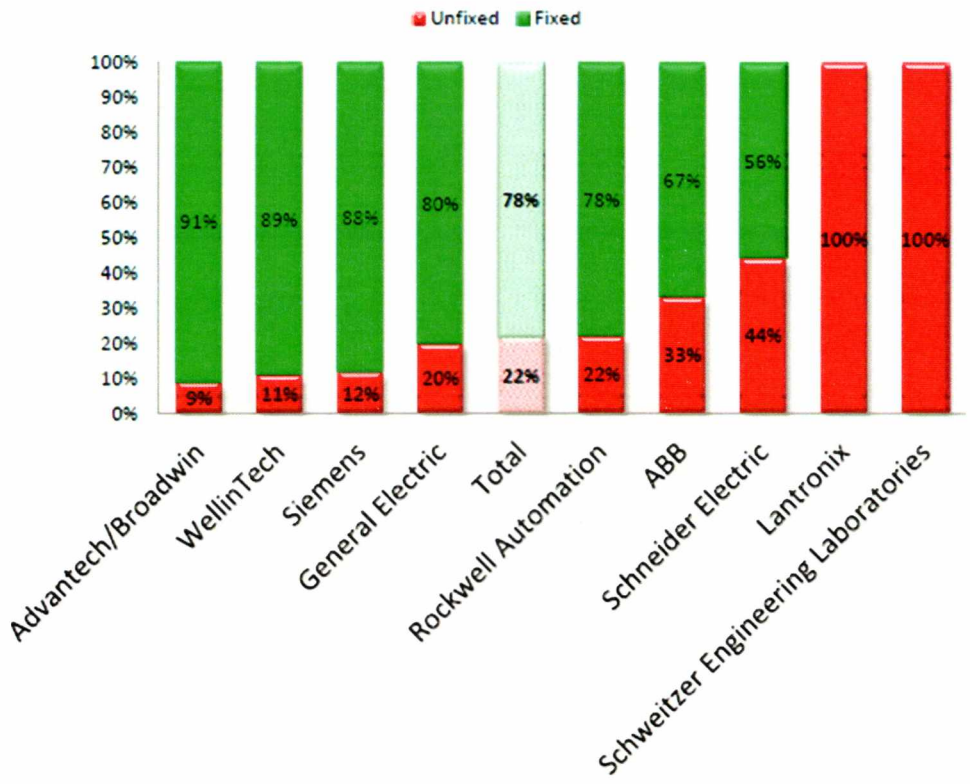
Γράφημα 4

Ποσοστό ευπαθειών που επιδιορθώθηκαν

Μια απεικόνιση των ποσοστών των ευπαθειών που επιδιορθώθηκαν δείχνει πόσο σοβαρά αντιμετώπισαν τα προβλήματα αυτά οι κατασκευαστές. Για παράδειγμα η Siemens επιδιόρθωσε το 88% των ευπαθειών και η Advantech το 91%

Εταιρεία	Ποσοστό
Advantech/Broadwin	91%
WellinTech	89,00%
Siemens	88,00%
General Electric	80,00%
Rockwell Automation	78,00%
ABB	67,00%
Schneider Electric	56,00%
Lantronix	0,00%
Schweitzer Engineering Laboratories	0,00%

Πίνακας 5



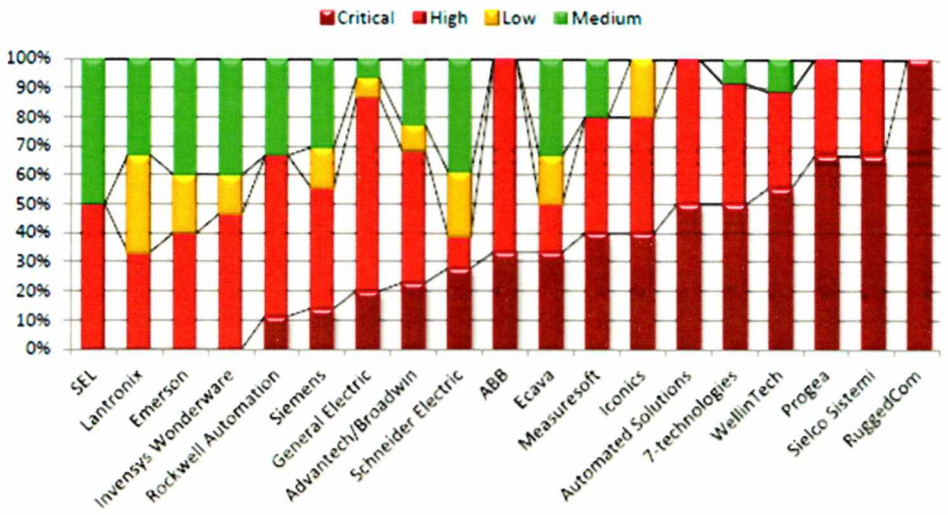
Γράφημα 5

Ποσοστό ευπαθειών αναλόγως της επικινδυνότητας

Οι ευπάθειες χωρίζονται σε 4 κατηγορίες.Critical,High,Medium και Low και αναπαριστώνται αναλόγως των κατασκευαστών.

	Critical, %	High, %	Medium, %	Low, %
SEL	–	50	50	–
Lantronix	–	33	33	33
Emerson	–	40	40	20
Invensys Wonderware	–	47	40	13
Rockwell Automation	11	56	33	–
Siemens	14	42	31	14
General Electric	20	67	7	7
Advantech/Broadwin	23	45	23	9
Schneider Electric	28	11	39	22
ABB	33	67	–	–
Ecava	33	17	33	17
Measuresoft	40	40	20	–
Iconics	40	40	–	20
Automated Solutions	50	50	–	–
7-Technologies	50	42	8	–
WellinTech	56	33	11	–
Progea	67	33	–	–
Sielco Sistemi	67	33	–	–
RuggedCom	100	–	–	–

