Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Ανάλυση Ευπαθειών σε Συστήματα Πλοίων

Ευάγγελος Ρίζος

Επιβλέπων Καθηγητής
Δρ. Στάυρος Σιαλής

5-2021

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ανάλυση Ευπαθειών σε Συστήματα Πλοίων

Ευάγγελος Ρίζος

Επιβλέπων Καθηγητής
Δρ. Στάυρος Σιαλής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

5-2021

Περίληψη

Στα μέσα το εικοστού πρώτου αιώνα ο κόσμος ήδη αντιμετωπίζει μια τέταρτη βιομηχανική επανάσταση που θα έχει ως αποτέλεσμα την τρομακτική αύξηση της υπολογιστικής ισχύς. Τα παραδοσιακά εμπορικά πλοία πολύ πιθανόν να αντικατασταθούν πλήρως με έξυπνα πλοία ή ακόμα και με αυτόνομα με κεντρική διαχείριση.

Στην εποχή του Internet of Things και των έξυπνων συσκευών παρατηρούνται πολλά κενά ασφαλείας που καλούμαστε πολλές φορές να τα διαχειριστούμε χωρίς να έχουμε προετοιμαστεί καταλλήλως.

Ο αυτοματισμός είναι από τους πιο δημοφιλείς όρους και είναι ζωτικής σημασίας όσον αναφορά στην βιομηχανοποίηση. Στόχος της αυτοματοποίησης είναι να ελαχιστοποιηθεί η ανθρώπινη συμμετοχή.

Πριν από τα αυτόνομα και τα έξυπνα πλοία πρέπει να λάβουμε υπόψιν τα προβλήματα που δημιουργούνται και τη μεθοδολογία που ακολουθείτε, είτε από τις κατασκευάστριες εταιρείες, είτε από τις εταιρείες που κατασκευάζουν εμπορικά πλοία χρησιμοποιώντας αυτά τα συστήματα.

Επομένως η προστασία τέτοιων συστημάτων είναι ζωτικής σημασίας. Είναι σημαντικό να διερευνηθεί η ευπάθεια των PLC & SCADA συστημάτων προκειμένου να επιλυθούν οι απειλές.

Η παρούσα διατριβή θα προσπαθήσει να αναδείξει τα συστήματα PLC & SCADA καθώς και την λειτουργία αυτών των συστημάτων στα εμπορικά πλοία. Ξεκινώντας με μια σύντομη ιστορική αναδρομή στα συστήματα αυτά, παραθέτοντας μερικούς από τους πιο γνωστούς κατασκευαστές PLC & SCADA καθώς και μερικές από τις πιο γνωστές εμπορικά οικογένειες προϊόντων τους μαζί με τις εφαρμογές τους πάνω στα πλοία. Τέλος θα αναλύσει τα πρωτόκολλά που χρησιμοποιούνται και θα προσπαθήσει σύμφωνα με την λίστα, των δέκα πιο σημαντικών ευπαθειών, καθώς και με τις υπάρχουσες έρευνες που έχουν γίνει, να εξηγήσει τα κενά που προκύπτουν στα συστήματα αυτά και να προτείνει λύσεις αντιμετώπισης.

Summary

In the middle of the twenty-first century the world is already facing a fourth industrial revolution that will result in a frightening increase in computing power. Traditional merchant ships will most likely be completely replaced by smart ships or even autonomously centrally managed.

In the age of the Internet of Things and smart devices, there are many security vulnerabilities that we are often called upon to manage without being properly prepared.

Automation is one of the most popular terms and is vital when it comes to industrialization. The goal in automation industry is to minimize human participation.

Before autonomous and smart ships, we must consider the problems that arises as well as the methodology that you follow, either from the companies of these systems, or from the companies that build merchant ships using these systems.

The protection of such systems is vital. It is important to investigate the vulnerability of PLCs & SCADA systems to resolve these threats.

