Πανεπιστήμιο Δυτικής Αττικής Σχολή Μηχανικών Τμήμα Μηχανικών Βιομηχανικής Σχεδίασης Και Παραγωγής

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΚΑΙ SCADA ΣΤΑ ΠΛΟΙΑ

Των φοιτητών

Κουράκου Θωμά *Αρ. Μητρώου 39075*
Κουρουνάρχη Αντώνη *Αρ. Μητρώου 42310*

Επιβλέπων καθηγητής:

Χρήστος Δρόσος

Αθήνα 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ (1η ή 2η σελίδα)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/Η κάτωθι υπογεγραμμένος/η ΚΟΥΡΟΥΜΙΑΡΧΗΣ ΑΝΤΩΝΙΟΣ του ΙΩΑΝΝΗ, φοιτητής του Τμήματος Βιομηχανικής Σχεδίασης και Παραγωγής του Πανεπιστήμιου Δυτικής Αττικής, πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε, ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα, σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασή της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση Π.Ε με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσής της.

Ο Δηλών

[signature]

Ημερομηνία

27/5/2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ (1η ή 2η σελίδα)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/Η κάτωθι υπογεγραμμένος/η ΚΟΥΡΑΤΟΣ ΦΩΤΗΣ, του ΒΑΣΙΛΕΙΟΥ, φοιτητής του Τμήματος ΒΙΟΜΗΧΑΝΙΚΗΣ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ του Πανεπιστημίου Δυτικής Αττικής, πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε, ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα, σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασή της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση Π.Ε με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε πρέπει να ολοκληρώθεί εντός τουλάχιστον ενός ημερολογιακού δμήνου από την ημερομηνία ανάθεσής της.

Ο Δηλών

Ημερομηνία
27/5/2019

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Εισαγωγή

Η ασφάλεια πληροφοριών διαδραματίζει σημαντικό ρόλο στην προστασία των περιουσιακών στοιχείων ενός οργανισμού. Ενώ η ασφάλεια των πληροφοριών διαδραματίζει σημαντικό ρόλο στην προστασία των δεδομένων και των περιουσιακών στοιχείων ενός οργανισμού, συχνά ακούγονται ειδήσεις για περιστατικά ασφάλειας, όπως αλλοίωση, δικτυακή πειρατεία και διαρροή δεδομένων. Είναι εξαιρετικά εύκολο να αποκτήσει κάποιος μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες σε ένα ανασφαλές περιβάλλον δικτύου, και είναι δύσκολο να πιάσει τους εισβολείς. Ακόμα κι αν οι χρήστες δεν έχουν τίποτα αποθηκευμένο στον υπολογιστή τους που θεωρούν σημαντικό, ο υπολογιστής μπορεί να είναι ένας "αδύναμος κρίκος", που επιτρέπει τη μη εξουσιοδοτημένη πρόσβαση στα συστήματα του οργανισμού και των πληροφοριών.

Για να αντιμετωπιστεί η κατάσταση, ορισμένες κυβερνήσεις και οργανώσεις έχουν δημιουργήσει σημεία αναφοράς, πρότυπα και, σε ορισμένες περιπτώσεις, νομικές ρυθμίσεις σχετικά με την ασφάλεια των πληροφοριών για να συμβάλουν στην εξασφάλιση επαρκούς επιπέδου ασφάλειας που να διατηρείται, πόρους που χρησιμοποιούνται με το σωστό τρόπο, και καλύτερη ασφάλεια στην υιοθέτηση πρακτικών.

Κεφάλαιο 1^{Ο}: Γενικά

1.1 Ορισμοί

Από τη μη εξουσιοδοτημένη πρόσβαση έως τις κακόβουλες πράξεις χειραγώγησης: οι απειλές που υπάρχουν κατά την αποθήκευση ή την αποστολή ηλεκτρονικών δεδομένων αυξάνονται. Για το λόγο αυτό, η ασφάλεια των δεδομένων έχει όλο και μεγαλύτερη σημασία. Η ασφάλεια πληροφοριακών συστημάτων παρέχει τα απαραίτητα εργαλεία για την ασφαλή επικοινωνία και την προστασία των δεδομένων.

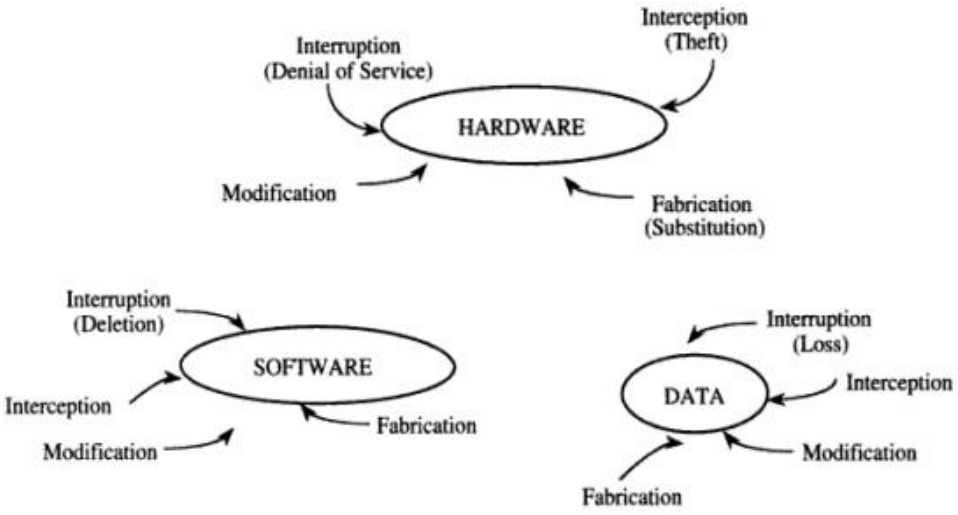
Από την άνοδο της εποχής του Διαδικτύου έχει γίνει πιο σημαντικό για το μέσο καταναλωτή να διασφαλίσει ότι οι πληροφορίες που αποτελούν κομμάτι του «εαυτό τους» θα είναι ασφαλής. Στην Αμερική μόνο, οι online καταγγελίες κλοπής ταυτότητας στην Ομοσπονδιακή Επιτροπή Εμπορίου αυξήθηκαν κατά 87,7% το 2012 έναντι του προηγούμενου έτους.

Αν και υπάρχουν μια σειρά από διαθέσιμα πρότυπα για ασφαλείς πληροφοριών, ένας οργανισμός μπορεί να ωφεληθεί μόνο εάν τα εν λόγω πρότυπα εφαρμόζονται σωστά. Η ασφάλεια πληροφοριών είναι κάτι στο οποίο πρέπει να συμμετέχουν όλα τα ενδιαφερόμενα μέλη. Τα ανώτερα διοικητικά στελέχη, οι επαγγελματίες της ασφάλειας των πληροφοριών, οι επαγγελματίες της πληροφορικής και ο χρήστες, όλοι πρέπει να έχουν ένα ρόλο στην εξασφάλιση των περιουσιακών στοιχείων ενός οργανισμού.

Η επιτυχία της ασφάλειας των πληροφοριών μπορεί να επιτευχθεί μόνο με την πλήρη συνεργασία σε όλα τα επίπεδα ενός οργανισμού, τόσο στο εσωτερικό όσο και στο εξωτερικό.

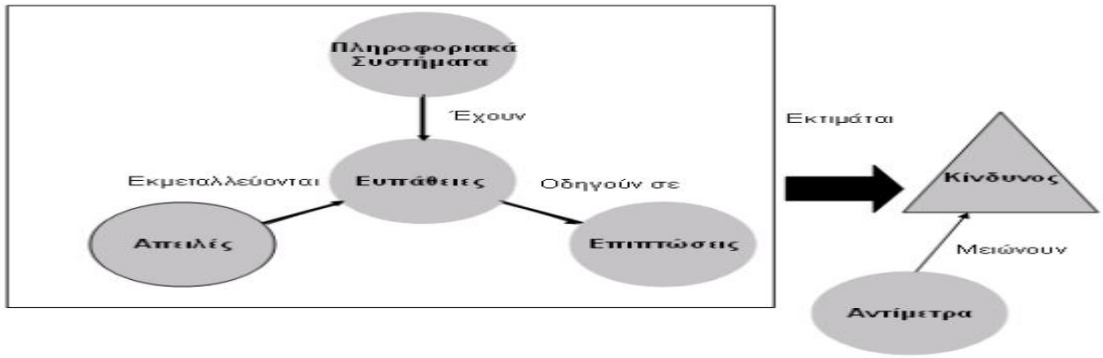
1.2 Βασικά στοιχεία της εκτίμησης κινδύνου και ασφάλεια δικτύων

Η πολιτική ασφάλειας για τα ΠΣ μιας επιχείρησης έπεται της αξιολόγησης του επιπέδου ασφάλειας των συστημάτων αυτών. (Spears & Barki, 2010)



Σχήμα 1.1. Ευπάθειες ενός πληροφοριακού συστήματος

Πηγή:Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS quarterly, 34(3), 503-522.



Σχήμα 1.2. Συσχέτισης των παραγόντων της ανάλυσης επικινδυνότητας

Πηγή:Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS quarterly, 34(3), 503-522.

Η Διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της προσβασιμότητας των πληροφοριών. Επιπλέον, άλλες ιδιότητες όπως η αυθεντικότητα, η λογοδοσία, μη άρνηση και η αξιοπιστία μπορεί να

συμπεριληφθούν.

Ο όρος "διαθεσιμότητα" δεν έχει χρησιμοποιηθεί σε αυτόν τον ορισμό, γιατί είναι ένας όρος που ορίζεται σε αυτό το τμήμα του ISO / IEC 20000 το οποίο δεν θα ήταν κατάλληλο για τον ορισμό αυτό .

Το Περιστατικό ασφάλειας πληροφορίας, αποτελεί ένα μεμονωμένο ή μια σειρά από ανεπιθύμητα ή απρόβλεπτα συμβάντα ασφάλειας των πληροφοριών που έχουν σημαντική πιθανότητα να θέτουν σε κίνδυνο τις επιχειρηματικές δραστηριότητες και απειλεί την ασφάλεια των πληροφοριών. Το Ενδιαφερόμενο μέρος είναι ένα άτομο ή ομάδα που έχει ένα ιδιαίτερο ενδιαφέρον για την απόδοση ή την επιτυχία της δραστηριότητας ή των δραστηριοτήτων του φορέα παροχής υπηρεσιών. Οι πελάτες, οι ιδιοκτήτες, η διαχείριση, οι άνθρωποι στην οργάνωση, οι προμηθευτές του φορέα παροχής υπηρεσιών, οι τραπεζίτες, οι συνδικαλιστικές οργανώσεις ή οι εταίροι.

Η Εσωτερική ομάδα αποτελεί μέρος της οργάνωσης του φορέα παροχής υπηρεσιών που συνάπτει τεκμηριωμένη συμφωνία με τον πάροχο υπηρεσιών να συμβάλλει στο σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση της υπηρεσίας ή υπηρεσιών. Η εσωτερική ομάδα είναι εκτός του πεδίου εφαρμογής των SMS του φορέα παροχής υπηρεσιών. Ένα άλλο σημαίνον στοιχείο αποτελεί ένα γνωστό σφάλμα, το αποτελεί ένα πρόβλημα που έχει εντοπισμένη αιτία ή μια μέθοδος μείωσης ή εξάλειψης των επιπτώσεων του σε μια υπηρεσία μέσω της εργασίας γύρω από αυτό

Σημαίνον στοιχείο στην ασφάλεια των πληροφοριακών συστημάτων καθίσταται η οργάνωση η οποία είναι μια ομάδα ανθρώπων και εγκαταστάσεων, με διάταξη των ευθυνών, των αρχών και των σχέσεων. Ένα άλλο σημαίνον στοιχείο είναι η λεγόμενη Προληπτική δράση, η οποία αποτελεί μια δράση για την αποφυγή ή την εξάλειψη των αιτίων ή τη μείωση της πιθανότητας εμφάνισης μιας πιθανής μη συμμόρφωσης ή άλλων δυνητικών ανεπιθύμητων καταστάσεων. Παρακάτω παραθέτονται επίσης σημαίνοντες ορισμοί(Γιαννόπουλος 2001):

1. Πρόβλημα: Αιτία από ένα ή περισσότερα επεισόδια. Η αιτία δεν είναι συνήθως γνωστή κατά το χρόνο καταγραφής του προβλήματος και

η διαδικασία διαχείρισης των προβλημάτων είναι υπεύθυνη για την περαιτέρω έρευνα.

2. Διαδικασία: Καθορισμένος τρόπος για την πραγματοποίηση μια δραστηριότητας ή διαδικασίας

3. Διεργασία: Το σύνολο των αλληλένδετων ή αλληλεπιδρώντων δραστηριοτήτων που μετατρέπει τις εισροές σε εκροές

4. Καταγραφή: Έγγραφο που αναφέρει αποτελέσματα που επιτεύχθηκαν ή παρέχει αποδείξεις δραστηριοτήτων που πραγματοποιήθηκαν

5. Απελευθέρωση: Συλλογή ενός ή περισσοτέρων νέων ή τροποποιημένων στοιχείων διαμόρφωσης που έχουν αναπτυχθεί στο ζωντανό περιβάλλον ως αποτέλεσμα μίας ή περισσοτέρων αλλαγών

6. Αίτημα για αλλαγή: Πρόταση για μια αλλαγή που πρέπει να γίνει σε μια υπηρεσία, στοιχείο υπηρεσίας ή του συστήματος διαχείρισης των υπηρεσιών. Μια αλλαγή σε μια υπηρεσία περιλαμβάνει την παροχή μιας νέας υπηρεσίας ή την αφαίρεση μιας υπηρεσίας η οποία δεν είναι πλέον απαραίτητη .

7. Κίνδυνος: Επίδραση της αβεβαιότητας για τους στόχους. Ένα αποτέλεσμα είναι μια απόκλιση από την αναμενόμενη - θετική ή / και αρνητική. Οι στόχοι μπορούν να έχουν διαφορετικές πτυχές (όπως οικονομικούς στόχους, την υγεία και την ασφάλεια, και περιβαλλοντικούς στόχους) και μπορεί να εφαρμοστεί σε διαφορετικά επίπεδα (όπως στρατηγικά, σε ολόκληρο τον οργανισμό, το έργο, το προϊόν και τη διαδικασία) .

8. Υπηρεσία: Μέσο για την παροχή αξίας στον πελάτη, διευκολύνοντας τα αποτελέσματα που θέλει να επιτύχει ο πελάτης. Μια υπηρεσία μπορεί επίσης να παραδοθεί με τον παροχέα υπηρεσιών από έναν προμηθευτή, μιας εσωτερικής ομάδας ή ενός πελάτη που ενεργεί ως προμηθευτής.

9. Συνιστώσα των υπηρεσιών: Ενιαία μονάδα μιας υπηρεσίας που όταν συνδυάζεται με άλλες μονάδες θα παραδώσει μια πλήρη υπηρεσία.

10. Συνέχεια των υπηρεσιών: Δυνατότητα διαχείρισης των κινδύνων και των γεγονότων που θα μπορούσαν να έχουν σοβαρές επιπτώσεις σε μια υπηρεσία ή υπηρεσίες, προκειμένου να παραδώσει συνεχώς τις υπηρεσίες σε αποδεκτά επίπεδα

11. Σύμβαση Παροχής Υπηρεσιών: Τεκμηριωμένη σύμβαση μεταξύ του παρόχου υπηρεσιών και του πελάτη που προσδιορίζει τις υπηρεσίες και τους στόχους των υπηρεσιών. Μια συμφωνία σε επίπεδο υπηρεσιών μπορεί επίσης να καθοριστεί μεταξύ του παρόχου υπηρεσιών και του προμηθευτή, μιας εσωτερικής ομάδας ή ενός πελάτη που ενεργεί ως προμηθευτής .Μια συμφωνία σε επίπεδο υπηρεσιών μπορεί να συμπεριληφθεί σε μια σύμβαση ή άλλου τύπου τεκμηριωμένη σύμβαση .

12. Διαχείριση υπηρεσιών: Το σύνολο των δυνατοτήτων και των διαδικασιών που κατευθύνουν και να ελέγχουν τις δραστηριότητες και τους πόρους του φορέα παροχής υπηρεσιών για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών για την κάλυψη των απαιτήσεων των υπηρεσιών

13. Σύστημα διαχείρισης υπηρεσιών: Σύστημα διαχείρισης για να κατευθύνει και να ελέγχει τις δραστηριότητες παροχής υπηρεσιών διαχείρισης του παρόχου υπηρεσιών Ένα σύστημα διαχείρισης είναι ένα σύνολο αλληλένδετων ή αλληλεπιδρώντων στοιχείων για τη δημιουργία της πολιτικής και των στόχων και την επίτευξη των στόχων αυτών .Το SMS περιλαμβάνει όλες τις πολιτικές διαχείρισης των υπηρεσιών, τους στόχους, τα σχέδια, τις διαδικασίες, την τεκμηρίωση και τους πόρους που απαιτούνται για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών και την εκπλήρωση των απαιτήσεων σε αυτό το τμήμα του ISO / IEC 20000 .

14. Πάροχος υπηρεσιών: Οργάνωση ή μέρος μιας οργάνωσης που διαχειρίζεται και παρέχει μια υπηρεσία ή υπηρεσίες για τον πελάτη. Ένας

πελάτης μπορεί να είναι εσωτερική ή εξωτερική οργάνωσης του φορέα παροχής υπηρεσιών .

15. Αίτηση υπηρεσίας: Αίτηση παροχής πληροφοριών, συμβουλών, την πρόσβαση σε μια υπηρεσία ή ένα προ-εγκεκριμένο αλλαγή

16. Απαίτηση υπηρεσίας: Ανάγκες του πελάτη και των χρηστών της υπηρεσίας, συμπεριλαμβανομένων των απαιτήσεων σε επίπεδο εξυπηρέτησης, και τις ανάγκες του παρόχου υπηρεσιών

17. Προμηθευτής: Οργάνωση ή μέρος μιας οργάνωσης που είναι εξωτερική οργάνωση του φορέα παροχής υπηρεσιών και να συνάπτει σύμβαση με τον πάροχο υπηρεσιών να συμβάλλουν στο σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση της υπηρεσίας ή υπηρεσιών ή διαδικασιών.