Πίνακας 6



Γράφημα 6

Συμπεράσματα στατιστικής

1. Η ιστορία των συστημάτων κυβερνοασφάλειας στη βιομηχανία χωρίζεται σε δύο μέρη , αυτό που είναι πριν την εμφάνιση του Stuxnet και αυτό που είναι μετά. Σε σχέση με το 2010 και την προηγούμενη πενταετία, οι ευπάθειες αυξήθηκαν 20 φορές.
2. Τα νούμερα των ευπαθειών αυξάνονται με δραματικό ρυθμό. Ο αριθμός των ελαττωμάτων στην κυβερνοασφάλεια που βρέθηκαν μέσα σε 10 μήνες το 2012 είναι ίσο με τον αριθμό που βρέθηκαν μέσα σε εφτά χρόνια.
3. Τα τρωτά σημεία που εντοπίζονται βρίσκονται πρωτίστως σε κοινά προϊόντα και το μεγαλύτερο μέρος των κατασκευαστών τις αντιμετωπίζουν αρκετά γρήγορα.
4. Πάνω από το 65% των ευπαθειών χαρακτηρίζονται υψηλού κινδύνου και ρίσκου.
5. Η αξιοποίηση κάθε δεύτερης ευπάθειας επιτρέπει σε έναν εισβολέα να εκτελέσει αυθαίρετο κώδικα στο σύστημα Scada.
6. Περισσότερο από το 40% των συστημάτων SCADA που διατίθενται από το Internet είναι ευάλωτα και μπορούν να παραβιαστούν από ανεπαρκώς εκπαιδευμένους χρήστες.
7. Οι Η.Π.Α. και η Ευρώπη ηγούνται στα Scada συστήματα τα οποία υπάρχουν στο Internet και επιδεικνύουν την πιο σκεπτικιστική συμπεριφορά απέναντι στην ασφάλεια τους σε σχέση με οποιαδήποτε άλλη περιοχή του πλανήτη.
8. Περισσότερο από το ένα τρίτο στα κενά ασφαλείας των διαθέσιμων συστημάτων Scada προκαλούνται από σφάλματα στη διαμόρφωση τους ,συμπεριλαμβανομένης και της χρήσης προεπιλεγμένων κωδικών πρόσβασης.
9. Το τέταρτο μέρος των τρωτών σημείων των διαθέσιμων συστημάτων Scada σχετίζεται με την έλλειψη στις απαραίτητες ενημερώσεις ασφαλείας.

5.3 Αποτελέσματα Πρακτικής Έρευνας

Σε αυτό το κεφάλαιο θα γίνει μια μικρή επίδειξη εισβολής σε συστήματα Scada. Όλες οι ενέργειες που έχουν γίνει δεν έχουν κακόβουλο σκοπό, απλά θα γίνει σάρωση για ευπαθή δίκτυα Scada σε όλο τον κόσμο και σε κάποια από αυτά θα γίνει προσπάθεια εισβολής με χρήση τεχνικών που έχουν αναφερθεί παραπάνω.

5.3.1 Μηχανή Αναζήτησης Shodan

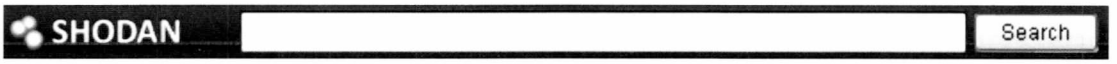
Για την έρευνα την σάρωση ευπαθών δικτύων βιομηχανικών δικτύων Scada θα γίνει η χρήση της μηχανής αναζήτησης Shodan. Είναι μια μηχανή αναζήτησης η οποία δημιουργήθηκε από τον προγραμματιστή John Matherly. Η μηχανή αναζήτησης Shodan βρίσκει διασυνδεδεμένες με το Internet συσκευές και έχει πολλές διαφορές με τις τυπικές μηχανές αναζήτησης που χρησιμοποιούνται ευρέως. Μια τυπική μηχανή αναζήτησης ψάχνει για δεδομένα σε ιστοσελίδες και στη συνέχεια τα κατηγοριοποιεί σε ένα ευρετήριο και επιστρέφει αυτό το ευρετήριο στον χρήστη. Η μηχανή αναζήτησης Shodan όμως «ανακρίνει» πόρτες (ports) και επιστρέφει τα αποτελέσματα των banner αφού πρώτα τα κατηγοριοποιήσει σε ευρετήριο. Τα banners είναι κείμενο με πληροφορίες που περιγράφουν τις υπηρεσίες της συσκευής στην οποία γίνεται αναζήτηση. Επίσης τα banner διαφοροποιούνται αναλόγως με τον τύπο των υπηρεσιών. Παρακάτω είναι ένα παράδειγμα ενός HTTP banner:

HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Sat, 03 Oct 2015 06:09:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6466
Connection: keep-alive

Στο επόμενο κείμενο είναι επίσης ένα banner για το βιομηχανικό πρωτόκολλο συστήματος ελέγχου Siemens S7:

Copyright: Original Siemens Equipment
PLC name: S7_Turbine
Module type: CPU 313C
Unknown (129): Boot Loader A
Module: 6ES7 313-5BG04-0AB0 v.0.3
Basic Firmware: v.3.3.8
Module name: CPU 313C
Serial number of module: S Q-D9U083642013
Plant identification:
Basic Hardware: 6ES7 313-5BG04-0AB0 v.0.3

Η κύρια λειτουργία της Shodan είναι η αναζήτηση, η οποία γίνεται συμπληρώνοντας τους όρους που ψάχνουμε σε ένα περιθώριο κειμένου όπως το παρακάτω:



Επιπλέον εκτός από τα banners η μηχανή αναζήτησης Shodan συλλέγει και μετα-δεδομένα για τις συσκευές όπως η γεωγραφική τους θέση, το λειτουργικό σύστημα που λειτουργεί, το όνομα τους μέσα στο δίκτυο και άλλα πολλά. Για να καταφέρουμε να περιορίσουμε και να έχουμε πιο ακριβή αποτελέσματα στους όρους που ψάχνουμε, είναι δυνατόν να κάνουμε χρήση κάποιων βασικών φίλτρων :

- After/before: περιορίζει τα αποτελέσματα ημερολογιακά
- Country: : περιορίζει τα αποτελέσματα ανά χώρα
- Hostname: περιορίζει τα αποτελέσματα από το hostname του domain
- Net: περιορίζει τα αποτελέσματα μιας συγκεκριμένης IP ή συγκεκριμένου υποδικτύου
- Operation system: περιορίζει τα αποτελέσματα σε συγκεκριμένο λειτουργικό σύστημα
- Ports: περιορίζει τα αποτελέσματα σε συγκεκριμένες υπηρεσίες

Όσον αφορά τις πόρτες των υπηρεσιών, παρακάτω υπάρχουν κάποια ενδεικτικά παραδείγματα:

- modbus port 502
- dnp port 19999
- dnp3 port 20000
- fieldbus port 1089-91
- ethernet/IP port 2222
- etherCAT port 34980
- profinet port 34962-64

Στην πρώτη αναζήτηση μας όπως φαίνεται και στην παρακάτω εικόνα, βρέθηκαν 13.849 ευπαθή συστήματα Scada τα οποία είναι διάσπαρτα σε όλον τον κόσμο με κάποια από αυτά και στην Ελλάδα.