This dissertation will try to highlight the PLC & SCADA systems as well as the operation of these systems on merchant ships. Starting with a brief historical overview of these systems, listing some of the most well-known PLC & SCADA manufacturers as well as some of the most well-known commercial product families along with their on-board applications. Finally, he will analyse the protocols used and will try, according to the list of the ten most important vulnerabilities, as well as the existing research that has been done, to explain the gaps that arise in these systems and to propose solutions.

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος στην Ασφάλειας Υπολογιστών και Δικτυών του τμήματος θετικών επιστήμων του Ανοιχτού Πανεπιστημίου Κύπρου . Ως την ελάχιστη δυνατή μνεία, με την παρούσα παράγραφο οφείλω να ευχαριστήσω όλους όσους συνέβαλαν στην εκπόνησή της και ιδιαίτερα: Τον επιβλέποντα καθηγητή μου, κο Σταύρο Σιαηλή, για την πολύτιμη υποστήριξή του, τις παραγωγικές υποδείξεις του και το πολύ καλό κλίμα συνεργασίας που διαμόρφωσε συμβάλλοντας τα μέγιστα για την κατάρτιση της διπλωματικής μου εργασίας καθώς και την κα Μπέτι Σαρίδου για τις πολύτιμες συμβουλές της. Επίσης θα ήθελα να ευχαριστήσω την οικογένειά μου για την υπομονή και το κουράγιο που συνεχώς μου έδιναν σε όλα τα στάδια της εργασίας μου.

Περιεχόμενα

Κεφάλαιο 1
PLC

1.1 Συνοπτική Αναφορά στα PLC

Πριν από τα PLC ο μόνος τρόπος για τον έλεγχο των μηχανημάτων ήταν μέσω της χρήσης ρελέ. Τα ρελέ λειτουργούν χρησιμοποιώντας ένα πηνίο που, όταν ενεργοποιείται, δημιουργεί μια μαγνητική δύναμη για να τραβήξει αποτελεσματικά έναν διακόπτη στη θέση ON ή OFF. Όταν το ρελέ απενεργοποιηθεί, ο διακόπτης απελευθερώνεται και επιστρέφει τη συσκευή στην τυπική θέση ON ή OFF. Έτσι, για παράδειγμα, αν θέλαμε να ελέγξουμε εάν ένας κινητήρας ήταν ON ή OFF, θα μπορούσαμε να συνδέσουμε ένα ρελέ μεταξύ της πηγής ισχύος και του κινητήρα. Τότε θα μπορούσαμε να ελέγξουμε όταν ο κινητήρας παίρνει ισχύ είτε ενεργοποιώντας είτε απενεργοποιώντας το ρελέ. Χωρίς την παροχή ρεύματος, φυσικά, ο κινητήρας δεν θα λειτουργούσε. Αυτός ο τύπος ρελέ είναι γνωστός ως ρελέ ισχύος. Θα μπορούσαν να υπάρχουν αρκετοί κινητήρες σε ένα εργοστάσιο που πρέπει να ελεγχθούν, με αποτέλεσμα να προσθέταμε πολλά ρελέ ισχύος. [1]

Έτσι τα εργοστάσια άρχισαν να συγκεντρώνουν ηλεκτρικά γραφεία γεμάτα με ρελέ ισχύος, τα οποία για να ελεγχθούν χρειαζόντουσαν τα γνωστά ως ρελέ ελέγχου, επειδή ελέγχουν τα ρελέ που ελέγχουν το διακόπτη που ενεργοποιεί και απενεργοποιεί τον κινητήρα.