18. Ανώτατα διοικητικά στελέχη: Πρόσωπο ή ομάδα ανθρώπων που διευθύνουν και ελέγχουν τον πάροχο υπηρεσιών στο υψηλότερο επίπεδο

19. Μετάβαση: Δραστηριότητες που εμπλέκονται στη μετακίνηση νέων ή τροποποιημένων δρομολογίων από και προς το ζωντανό περιβάλλον(Γιαννόπουλος 2001).

Κεφάλαιο 2^{Ο} Συστήματα βιομηχανικού ελέγχου

Το σύστημα βιομηχανικού ελέγχου (ICS) είναι ένας γενικός όρος που περιλαμβάνει πολλούς τύπους συστημάτων ελέγχου, όπως συστήματα εποπτικού ελέγχου και λήψης δεδομένων (SCADA), διανεμημένα συστήματα ελέγχου (DCS) και άλλες διαμορφώσεις συστημάτων ελέγχου, όπως οι προγραμματιζόμενοι λογικοί ελεγκτές (PLC) που βρίσκονται σε βιομηχανικούς τομείς και σε υποδομές ζωτικής σημασίας.

Ένα ICS αποτελείται από συνδυασμούς εξαρτημάτων ελέγχου (π.χ. ηλεκτρικά, μηχανικά, υδραυλικά, πνευματικά) που λειτουργούν μαζί για να επιτύχουν έναν βιομηχανικό στόχο (π.χ. κατασκευή, μεταφορά υλικών ή ενέργειας). Το τμήμα του συστήματος που ασχολείται κυρίως με την παραγωγή αναφέρεται ως η διαδικασία. Το τμήμα ελέγχου του συστήματος περιλαμβάνει την προδιαγραφή της επιθυμητής απόδοσης ή παραγωγής.

Ο έλεγχος μπορεί να είναι πλήρως αυτοματοποιημένος ή μπορεί να περιλαμβάνει έναν άνθρωπο στον βρόγχο. Τα συστήματα μπορούν να ρυθμιστούν ώστε να λειτουργούν ως συστήματα ανοιχτού βρόγχου, κλειστού βρόγχου και με χειροκίνητη λειτουργία. Στα συστήματα ελέγχου ανοιχτού βρόγχου η έξοδος ελέγχεται από τις καθορισμένες ρυθμίσεις. Σε συστήματα ελέγχου κλειστού βρόχου, η έξοδος επηρεάζει την είσοδο με τέτοιο τρόπο ώστε να διατηρεί τον επιθυμητό στόχο. Στην χειροκίνητη λειτουργία το σύστημα ελέγχεται πλήρως από τους ανθρώπους. Το τμήμα του συστήματος που αφορά κυρίως στην διατήρηση της συμμόρφωσης με τις προδιαγραφές αναφέρεται ως ελεγκτής (ή έλεγχος).

Ένα τυπικό ICS μπορεί να περιέχει πολυάριθμους βρόγχους ελέγχου, διεπαφές ανθρώπου μηχανής και εργαλεία απομακρυσμένης διάγνωσης και συντήρησης που κατασκευάζονται με την χρήση μιας σειράς πρωτοκόλλων δικτύου. Οι βιομηχανικές διεργασίες ελέγχου ICS χρησιμοποιούνται συνήθως στις βιομηχανίες ηλεκτρικής ενέργειας, ύδρευσης και αποχέτευσης, πετρελαίου και φυσικού αερίου, χημικών, μεταφορών, φαρμάκων, χαρτοπολτού και χαρτιού, τροφίμων και ποτών και βιομηχανιών διακριτής κατασκευής (π.χ. αυτοκινητοβιομηχανία, αεροδιαστημική βιομηχανία και διαρκή αγαθά).

2.1 Εξέλιξη συστημάτων βιομηχανικού ελέγχου

Πολλά από τα σημερινά ICS εξελίχθηκαν από την εισαγωγή των δυνατοτήτων της πληροφορικής σε υπάρχοντα φυσικά συστήματα, συχνά αντικαθιστώντας ή συμπληρώνοντας τους μηχανισμούς φυσικού ελέγχου. Για παράδειγμα, τα ενσωματωμένα ψηφιακά στοιχεία ελέγχου αντικατέστησαν τα αναλογικά μηχανικά στοιχεία ελέγχου σε περιστρεφόμενες μηχανές και μηχανήματα. Οι βελτιώσεις στο κόστος και την απόδοση έχουν ενθαρρύνει αυτήν την εξέλιξη, με αποτέλεσμα πολλές από τις «έξυπνες» τεχνολογίες του σήμερα, όπως το έξυπνο ηλεκτρικό δίκτυο, οι έξυπνες μεταφορές, τα έξυπνα κτίρια και η έξυπνη κατασκευή. Ενώ αυτό αυξάνει την συνδεσιμότητα και την κρισιμότητα αυτών των συστημάτων, δημιουργεί επίσης μεγαλύτερη ανάγκη για προσαρμοστικότητα, ανθεκτικότητα και ασφάλεια.

Η μηχανική των ICS συνεχίζει να εξελίσσεται και να παρέχει νέες δυνατότητες διατηρώντας παράλληλα τους τυπικούς μεγάλους κύκλους ζωής αυτών των συστημάτων. Η εισαγωγή των δυνατοτήτων πληροφορικής στα φυσικά συστήματα παρουσιάζει μια αναδυόμενη συμπεριφορά που έχει επιπτώσεις στην ασφάλεια. Τα μοντέλα και οι τεχνικές ανάλυσης εξελίσσονται για να αντιμετωπίσουν αυτές τις αναδυόμενες ιδιότητες, συμπεριλαμβανομένης της ασφάλειας, της ιδιωτικότητας και των αλληλεπιδράσεων των περιβαλλοντικών επιπτώσεων.

2.2 Βιομηχανικοί τομείς, ICS και οι αλληλεξαρτήσεις τους

Τα συστήματα ελέγχου χρησιμοποιούνται σε πολλούς διαφορετικούς βιομηχανικούς τομείς και κρίσιμες υποδομές, συμπεριλαμβανομένης της κατασκευής, της διανομής και των μεταφορών.

2.2.1 Βιομηχανίες Μεταποίησης

Η μεταποίηση παρουσιάζει ένα μεγάλο και ποικίλο βιομηχανικό τομέα με

πολλές διαφορετικές διεργασίες, οι οποίες μπορούν να κατηγοριοποιηθούν σε παραγωγή με βάση την διαδικασία και σε διακριτή παραγωγή.

Οι μεταποιητικές βιομηχανίες που βασίζονται στην διαδικασία χρησιμοποιούν συνήθως δύο κύριες διαδικασίες (Fraser, et al., 2001):

- Συνεχείς διαδικασίες παραγωγής.
- Διαδικασίες παραγωγής παρτίδων.

2.2.2 Βιομηχανίες διανομής

Τα ICS χρησιμοποιούνται για τον έλεγχο γεωγραφικά διασκορπισμένων περιουσιακών στοιχείων, συχνά διασκορπισμένων σε χιλιάδες τετραγωνικά χιλιόμετρα, συμπεριλαμβανομένων των συστημάτων διανομής όπως συστήματα διανομής ύδατος και συλλογής λυμάτων, γεωργικά συστήματα άρδευσης, αγωγούς πετρελαίου και φυσικού αερίου, ηλεκτρικά δίκτυα και συστήματα σιδηροδρομικών μεταφορών.

2.2.3 Διαφορές των ICS στην μεταποίηση και την διανομή

Ενώ τα συστήματα ελέγχου που χρησιμοποιούνται στις βιομηχανίες μεταποίησης και διανομής είναι αρκετά παρόμοια σε επίπεδο λειτουργίας, είναι διαφορετικά σε ορισμένες πτυχές. Οι μεταποιητικές βιομηχανίες λειτουργούν συνήθως μέσα σε ένα εργοστάσιο ή σε μια περιοχή με επίκεντρο το εργοστάσιο, σε σύγκριση με τις γεωγραφικά διασκορπισμένες βιομηχανίες διανομής. Οι επικοινωνίες στις μεταποιητικές βιομηχανίες εκτελούνται συνήθως χρησιμοποιώντας τεχνολογίες τοπικού δικτύου (LAN), οι οποίες κατά κανόνα είναι πιο αξιόπιστες και υψηλής ταχύτητας σε σύγκριση με τις τεχνολογίες WAN και ασύρματων / ραδιοσυχνοτήτων που χρησιμοποιούνται από τις βιομηχανίες διανομής. Τα ICS που χρησιμοποιούνται στις βιομηχανίες διανομής έχουν σχεδιαστεί για να αντιμετωπίζουν τις προκλήσεις επικοινωνίας μεγάλων

αποστάσεων, όπως οι καθυστερήσεις και η απώλεια δεδομένων που θέτουν τα διάφορα μέσα επικοινωνίας που χρησιμοποιούνται. Τα στοιχεία ελέγχου ασφαλείας ενδέχεται να διαφέρουν μεταξύ των τύπων δικτύου.

2.2.4 ICS και αλληλεπιδράσεις υποδομών ζωτικής σημασίας

Οι κρίσιμες υποδομές στις ΗΠΑ αναφέρονται συχνά ως ένα «σύστημα συστημάτων» λόγω των αλληλεξαρτήσεων που υπάρχουν μεταξύ των διαφόρων βιομηχανικών τομέων τους καθώς και των διασυνδέσεων μεταξύ των επιχειρηματικών εταίρων (Falco, et al., 2002)

Ορισμένα συστήματα SCADA παρακολουθούν και ελέγχουν την διανομή ηλεκτρικής ενέργειας συλλέγοντας δεδομένα από και εκδίδοντας εντολές σε γεωγραφικά απομακρυσμένους σταθμούς ελέγχου πεδίου από μία κεντρική θέση. Τα συστήματα SCADA χρησιμοποιούνται επίσης για την παρακολούθηση και τον έλεγχο της διανομής νερού, πετρελαίου και φυσικού αερίου, συμπεριλαμβανομένων αγωγών, πλοίων, φορτηγών και σιδηροδρομικών συστημάτων, καθώς και συστημάτων συλλογής λυμάτων.

Τα συστήματα SCADA και DCS συχνά δικτυώνονται μαζί. Αυτό ισχύει για τα κέντρα ελέγχου ηλεκτρικής ενέργειας και τις μονάδες παραγωγής ηλεκτρικής ενέργειας. Αν και η λειτουργία της μονάδας παραγωγής ηλεκτρικής ενέργειας ελέγχεται από τα DCS, τα DCS πρέπει να επικοινωνούν με τα συστήματα SCADA για να συντονίσουν την παραγωγή με τις απαιτήσεις μετάδοσης και διανομής (Rinaldi, et al., 2001)

2.3 Λειτουργία και συστατικά στοιχεία των ICS

Ορισμένες κρίσιμες διαδικασίες μπορεί επίσης να περιλαμβάνουν συστήματα ασφαλείας. Τα βασικά στοιχεία περιλαμβάνουν τα ακόλουθα (Rinaldi, et al., 2001):

Ένα τυπικό σύστημα ICS περιέχει πολυάριθμους βρόγχους ελέγχου, ανθρώπινες διεπαφές και εργαλεία απομακρυσμένης διάγνωσης και συντήρησης που κατασκευάζονται χρησιμοποιώντας μια σειρά πρωτοκόλλων δικτύου σε αρχιτεκτονικές πολυεπίπεδων δικτύων. Ένας βρόγχος ελέγχου χρησιμοποιεί αισθητήρες, ενεργοποιητές και ελεγκτές (π.χ. PLCs) για να χειριστεί κάποια ελεγχόμενη διαδικασία. Ένας αισθητήρας είναι μια συσκευή που παράγει μια μέτρηση κάποιας φυσικής ιδιότητας και στην συνέχεια στέλνει αυτές τις πληροφορίες ως ελεγχόμενες μεταβλητές στον ελεγκτή. Ο ελεγκτής ερμηνεύει τα σήματα και παράγει τις αντίστοιχες μεταβλητές χειρισμού, με βάση έναν αλγόριθμο ελέγχου και τα καθορισμένα σημεία στόχου, τα οποία μεταδίδει στους ενεργοποιητές. Οι ενεργοποιητές, όπως οι βαλβίδες ελέγχου, οι διακόπτες και οι κινητήρες χρησιμοποιούνται για τον άμεσο χειρισμό της ελεγχόμενης διαδικασίας βάσει εντολών από τον ελεγκτή.

Οι χειριστές και οι μηχανικοί χρησιμοποιούν ανθρώπινες διεπαφές για να παρακολουθούν και να διαμορφώνουν τα σημεία ρύθμισης, τους αλγόριθμους ελέγχου και να ρυθμίζουν και να καθορίζουν τις παραμέτρους στον ελεγκτή. Η ανθρώπινη διεπαφή εμφανίζει επίσης πληροφορίες σχετικά με την κατάσταση της διαδικασίας και ιστορικές πληροφορίες. Τα βοηθήματα διαγνωστικού ελέγχου και συντήρησης χρησιμοποιούνται για την πρόληψη, τον εντοπισμό και την αποκατάσταση από μη φυσιολογική λειτουργία ή αποτυχίες.

Μερικές φορές αυτοί οι βρόγχοι ελέγχου είναι ενσωματωμένοι και / ή επικαλυπτόμενοι, όπου το καθορισμένο σημείο για έναν βρόγχο βασίζεται στην μεταβλητή της διαδικασίας που καθορίζεται από έναν άλλο βρόγχο. Οι βρόγχοι επιπέδου εποπτείας και οι βρόγχοι χαμηλότερου επιπέδου λειτουργούν συνεχώς καθ’ όλη την διάρκεια μίας διαδικασίας με χρονικούς κύκλους που κυμαίνονται από χιλιοστά του δευτερολέπτου έως λεπτά.

Η ηλεκτρική ενέργεια θεωρείται συχνά μια από τις πλέον διαδεδομένες πηγές διακοπών των αλληλεξαρτώμενων υποδομών ζωτικής σημασίας. Για παράδειγμα, μπορεί να ξεκινήσει μια αποτυχία λόγω διακοπής του δικτύου επικοινωνιών μικροκυμάτων που χρησιμοποιείται σε ένα σύστημα SCADA μεταφοράς ηλεκτρικής ενέργειας. Η έλλειψη δυνατοτήτων παρακολούθησης και

ελέγχου θα μπορούσε να καταστήσει μια μεγάλη μονάδα παραγωγής εκτός σύνδεσης, πράγμα που θα οδηγούσε σε απώλεια ισχύος στον υποσταθμό μετάδοσης.

2.3.1 Σχεδιασμός συστήματος ICS

Οι τοπολογίες που βασίζονται στα PLC εξαρτώνται από πολλούς παράγοντες. Αυτή η ενότητα προσδιορίζει τους βασικούς παράγοντες που καθοδηγούν τις αποφάσεις σχεδιασμού σχετικά με τις ιδιότητες ελέγχου, επικοινωνίας, αξιοπιστίας και εφεδρείας του ICS. Επειδή αυτοί οι παράγοντες επηρεάζουν σε μεγάλο βαθμό το σχεδιασμό του ICS, βοηθούν επίσης στον προσδιορισμό των αναγκών ασφαλείας του συστήματος.

Απαιτήσεις χρονισμού ελέγχου. Οι διεργασίες των ICS έχουν ένα ευρύ φάσμα απαιτήσεων που σχετίζονται με τον χρόνο, συμπεριλαμβανομένης της υψηλής ταχύτητας, της συνέπειας, της κανονικότητας και του συγχρονισμού.

Γεωγραφική κατανομή. Τα συστήματα έχουν διάφορους βαθμούς κατανομής, που κυμαίνονται από ένα μικρό σύστημα (π.χ. τοπική ελεγχόμενη διαδικασία PLC) έως μεγάλα και κατανεμημένα συστήματα (π.χ. αγωγούς πετρελαίου, ηλεκτρικό δίκτυο). Η μεγαλύτερη κατανομή συνήθως συνεπάγεται την ανάγκη για την κάλυψη μιας ευρείας περιοχής (π.χ. μισθωμένες γραμμές, εναλλαγή κυκλώματος και μεταγωγή πακέτων) και την κινητή επικοινωνία.

Ιεραρχία. Ο εποπτικός έλεγχος χρησιμοποιείται για την παροχή μιας κεντρικής θέσης που μπορεί να συγκεντρώνει δεδομένα από πολλαπλές τοποθεσίες για να υποστηρίξει τις αποφάσεις ελέγχου βάσει της τρέχουσας κατάστασης του συστήματος. Συχνά χρησιμοποιείται ένας ιεραρχικός / κεντρικός έλεγχος που παρέχει στους χειριστές μια ολοκληρωμένη εικόνα ολόκληρου του συστήματος.

Πολυπλοκότητα ελέγχου. Συχνά οι λειτουργίες ελέγχου μπορούν να εκτελεστούν με απλούς ελεγκτές και προκαθορισμένους αλγορίθμους.

Διαθεσιμότητα. Οι απαιτήσεις διαθεσιμότητας (δηλ. αξιοπιστίας) του

συστήματος αποτελούν επίσης σημαντικό παράγοντα σχεδιασμού. Τα συστήματα με ισχυρές απαιτήσεις διαθεσιμότητας / χρόνου λειτουργίας ενδέχεται να απαιτούν περισσότερες δυνατότητες εφεδρείας ή εναλλακτικές υλοποιήσεις σε όλες τις επικοινωνίες και έλεγχο.