Στη συνέχεια θα γίνει αναζήτηση σύμφωνα με τις πόρτες των πρωτοκόλλων που αναφέραμε και πριν

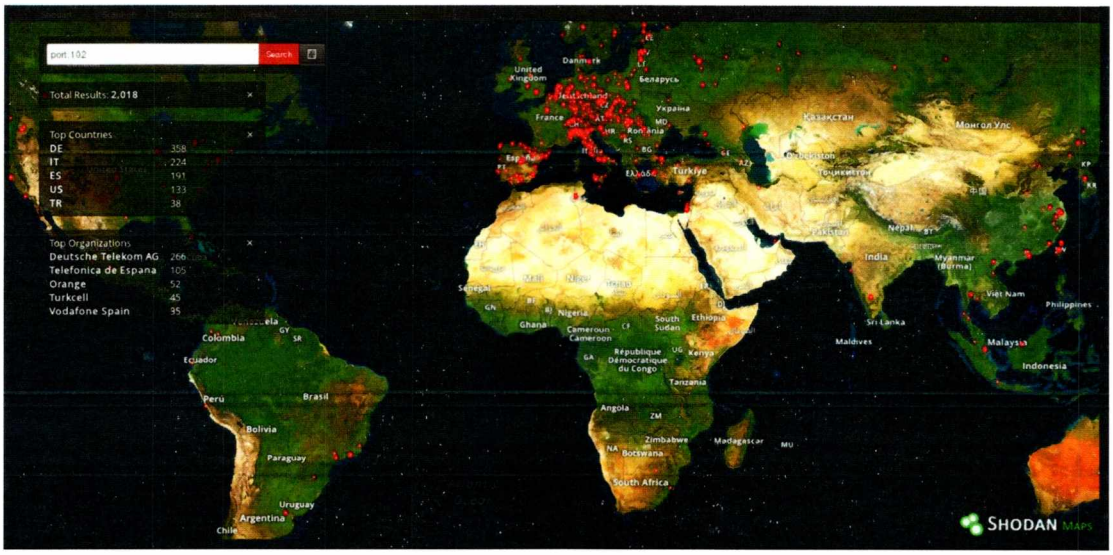
MODBUS

Το Modbus είναι ίσως το πιο δημοφιλές πρωτόκολλο για βιομηχανικά συστήματα ελέγχου. Παρέχει εύκολη πρόσβαση στα συστήματα ελέγχου χωρίς να χρειάζεται αυθεντικοποίηση .

Στην έρευνα πού έγινε βρέθηκαν 11.205 αποτελέσματα με πιθανά ευπαθές στοιχεία.

SIEMENS S7

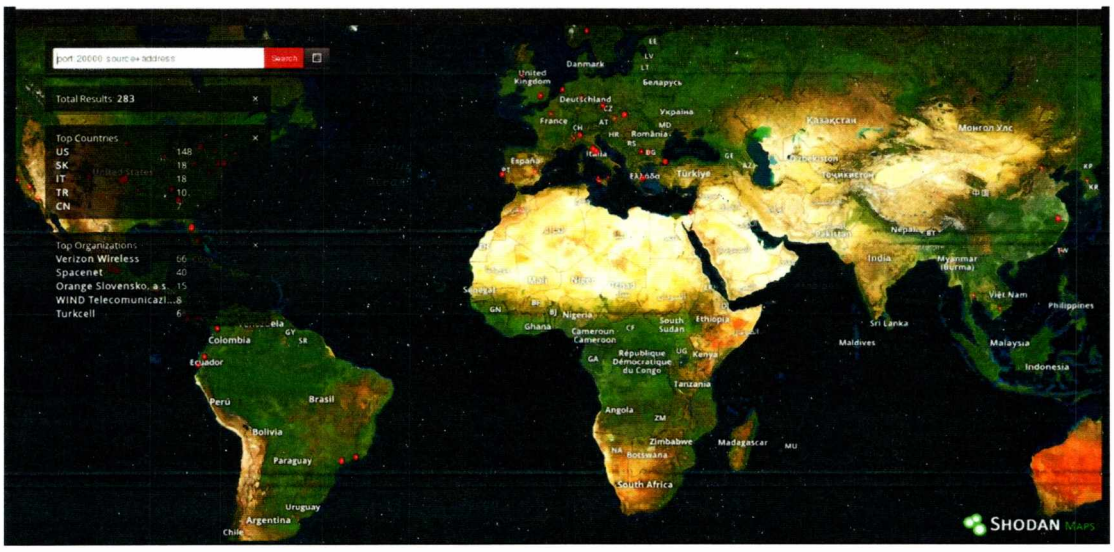
Το S7 είναι ένα ιδιόκτητο πρωτόκολλο που τρέχει μεταξύ προγραμματιζόμενων λογικών ελεγκτών της σειράς Siemens S7.
Στην έρευνα πού έγινε βρέθηκαν 2.018 αποτελέσματα με πιθανά ευπαθές στοιχεία.



DNP 3

Το DNP3 (Distributed Network Protocol) είναι ένα σύνολο πρωτοκόλλων επικοινωνιών που χρησιμοποιούνται μεταξύ εξαρτημάτων σε συστήματα αυτόματου ελέγχου. Η κύρια χρήση του είναι σε επιχειρήσεις κοινής ωφελείας, όπως ηλεκτρικό και νερό εταιρείες.

Στην έρευνα πού έγινε βρέθηκαν 283 αποτελέσματα με πιθανά ευπαθές στοιχεία.



TRIDIUM

Το πρωτόκολλο Fox, αναπτύχθηκε ως μέρος του πλαισίου Niagara από την εταιρεία Tridium, και πιο συχνά εμφανίζεται σε συστήματα αυτοματισμού κτιρίων (γραφεία, βιβλιοθήκες, πανεπιστήμια, κλπ)

Στην έρευνα πού έγινε βρέθηκαν 18.351 αποτελέσματα με πιθανά ευπαθές στοιχεία.

BACNet

Το BACnet είναι ένα πρωτόκολλο επικοινωνίας για κατασκευή δικτύων αυτοματισμού και ελέγχου έχει σχεδιαστεί για να επιτρέπει την επικοινωνία κτιριακών συστημάτων αυτοματισμού και ελέγχου για εφαρμογές όπως θέρμανση, κλιματισμό, φωτισμό, και συστήματα πυρανίχνευσης.

Στην έρευνα πού έγινε βρέθηκαν 10.254 αποτελέσματα με πιθανά ευπαθές στοιχεία.

Ethernet/IP

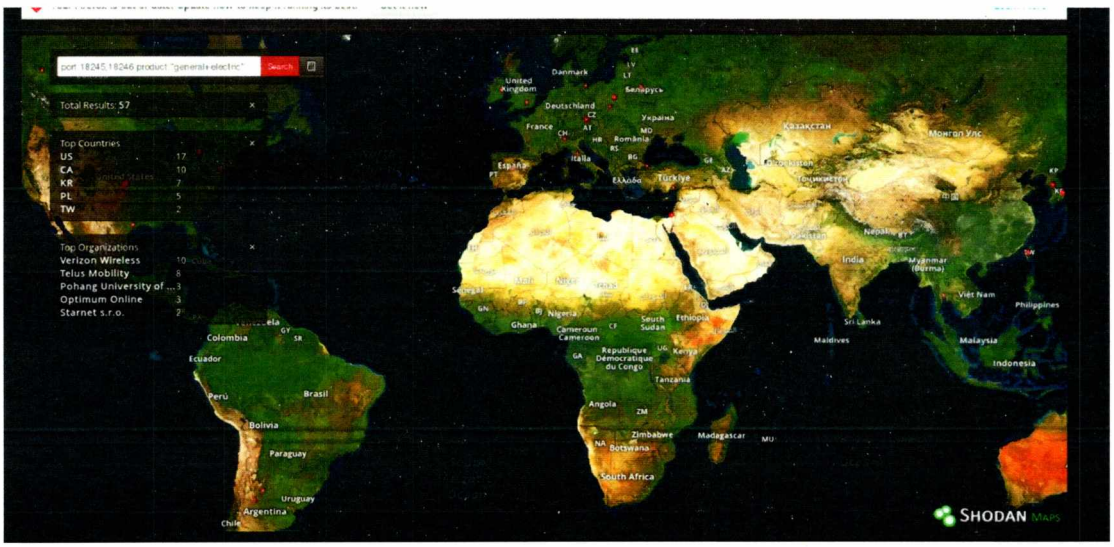
Το Ethernet / IP εισήχθη το 2001 και είναι μια βιομηχανική λύση δικτύου Ethernet διαθέσιμη για την κατασκευή αυτοματισμού.