Επιπτώσεις των αποτυχιών. Η αποτυχία μιας λειτουργίας ελέγχου μπορεί να προκαλέσει ουσιαστικά διαφορετικές επιπτώσεις σε όλους τους τομείς. Τα συστήματα με μεγαλύτερες επιπτώσεις απαιτούν συχνά την ικανότητα συνέχισης της λειτουργίας τους μέσω περιττών ελέγχων ή την ικανότητα να λειτουργούν σε υποβαθμισμένη κατάσταση.

Ασφάλεια. Ο τομέας των απαιτήσεων ασφάλειας του συστήματος αποτελεί επίσης σημαντικό παράγοντα σχεδιασμού. Τα συστήματα πρέπει να είναι σε θέση να εντοπίζουν μη ασφαλείς συνθήκες και να ενεργοποιούν δράσεις για την μετατροπή των μη ασφαλών συνθηκών σε ασφαλείς συνθήκες.

2.3.2 Κατανεμημένα Συστήματα Ελέγχου

Τα συστήματα DCS χρησιμοποιούνται για τον έλεγχο των συστημάτων παραγωγής στην ίδια γεωγραφική θέση για βιομηχανίες όπως διυλιστήρια πετρελαίου, επεξεργασία νερού και λυμάτων, μονάδες παραγωγής ηλεκτρικής ενέργειας, μονάδες παραγωγής χημικών, αυτοκινητοβιομηχανίες και φαρμακευτικές εγκαταστάσεις επεξεργασίας. Αυτά τα συστήματα είναι συνήθως συστήματα ελέγχου διαδικασιών ή διακριτά συστήματα ελέγχου.

Τα DCS είναι ενσωματωμένα ως μία αρχιτεκτονική ελέγχου που περιλαμβάνει ένα εποπτικό επίπεδο ελέγχου που εποπτεύει πολλά, ολοκληρωμένα υποσυστήματα που είναι υπεύθυνα για τον έλεγχο των λεπτομερειών μιας τοπικής διαδικασίας. Ένα DCS χρησιμοποιεί έναν κεντρικό βρόγχο ελέγχου για την μεσολάβηση μιας ομάδας τοπικών ελεγκτών που μοιράζονται τα συνολικά καθήκοντα διεξαγωγής μιας ολόκληρης παραγωγικής διαδικασίας (Erickson et al., 1999).

Ο έλεγχος προϊόντων και διαδικασιών επιτυγχάνεται συνήθως με την

ανάπτυξη βρόγχων ελέγχου ή ανατροφοδότησης, όπου τα βασικά προϊόντα και / ή συνθήκες διεργασίας διατηρούνται αυτόματα γύρω από ένα επιθυμητό σημείο ρύθμισης. Για να επιτευχθεί η επιθυμητή ανοχή προϊόντος ή / και διεργασίας γύρω από ένα καθορισμένο σημείο ρύθμισης, ειδικοί ελεγκτές διεργασίας ή πιο ικανά PLC χρησιμοποιούνται στο πεδίο και ρυθμίζονται για να παρέχουν την επιθυμητή ανοχή καθώς και τον ρυθμό αυτο-διόρθωσης κατά την διάρκεια διαταραχών της διαδικασίας.

Με την μορφοποίηση του συστήματος παραγωγής, το DCS μειώνει την επίπτωση ενός μόνο σφάλματος στο συνολικό σύστημα. Σε πολλά σύγχρονα συστήματα, το DCS διασυνδέεται με το εταιρικό δίκτυο για να δώσει στις επιχειρησιακές λειτουργίες μια εικόνα της παραγωγής.

Ο επιβλέπων στέλνει τα καθορισμένα σημεία και ζητά δεδομένα από τους ελεγκτές κατανεμημένου πεδίου. Οι κατανεμημένοι ελεγκτές ελέγχουν τους ενεργοποιητές της διαδικασίας βασισμένοι στις εντολές του διακομιστή ελέγχου και την ανατροφοδότηση των αισθητήρων από τους αισθητήρες διαδικασίας. Επιπλέον, ένα fieldbus επιτρέπει μεγαλύτερη λειτουργικότητα πέρα από τον έλεγχο, συμπεριλαμβανομένης της διάγνωσης συσκευής πεδίου, και μπορεί να πραγματοποιήσει αλγόριθμους ελέγχου εντός του δικτύου fieldbus, αποφεύγοντας έτσι την δρομολόγηση σήματος πίσω στο PLC για κάθε λειτουργία ελέγχου. Τα πρότυπα πρωτόκολλα βιομηχανικής επικοινωνίας που σχεδιάστηκαν από βιομηχανικές ομάδες όπως το Modbus και το Fieldbus (Berge, et al., 2002) χρησιμοποιούνται συχνά σε δίκτυα ελέγχου και δίκτυα fieldbus.

Εκτός από τους βρόγχους ελέγχου σε επίπεδο εποπτείας και σε επίπεδο τομέα, ενδέχεται επίσης να υπάρχουν ενδιάμεσα επίπεδα ελέγχου.

2.3.3 Προγραμματιζόμενες τοπολογίες βασισμένες σε λογικό ελεγκτή

Τα PLC χρησιμοποιούνται τόσο σε συστήματα SCADA όσο και DCS ως στοιχεία ελέγχου ενός συνολικού ιεραρχικού συστήματος για την παροχή

τοπικής διαχείρισης διαδικασιών μέσω ελέγχου ανατροφοδότησης όπως περιγράφεται παραπάνω.

Εκτός από την χρήση PLC στα SCADA και DCS, τα PLC υλοποιούνται επίσης ως ο πρωτεύον ελεγκτής σε μικρότερες διαμορφώσεις συστήματος ελέγχου για να παρέχουν επιχειρησιακό έλεγχο διακεκριμένων διαδικασιών όπως γραμμές συναρμολόγησης αυτοκινήτων και ρυθμιστές του φυσητήρα αιθάλης σε εργοστάσιο παραγωγής ηλεκτρισμού. Αυτές οι τοπολογίες διαφέρουν από τα SCADA και τα DCS στο ότι γενικά δεν διαθέτουν έναν κεντρικό διακομιστή ελέγχου και HMI και κατά συνέπεια παρέχουν κυρίως έλεγχο κλειστού βρόγχου χωρίς άμεση ανθρώπινη συμμετοχή. Τα PLC έχουν μνήμη προγραμματιζόμενη από τον χρήστη για την αποθήκευση οδηγιών για την υλοποίηση συγκεκριμένων λειτουργιών όπως έλεγχος I/O, λογική, χρονισμός, μέτρηση, έλεγχος PID, έλεγχος, επικοινωνία, αριθμητική, και επεξεργασία δεδομένων και αρχείων.

2.4 Σύγκριση σε επίπεδο ασφάλειας μεταξύ ICS και συστημάτων πληροφορικής

Τα συστήματα ICS ελέγχουν τον φυσικό κόσμο και τα συστήματα πληροφορικής διαχειρίζονται δεδομένα. Τα ICS έχουν πολλά χαρακτηριστικά που διαφέρουν από τα παραδοσιακά συστήματα ΤΠ, συμπεριλαμβανομένων των διαφορετικών κινδύνων και προτεραιοτήτων. Ορισμένα από αυτά περιλαμβάνουν τον σημαντικό κίνδυνο για την υγεία και την ασφάλεια της ανθρώπινης ζωής, σοβαρές ζημιές στο περιβάλλον και οικονομικά ζητήματα όπως απώλειες στην παραγωγή και αρνητικές επιπτώσεις στην οικονομία ενός έθνους. Τα ICS έχουν διαφορετικές απαιτήσεις απόδοσης και αξιοπιστίας και χρησιμοποιούν επίσης λειτουργικά συστήματα και εφαρμογές που μπορεί να θεωρούνται μη συμβατικά σε ένα τυπικό περιβάλλον δικτύου πληροφορικής. Οι προστασίες ασφαλείας πρέπει να εφαρμόζονται με τρόπο που να διατηρείται η ακεραιότητα του συστήματος κατά την διάρκεια της κανονικής λειτουργίας καθώς και σε περιόδους επιθέσεων στον κυβερνοχώρο (Knapp, et al., 2011).

Καθώς τα ICS υιοθετούν λύσεις από τον τομέα της πληροφορικής για την

προώθηση της εταιρικής συνδετικότητας και των δυνατοτήτων απομακρυσμένης πρόσβασης και σχεδιάζονται και υλοποιούνται χρησιμοποιώντας βιομηχανικούς υπολογιστές, λειτουργικά συστήματα και πρωτόκολλα δικτύου, αρχίζουν να μοιάζουν με συστήματα πληροφορικής. Αυτή η ενσωμάτωση υποστηρίζει νέες δυνατότητες πληροφορικής, αλλά προσφέρουν σημαντικά λιγότερη απομόνωση των ICS από τον έξω κόσμο σε σχέση με τα παλαιότερα συστήματα, δημιουργώντας μεγαλύτερη ανάγκη για την ασφάλεια αυτών των συστημάτων.

Ενώ οι λύσεις ασφάλειας σχεδιάστηκαν για να αντιμετωπίζουν αυτά τα ζητήματα ασφάλειας σε τυπικά συστήματα πληροφορικής, πρέπει να ληφθούν ειδικές προφυλάξεις κατά την εισαγωγή αυτών των ίδιων λύσεων σε περιβάλλοντα ICS. Σε ορισμένες περιπτώσεις χρειάζονται νέες λύσεις ασφάλειας που να προσαρμόζονται στο περιβάλλον ICS. Τα περιβάλλοντα στα οποία λειτουργούν τα συστήματα ICS και ΤΠ αλλάζουν διαρκώς.

Τα περιβάλλοντα λειτουργίας περιλαμβάνουν, αλλά δεν περιορίζονται: χώρος απειλής, ευπάθειες, αποστολές / επιχειρηματικές λειτουργίες, αποστολές / επιχειρηματικές διαδικασίες, αρχιτεκτονικές ασφάλειας επιχειρήσεων και πληροφοριών, τεχνολογίες πληροφορικής, προσωπικό, εγκαταστάσεις, σχέσεις εφοδιαστικής αλυσίδας, εταιρική διακυβέρνηση / κουλτούρα, διαδικασίες ανάθεσης / προμήθειας, οργανωτικές πολιτικές / διαδικασίες, οργανωτικές παραδοχές, περιορισμοί, ανοχή κινδύνου και προτεραιότητες / αντισταθμίσεις.

Τα παρακάτω παραθέτουν κάποιες ιδιαίτερες εκτιμήσεις κατά την εξέταση της ασφάλειας για τα ICS:

Χρόνος και απαιτήσεις απόδοσης. Τα ICS είναι γενικά κρίσιμα με τον χρόνο, με το κριτήριο για αποδεκτά επίπεδα καθυστέρησης και την μεταβλητότητα να υπαγορεύονται από την επιμέρους εγκατάσταση. Ορισμένα συστήματα απαιτούν αξιόπιστες, αιτιοκρατικές αποκρίσεις.

Απαιτήσεις διαθεσιμότητας. Πολλές διεργασίες ICS έχουν συνεχή χαρακτήρα. Δεν είναι αποδεκτές οι απροσδόκητες διακοπές των συστημάτων που ελέγχουν τις βιομηχανικές διεργασίες. Οι διακοπές συχνά πρέπει να σχεδιάζονται και να προγραμματίζονται ημέρες ή εβδομάδες εκ των προτέρων.

Απαιτήσεις διαχείρισης κινδύνου. Σε ένα τυπικό σύστημα πληροφορικής, το απόρρητο και η ακεραιότητα των δεδομένων είναι συνήθως οι κύριοι προβληματισμοί. Για ένα ICS, οι πρωταρχικές ανησυχίες είναι η ασφάλεια των ανθρώπων και η αντοχή σε βλάβες για την πρόληψη της απώλειας ζωής ή της απειλής της δημόσιας υγείας ή της εμπιστοσύνης, της κανονιστικής συμμόρφωσης, της απώλειας εξοπλισμού, της απώλειας πνευματικής ιδιοκτησίας ή απώλειας ή βλάβης των προϊόντων. Το προσωπικό που είναι υπεύθυνο για την λειτουργία, την εξασφάλιση και την συντήρηση του ICS πρέπει να κατανοεί τον σημαντικό σύνδεσμο μεταξύ ασφάλειας και προστασίας. Οποιοδήποτε μέτρο προστασίας που παρακωλύει την ασφάλεια είναι μη αποδεκτό.

Φυσικές Επιδράσεις. Οι συσκευές πεδίου ICS (π.χ. PLC, σταθμός χειριστή, ελεγκτής DCS) είναι άμεσα υπεύθυνες για τον έλεγχο των φυσικών διεργασιών. Το ICS μπορεί να έχει πολύ σύνθετες αλληλεπιδράσεις με τις φυσικές διεργασίες και οι συνέπειες στον τομέα ICS μπορεί να εκδηλωθούν στα φυσικά γεγονότα. Η κατανόηση αυτών των πιθανών φυσικών επιπτώσεων απαιτεί συχνά επικοινωνία μεταξύ εμπειρογνωμόνων σε συστήματα ελέγχου και σε συγκεκριμένο φυσικό τομέα.

Λειτουργία συστήματος. Τα λειτουργικά συστήματα ICS και τα δίκτυα ελέγχου είναι συχνά αρκετά διαφορετικά από τα αντίστοιχα της ΤΠ, απαιτώντας διαφορετικά σύνολα δεξιοτήτων, εμπειρία και επίπεδα εξειδίκευσης. Τα δίκτυα ελέγχου συνήθως τα διαχειρίζονται οι μηχανικοί ελέγχου, όχι το προσωπικό πληροφορικής. Οι υποθέσεις ότι οι διαφορές δεν είναι σημαντικές μπορεί να έχουν καταστροφικές συνέπειες για τις λειτουργίες του συστήματος.

Περιορισμοί πόρων. Το ICS και τα λειτουργικά του συστήματα σε πραγματικό χρόνο είναι συχνά συστήματα περιορισμένων πόρων, τα οποία δεν περιλαμβάνουν τυπικές σύγχρονες δυνατότητες ασφάλειας ΤΠ. Τα συστήματα παλαιού τύπου συχνά δεν διαθέτουν πόρους που να είναι κοινοί στα σύγχρονα συστήματα ΤΠ. Πολλά συστήματα ενδέχεται να μην έχουν επιθυμητά χαρακτηριστικά, συμπεριλαμβανομένων των δυνατοτήτων κρυπτογράφησης, καταγραφής σφαλμάτων και προστασίας με κωδικό πρόσβασης. Η αδιάκριτη χρήση των πρακτικών ασφαλείας ΤΠ στα ICS ενδέχεται να προκαλέσει διακοπές

στην διαθεσιμότητα και διαταραχές σε επίπεδο χρόνου. Ενδέχεται να μην υπάρχουν διαθέσιμοι υπολογιστικοί πόροι στα εξαρτήματα ICS για την εκ των υστέρων εγκατάσταση αυτών των συστημάτων με τις τρέχουσες δυνατότητες ασφαλείας. Η προσθήκη πόρων ή δυνατοτήτων ενδέχεται να μην είναι δυνατή.

Επικοινωνίες. Τα πρωτόκολλα επικοινωνίας και τα μέσα που χρησιμοποιούνται από τα περιβάλλοντα ICS για τον έλεγχο της συσκευής πεδίου και την επικοινωνία εντός του επεξεργαστή είναι συνήθως διαφορετικά από τα περισσότερα περιβάλλοντα ΤΠ και ενδέχεται να είναι ιδιοκτησιακά.

Διαχείριση αλλαγών. Η διαχείριση της αλλαγής είναι υψίστης σημασίας για την διατήρηση της ακεραιότητας τόσο των συστημάτων ΤΠ όσο και των συστημάτων ελέγχου. Το μη καταχωρημένο λογισμικό αντιπροσωπεύει μία από τις μεγαλύτερες ευπάθειες σε ένα σύστημα. Οι ενημερώσεις λογισμικού στα συστήματα πληροφορικής, συμπεριλαμβανομένων των ενημερωμένων εκδόσεων ασφαλείας, συνήθως εφαρμόζονται έγκαιρα βάσει της κατάλληλης πολιτικής και των διαδικασιών ασφαλείας. Επιπλέον, αυτές οι διαδικασίες είναι συνήθως αυτοματοποιημένες με την χρήση εργαλείων που βασίζονται σε διακομιστές. Οι ενημερώσεις λογισμικού στα ICS δεν μπορούν πάντα να υλοποιηθούν σε εύθετο χρόνο. Αυτές οι ενημερώσεις πρέπει να υποβληθούν σε ενδελεχή δοκιμή τόσο από τον προμηθευτή της εφαρμογής βιομηχανικού ελέγχου όσο και από τον τελικό χρήστη της εφαρμογής πριν υλοποιηθεί. Επιπλέον, ο ιδιοκτήτης του ICS πρέπει να σχεδιάζει και να προγραμματίζει τις ημέρες / εβδομάδες διακοπής του ICS εκ των προτέρων. Το ICS ενδέχεται επίσης να απαιτεί επανεπικύρωση στο πλαίσιο της διαδικασίας ενημέρωσης. Ένα άλλο ζήτημα είναι ότι πολλά ICS χρησιμοποιούν παλαιότερες εκδόσεις λειτουργικών συστημάτων που δεν υποστηρίζονται πλέον από τον προμηθευτή. Συνεπώς, τα διαθέσιμα patches ενδέχεται να μην ισχύουν. Η διαχείριση της αλλαγής ισχύει επίσης για το υλικό και το υλικολογισμικό. Η διαδικασία διαχείρισης αλλαγών, όταν εφαρμόζεται στο ICS, απαιτεί προσεκτική αξιολόγηση από τους ειδικούς του ICS (π.χ. μηχανικοί ελέγχου) που εργάζονται σε συνεργασία με το προσωπικό ασφαλείας και πληροφορικής.

Διαχείριση της Υποστήριξης. Τα τυπικά συστήματα πληροφορικής επιτρέπουν

διαφοροποιημένες μορφές υποστήριξης, ίσως υποστηρίζοντας διαφορετικές αλλά διασυνδεδεμένες τεχνολογικές αρχιτεκτονικές. Για τα ICS, η υπηρεσία υποστήριξης παρέχεται μερικές φορές μέσω ενός μόνο προμηθευτή, ο οποίος μπορεί να μην παρέχει μια διαφοροποιημένη και διαλειτουργική λύση υποστήριξης από άλλο προμηθευτή. Σε ορισμένες περιπτώσεις, δεν επιτρέπονται λύσεις ασφάλειας τρίτων κατασκευαστών εξαιτίας των συμφωνιών παροχής αδείας και παροχής υπηρεσιών με τους προμηθευτές των ICS και μπορεί να προκύψει απώλεια της υπηρεσίας υποστήριξης εάν εγκατασταθούν εφαρμογές τρίτων κατασκευαστών χωρίς την επιβεβαίωση ή έγκριση του προμηθευτή.

2.5 Άλλοι τύποι συστημάτων ελέγχου

Υπάρχουν και άλλα είδη συστημάτων ελέγχου με παρόμοια χαρακτηριστικά και πολλές από τις συστάσεις για τα ICS είναι εφαρμόσιμες και θα μπορούσαν να χρησιμοποιηθούν ως αναφορά για την προστασία αυτών των συστημάτων από απειλές στον κυβερνοχώρο (US, 2014). Παραδείγματα ορισμένων από αυτά τα συστήματα και τα πρωτόκολλα περιλαμβάνουν:

Άλλοι τύποι συστημάτων ελέγχου

- Υποδομή προηγμένης μέτρησης
- Συστήματα αυτοματισμού κτιρίων
- Συστήματα Ελέγχου Διαχείρισης Κτιρίων
- Συστήματα επιτήρησης κλειστού κυκλώματος τηλεόρασης (CCTV)
- Παρακολούθηση CO2
- Συστήματα ψηφιακή σήμανσης
- Συστήματα Διαχείρισης Ψηφιακών Βίντεο
- Συστήματα Ηλεκτρονικής Ασφάλειας

- Συστήματα διαχείρισης έκτακτης ανάγκης
- Συστήματα Διαχείρισης Ενέργειας
- Συστήματα ελέγχου εξωτερικού φωτισμού
- Συστήματα πυρανίχνευσης
- Συστήματα πυρόσβεσης καταιονισμού
- Συστήματα ελέγχου εσωτερικού φωτισμού
- Συστήματα ανίχνευσης εισβολής
- Συστήματα Ελέγχου Φυσικής Πρόσβασης
- Δημόσιας ασφάλειας/Επίγειες Κινητές Ραδιοεπικοινωνίες
- Γεωθερμικά Συστήματα Ανανεώσιμων Πηγών Ενέργειας
- Φωτοβολταϊκά Συστήματα Ανανεώσιμων Πηγών Ενέργειας
- Συστήματα ελέγχου σκίασης
- Συστήματα καπνού και καθαρισμού
- Συστήματα κατακόρυφων μεταφορών (ανελκυστήρες και κυλιόμενες σκάλες)
- Συστήματα ελέγχου εργαστηριακών οργάνων
- Συστήματα Διαχείρισης Εργαστηριακών Πληροφοριών

Πρωτόκολλα / Θύρες και Υπηρεσίες

- Modbus: Master / Slave - Θύρα 502.
- BACnet2: Master / Slave - Θύρα 47808.

- LonWorks / LonTalk3: Peer to Peer - Θύρα 1679.

- DNP3: Master / Slave - Θύρα 19999 όταν χρησιμοποιείτε Ασφάλεια Layer Transport (TLS), Port 20000 όταν δεν χρησιμοποιείται το TLS.

- IEEE 802.x - Peer to Peer

- ZigBee - Peer to Peer

- Bluetooth - Master / Slave

Οι έλεγχοι ασφαλείας είναι αρκετά γενικοί και ευέλικτοι και μπορούν να χρησιμοποιηθούν για την αξιολόγηση άλλων τύπων συστημάτων ελέγχου, αλλά οι ειδικοί του χώρου πρέπει να αναθεωρήσουν τους ελέγχους και να τους προσαρμόσουν όπως αρμόζει για την αντιμετώπιση της μοναδικότητας άλλων τύπων συστημάτων ελέγχου. Δεν υπάρχει ένα γενικό πρότυπο που να ταιριάζει σε όλα και οι κίνδυνοι μπορεί να μην είναι ίδιοι, ακόμη και μέσα σε μια συγκεκριμένη ομάδα. Για παράδειγμα, ένα κτίριο διαθέτει πολλά διαφορετικά υποσυστήματα όπως αυτοματισμοί κτιρίων, συναγερμός πυρκαγιάς, έλεγχος φυσικής πρόσβασης, ψηφιακή σήμανση, CCTV κλπ. Τα κρίσιμα συστήματα ασφάλειας της ζωής, όπως τα συστήματα συναγερμού πυρκαγιάς και φυσικού ελέγχου πρόσβασης, μπορεί να αυξήσουν το επίπεδο ασφαλείας σε «υψηλό», ενώ τα άλλα συστήματα θα είναι συνήθως σε «χαμηλό» επίπεδο κινδύνου. Ένας οργανισμός μπορεί να αποφασίσει να αξιολογήσει κάθε υποσύστημα μεμονωμένα ή να αποφασίσει να χρησιμοποιήσει μια συνολική προσέγγιση. Η αξιολόγηση των συστημάτων ελέγχου θα πρέπει να συνδυαστεί με τον επιχειρηματικό αντίκτυπο, το σχέδιο έκτακτης ανάγκης και το σχέδιο αντιμετώπισης περιστατικών, ώστε να διασφαλιστεί ότι οι κρίσιμες λειτουργίες και ενέργειες του οργανισμού θα μπορούν να ανακτηθούν και να αποκατασταθούν όπως ορίζονται από τους χρονικούς στόχους της ανάκτησης.

Κεφάλαιο 3^{Ο} Ασφάλεια SCADA

Αυτό το κεφάλαιο περιλαμβάνει μία σύντομη εξήγηση για το τι είναι το SCADA, ποιες είναι οι αυξανόμενες απειλές γι' αυτό και πού και γιατί το περιβάλλον της Αυτοματοποίησης Διαδικασιών είναι ευάλωτο. Με τη συναίνεση του Ολλανδικού Υπουργείου Οικονομικών, το περιεχόμενο αυτού του κεφαλαίου βασίζεται στην έκθεση TNO-KEMA με τίτλο «SCADA (in) security: a role for the government» (Luiijf and. Lassche, 2006), όπου εξετάζεται λεπτομερώς το πρόβλημα της ασφάλειας πληροφοριών SCADA, συμπεριλαμβανομένης μίας επισκόπησης των εθνικών και διεθνών πρωτοβουλιών και άλλων δραστηριοτήτων στον τομέα της ασφάλειας SCADA.

3.1 Τι σημαίνουν οι όροι SCADA, PCS, DCS, RTU και PLC;

Τα συστήματα SCADA ενσωματώνουν συστήματα λήψης δεδομένων με συστήματα μετάδοσης δεδομένων και λογισμικό HMI για να παρέχουν ένα κεντρικό σύστημα παρακολούθησης και ελέγχου για πολλές εισόδους και εξόδους της διαδικασίας. Τα συστήματα SCADA έχουν σχεδιαστεί για να συλλέγουν πληροφορίες πεδίου, να τις μεταφέρουν στην κεντρική εγκατάσταση υπολογιστών και να προβάλλουν τις πληροφορίες στον χρήστη γραφικά ή σε κείμενο, επιτρέποντας έτσι στον χειριστή να παρακολουθεί ή να ελέγχει ολόκληρο το σύστημα από μια κεντρική τοποθεσία σχεδόν σε πραγματικό χρόνο.

Με βάση την πολυπλοκότητα και την ρύθμιση του επιμέρους συστήματος, ο έλεγχος κάθε επιμέρους συστήματος, λειτουργίας ή εργασίας μπορεί να είναι αυτόματος ή μπορεί να πραγματοποιηθεί μέσα από εντολές του χειριστή. Το σύνηθες υλικό περιλαμβάνει έναν διακομιστή ελέγχου τοποθετημένο σε ένα κέντρο ελέγχου, τον εξοπλισμό επικοινωνιών (π.χ. ραδιόφωνο, τηλεφωνική γραμμή, καλώδιο ή δορυφόρο) και έναν ή περισσότερους γεωγραφικά κατανεμημένους χώρους πεδίου που αποτελούνται από απομακρυσμένες μονάδες τερματικών (RTU) ή / και PLC τα οποία ελέγχουν τους ενεργοποιητές και / ή παρακολουθούν τους αισθητήρες.

Ο διακομιστής ελέγχου αποθηκεύει και επεξεργάζεται τις πληροφορίες από τις εισόδους και τις εξόδους RTU, ενώ το RTU ή το PLC ελέγχει την τοπική διαδικασία. Το υλικό επικοινωνίας επιτρέπει την μεταφορά πληροφοριών και δεδομένων εμπρός και πίσω μεταξύ του διακομιστή ελέγχου και των RTU ή PLC. Το λογισμικό προγραμματίζεται για να ενημερώνει το σύστημα τι και πότε πρέπει να παρακολουθεί, ποιες περιοχές παραμέτρων είναι αποδεκτές και ποια απόκριση πρέπει να ξεκινήσει όταν οι παράμετροι αλλάζουν εκτός αποδεκτών τιμών. Μια έξυπνη ηλεκτρονική συσκευή (IED), όπως ένα προστατευτικό διακόπτη (ρελέ), μπορεί να επικοινωνεί απευθείας με τον διακομιστή ελέγχου ή μια τοπική μονάδα RTU μπορεί να διερευνά τα IED για να συλλέξει τα δεδομένα και να τα μεταβιβάσει στον διακομιστή ελέγχου.

Το κέντρο ελέγχου είναι επίσης υπεύθυνο για τις ειδοποιήσεις, τις αναλύσεις τάσεων και τις αναφορές.

Οι χώροι του πεδίου εκτελούν τον τοπικό έλεγχο των ενεργοποιητών και των αισθητήρων των οθονών. Οι χώροι του πεδίου είναι συχνά εξοπλισμένοι με την δυνατότητα απομακρυσμένης πρόσβασης ώστε να επιτρέπουν στους χειριστές να πραγματοποιούν απομακρυσμένες διαγνώσεις και επισκευές συνήθως μέσω ενός ξεχωριστού dial-up μόντεμ ή μέσω σύνδεσης WAN. Τα πρότυπα πρωτόκολλα και τα πρωτόκολλα επικοινωνίας που εκτελούνται μέσω σειριακών και δικτυακών επικοινωνιών χρησιμοποιούνται για την μεταφορά πληροφοριών μεταξύ του κέντρου ελέγχου και των χώρων πεδίου χρησιμοποιώντας τεχνικές τηλεμετρίας όπως τηλεφωνικής γραμμής, καλωδίου, ινών και ραδιοσυχνοτήτων π.χ. εκπομπών, μικροκυματικών και δορυφορικών.

Για την Αυτοματοποίηση Διαδικασιών, το μοντέλο ISA-95 (ANSI/ISA-95.00.01-2000), για τη μοντελοποίηση της παραγωγής διακρίνει πέντε επίπεδα ιεραρχίας στην παραγωγή (βλ. Σχήμα 1). Αυτά είναι:

• Επίπεδο 0: Το φυσικό επίπεδο: αισθητήρες, ενεργοποιητές και εξοπλισμός επεξεργασίας.

• Επίπεδο 1: Έξοδος αισθητήρα, εντολές για ενεργοποιητές και ηλεκτρονικό έλεγχο και παρακολούθηση (PLC).

• Επίπεδο 2: Επίπεδο εποπτικού ελέγχου (SCADA) και Διεπαφή

Ανθρώπου-Μηχανής (HMI).

• Επίπεδο 3: Σύστημα Εκτέλεσης Βιομηχανικής Παραγωγής (MES): υποστήριξη της βέλτιστης χρήσης των παραγωγικών πόρων, βασικών υλικών και ανθρώπων (εν συντομία: πόρων) για την παραγωγή (λειτουργίες).

• Επίπεδο 4: Σχεδιασμός Επιχειρησιακών Πόρων, συμπεριλαμβανομένου του Επιχειρηματικού Σχεδιασμού και των Logistics όπως η Διαχείριση Επιχειρηματικών Πόρων (ERM) και η Διαχείριση Εφοδιαστικής Αλυσίδας (SCM).

Εικόνα 1 Πρότυπο ISA95-1 για μοντελοποίηση παραγωγής.

SCADA / HMI, Επίπεδο 2 στο μοντέλο, εκτελεί τις ακόλουθες εργασίες:

1 Οπτικοποίηση και λειτουργία των στοιχείων της διαδικασίας σε διάφορα μέρη (αλληλεπίδραση ανθρώπου-μηχανής).

2 Ελεγχόμενη ανταλλαγή δεδομένων με το επίπεδο ελέγχου διαδικασίας, συνήθως Προγραμματιζόμενοι Λογικοί Ελεγκτές (Programmable Logic Controllers - PLC).

3 Διαχείριση συναγερμών, ανάλυση τάσεων και αναφορές.

4 Καταγραφή και αποθήκευση ιστορικών δεδομένων («ιστορικός»).

5 Χειρισμός λειτουργιών παρτίδας - προαιρετικά σε ένα πακέτο SCADA.

6 Διαχείριση χρήστη.

7 Ανάλυση και επεξεργασία δεδομένων.

8 Ελεγχόμενη ανταλλαγή δεδομένων με το επίπεδο MES/τον τομέα της διαχείρισης.

Είναι σημαντικό να γνωρίζουμε ότι κάθε ένα από αυτά τα επίπεδα έχει τα δικά του μέτρα ασφαλείας. Ωστόσο, η παρούσα έκθεση εξετάζει την ασφάλεια των πληροφοριών των τριών χαμηλότερων επιπέδων και την ανταλλαγή πληροφοριών με τα υψηλότερα επίπεδα.

Συζητούνται εν συντομία τα βασικά στοιχεία του συστήματος στα επίπεδα μηδέν, ένα και δύο του ISA95-1 και οι λειτουργίες τους. Μία πλήρης επισκόπηση των διαφόρων συστατικών του συστήματος SCADA και των

λειτουργιών τους παρουσιάζεται στον Πίνακα 1. Οι τοπικοί επεξεργαστές συλλέγουν δεδομένα μέτρησης από αισθητήρες και βαλβίδες ελέγχου, κινητήρες κλπ. χρησιμοποιώντας υδραυλικά και πνευματικά συστήματα και ηλεκτρονικά συστήματα ισχύος. Αυτά τα είδη τοπικών επεξεργαστών ονομάζονται Προγραμματιζόμενοι Λογικοί Ελεγκτές (PLC) όταν αποτελούνται από επεξεργαστή σε μία ηλεκτρονική πλακέτα. Συχνά, αρκετά PLC είναι ενσωματωμένα σε ένα μεμονωμένο πλαίσιο στήριξης ή περίβλημα.

Μία Απομακρυσμένη Τερματική Μονάδα (Remote Terminal Unit - RTU) είναι ένας τοπικός επεξεργαστής, συνήθως με περισσότερη χωρητικότητα επεξεργαστή από ένα PLC, το οποίο λειτουργεί μια σειρά ηλεκτρονικής πλακέτας. Τα διάφορα συστήματα συνήθως επικοινωνούν μέσω ανοικτών πρωτοκόλλων επικοινωνίας, όπως το TCP/IP (H.A.M 2006)

Παράδειγμα

Η «λειτουργία των πληροφοριών» στο επίπεδο 1 ανιχνεύει μια διαρροή αγωγού χρησιμοποιώντας αισθητήρες υγρού ή μια διαφορά στην ταχύτητα ή την πίεση ροής (επίπεδο 0). Αυτό μπορεί να σταλεί σε ένα (κεντρικό) κέντρο ελέγχου (επίπεδο 2) ως μήνυμα. Δημιουργείται ένας συναγερμός στο κέντρο ή η ομάδα συντήρησης ενημερώνεται αυτόματα. Ο συναγερμός μπορεί επίσης να εμφανίζεται στην οθόνη του χειριστή με λογικό και οργανωμένο τρόπο.

Το SCADA είναι μία συγκεκριμένη εφαρμογή Συστημάτων Ελέγχου Διαδικασιών (PCS). Μία άλλη αρχιτεκτονική PCS που βασίζεται στον κατανεμημένο έλεγχο καλείται Κατανεμημένα Συστήματα Ελέγχου (DCS), η οποία παρακολουθεί και ελέγχει συστήματα από το όργανο μέτρησης έως την κονσόλα ελέγχου. Κανονικά, τα συστήματα ελέγχου διαδικασιών κατανέμονται σε μεγάλες αποστάσεις και μερικές φορές έχουν προ-προγραμματισμένες λειτουργίες ελέγχου στο κεντρικό σύστημα υπολογιστή. Τα DCS χρησιμοποιούνται σε μεγάλες αυτόνομες εγκαταστάσεις όπου ο τοπικός επεξεργαστής παρέχει τις λειτουργίες ελέγχου. Η διαφορά μεταξύ του SCADA και του DCS γίνεται ολοένα και λιγότερο ευδιάκριτη, γεγονός που αποτελεί έναν από τους λόγους για τους οποίους το μεγαλύτερο μέρος της βιβλιογραφίας (συμπεριλαμβανομένης αυτής της έκθεσης) χρησιμοποιεί γενικά τον όρο

SCADA. Με την ευρύτερη έννοια, ο όρος SCADA μπορεί να θεωρηθεί ως ο τομέας της Αυτοματοποίησης Διαδικασιών.