Στην έρευνα πού έγινε βρέθηκαν 25.571 αποτελέσματα με πιθανά ευπαθές στοιχεία.

General Electric Industrial Systems

Το Service Request Transport Protocol (GE-SRTP) είναι ένα πρωτόκολλο που αναπτύχθηκε από την GE Intelligent πλατφόρμα για τη μεταφορά των δεδομένων από PLCs.

Στην έρευνα πού έγινε βρέθηκαν 57 αποτελέσματα με πιθανά ευπαθές στοιχεία.



HART IP

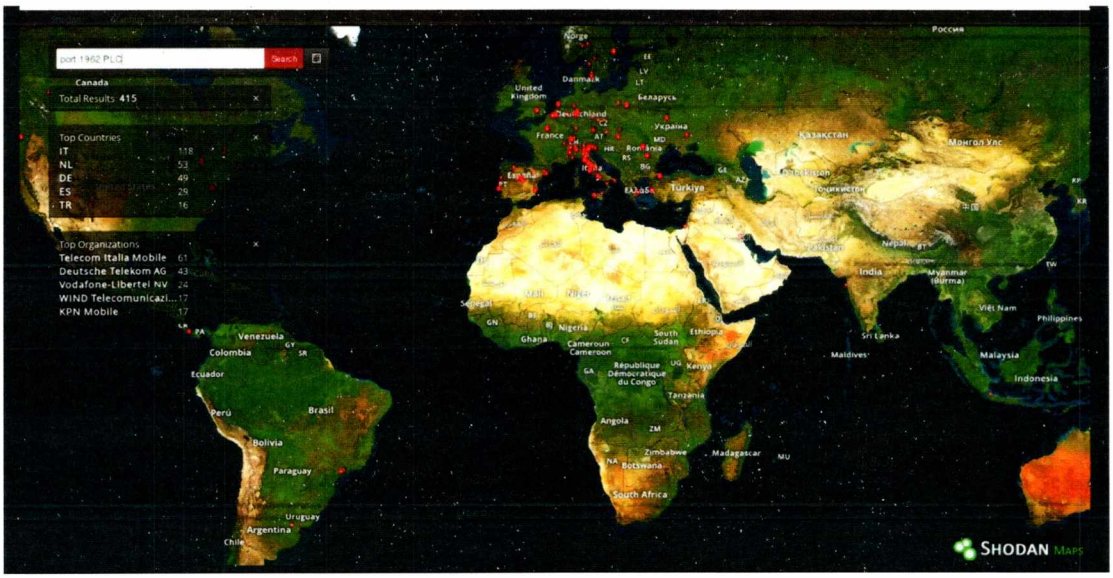
Το HART Communications Protocol (Highway Addressable Remote Transducer Protocol) είναι μια πρώιμη εκτέλεση του Filed bus, ένα ψηφιακό πρωτόκολλο βιομηχανικού αυτοματισμού.

Στην έρευνα πού έγινε βρέθηκαν 4 αποτελέσματα με πιθανά ευπαθές στοιχεία.

PCWorx

Το PCWorx είναι ένα πρωτόκολλο και πρόγραμμα της Phoenix Contact και έχει χρησιμοποιηθεί από ένα ευρύ φάσμα βιομηχανιών.

Στην έρευνα πού έγινε βρέθηκαν 415 αποτελέσματα με πιθανά ευπαθές στοιχεία.



MELSEC-Q

Το MELSEC-Q Series χρησιμοποιεί ένα ιδιόκτητο πρωτόκολλο δικτύου για επικοινωνία. Οι συσκευές χρησιμοποιούνται από παραγωγικό εξοπλισμό για την

παροχή υψηλής ταχύτητας, επεξεργασίας μεγάλου όγκου δεδομένων και έλεγχο της μηχανής .

Στην έρευνα πού έγινε βρέθηκαν 76 αποτελέσματα με πιθανά ευπαθές στοιχεία.

OMRON FINS

Το FINS, Factory Interface Network Service, είναι ένα πρωτόκολλο δικτύου της Omron PLCs, που χρησιμοποιείται σε διαφορετικά δίκτυα όπως το Ethernet,το Controller Link,το Device Net και το RS-232C.

Στην έρευνα πού έγινε βρέθηκαν 796 αποτελέσματα με πιθανά ευπαθές στοιχεία.

REDLION Crimson V3.0

Το πρωτόκολλο που το πρόγραμμα Crimson V3.0 χρησιμοποιεί όταν επικοινωνεί με το HMI Controls G306a

Στην έρευνα πού έγινε βρέθηκαν 780 αποτελέσματα με πιθανά ευπαθές στοιχεία.

CODESyS

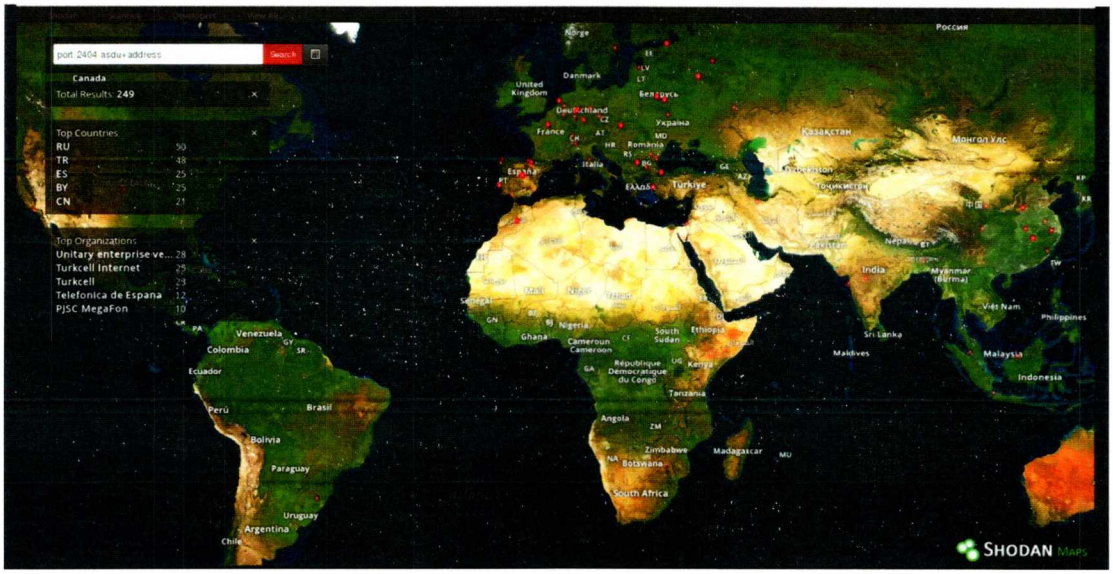
Πάνω από 250 κατασκευαστές από διαφορετικούς τομείς βιομηχανίας προσφέρουν συσκευές αυτοματισμού με το προγραμματιστικό interface CODESYS.