Πίνακας 1 Ορολογία και λειτουργίες

Εξάρτημα	**Λειτουργίες**
Αισθητήρες και όργανα	Αισθητήρες και όργανα στο πεδίο που ανιχνεύουν συνθήκες όπως τάση, ισχύ, πίεση, θερμοκρασία, ταχύτητα ροής και κατάσταση βαλβίδας.
Ενεργοποιητές	Ενεργοποιητές όπως αντλίες, βαλβίδες, κινητήρες και διακόπτες κυκλωμάτων που λειτουργούν εξ αποστάσεως ή τοπικά.
Τοπικοί επεξεργαστές	Οι τοπικοί επεξεργαστές επικοινωνούν τόσο με τους αισθητήρες και τους ενεργοποιητές όσο και με τις λειτουργίες στο δίκτυο. Μπορούν να διαδραματίσουν έναν ή όλους τους παρακάτω ρόλους: • Συλλογή δεδομένων που παράγονται από τους αισθητήρες και τα όργανα. • Ενεργοποίηση και απενεργοποίηση των συνδεδεμένων ενεργοποιητών μέσω εσωτερικής (προγραμματισμένης) λογικής ή βάσει εντολών που αποστέλλονται από το προσωπικό χειρισμού ή υπολογιστές. • Μετάφραση πρωτοκόλλων

	επικοινωνίας έτσι ώστε πολλά συστήματα και όργανα ελέγχου διαδικασιών να μπορούν να επικοινωνούν μεταξύ τους. • Προσδιορισμός συνθηκών συναγερμού. Προς το παρόν, οι τοπικοί επεξεργαστές έχουν διάφορα ονόματα, όπως Προγραμματιζόμενος Λογικός Ελεγκτής (PLC), Απομακρυσμένη Τερματική Μονάδα (RTU), Έξυπνη Ηλεκτρονική Συσκευή (IED) και Ελεγκτής Αυτοματοποίησης Διαδικασιών (PAC). Ένας μόνο τοπικός επεξεργαστής μπορεί να είναι υπεύθυνος για τη συλλογή δεδομένων και τον έλεγχο δεκάδων οργάνων και ενεργοποιητών.
Εξοπλισμός επικοινωνίας μικρής απόστασης	Ο εξοπλισμός επικοινωνίας μικρής απόστασης εξασφαλίζει την επικοινωνία μεταξύ των τοπικών επεξεργαστών και των αισθητήρων και ενεργοποιητών. Τα αναλογικά ή ψηφιακά σήματα μεταδίδονται κατά μήκος σχετικά μικρών καλωδίων ή ασύρματων συνδέσεων.
Κεντρικό Σύστημα Υπολογιστών	Το Κεντρικό Σύστημα Υπολογιστών λειτουργεί ως κεντρικό σύστημα ελέγχου και λειτουργίας, επιτρέποντας στο προσωπικό χειρισμού να

	παρακολουθεί τις διαδικασίες, να λαμβάνει και να αξιολογεί τους συναγερμούς, να αναλύει δεδομένα και να στέλνει σήματα ελέγχου στους ενεργοποιητές. Σε ορισμένες περιπτώσεις, το σύστημα περιλαμβάνει προγραμματισμένη λογική που χρησιμοποιείται για τον αυτόματο έλεγχο των τοπικών επεξεργαστών. Σε άλλες περιπτώσεις, αυτό το σύστημα είναι καθαρά μια διεπαφή μεταξύ του προσωπικού χειρισμού και των τοπικών επεξεργαστών. Άλλες εργασίες που εκτελούνται από το κεντρικό σύστημα υπολογιστών περιλαμβάνουν την αποθήκευση δεδομένων μέτρησης και των συνθηκών του συστήματος σε μια (ιστορική) βάση δεδομένων και τη δημιουργία αναφορών. Το κεντρικό σύστημα υπολογιστών μπορεί επίσης να ονομαστεί Κεντρική Τερματική Μονάδα (MTU) ή διακομιστής SCADA. Σε πολλές περιπτώσεις, είναι απλώς ένας προσωπικός υπολογιστής (PC) με λογισμικό διεπαφής ανθρώπου-μηχανής (HMI).
Εξοπλισμός επικοινωνίας μεγάλης απόστασης	Ο εξοπλισμός επικοινωνίας μεγάλης απόστασης είναι υπεύθυνος για την επικοινωνία μεταξύ των τοπικών επεξεργαστών και του κεντρικού

	συστήματος υπολογιστών. Το δίκτυο εκτείνεται για αρκετά χιλιόμετρα. Χρησιμοποιεί μισθωμένες γραμμές, xDSL, σκοτεινές ίνες, δορυφορικές συνδέσεις, μικροκυματικές συνδέσεις, συνδέσεις από σημείο σε σημείο, GSM, GPRS, UMTS και αναμετάδοση πλαισίου.

3.2 Χρήση SCADA στον τομέα του πόσιμου νερού

Με την ευρύτερη έννοια, τα συστήματα και τα δίκτυα SCADA - ή Αυτοματοποίησης Διαδικασιών - αποτελούν έναν ουσιαστικό σύνδεσμο στην αλυσίδα εγγυημένης παροχής και ποιότητας πόσιμου νερού στην Ολλανδία.

Τα συστήματα SCADA στον τομέα του πόσιμου νερού μετρούν, ελέγχουν και παρακολουθούν (χειρισμός συναγερμού και συμβάντων) τις ακόλουθες διαδικασίες πόσιμου νερού, τόσο σε τοπικό επίπεδο όσο και σε απόσταση (*SCADA 2019)*:

• εξόρυξη νερού ή/και συλλογή ακατέργαστου νερού.

• μεταφορά ακατέργαστου νερού σε δεξαμενές συλλογής και δεξαμενές απορροής.

• μεταφορά στις διαδικασίες καθαρισμού/διήθησης του νερού.

• Παρακολούθηση και έλεγχος των διαδικασιών καθαρισμού και διήθησης του νερού.

• Παρακολούθηση και έλεγχος της διαδικασίας ελέγχου ποιότητας.

• Διανομή επεξεργασμένου νερού και

• Έλεγχος αντλιών πίεσης.

Αυτό περιλαμβάνει την παρακολούθηση και τον έλεγχο της ταχύτητας ροής στους αγωγούς, την πίεση στις δεξαμενές αποθήκευσης, την ενεργοποίηση και απενεργοποίηση των αντλιών, τις βαλβίδες ελέγχου και τις πτυχές

παρακολούθησης της ποιότητας του νερού, όπως η τιμή του pH και η θολερότητα. Οι επιλογές συναγερμού και παρέμβασης είναι κυρίως συγκεντρωμένες σε ένα κέντρο ελέγχου και παρακολούθησης. Στον τομέα του πόσιμου νερού, αυτό είναι συχνά γνωστό ως «κεντρικό ρολόι» (H.A.M 2007)

3.3 Ανασφάλεια του SCADA και ο κίνδυνος

Το γεγονός ότι τα συστήματα και τα δίκτυα SCADA είναι ολοένα και πιο ανασφαλή είναι το αποτέλεσμα ορισμένων τεχνικών και οργανωτικών εξελίξεων. Πρώτον, το SCADA είναι ένα προϊόν κλασσικής Αυτοματοποίησης Διαδικασιών με πλαίσια στήριξης γεμάτα με ηλεκτρονικά και ηλεκτρονόμους (ρελέ), ένα περιβάλλον στο οποίο η ασφάλεια των πληροφοριών δεν έπαιξε καθόλου ρόλο. Ούτε ήταν απαραίτητο, δεδομένου ότι τα συστήματα και τα πρωτόκολλα SCADA βασίστηκαν σε:

• ιδιόκτητα πρωτόκολλα, τεχνικές και υποκείμενο σύστημα ελέγχου.

• καμία δημόσια ενημέρωση σχετικά με τον τρόπο λειτουργίας της SCADA.

• δεν υπάρχουν τηλεπικοινωνίες ή μόνο συνδέσεις από σημείο σε σημείο μέσω μισθωμένων ή ιδιοκτησιακών γραμμών.

• δεν υπάρχει σύνδεση με το διαχειριστικό δίκτυο επιχειρήσεων και το Διαδίκτυο.

• υλοποιήσεις χωρίς επαρκείς μηχανισμούς ασφαλείας, επειδή το περιβάλλον θεωρείται ότι είναι απαλλαγμένο από χάκερ.

• εφαρμογές πρωτοκόλλου που δεν έλαβαν υπόψη τις «συνθήκες στρες» όπως εκείνες που μπορούν να προκληθούν από υπερφόρτωση δικτύου ή ακατάλληλη συμπεριφορά πρωτοκόλλου.

• συστήματα που δεν χρειάστηκε να διορθωθούν με λογισμικά επιδιόρθωσης (patches).

• πλήρως ελεγχόμενα και κλειστά ασφαλή περιβάλλοντα.

Σήμερα, η πρακτική κατάσταση είναι διαφορετική. Οι βασικές αρχές που

αναφέρθηκαν παραπάνω δεν ισχύουν πλέον. Δυστυχώς, από άποψη ασφάλειας των πληροφοριών, συχνά δεν υπάρχει ανάλογη εξέλιξη με τις ταχείες επιχειρησιακές και τεχνικές εξελίξεις ούτε στην εφαρμοσμένη τεχνολογία SCADA ούτε στο επιχειρησιακό περιβάλλον:

• Τα πρωτόκολλα SCADA έχουν μετατραπεί σε ανοικτά πρότυπα και η περιγραφή τους μπορεί να βρεθεί στο Διαδίκτυο.

• Το SCADA εκτελείται ως εφαρμογή σε Windows ή Linux και χρησιμοποιεί πρωτόκολλα Διαδικτύου (TCP / IP) για τη μεταφορά δεδομένων. Τα τρωτά σημεία αυτών των συστημάτων και πρωτοκόλλων είναι γνωστά από τους χάκερ σε όλο τον κόσμο και μπορούν να αξιοποιηθούν χρησιμοποιώντας εργαλειοθήκες.

• Η τρέχουσα διεπαφή ανθρώπου-μηχανής δεν απαιτεί πλέον περίπλοκες εντολές και βασίζεται σε ένα περιβάλλον περιήγησης ιστού.

• Για τον επιχειρηματικό κόσμο, είναι απαραίτητο να δημιουργηθούν συνδέσεις με τα δίκτυα εταιρειών και τα δημόσια δίκτυα. Υπάρχουν επίσης σημεία πρόσβασης μόντεμ στο δίκτυο SCADA για έλεγχο από το σπίτι και για συντήρηση από κατασκευαστές και προμηθευτές SCADA.

• Οι χάκερ και άλλοι ολοένα και περισσότερο ενδιαφέρονται να εισβάλλουν στα συστήματα και τα δίκτυα SCADA.

• Οι απλές δοκιμές δείχνουν ότι τα συστήματα SCADA «στρεσάρονται» ή ακόμα και παύουν να λειτουργούν εντελώς μόλις αποστέλλεται σε αυτά ένα άγνωστο πακέτο μέσω του δικτύου.

• Μια νέα επιλογή στις πλακέτες PLC που δεν μπορεί πάντα να απενεργοποιηθεί είναι ένας ενσωματωμένος διακομιστής ιστού ο οποίος παρέχει απομακρυσμένη πρόσβαση σε όλες τις ρυθμίσεις παραμέτρων.

• Ο εξοπλισμός SCADA περιλαμβάνει μερικές φορές ένα πρότυπο μόντεμ για την απομακρυσμένη πρόσβαση από τον προμηθευτή SCADA.

• Οι κωδικοί πρόσβασης δεν αλλάζουν ποτέ και δεν είναι προσωπικοί, επειδή «το περιβάλλον είναι κλειστό, έτσι δεν είναι;»

Όλα αυτά συμβαίνουν σε περιβάλλον Αυτοματοποίησης Διαδικασιών που αγνοεί εν πολλοίς τον κίνδυνο SCADA (SCADA Security and Terrorism). Αυτό

το περιβάλλον συνήθως υποστηρίζει μια εντελώς διαφορετική κουλτούρα από αυτή του κόσμου του εταιρικού αυτοματισμού, όπου η ασφάλεια των πληροφοριών λαμβάνει περισσότερη προσοχή και όπου η προστασία από τους χάκερ, τους ιούς, τον κωδικό Trojan και το spam είναι η ρουτίνα της ημέρας. Επιπλέον, οι οργανισμοί που εφαρμόζουν Αυτοματοποίηση Διαδικασιών δεν έχουν εξελιχθεί παράλληλα με τις εξελίξεις στην προστασία της Αυτοματοποίησης Διαδικασιών.

Η ασφάλεια δεν είναι ενσωματωμένη στη διαδικασία λειτουργίας και είναι συχνά ασαφές ποιος είναι ο ιδιοκτήτης της διαδικασίας.

Η προηγούμενη ανάλυση (Luiijf, 2006) έδειξε ότι ορισμένες πτυχές του περιβάλλοντος αυτοματοποίησης της διαδικασίας SCADA των επιχειρήσεων πόσιμου νερού δεν διαφέρουν:

• συχνά δεν υπάρχει συγκεκριμένη πολιτική ασφαλείας SCADA.

• δεν γίνεται τίποτα για την πιο ενδελεχή ενημέρωση του προσωπικού σχετικά με την ασφάλεια.

• δεν λαμβάνονται μέτρα περιορισμού του κινδύνου για τους αναγνωρισμένους παράγοντες κινδύνου («τι κρατά τον τομέα ξύπνιο τη νύχτα»;)

• τρίτα μέρη μπορούν να συνδέσουν εξοπλισμό στο δίκτυο SCADA χωρίς επίβλεψη.

• Σπάνια εκτελούνται έλεγχοι σάρωσης για ιούς

• δεν έχουν εγκατασταθεί τα απαραίτητα λογισμικά επιδιόρθωσης (patches) ή έχουν εγκατασταθεί αργά.

Πίνακας 2 Περισσότερες παρανοήσεις σχετικά με τη μη ευπάθεια του SCADA.

Η πραγματικότητα των υποθέσεων

Χρησιμοποιούμε μισθωμένες γραμμές, οπότε κανείς δεν μπορεί να έχει πρόσβαση στις επικοινωνιακές μας συνδέσεις	Είναι εύκολο να εισχωρήσει κανείς σε αυτές τις γραμμές επικοινωνίας (για παράδειγμα, δείτε www.tscm.com/outsideplant.html).

Χρησιμοποιούμε τηλεφωνικές συνδέσεις (dial-up) και κανείς δεν γνωρίζει τους αριθμούς τηλεφώνου	Μία πρόσβαση στην εξερχόμενη γραμμή ή σε έναν αναλυτικό τηλεφωνικό λογαριασμό αποκαλύπτει γρήγορα όλους τους αριθμούς που έχουν κληθεί. Το λογισμικό τηλεφωνικής κλήσης καλεί αυτόματα μια σειρά αριθμών και μπορεί να αναγνωρίσει τους αριθμούς που έχουν σύνδεση μόντεμ.
Χρησιμοποιούμε μόντεμ call-back έτσι ώστε τα μη εξουσιοδοτημένα μέρη να μην έχουν πρόσβαση.	Αν είναι δυνατή η πρόσβαση σε μία σύνδεση, είναι εύκολο να ξεφύγει κανείς από τον μηχανισμό call-back. Υπάρχουν ακόμη και μέθοδοι για τις οποίες δεν είναι απαραίτητη μια πρόσβαση.
Τα απομακρυσμένα μας συστήματα προστατεύονται από κωδικούς πρόσβασης.	Οι μέθοδοι που χρησιμοποιούνται για την κλοπή κωδικών πρόσβασης είναι κοινώς γνωστή. Η πιο εύκολη μέθοδος είναι η υποκλοπή της κίνησης δεδομένων με ένα sniffer. Ο κωδικός πρόσβασης μπορεί στη συνέχεια να υποκλαπεί όταν αποστέλλεται ως κανονικό κείμενο μέσω της γραμμής επικοινωνίας. Οι μέθοδοι εικασίας των κωδικών πρόσβασης με τη βοήθεια ενός λεξικού είναι επίσης γνωστές. Η ανταλλαγή των κωδικών πρόσβασης ή η μη αλλαγή ενός κωδικού πρόσβασης ποτέ είναι επίσης πολύ συνηθισμένα. Συχνά, ένας κωδικός πρόσβασης είναι πολύ απλός με λίγους μόνο χαρακτήρες

	και δεν αλλάζει ποτέ.
Χρησιμοποιούμε τεχνολογία διαμόρφωσης συχνότητας όπως αυτή που χρησιμοποιείται από τον στρατό για ασφαλή επικοινωνία.	Υπάρχουν απλές μέθοδοι για την αποκωδικοποίηση σειρών διαμόρφωσης συχνότητας. Ο σύλλογος ασύρματου LAN συνιστά τη χρήση κρυπτογράφησης σε όλα τα δίκτυα, ακόμη και σε δίκτυα διαμόρφωσης συχνοτήτων.
Χρησιμοποιούμε ένα πρωτόκολλο που είναι γνωστό μόνο στον προμηθευτή και μερικούς άλλους ανθρώπους. Οι εισβολείς δεν καταλαβαίνουν τα μηνύματα SCADA.	Ακόμη και τα πρωτόκολλα που ανήκουν σε ορισμένους προμηθευτές είναι γενικότερα γνωστά από όσο θεωρούν οι περισσότεροι. Οι προμηθευτές, οι σύμβουλοι και οι υφιστάμενοι και πρώην υπάλληλοι μιας εταιρείας και άλλες εταιρείες που χρησιμοποιούν το ίδιο πρωτόκολλο SCADA γνωρίζουν όλες τις λεπτομέρειες. Τα εγχειρίδια και το λογισμικό για την ανάλυση των πρωτοκόλλων μπορούν να βρεθούν στο Διαδίκτυο.

3.4 Περιστατικά που αφορούν το SCADA στον τομέα του πόσιμου νερού και σε άλλους τομείς

Οι απειλές κατά της Αυτοματοποίησης Διαδικασιών μπορούν να αναλυθούν σε:

• Οργανωσιακές απειλές όπως η έλλειψη πολιτικής ασφάλειας, η έλλειψη προσοχής στην ευαισθητοποίηση σχετικά με την ασφάλεια, η ανεπαρκώς ρυθμισμένη πρόσβαση στα συστήματα, η πολιτική μη χρήσης κωδικού πρόσβασης κλπ.

• Φυσικές απειλές όπως εκρήξεις, πυρκαγιά ή βανδαλισμοί.