Στην έρευνα πού έγινε βρέθηκαν 1.221 αποτελέσματα με πιθανά ευπαθές στοιχεία.

IEC 60870 part 5

Το IEC 60870 part 5 είναι ένα από τα πρότυπα IEC 60870 τα οποία προσδιορίζουν συστήματα Scada για χρήσεις σε ηλεκτρολογικούς αυτοματισμού και παροχής και διανομής ενέργειας

Στην έρευνα πού έγινε βρέθηκαν 249 αποτελέσματα με πιθανά ευπαθές στοιχεία.

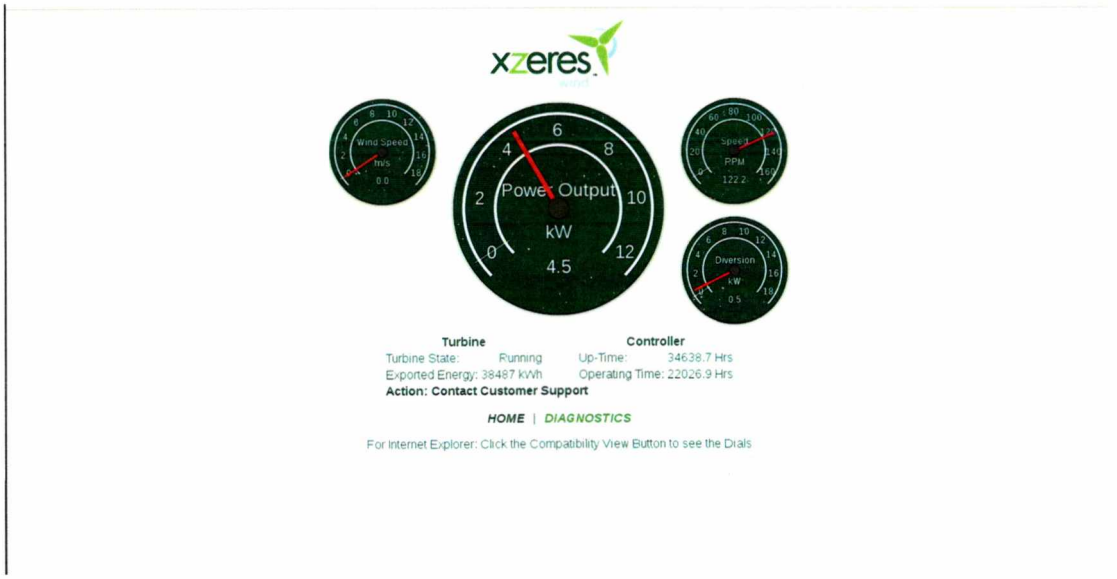


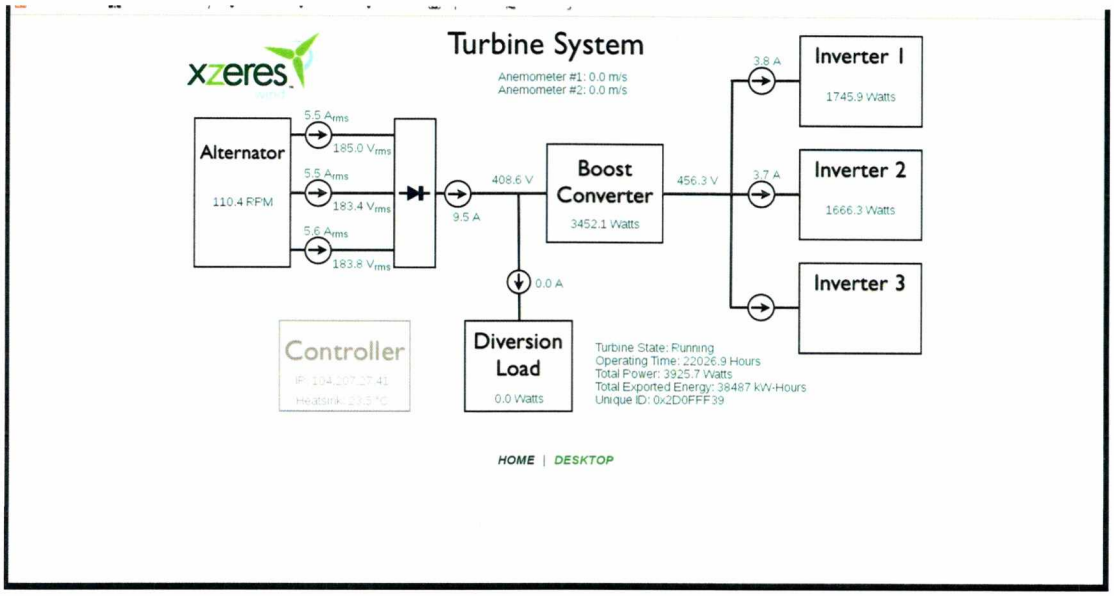
ProConOS

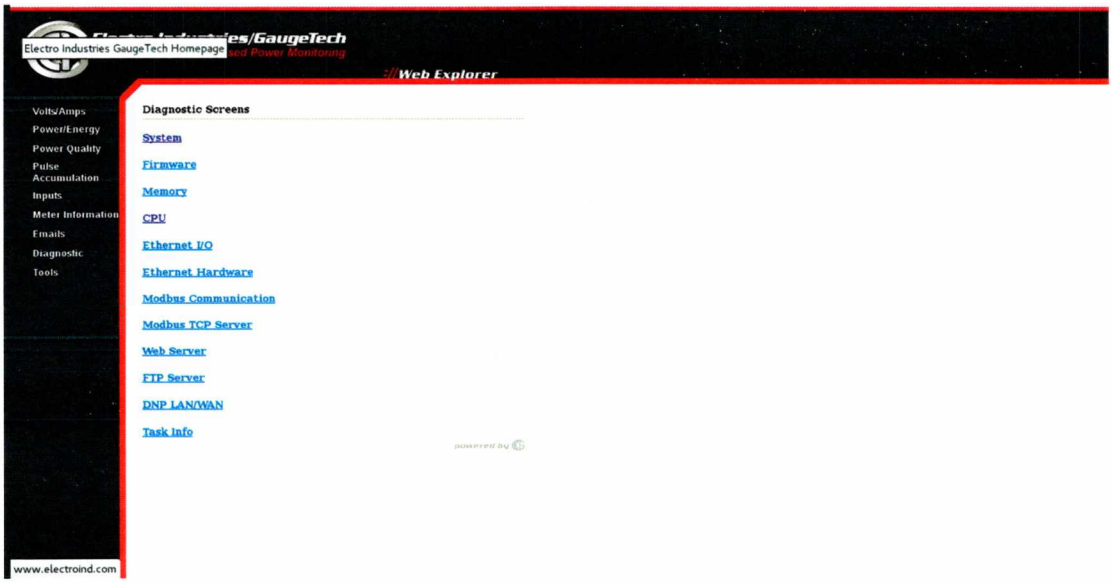
Το ProConOS είναι μια υψηλής απόδοσης PLC μηχανή σχεδιασμένη για ενσωματωμένες και με βάση τους υπολογιστές εφαρμογές αυτόματου ελέγχου.