• Τεχνικές απειλές, όπως δυσλειτουργίες λογισμικού και υλικού, ιοί, επιθέσεις άρνησης εξυπηρέτησης κ.λπ.

Σε όλο τον κόσμο, τα περιστατικά που εμπλέκονται με το SCADA δεν δημοσιεύονται ποτέ και όταν δημοσιεύονται, αυτό συμβαίνει συχνά εκτός Ευρώπης. Οι ευρωπαϊκές εταιρείες προτιμούν να σιωπούν για τα περιστατικά ή να αναφέρουν μόνο μια «τεχνική δυσλειτουργία». Η ολλανδική έκθεση SCADA (Luiijf and R. Lassche,2006) περιέχει έναν κατάλογο δημοσιευμένων περιστατικών που αφορούν στα συστήματα SCADA σε ορισμένους τομείς. Οι εταιρείες πόσιμου νερού έχουν δημοσιεύσει μόνο λίγα περιστατικά σε διεθνές επίπεδο. Τουλάχιστον ένα περιστατικό ασφαλείας SCADA σημειώθηκε στην Ολλανδία.

Ακολουθούν μερικά παραδείγματα δημοσιευμένων συμβάντων στον τομέα του πόσιμου νερού:

• Χειρισμός εγκαταστάσεων επεξεργασίας πόσιμου ύδατος και επεξεργασίας λυμάτων, Αυστραλία

Το πιο συνηθισμένο παράδειγμα που χρησιμοποιήθηκε για να αποδειχθεί η ευπάθεια των συστημάτων και των δικτύων SCADA είναι εκείνο της μη εξουσιοδοτημένης πρόσβασης του πρώην εργολάβου της Vitek Boden στο σύστημα ελέγχου των εγκαταστάσεων επεξεργασίας πόσιμου ύδατος και επεξεργασίας λυμάτων της Hunter Watertech στο Maroochy Shire της Αυστραλίας.

Ο Boden ήταν ο μηχανικός του χώρου που εγκατέστησε συστήματα SCADA για την Hunter Watertech. Το σύστημα SCADA περιελάμβανε έναν τοπικό επεξεργαστή σε κάθε έναν από τους 300 σταθμούς άντλησης. Κάθε τοπικός επεξεργαστής επικοινωνούσε με το κεντρικό σύστημα υπολογιστή μέσω ραδιοζεύκτη. Ο Boden παραιτήθηκε από την εταιρεία του καθώς το έργο άρχισε να ολοκληρώνεται το 1999 έχοντας εργαστεί σε αυτό για δύο χρόνια και ζήτησε από την Hunter Watertech να εργαστεί σε αυτήν. Η εταιρεία αρνήθηκε να τον απασχολήσει και λίγο αργότερα, τα αντλιοστάσια για το σύστημα αποχέτευσης άρχισαν να δυσλειτουργούν και οι βαλβίδες στο σύστημα πόσιμου νερού άρχισαν να κλείνουν από μόνες τους.

Κατά τη διάρκεια αστυνομικού ελέγχου στις 23 Απριλίου 2000, η αστυνομία ανακάλυψε εξοπλισμό υπολογιστή και ραδιομετάδοσης στο αυτοκίνητο του Vitek Boden. Στη συνέχεια ο Boden παραδέχτηκε 46 περιπτώσεις εξ αποστάσεως χειρισμού των συστημάτων SCADA της Hunter Watertech.

Απενεργοποίησε τους συναγερμούς, παρενέβη στις επικοινωνίες, σταμάτησε τις αντλίες από την εκκίνηση την κατάλληλη στιγμή και ήταν υπεύθυνος για την υπερχείλιση και την απελευθέρωση ακατέργαστων λυμάτων. Εκτιμάται ότι από τον Ιανουάριο του 2000 έως τις 23 Απριλίου 2000 απελευθερώθηκαν στο περιβάλλον σχεδόν ένα εκατομμύριο λίτρα μη επεξεργασμένων λυμάτων (www.theregister.co.uk).

• Καταστροφή ενός συστήματος SCADA στο Tshwane, Νότια Αφρική

Στις 18 Αυγούστου 2006, βάνδαλοι κατέστρεψαν το σύστημα SCADA σε μία δεξαμενή στο Tshwane της Νότιας Αφρικής. Το αποτέλεσμα ήταν ότι οι πόλεις Mamelodi και Eersterust (Πραιτόρια) να μην έχουν πόσιμο νερό για έντεκα ημέρες.

• Χάκερ στο σύστημα διήθησης πόσιμου νερού στο Harrisburg της Pennsylvania των ΗΠΑ

Ένας χάκερ μπήκε στο σύστημα διήθησης πόσιμου νερού SCADA στο Harrisburg της Pennsylvani των ΗΠΑ. Το κατάφερε παίρνοντας τον έλεγχο εξ αποστάσεως του φορητού υπολογιστή ενός από τους υπαλλήλους της εταιρείας πόσιμου νερού, αφού εγκατέστησε κωδικό Trojan. Μόλις ο υπάλληλος συνδέθηκε από το σπίτι, ο χάκερ μπόρεσε να διεισδύσει στο δίκτυο SCADA μέσω του φορητού υπολογιστή χρησιμοποιώντας το Διαδίκτυο. Ο χάκερ έπειτα εγκατέστησε κακόβουλο λογισμικό (λογισμικό Trojan) και spyware στα συστήματα SCADA. Θεωρητικά, ο εισβολέας ήταν τότε σε θέση να ελέγξει το δίκτυο SCADA, να δώσει ψευδείς εντολές και να υπερφορτώσει εντελώς το δίκτυο (blogs.abcnews.com**).**

• Προβλήματα επικοινωνίας στο σύστημα διανομής πόσιμου νερού στο Fort Worth των ΗΠΑ

Στις 14 Ιανουαρίου 2007, τα προβλήματα επικοινωνίας με τα αποκεντρωμένα συστήματα SCADA προκάλεσαν οκτάωρη διακοπή μέρους της παροχής πόσιμου νερού στο Forth Worth. Ο έλεγχος όλων των αντλιών και των δεξαμενών αποβλήτων είχε χαθεί.

• Διείσδυση χάκερ σε ένα σύστημα πόσιμου νερού στις ΗΠΑ

Η American Water ISAC ανέφερε ότι το 2000, ένας χάκερ διείσδυσε στο σύστημα SCADA σε μια επιχείρηση πόσιμου νερού.

• **Ένα σφάλμα λογισμικού στο SCADA** ήταν υπεύθυνο για υπερβολικά χαμηλό επίπεδο χλωρίου, καθιστώντας το νερό μη πόσιμο στο Lewiston των ΗΠΑ (2003).

Δημοσιευμένα περιστατικά που αφορούν συστήματα SCADA σε άλλους τομείς αποτελούν παραδείγματα ανασφαλών πτυχών του SCADA που αναφέρθηκαν προηγουμένως στην παράγραφο 2.3:

• Αδύνατα και συχνά μη ασφαλή πρωτόκολλα SCADA που οδηγούν σε αποτυχία του συστήματος.

• Αδύναμοι ή μη ασφαλείς σύνδεσμοι επικοινωνίας μεταξύ των δικτύων των επιχειρήσεων και του εξωτερικού κόσμου που επιτρέπουν στους χάκερ και τους ιούς να εισχωρήσουν.

• Οι προμηθευτές συντήρησης που μπορούν να αποφύγουν τα μέτρα ασφαλείας λόγω έλλειψης εποπτείας του εξοπλισμού που μπορεί να συνδεθεί (ακόμα και σε πυρηνικό σταθμό παραγωγής ενέργειας).

• Έλλειψη διαχείρισης αλλαγών.

• Έλλειψη φυσικής προστασίας και ασφάλειας των συστημάτων και δικτύων SCADA.

Η εκτέλεση δοκιμών διείσδυσης μπορεί να φέρει μερικές φορές εκπληκτικά αποτελέσματα. Ωστόσο, η διενέργεια δοκιμών διείσδυσης στους κρίσιμους

στόχους δεν πρέπει να φέρει εκπληκτικά αποτελέσματα. Ο Scott Lunsford προσφέρθηκε να διεισδύσει σε πυρηνικό σταθμό παραγωγής ενέργειας, καθώς ο ιδιοκτήτης της μονάδας ισχυριζόταν πως δεν ήταν δυνατή η πρόσβαση σε κρίσιμα εξαρτήματα από το Διαδίκτυο. «Αποδείχθηκε ότι ήταν μια από τις πιο απλές δοκιμές διείσδυσης που είχα κάνει ποτέ», είπε ο Lunsford. Πρόσθεσε: «Από την πρώτη μέρα είχαμε διεισδύσει στο δίκτυο. Μέσα σε μια εβδομάδα ελέγχαμε (το σύστημα SCADA) ενός πυρηνικού σταθμού ηλεκτροπαραγωγής».

3.5 Ανάγκη ασφάλειας SCADA στον τομέα του πόσιμου νερού

Η αποτελεσματική ασφάλεια του περιβάλλοντος SCADA, των συστημάτων και των δικτύων στον τομέα του πόσιμου νερού είναι απαραίτητη για να εξασφαλιστεί η παροχή και η ποιότητα του πόσιμου νερού και να διασφαλιστεί ότι τα συστήματα SCADA δεν μπορούν να τα χειριστούν μη εξουσιοδοτημένα μέρη. Τα προβλήματα χάκερ, ιών και η απώλεια επικοινωνίας μεταξύ των εξαρτημάτων του δικτύου SCADA που αναφέρθηκαν παραπάνω μπορούν να συμβούν και στον τομέα πόσιμου νερού στην Ολλανδία και αλλού.

Οι πιθανές κοινωνικές επιπτώσεις από τη διακοπή της παροχής νερού είναι σοβαρές.

Οι πιθανές συνέπειες θα μπορούσαν να είναι κοινωνικές αναταραχές, επιπτώσεις στη δημόσια υγεία και μεγάλες οικονομικές ζημίες. Συνεπώς, οι εταιρείες υποδομών ζωτικής σημασίας στην παροχή πόσιμου νερού πρέπει να ελέγχουν τον κίνδυνο στα συστήματα SCADA τους ως μέρος του συνολικού κινδύνου της εταιρείας.

Συνοψίζοντας, μπορούμε να συμπεράνουμε ότι είναι ουσιαστικής σημασίας η αποτελεσματική ασφάλεια των συστημάτων και δικτύων SCADA στον τομέα του πόσιμου νερού. Η ασφάλεια αυτή απαιτεί μια προσέγγιση στην οποία θα δοθεί ίση προσοχή στις οργανωτικές, φυσικές και τεχνικές πτυχές της ασφάλειας των πληροφοριών. Οι ακόλουθες Καλές Πρακτικές για την ασφάλεια του συστήματος SCADA στον τομέα του πόσιμου νερού παρέχουν κατευθυντήριες γραμμές για την ομάδα διαχείρισης και τη διαχείριση αυτοματοποίησης τεχνικών διαδικασιών.

Κεφάλαιο 4^{Ο}: Επανεξέταση και αναθεώρηση σε βιομηχανική εγκατάσταση

4.1 Βασικό υπόβαθρο για την αξιολόγηση του κινδύνου και του βιώσιμου μοντέλου

Κάθε επιχείρηση είναι εκτεθειμένη σε διάφορες μορφές κινδύνων και προϋπόθεση για την αναγνώρισή τους είναι η βαθιά γνώση των λειτουργιών και της μορφής της επιχείρησης, της αγοράς, του νομικού, κοινωνικοπολιτικού και πολιτισμικού περιβάλλοντος που δραστηριοποιείται, αλλά και των στρατηγικών και λειτουργικών στόχων και της λειτουργίας υλοποίησής τους.

Για να υπάρξει μια μεθοδική προσέγγιση στην αναγνώριση του κινδύνου θα πρέπει να προσδιορίζονται και κατηγοριοποιούνται όλες οι δραστηριότητες μιας επιχείρησης καθώς και οι κίνδυνοι που απορρέουν από αυτές.

Οι βασικότερες δραστηριότητες μιας επιχείρησης μπορεί να είναι στρατηγικές, λειτουργικές, χρηματοοικονομικές, σχετικές με την γνώση τεχνολογιών, πνευματικής ιδιοκτησίας, κλπ και συμμόρφωσης (Sandberg, et al., 2015).

Η αναγνώριση των κινδύνων μπορεί να βασίζεται σε τεχνικές όπως η ανταλλαγή ιδεών, ερωτηματολόγια, επιχειρησιακές μελέτες, ανάλυση σεναρίων, μελέτες κινδύνου και λειτουργικότητας, κλπ. Έπειτα από την διαδικασία αναγνώρισης των κινδύνων, σκόπιμο είναι να υπάρξει η απεικόνισή τους, πχ με την χρήση πινάκων, ώστε να είναι πιο εύκολη η περιγραφή και αποτίμησή τους.

Η αποτύπωση θα πρέπει να δομημένη και περιεκτική, ιεραρχώντας τις πιθανές συνέπειες και τις πιθανότητες πραγματοποίησής τους, εστιάζοντας στους βασικότερους.

Οι κίνδυνοι είναι δυνατό να εκτιμηθούν ποσοτικά, ποιοτικά ή και εν μέρει ποσοτικά και ποιοτικά, αναφορικά με την πιθανότητα εμφάνισής τους και τις πιθανές συνέπειές τους. Η ανάλυση των κινδύνων μπορεί να στηρίζεται σε διάφορες τεχνικές και μεθόδους και να στηρίζεται στις πιθανές ευκαιρίες, απειλές ή στον συνδυασμό και των δύο. Κάποιες από τις εφαρμοζόμενες τεχνικές και μεθόδους ανάλυσης είναι (Kriaaet al., 2015):

- η έρευνα αγοράς
- η έρευνα και ανάπτυξη

- η ανάλυση SWOT (δυνάμεις – αδυναμίες – ευκαιρίες – απειλές)
- η λήψη αποφάσεων υπό συνθήκες κινδύνου και αβεβαιότητας
- η εξαγωγή στατιστικών συμπερασμάτων
- η ανάλυση BPEST (ανάλυση επιχειρησιακού, πολιτικού, οικονομικού, κοινωνικού και τεχνολογικού περιβάλλοντος)
- η δεντρική ανάλυση σφαλμάτων

Τέλος έπειτα από την διαδικασία ανάλυσης των κινδύνων, σκόπιμο είναι οι κίνδυνοι που έχουν αναγνωριστεί να συγκρίνονται με τα κριτήρια κινδύνου που έχουν τεθεί από την επιχείρηση, σχετικά με τα κόστη και τις ωφέλειες, τις νομικές απαιτήσεις, πιθανές ανησυχίες των μετόχων , κλπ. Κατά συνέπεια η αξιολόγηση των κινδύνων και η λήψη αποφάσεων θα πρέπει να λαμβάνει υπόψη την σημαντικότητα αυτών για την επιχείρηση.

4.2 Η διαδικασία αξιολόγησης των κινδύνων

Η αναγνώριση και η αξιολόγηση των κινδύνων θα πρέπει να κοινοποιείται τόσο εντός όσο και εκτός της επιχείρησης.

Η εντός της επιχείρησης κοινοποίηση αναφέρεται στις εσωτερικές αναφορές ως προς τα διάφορα επίπεδα και διαφοροποιείται ανάλογα με τις απαιτούμενες πληροφορίες για την διαχείριση τους κατά περίπτωση.

Έτσι διαφορετική πληροφόρηση υπάρχει στις αναφορές προς την διοίκηση, τα διάφορα επιχειρηματικά τμήματα, τα μεμονωμένα άτομα. Η περιεκτικότητα και η ανάλυση κάθε αναφοράς είναι διαφορετική ανάλογα τον αποδέκτη και εστιάζει σε διαφορετικούς τομείς.

Η διοίκηση οφείλει να έχει μια πλήρη εικόνα των κινδύνων που είναι εκτεθειμένη η επιχείρηση, της αξιολόγησή τους και του τρόπου διαχείρισης, τα τμήματα της επιχείρησης ότι εμπίπτει στην δική τους δραστηριότητα, ενώ τα μεμονωμένα άτομα θα πρέπει να γνωρίζουν τον τρόπο δράσης και επικοινωνίας.

Οι εξωτερικές αναφορές προορίζονται προς τους μετόχους και οφείλουν να περιγράφουν τις υιοθετούμενες πολιτικές διαχείρισης των κινδύνων και την αποτελεσματικότητά τους σχετικά με την επίτευξη των στόχων.

Η καλή εταιρική διακυβέρνηση περιλαμβάνει εφαρμογή κατάλληλων

ρυθμίσεων που να προστατεύουν τα συμφέροντα των μετόχων, να διασφαλίζουν την τέλεση των καθηκόντων της διοίκηση με τρόπο που προσδίδει αξία στην επιχείρηση και να διασφαλίζουν την αποτελεσματικότητα των ελέγχων (Bodungen, et al., 2017).

4.3 Το βιώσιμο μοντέλο του συστήματος

4.3.1 Προτεινόμενο μοντέλο

Σε αυτήν την ενότητα παρέχουμε την περιγραφή του προτεινόμενου μοντέλου μας και των συστατικών του. Παρουσιάζεται και μία ανάλυση του μοντέλου βιώσιμου συστήματος (VSM) και του τρόπου που αξιοποιούμε τις δυνατότητές του για τους σκοπούς της εκτίμησης των κινδύνων στα βιομηχανικά συστήματα ελέγχου (ICS).

Τέλος, παρέχεται μία σύγκριση μεταξύ του μοντέλου μας και των αποτελεσμάτων που έχουμε σχηματίσει από περιπτώσεις μελετών διαχείρισης κινδύνου, όπου χρησιμοποιήθηκε η μέθοδος CRAMM (CCTA Risk Analysis and Management Method) (Bodungen, et al., 2017).