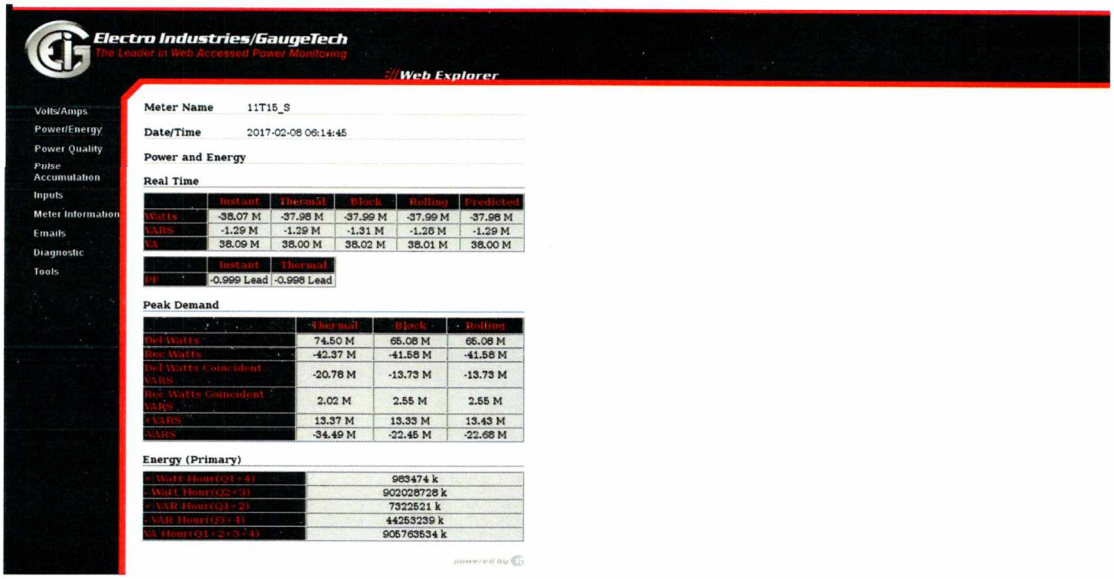
Στην έρευνα πού έγινε βρέθηκαν 152 αποτελέσματα με πιθανά ευπαθές στοιχεία.

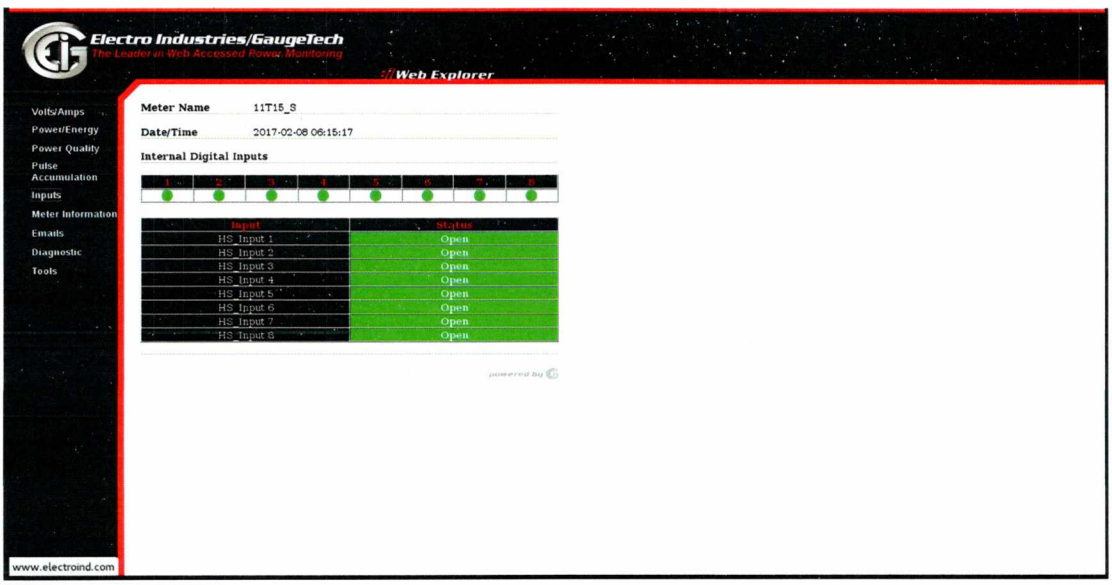
Οι παρακάτω εικόνες είναι στιγμιότυπα οθόνης τα οποία αποδεικνύουν την παραβίαση σε μερικά συστήματα αυτοματισμού που έγιναν για τις ανάγκες της διατριβής. Σε κανένα από αυτά τα συστήματα δεν έγιναν αλλαγές ή επεμβάσεις για να μην δημιουργηθούν προβλήματα. Σε όλες τις παραβιάσεις που έγιναν αποκτήσαμε δικαιώματα διαχειριστή που σημαίνει ότι υπήρχε η δυνατότητα να γίνουν ρυθμίσεις που αφορούν όλες τις παραμέτρους των συστημάτων.

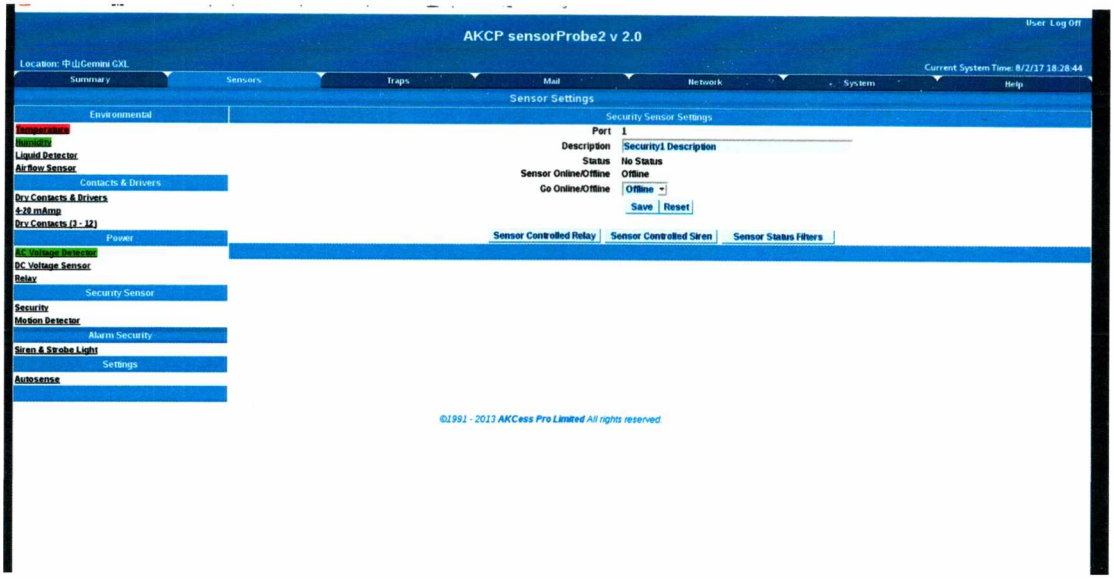


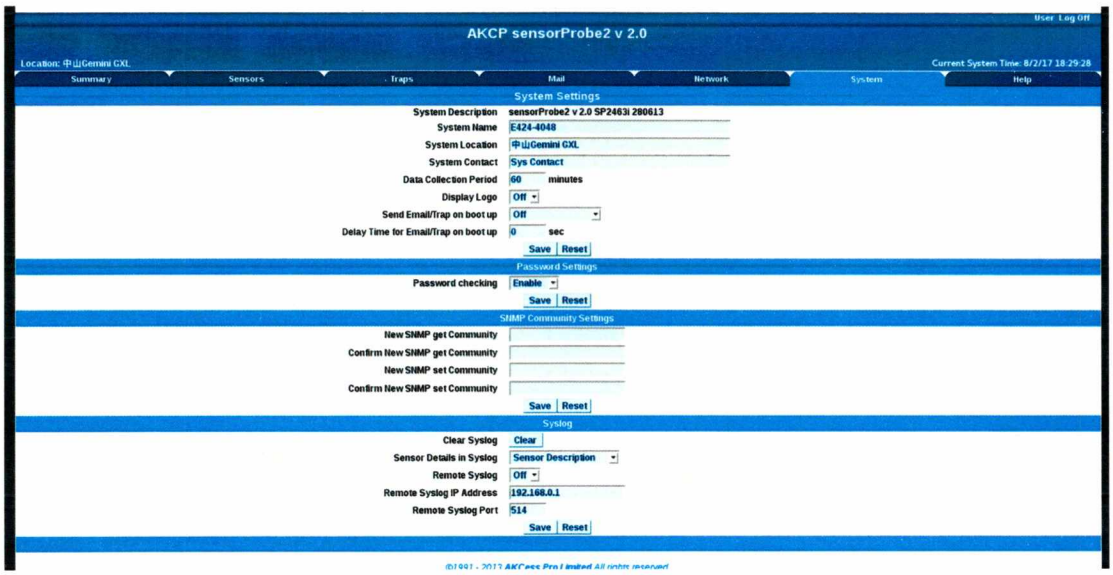


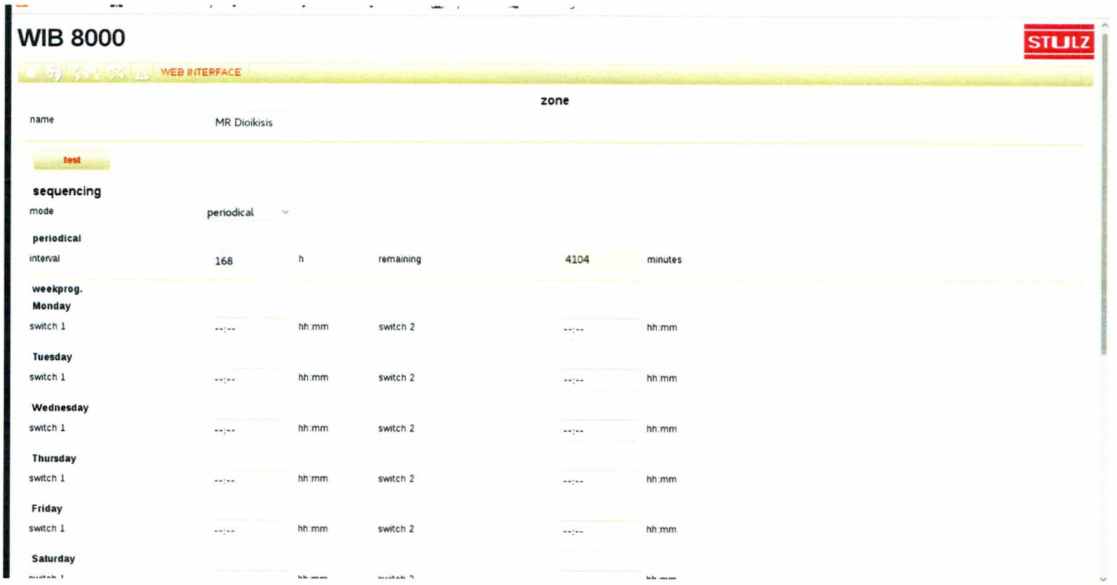


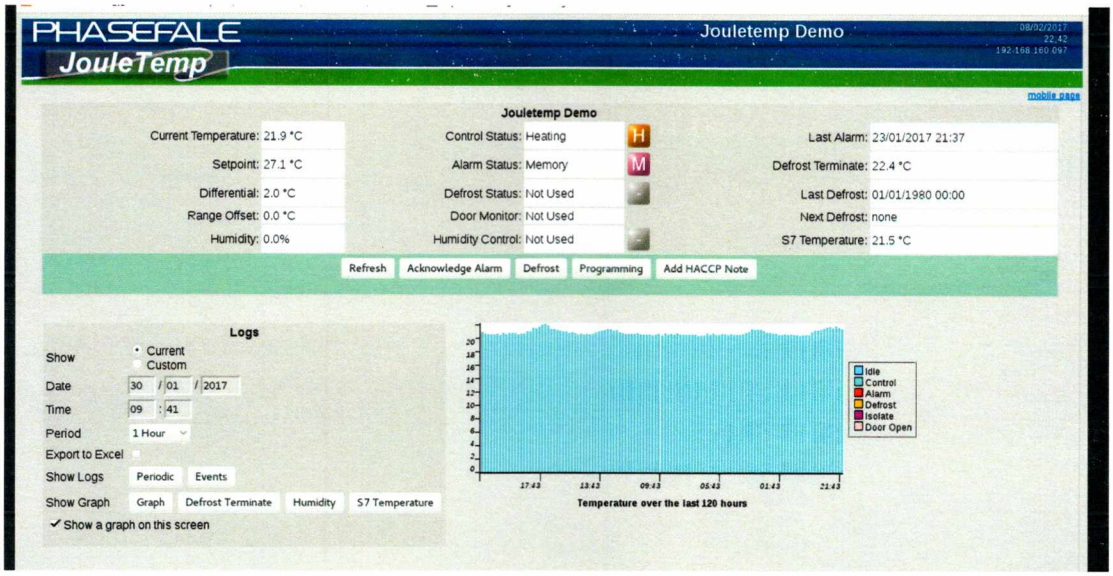


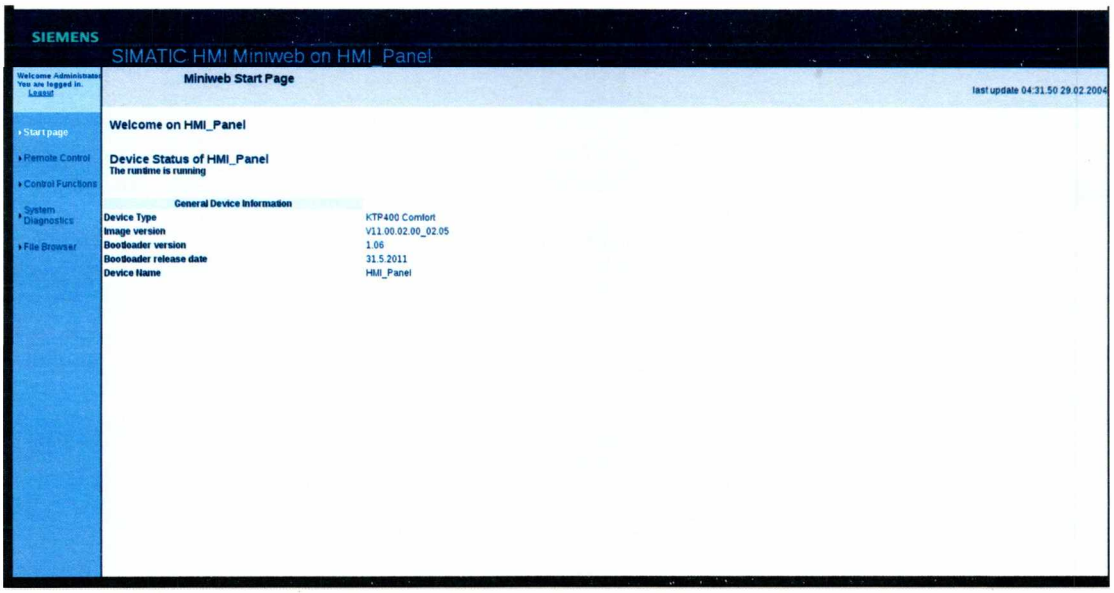












6. Καλύτερες στρατηγικές αντιμετώπισης ασφάλειας Scada

Για την καλύτερη δυνατή εξασφάλιση ενός ασφαλούς δικτύου Scada, δεν είναι αρκετό η χρήση μεμονωμένων πρακτικών και προγραμμάτων, αλλά η χρήση στρατηγικών που είναι αλληλένδετες μεταξύ τους. Θα αναφέρουμε παρακάτω εφτά στρατηγικές οι οποίες είναι οι σημαντικές για την σωστή ασφάλεια ενός Scada και την σωστή αντιμετώπιση περιστατικών ασφαλείας.

1. Υιοθέτηση λίστας «καλών» εφαρμογών.

Η υιοθέτηση μιας τέτοιας λίστας μπορεί να εντοπίσει και να αποτρέψει προσπάθειες εκτέλεσης malware. Η στατική φύση μερικών συστημάτων όπως οι servers βάσεων δεδομένων και οι HMI υπολογιστές είναι οι καταλληλότεροι υποψήφιοι για δημιουργία και χρήση τέτοιων λιστών.

2. Εξασφαλίστε ορθή διαμόρφωση ρυθμίσεων και update.

Οι επιτιθέμενοι στοχεύουν συστήματα τα οποία έχουν καιρό να κάνουν update. Εάν χρησιμοποιηθεί σωστή διαχείριση των ενημερώσεων των συστημάτων και των εφαρμογών τότε τα συστήματα δεν είναι τόσο ευάλωτα σε επιθέσεις.

3. Μειώστε την επιφάνεια επιθέσεων

Απομονώστε τα δίκτυα Scada από οποιοδήποτε μη ελεγχόμενο και άγνωστο δίκτυο, ιδιαιτέρως από το Internet. Απενεργοποιήστε όλες τις υπηρεσίες που δεν χρησιμοποιούνται.

4. Χτίστε ένα περιβάλλον που εύκολα αμύνεται

Περιορίστε την ζημιά από τα ρήγματα της περιμέτρου του δικτύου. Απαγορεύστε συνδέσεις host to host το οποίο αποτρέπει τον επιτιθέμενο να εισβάλει από ένα μόνο σύστημα σε πολλά περισσότερα.