4.4 Περιγραφή μοντέλου

Η προσέγγισή μας στην εκτίμηση των κινδύνων κυβερνασφάλειας για τα ICS βασίζεται στο VSM. Πιο συγκεκριμένα, έχουμε χρησιμοποιήσει το VSM προκειμένου να μοντελοποιήσουμε τα περιουσιακά στοιχεία του συστήματος και των σχέσεων που δημιουργούνται μεταξύ των εν λόγω περιουσιακών στοιχείων και του εσωτερικού και εξωτερικού περιβάλλοντος αντίστοιχα.

Λαμβάνοντας υπόψη αυτές τις σχέσεις ως μέρος της «ομάδας των περιουσιακών στοιχείων», εντοπίζουμε τις απειλές εναντίον τους και εξετάζουμε τα τρωτά σημεία του συστήματος που μπορούν να αξιοποιηθούν από τις προσδιορισμένες απειλές.

Ωστόσο, δεδομένου ότι το μοντέλο χρησιμοποιήθηκε αρχικά για την μοντελοποίηση της βιωσιμότητας του συστήματος, ο προσδιορισμός των απειλών κατά της ασφάλειας των συστατικών του συστήματος και τις σχέσεις τους, παραπέμπει στον εντοπισμό των απειλών κατά της βιωσιμότητας του συστήματος (Sajid, et al., 2016).

Ως εκ τούτου, προκειμένου να εντοπιστούν οι απειλές εναντίον του οργανισμού, μπορούμε να προσδιορίσουμε τις πιθανές επιθέσεις κατά της βιωσιμότητας του συστήματος.

Με αυτόν τον τρόπο, σε κάθε ένα από τα έξι συστήματα του VSM εντοπίζουμε τις απειλές που μπορούν να:

- καταστήσουν το σύστημα μη διαθέσιμο για τα υπόλοιπα συστήματα διαταράσσοντας την σύνδεση μεταξύ τους (επίθεση Denial of Service)

- φθείρουν την σύνδεση του συστήματος με τα υπόλοιπα συστήματα στέλνοντας ψευδή στοιχεία σε αυτά (επίθεση man-in-the-middle),

- καταστήσουν το σύστημα μη διαθέσιμο στο εξωτερικό περιβάλλον του (επίθεση Denial of Service),

- φθείρουν την σύνδεση του συστήματος με το εξωτερικό του περιβάλλον του (επίθεση man-in-the-middle),

- γνωστοποιήσουν ή να καταστρέψουν δεδομένα που μεταφέρονται από/προς το σύστημα προς/από το εξωτερικό περιβάλλον ή σε άλλο σύστημα στο εσωτερικό του οργανισμού (κλοπή δεδομένων, παραποίηση των δεδομένων),

- γνωστοποιήσουν ή να καταστρέψουν δεδομένα που βρίσκονται εντός του συστήματος (κλοπή δεδομένων, παραποίηση των δεδομένων),

- καταστήσουν τα υποσυστήματά του ή το υπερσύστημά του μη διαθέσιμα,

- φθείρουν την σύνδεση με τα υποσυστήματά του ή το υπερσύστημά του,

- τροποποιήσουν ή να γνωστοποιήσουν τα δεδομένα που μεταφέρονται στα υποσυστήματά του ή το υπερσύστημά του.

Στην συνέχεια διερευνούνται τα τρωτά σημεία που μπορούν να αξιοποιηθούν από τις απειλές που εντοπίστηκαν στο προηγούμενο βήμα.

Το πρώτο βήμα της προτεινόμενης διαδικασίας περιλαμβάνει όχι μόνο την κατασκευή του VSM του ανώτερου επιπέδου του οργανισμού, αλλά επίσης επαναλαμβάνεται για κάθε υποσύστημα του αρχικού συστήματος μέχρι το χαμηλότερο επίπεδο του οργανισμού όπου οι εργασίες εκτελούνται από το υλικό υπολογιστών. Με αυτόν τον τρόπο, λαμβάνονται υπόψη όλες οι πιθανές απαιτήσεις και οι αλληλεπιδράσεις.

Σε αυτό το σημείο είναι σημαντικό να σημειωθεί ότι προκειμένου να εντοπιστούν όλα τα περιουσιακά στοιχεία και να χαρτογραφηθούν στο VSM ως λειτουργικά συστήματα ή συστήματα διαχείρισης, θα πρέπει να μεταφερθεί η γνώση από ανθρώπους εντός του ICS. (Demertzis, et al., 2017)

Οι εργαζόμενοι στα υψηλότερα επίπεδα της διαχείρισης του ICS μαζί με τους μηχανικούς από τα χαμηλότερα επίπεδα λειτουργίας θα πρέπει να έλθουν σε επαφή.

Κατασκευή του VSM

Εντοπισμός των απειλών στην βιωσιμότητα

Εντοπισμός των τρωτών σημείων της βιωσιμότητας

Ανάλυση ελέγχου

Σύσταση ελέγχου

Προσδιορισμός των κινδύνων

Ανάλυση των επιπτώσεων

Προσδιορισμός πιθανότητας

4.5 Ανάλυση μοντέλου

Σε γενικές γραμμές, η προτεινόμενη διαδικασία εκτίμησης κινδύνου του VSM ξεκινά με την κατασκευή του VSM των άνω οργανωτικών επιπέδων. Ένα γενικό μοντέλο VSM που περιλαμβάνει τις πιο κοινές λειτουργίες ανωτέρου επιπέδου που μπορούν να βρεθούν σε ένα ICS, όπως τα τμήματα Οικονομικών, Πωλήσεων και Μάρκετινγκ, Παραγωγής, Νομικών Υπηρεσιών, IT, Ανθρώπινων Σχέσεων κλπ..

Όλα τα τμήματα του Συστήματος 1 συντονίζονται μέσω τακτικών συναντήσεων μεταξύ των διευθυντών των δραστηριοτήτων, μία δράση που αποτελεί το Σύστημα 2 και η οποία διοργανώνεται από τον εκτελεστικό διευθυντή (Σύστημα 3). Η Κατεύθυνση του Ποιοτικού Ελέγχου σχηματίζει το Σύστημα 3*, το οποίο είναι υπεύθυνο για τις δραστηριότητες παρακολούθησης και ελέγχου για τα διάφορα τμήματα.

Το Σύστημα 4 και το Σύστημα 5 ορίζονται ως η Κατεύθυνση του Μάρκετινγκ και Μελλοντικού Προγραμματισμού και του Διοικητικού Συμβουλίου αντίστοιχα. Με μια πρώτη ματιά, το VSM σε αυτό το επίπεδο δεν έχει τίποτα να προσφέρει στην εκτίμηση των κινδύνων κυβερνασφάλειας.

Ωστόσο, η έλλειψη ενός συστήματος (για παράδειγμα το Σύστημα 3*) μπορεί να οδηγήσει σε σημαντικές επιπτώσεις στα υποσυστήματα των διαφόρων τμημάτων του Συστήματος 1, ή μία λιγότερο αποτελεσματική Κατεύθυνση Μελλοντικού Προγραμματισμού μπορεί να οδηγήσει σε απώλεια κρίσιμων ειδήσεων σε επίπεδο ασφαλείας. Ως εκ τούτου, ακόμη και σε αυτό το επίπεδο, μπορούν να προσδιοριστούν ορισμένες απειλές κατά της κυβερνασφάλειας του ICS που απορρέουν από την κακή οργάνωση του ICS.

Στο πλαίσιο του VSM, η βιωσιμότητα του όλου συστήματος είναι άρρηκτα συνδεδεμένη με την βιωσιμότητα των υποσυστημάτων του και ως εκ τούτου, κάθε μονάδα θα πρέπει να λειτουργεί ως καθεαυτό VSM. Εφαρμόζοντας

επαναληπτικά το VSM σε κάθε τμήμα του ICS και αναζητώντας βαθύτερα μέσα στα χαμηλότερα επίπεδα μπορούν να αποκαλυφθούν πολύ περισσότερες απειλές κατά της κυβερνασφάλειας.

Μετά την επαναληπτική εφαρμογή του VSM βρισκόμαστε σε επίπεδο συστήματος SCADA. Σε αυτό το επίπεδο όλες οι δράσεις αποτελούνται από στοιχεία υλικού υπολογιστών, γνωστά ως συσκευές πεδίου. Σε αυτό το επίπεδο ο αντίκτυπος μιας επιτυχημένης κυβερνοεπίθεσης είναι πολύ υψηλότερος, δεδομένου ότι μπορεί να επηρεάσει άμεσα την λειτουργία ολόκληρου του ICS.

Το VSM μας βοηθά να προσδιορίσουμε όλες τις αλληλεπιδράσεις μεταξύ των διαφόρων συσκευών πεδίου και του ελέγχου /του εξοπλισμού διαχείρισης /του τμήματος. Επιπλέον, μπορούν επίσης να ταυτοποιηθούν οι διασυνδέσεις με το εξωτερικό περιβάλλον.

Για παράδειγμα οι κυβερνοαπειλές μπορεί να προέρχονται από το εσωτερικό, πιθανόν από άτομα τα οποία μεταφέρουν υλικό που έχει εκτεθεί σε κίνδυνο, σκόπιμα ή μη, όπως ένα USB flash ή μία κινητή συσκευή που έχει προσβληθεί από κάποιο ιό (Drias, et al., 2015)

Κεφάλαιο 5^{Ο}: Καλές πρακτικές ασφαλείας SCADA

Για να βρεθούν αποτελεσματικές λύσεις για τον μετριασμό των πτυχών κινδύνου SCADA, στη συνέχεια αναφέρονται μία σειρά από καλές πρακτικές ασφαλείας SCADA. Οι καλές πρακτικές δεν είναι ούτε νομοθετικά μέτρα ούτε απαιτήσεις.

Για λόγους όπως η εσωτερική κουλτούρα ή οργανωτικού, αρχιτεκτονικού ή τεχνικού χαρακτήρα, οι εταιρείες ύδρευσης μπορούν να επιλέξουν ένα εντελώς διαφορετικό σύστημα ασφάλειας που παρέχει το ίδιο επίπεδο εγγύησης. Εντούτοις, είναι καλή ιδέα να αξιολογηθεί κάθε εναλλακτική δέσμη μέτρων ασφαλείας υπό το πρίσμα των Καλών Πρακτικών που περιγράφονται παρακάτω, προκειμένου να διασφαλιστεί ότι θα «κλείσουν» όλα τα κενά ασφαλείας.

Οι Καλές Πρακτικές χωρίζονται σε δύο ομάδες. Η πρώτη ομάδα περιλαμβάνει τις καλές πρακτικές σε επίπεδο διοίκησης επιχειρήσεων.

Οι καλές πρακτικές στον τομέα του πόσιμου νερού σε επίπεδο εταιρικής διαχείρισης αποτελούν επέκταση της γενικής πολιτικής της ασφάλειας των πληροφοριών που υπάρχει ήδη στον τομέα του πόσιμου νερού και είναι προσανατολισμένες στην γενική εταιρική κουλτούρα διαχείρισης κινδύνων. Οι καλές πρακτικές έχουν συγκεντρωθεί στα ακόλουθα κύρια θέματα:

• Πολιτική ασφαλείας της εταιρείας και συγκεκριμένη πολιτική ασφαλείας SCADA.

• Διαχείριση κινδύνου.

• Έλεγχος.

• Πολιτική αγορών για συστήματα, δίκτυα και υπηρεσίες SCADA.

5.1 Πολιτική εταιρικής ασφάλειας και ειδική πολιτική ασφάλειας SCADA

Η σωστή εφαρμογή της ασφάλειας των πληροφοριών για τα συστήματα και τα δίκτυα SCADA απαιτεί ένα περιβάλλον στο οποίο η διοίκηση δίνει προσοχή στην ασφάλεια. Αυτό συνεπάγεται ότι η πολιτική ασφάλειας θα είναι

ενσωματωμένη στη διαδικασία λειτουργίας με βάση τη σχετική ανάλυση κινδύνου και τη διαδικασία διαχείρισης κινδύνου που ισχύει για ολόκληρη την εταιρεία ύδρευσης.

Καλή πρακτική 1

Η εταιρεία ύδρευσης έχει μια γενική πολιτική ασφάλειας των πληροφοριών και μια συγκεκριμένη πολιτική ασφάλειας SCADA που είναι άρρηκτα συνδεδεμένη με αυτή τη γενική πολιτική ασφάλειας των πληροφοριών.

Καλή πρακτική 2

Η γενική πολιτική ασφάλειας των πληροφοριών βασίζεται στον Κώδικα Πρακτικής για την Ασφάλεια των Πληροφοριών[1] και στο σχετικό σύστημα διαχείρισης της ασφάλειας [2]

Καλή πρακτική 3

Η βασική προϋπόθεση για την συγκεκριμένη πολιτική ασφάλειας του SCADA είναι ότι μπορεί να υλοποιηθεί με τέτοιον τρόπο ώστε τα μέτρα που λαμβάνονται να αποτελέσουν για τους εργαζόμενους μία λογική επέκταση της γενικής (πληροφοριών) πολιτικής ασφαλείας και της ασφάλειας του περιβάλλοντος γραφείου.

Καλή πρακτική 4

Η συγκεκριμένη πολιτική ασφάλειας SCADA πρέπει να περιλαμβάνει τη φυσική προστασία των συστημάτων και δικτύων SCADA.

Καλή πρακτική 5

Για το περιβάλλον SCADA, καθορίζονται οι αρμοδιότητες ασφαλείας, τα καθήκοντα και οι αρχές για το διευθυντικό προσωπικό και τους χρήστες του SCADA (βλέπε επίσης [3]σημείο 12).

---

[1] ISO, Code voor Informatiebeveiliging/*Information technology - Security techniques - Code of practice for information security management framework*, ISO/IEC 17799:2005 Note: is soon to be renumbered to ISO/IEC 27002; the Dutch version was published as NEN-ISO/IEC 17799:2005.

[2] ISO, Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27001:2005.

[3] Department of Energy, *21 Steps to Improve Cyber Security of SCADA Networks*, Office of Energy Assurance, Office of Independent Oversight And Performance

Υπόβαθρο

• Η έλλειψη ειδικής προς το SCADA πολιτικής ασφαλείας, διαδικασιών ασφαλείας και κουλτούρας ασφαλείας ξεπερνά τα αμερικάνικα κορυφαία 10 τρωτά σημεία του SCADA (NERC, 2007)

• Η έλλειψη πολιτικής για την ασφάλεια των πληροφοριών και η έλλειψη ανάλυσης κινδύνου οδηγεί στην ad hoc εφαρμογή των μέτρων ασφαλείας, επομένως δεν είναι ποτέ σαφές εάν έχουν ληφθεί τα σωστά μέτρα ασφαλείας και ποια κενά υπάρχουν στην ασφάλεια.

• Η πολιτική ασφαλείας των πληροφοριών που βασίζεται στον Κώδικα Πρακτικής για την Ασφάλεια των Πληροφοριών περιλαμβάνει έναν αριθμό ελέγχων που δεν είναι άμεσα κατάλληλοι για το περιβάλλον SCADA 24 ώρες την ημέρα/7 ημέρες την εβδομάδα. Ορισμένα από τα στοιχεία ελέγχου που περιλαμβάνονται στον Κώδικα Πρακτικής απαιτούν κάποιο βαθμό συμπλήρωσης. Τα βασικά στοιχεία είναι: η εξωτερική ανάθεση, ο συντονισμός της ασφάλειας των πληροφοριών και των διαδικασιών, η φυσική ασφάλεια του περιβάλλοντος ΤΠΕ (π.χ. το περιβάλλον SCADA), οι επιχειρησιακές διαδικασίες σε λειτουργικό περιβάλλον24 ώρες την ημέρα/7 ημέρες την εβδομάδα, η πολιτική κατά των ιών, η καταγραφή και οι συναγερμοί, έλεγχοι πρόσβασης, πολιτική για τους κωδικούς πρόσβασης και η διαχείριση της συνέχειας των επιχειρήσεων. Αυτός είναι ο λόγος για τον οποίο συνιστάται η ανάπτυξη ξεχωριστής συμπληρωματικής πολιτικής ασφαλείας για το SCADA. Είναι επίσης λογικό να υπάρχει σαφής γραμμή για την αναφορά οποιωνδήποτε συμβάντων ασφαλείας που ενδέχεται να προκύψουν (βλ. επίσης τον Κώδικα Πρακτικής για την Ασφάλεια Πληροφοριών

• Τα στοιχεία που περιέχονται στο τρέχον, τακτικά ενημερωμένο έγγραφο πολιτικής ασφαλείας του SCADA είναι οι στόχοι για την ασφάλεια, η οργάνωση της ασφάλειας, οι κανόνες και οι διαδικασίες που απορρέουν σαφώς και κατανοητά από τους επιχειρηματικούς στόχους της εταιρείας ύδρευσης (εγγυημένη προσφορά και ποιότητα πόσιμου νερού). Ποιοι είναι οι ρόλοι και οι ευθύνες των συγκεκριμένων θέσεων και των λοιπών υπαλλήλων

Assurance, U.S. Department of Energy, USA, 2005.
On-line: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

που συμμετέχουν ή εργάζονται με την PA; Τι απαγορεύεται ρητά και τι αναμένεται από τον υπάλληλο ή τον υπάλληλο της διοίκησης όταν εντοπίζεται ένα (ενδεχόμενο) περιστατικό ασφαλείας;

5.2 Διαχείριση κινδύνων

Καλή πρακτική 6

Το περιβάλλον αυτοματοποίησης διαδικασιών/SCADA αποτελεί αναπόσπαστο μέρος της διαδικασίας διαχείρισης κινδύνων στο υψηλότερο εταιρικό επίπεδο.

Υπόβαθρο: Το περιβάλλον αυτοματοποίησης διαδικασιών/SCADA αποτελεί ουσιαστικό μέρος της διαδικασίας λειτουργίας πόσιμου νερού που εγγυάται την παροχή και την ποιότητα πόσιμου νερού. Η ασφάλεια σε όλους τους τομείς (διαθεσιμότητα, αξιοπιστία, ακεραιότητα, εμπιστευτικότητα) των συστημάτων και δικτύων SCADA, η ανάλυση κινδύνων, η διαχείριση κινδύνων και ο σχετικός σχεδιασμός συνέχειας της επιχείρησης είναι όλα προσανατολισμένα σε αυτό.