5. Διαχειριστείτε την αυθεντικοποίηση

Οι επιτιθέμενοι εστιάζονται στο να αποκτούν έλεγχο από κωδικούς σε λογαριασμούς με υψηλά διαχειριστικά δικαιώματα. Έτσι αποκτώντας αυτούς τους κωδικούς μπορούν να μεταμφιεστούν σε χρήστες που είναι «νόμιμοι» χρήστες του δικτύου.

6. Υιοθετείστε ασφαλή απομακρυσμένη πρόσβαση

Πολλοί επιτιθέμενοι αποκτούν πρόσβαση σε συστήματα Scada , ανακαλύπτοντας προσβάσεις οι οποίες έχουν δημιουργηθεί από τους διαχειριστές των συστημάτων.

7. Ελέγξτε και απαντήστε

Για την άμυνα ενός δικτύου εναντίον των σύγχρονων απειλών χρειάζεται ενεργός έλεγχος για διεισδύσεις επιτιθέμενων και άμεση απάντηση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems – Eric Knapp 2011
2. Securing Scada and Industrial Control Systems – U.S. Department of Homeland Security
3. Vulnerability Analysis of Energy Delivery Control System – Idaho National Laboratory 2011
4. The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems – Eric J. Byres
5. Industrial Control System Vulnerability Trends 2015 – Amol Sarwate
6. A taxonomy of Cyber Attacks on SCADA System - Bonnie Zhu, Anthony Joseph, Shankar Sastry Department of Electrical Engineering and Computer Sciences
7. SCADA safety in numbers – POSITIVE TECHNOLOGIES 2012
8. Guide to Industrial Control Systems Security – Keith Stoufer, Victoria Pilliteri, Suzanne Lightman, Marshall Abrams, Adam Hahn
9. 21 Steps to improve Cyber Security of Scada Networks - U.S. Department of Homeland Security
10. Security for Critical Infrastructure SCADA Systems – SANS Institute
11. Cyber Security for SCADA Systems – THALES security 2013