5.3 Ευαισθητοποίηση για την ασφάλεια

Ένας από τους κύριους παράγοντες κινδύνου που απαιτεί εσωτερικό έλεγχο είναι το ανθρώπινο στοιχείο. Αυτό αποτελεί σημαντικό παράγοντα κινδύνου και στο περιβάλλον SCADA. Η ευαισθητοποίηση σχετικά με την ασφάλεια βοηθά τη διοίκηση (υποδειγματική λειτουργία) και τους υπαλλήλους να παραμείνουν εστιασμένοι στην ασφάλεια και να συμβάλλουν στη βελτίωση του επιπέδου ασφάλειας του οργανισμού.

Καλή πρακτική 7

Η εταιρεία ύδρευσης διαθέτει ένα πρόγραμμα συνεχούς ενημέρωσης για την ασφάλεια.

Υπόβαθρο: Η αποτελεσματική ασφάλεια των πληροφοριών απαιτεί συνεχή προσοχή στην ευαισθητοποίηση της ασφάλειας και στη στάση των εργαζομένων απέναντι στην ασφάλεια, ιδιαίτερα όταν πρόκειται για κρίσιμες λειτουργικές διαδικασίες. Εάν οι υπάλληλοι της εταιρίας ύδρευσης δεν γνωρίζουν την ασφάλεια, αυτό θα γίνει αισθητό από τρίτους (προμηθευτές, τεχνικούς συντήρησης και επισκευής) που πρέπει να εργαστούν στα συστήματα και τα δίκτυα SCADA, επιδεινώνοντας τον πιθανό κίνδυνο σκόπιμης ή ασυνείδητης επιρροής στα συστήματα SCADA εξ ου και η διαδικασία πόσιμου νερού με μη εξουσιοδοτημένο τρόπο (Department of Energy, 2005)

5.4 Έλεγχος

Καλή Πρακτική 8

Ένας έλεγχος EDP των συστημάτων και δικτύων SCADA πραγματοποιείται τουλάχιστον μία φορά το χρόνο.

Υπόβαθρο: Στην ενότητα 393 του τμήματος 2 του ολλανδικού αστικού κώδικα αναφέρονται τα εξής σχετικά με τους ετήσιους λογαριασμούς: «*Ο λογιστής υποβάλλει στο εποπτικό συμβούλιο και στο διοικητικό συμβούλιο έκθεση σχετικά με τον έλεγχό του. Αυτή θα περιλαμβάνει ελάχιστα μία καταγραφή των πορισμάτων του όσον αφορά στην αξιοπιστία και τη συνέχεια της αυτοματοποιημένης επεξεργασίας δεδομένων*». Αυτή η ενότητα του νόμου αποτελεί μέρος του Νόμου Ι για την Ηλεκτρονική Εγκληματικότητα. Ο λόγος για την ανάθεση αυτού του πρόσθετου έργου σε λογιστή έχει ως εξής: στην περίπτωση ηλεκτρονικής πειρατείας, κυβερνοτρομοκρατίας ή οποιασδήποτε άλλης μορφής ηλεκτρονικής εγκληματικότητας, ένας συλληφθείς και διωκόμενος δράστης ο οποίος παρουσιάζεται ενώπιον δικαστηρίου μπορεί να διατυπώσει μία υπεράσπιση ότι δεν γνώριζε ότι παραβίαζε, ότι δεν υπήρχε καμία μορφή ασφάλειας και ότι είχε πρόσβαση σε ένα σύστημα ή δίκτυο χωρίς κανένα πρόβλημα κ.λπ. Ο δικηγόρος του δράστη μπορεί να ζητήσει από την εταιρεία ύδρευσης να αποδείξει ότι υπάρχει επαρκές επίπεδο ασφάλειας.

Σύμφωνα με τον Αστικό Κώδικα, η έκθεση του ελεγκτή που εκδίδεται ως μέρος των ετήσιων λογαριασμών - εάν υπάρχει και στην προκειμένη περίπτωση, που καλύπτει αποδεδειγμένα τα συστήματα και τα δίκτυα SCADA - αρκεί για να αποδείξει ότι ικανοποιούνται οι κανονιστικές απαιτήσεις «κάποιου βαθμού ασφαλείας» και ότι ο ύποπτος διείσδυσε εν γνώσει του. Συνεπώς, δεν είναι απαραίτητο να υποβληθούν λεπτομερείς πληροφορίες σχετικά με τα ληφθέντα μέτρα ασφαλείας. Ο κίνδυνος να μην έχει εκδοθεί έκθεση ελεγκτή ως μέρος των ετήσιων λογαριασμών που περιλαμβάνουν ρητά τα δίκτυα SCADA είναι συνεπώς ότι η δίωξη του ή των δραστών είναι πολύ δυσκολότερη, καθώς και ο κίνδυνος δημοσιοποίησης ευαίσθητων μέτρων ασφαλείας.

Ο έλεγχος θα εξετάσει, τουλάχιστον, τα ακόλουθα:

• Την πολιτική για την πρόσβαση και τους κωδικούς πρόσβασης.

• Την ασφάλεια των συνδέσεων μεταξύ των συστημάτων SCADA και των δικτύων, αφενός και του αυτοματισμού γραφείου, των δημόσιων δικτύων και του Διαδικτύου, αφετέρου (*SCADA 20*06)

• Την κατάσταση ασφαλείας των τοποθεσιών που παρακολουθούνται και ελέγχονται από απόσταση (NERC, 2007)

• Τα πιθανά σημεία πρόσβασης μόντεμ.

• Τη μέθοδο αναφοράς περιστατικών ασφαλείας, καταγραφής ασφαλείας και παρακολούθησης.

• Τη φυσική και ηλεκτρονική προστασία των εξαρτημάτων και των δικτύων του συστήματος SCADA όπως κλειδαριές στις θήκες, συναγερμοί στις πόρτες και ούτω καθεξής.

Εκτός από τον επίσημο έλεγχο, είναι επίσης σκόπιμο να διενεργείται ένας έλεγχος εσωτερικής ασφάλειας αρκετές φορές το χρόνο, ο οποίος μπορεί να συγχρονιστεί με τις φάσεις του προγράμματος ευαισθητοποίησης για την ασφάλεια.

5.5 Πολιτική αγορών για συστήματα και υπηρεσίες SCADA

Η ασφάλεια των πληροφοριών ισχύει για ολόκληρο τον κύκλο ζωής του εξοπλισμού SCADA, του λογισμικού και των υπηρεσιών. Η απόκτηση είναι ένα σημαντικό βήμα όπου οι απαιτήσεις εσωτερικής ασφάλειας μπορούν να επιβληθούν στους προμηθευτές και σε τρίτους. Βοηθά επίσης ώστε να καθίσταται σαφές στους εξωτερικούς φορείς ότι η εταιρεία ύδρευσης αντιμετωπίζει την ασφάλεια με επαγγελματικό και σοβαρό τρόπο.

Καλή πρακτική 9

Οι συμβάσεις που συνάπτονται με προμηθευτές για (μεγάλα) συστήματα και δίκτυα SCADA περιλαμβάνουν ρήτρα συνέχισης με στόχο την εξασφάλιση της προσφοράς και της ποιότητας του πόσιμου νερού:

1 Ο προμηθευτής αναλαμβάνει την υποχρέωση να διατηρεί αρκετά αποθέματα διαθέσιμα για συμφωνημένο αριθμό ετών.

2 Ο προμηθευτής εγγυάται ότι σε περίπτωση καταστροφής, θα παράσχει υποστήριξη για την εξεύρεση λύσης.

3 Σε περίπτωση απώλειας του συστήματος SCADA ή/και του δικτύου για οποιονδήποτε λόγο, ο προμηθευτής θα προσφέρει συνεργασία κατά προτεραιότητα στην αντικατάσταση του συστήματος ή/και του δικτύου SCADA.

4 Ο προμηθευτής επιβεβαιώνει τις ενημερώσεις από τρίτους που παρέχουν τα βασικά στοιχεία του συστήματος (για παράδειγμα, το λειτουργικό σύστημα της Microsoft) σε σύντομο χρονικό διάστημα και τα καθιστά διαθέσιμα με αξιόπιστο και έμπιστο τρόπο.

Υπόβαθρο: Για να διασφαλιστεί ο εφοδιασμός και η ποιότητα του πόσιμου νερού, τα συστήματα SCADA που παρακολουθούν και ελέγχουν τις διαδικασίες κρίσιμου πόσιμου νερού θα πρέπει να λειτουργούν και πάλι το συντομότερο δυνατό μετά από μια συνήθη δυσλειτουργία ή καταστροφή.

Καλή πρακτική 10

Πριν από την απόκτηση, η εταιρεία ύδρευσης θέτει απαιτήσεις για την ασφάλεια των πληροφοριών, τις οποίες αναμένεται να ικανοποιούν τα συστήματα, τα δίκτυα και το λογισμικό SCADA.

Υπόβαθρο: Δεδομένου ότι ένα σύστημα και ένα δίκτυο SCADA εισάγονται συχνά ως ένα αναπόσπαστο έργο, είναι σημαντικό να αποφασιστεί εκ των προτέρων ποιες απαιτήσεις ασφαλείας πρέπει να πληροί το σύστημα που πρέπει να παραδοθεί. Στο περιέχεται μία σειρά αρχικών προτάσεων για τεχνικές απαιτήσεις. Θα πρέπει να δηλώνετε επίσης ότι, χωρίς τη ρητή άδεια, οι προμηθευτές δεν επιτρέπεται να ενημερώνουν τρίτους ότι έχουν προμηθεύσει συστήματα SCADA στην εταιρεία ύδρευσης (Gary Finco et al., 2006)

Καλή πρακτική 11

Οι συμβάσεις συντήρησης και υποστήριξης που έχουν υπογραφεί με τρίτους περιλαμβάνουν ρήτρα ασφαλείας. Αυτή θα ρυθμίζει τα εξής τουλάχιστον:

1 Συμμόρφωση από τους τεχνικούς συντήρησης και τεχνικής υποστήριξης με την επικρατούσα πολιτική ασφαλείας της εταιρείας για συστήματα και δίκτυα SCADA.

2 Συμβάσεις εξουσιοδότησης και πρόσβασης για τους τεχνικούς συντήρησης.

3 Εγγυήσεις σχετικά με την προστασία εμπιστευτικών πληροφοριών της εταιρείας (ISA, 2007)

4 Επίβλεψη από την εταιρεία ύδρευσης των εργασιών που εκτελούνται από τρίτους.

5 Διαγραφή (ελαττωματικών) φορέων πληροφοριών που φέρουν πιθανές ευαίσθητες για την εταιρεία πληροφορίες.

Υπόβαθρο: Η επικρατούσα πολιτική ασφαλείας των εταιρειών για τα συστήματα και τα δίκτυα SCADA ισχύει και για τους υπαλλήλους τρίτων. Η βασική προϋπόθεση είναι η περιορισμένη πρόσβαση στα συστήματα SCADA.

Τα τρίτα μέρη πρέπει τουλάχιστον να παρέχουν εγγυήσεις ότι οι εργαζόμενοί τους είναι αξιόπιστοι (π.χ. με ευθύνη τρίτων για όλες τις ενέργειες των υπαλλήλων τους, πιστοποιητικό καλής συμπεριφοράς κλπ.). Οι προϋποθέσεις υπό τις οποίες μπορεί να συνδεθεί το δίκτυο και το λογισμικό τρίτων μερών (συμπεριλαμβανομένων των φορητών υπολογιστών για τον τεχνικό συντήρησης, το μόντεμ) με τα συστήματα ή το δίκτυο SCADA έχουν συμφωνηθεί και καθοριστεί γραπτώς. Όλες οι εργασίες που εκτελούνται από τρίτους για τα συστήματα και τα στοιχεία του δικτύου στο περιβάλλον SCADA εποπτεύονται. Αυτό αποτρέπει τις σοβαρές βλάβες που θέτουν σε κίνδυνο την εγγυημένη παροχή πόσιμου νερού . Οι αποκλίσεις από τη διαδικασία επιτρέπονται μόνο με την άδεια του υπεύθυνου ασφαλείας της εταιρείας ύδρευσης.

Τα ελαττωματικά μέσα που είναι ενσωματωμένα σε συστήματα SCADA που πρέπει να αντικατασταθούν (σκληροί δίσκοι και μονάδες ROM για παράδειγμα) ενδέχεται να φέρουν ευαίσθητα δεδομένα της εταιρείας. Πρέπει να συμφωνηθεί ότι καμία τέτοια πληροφορία δεν θα φύγει από τις εγκαταστάσεις της εταιρείας ύδρευσης μέχρι να διασφαλιστεί ότι οι ευαίσθητες πληροφορίες έχουν διαγραφεί ή καταστραφεί σωστά.

Βιβλιογραφία

- Berge, Jonas, Fieldbuses for Process Control: Engineering, Operation, and Maintenance, Research Triangle Park, North Carolina: ISA, 2002

- Bodungen, C. E., Singer, B. L., Shbeeb, A., Hilt, S., & Wilhoit, K. (2017). *Hacking Exposed Industrial*

- Bodungen, C. E., Singer, B. L., Shbeeb, A., Hilt, S., & Wilhoit, K. (2017). *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions*. McGraw-Hill Education.

- Department of Energy, *21 Steps to Improve Cyber Security of SCADA Networks*, Office of Energy Assurance, Office of Independent Oversight And Performance Assurance, U.S. Department of Energy, USA, 2005. On-line: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

- Department of Energy, *21 Steps to Improve Cyber Security of SCADA Networks*, Office of Energy Assurance, Office of Independent Oversight And Performance Assurance, U.S. Department of Energy, USA, 2005. On-line: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

- Erickson, Kelvin, and John Hedrick, Plantwide Process Control, New York: John Wiley & Sons, Inc., 1999.

- Falco, Joe, et al., IT Security for Industrial Control Systems, NIST Internal Report (NISTIR) 6859, February 2002,http://www.nist.gov/customcf/get_pdf.cfm?pub_id=821684

- Fraser, Roy E., Process Measurement and Control: Introduction to Sensors, Communication, Adjustment, and Control, Upper Saddle River, New Jersey: Prentice-Hall, Inc., 2001

- Gary Finco et al., *Cyber Procurement Language for Control Systems,version 1.6*, INL Critical Infrastructure Protection/Resilience

Center, Idaho Falls, USA, June 2006

- H.A.M. Luiijf and R. Lassche, *SCADA (on)veiligheid: een rol voor de overheid?(SCADA (in)security: a role for the government)*, TNO-KEMA report, April 2006.

- H.A.M. Luiijf, *Analyse SCADA-veiligheid in de Nederlandse drinkwatersector (Analysis of SCADA security in the Dutch drinking water sector)*, TNO Report, TNO-DV 2007 C317, July 2007. Classification: NICC Confidential.

- ISO, Code voor Informatiebeveiliging/*Information technology - Security techniques - Code of practice for information security management framework*, ISO/IEC 17799:2005 Note: is soon to be renumbered to ISO/IEC 270 02; the Dutch version was published as NEN-ISO/IEC 17799:2005.

- ISO, Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27001:2005.

- Knapp, Eric, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid,SCADA, and Other Industrial Control Systems, Waltham, Massachusetts: Syngress, 2011

- Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability engineering & system safety*, *139*, 156-178.

- NERC, *Top 10 Vulnerabilities of Control Systems*, version 2007. On-line: http://www.us-cert.gov/control_systems/pdf/2007_Top_10_Formatted_12-07-06.pdf

- NERC, *Top 10 Vulnerabilities of Control Systems*, version 2007. On-line:http://www.uscert.gov/control_systems/pdf/2007_Top_10_Formatted_12-07-06.pdf

- Rinaldi, Steven, et al., "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," IEEE Control Systems Magazine, (December 2001), pp. 11-25, http://dx.doi.org/10.1109/37.969131

- Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, *4*, 1375-1384.

- Sandberg, H., Amin, S., & Johansson, K. H. (2015). Cyberphysical security in networked control systems: An introduction to the issue. *IEEE Control Systems Magazine*, *35*(1), 20-23.

- *SCADA Security and Terrorism: We're not crying wolf*. On-line: http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS quarterly, 503-522.

- Γιαννόπουλος Γ.Ν.,(2001), Προστασία Προσωπικών Δεδομένων και διανοσυριακή ροή πληροφοριών, Τόμος 11, Εκδόσεις Σάκουλας, σελ. 733

- ISO, Code voor Informatiebeveiliging/*Information technology - Security techniques - Code of practice for information security management framework*, ISO/IEC 17799:2005 Note: is soon to be renumbered to ISO/IEC 27002; the Dutch version was published as NEN-ISO/IEC 17799:2005.

- ISO, Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27001:2005.

- Department of Energy, *21 Steps to Improve Cyber Security of SCADA Networks*, Office of Energy Assurance, Office of Independent Oversight And Performance Assurance, U.S. Department of Energy, USA, 2005.

- On-line: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

- Drias, Z., Serhrouchni, A., & Vogel, O. (2015, August). Analysis of cyber security for industrial control systems. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)* (pp. 1-8). IEEE.

- Demertzis, K., Iliadis, L., & Spartalis, S. (2017, August). A spiking one-class anomaly detection framework for cyber-security on industrial control systems. In *International Conference on Engineering Applications of Neural Networks* (pp. 122-134). Springer, Cham.

- ANSI/ISA-95.00.01-2000: Enterprise Control System Integration 1: Models and terminology. On-line: http://www.isa95.com Πρόσβαση 17-03-2019

- ISA, ISA-TR99.00.01-2007 -- Security Technologies for Industrial Automation and Control Systems, Instrumentation, Systems, and Automation Society, (draft) Technical Report 2007. Note: will become IEC/TR 62443-5.

- U.S. Government Accountability Office (GAO), GAO-15-6, Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems, December 12, 2014, http://www.gao.gov/products/GAO-15-6