Σκεφτείτε για πόσους κινητήρες και διακόπτες τροφοδοσίας ON / OFF θα χρειαστούμε για να ελέγξουμε μόνο ένα μηχάνημα. Όλα αυτά τα ρελέ έπρεπε να είναι ενσύρματα με μια πολύ συγκεκριμένη σειρά ώστε το μηχάνημα να δουλεύει σωστά και αν ένας από τα ρελέ θα είχε πρόβλημα, το σύστημα στο σύνολό του δεν θα λειτουργούσε και

αντιμετώπιση προβλημάτων θα χρειαζόταν ώρες. Αυτά τα μηχανήματα έπρεπε να ακολουθήσουν ένα αυστηρό πρόγραμμα συντήρησης και καταλάμβαναν πολύ χώρο.

Κάπως έτσι ξεκίνησε η έλευση του PLC στις αρχές της δεκαετίας του 1960 για να αντικαταστήσει πλέον τα παραδοσιακά «ενσύρματα» ρελέ και έκτοτε έχει γίνει η κυρίαρχη επιλογή για βιομηχανικούς ελέγχους.[2]

1.1.1 Τα πρώτα PLC

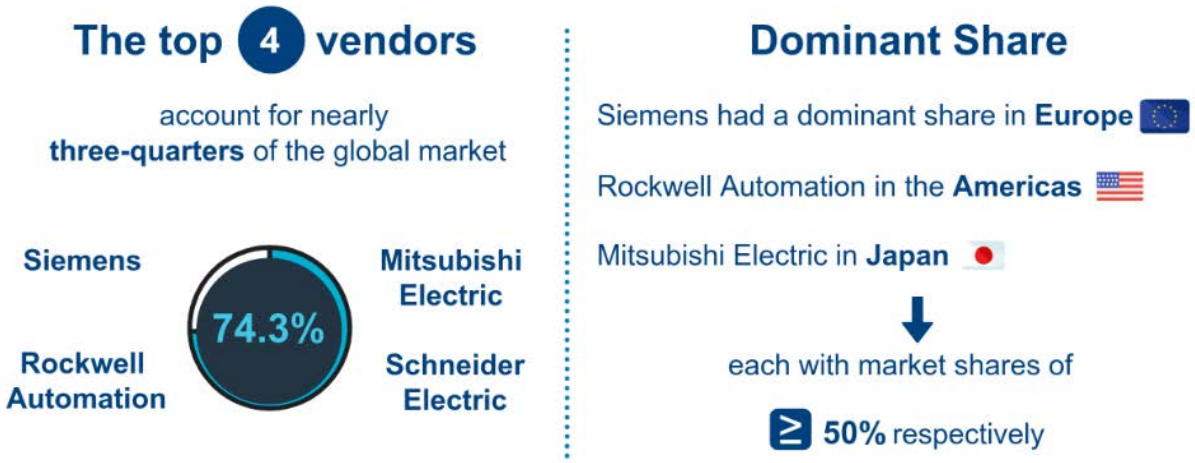
Τα πρώτα PLC είχαν τη δυνατότητα να δουλεύουν με σήματα εισόδου και εξόδου, με χρονόμετρα και μετρητές. Το PLC συνέχισε να εξελίσσεται με την προσθήκη αναλογικών σημάτων εισόδου και εξόδου, βελτιωμένων χρονιστών και μετρητών, μαθηματικών κινητών σημείων, αλληλουχιών τυμπάνου και μαθηματικών συναρτήσεων. Το να υπάρχει ενσωματωμένη λειτουργικότητα PID (Proportional-Integral-Derivative) ήταν ένα τεράστιο πλεονέκτημα για τα PLC που χρησιμοποιούνταν στη βιομηχανία πλοίων. Τα κοινά σύνολα οδηγιών εξελίχθηκαν συμπληρώνοντας έτσι τα κενά πλαίσια δεδομένων που έχουν κάνει τον προγραμματισμό πιο αποτελεσματικό. Η ικανότητα χρήσης σημαντικών ονομάτων ετικετών αντί των περιγραφικών ετικετών επέτρεψε στον τελικό χρήστη να ορίσει με μεγαλύτερη σαφήνεια την εφαρμογή του και η δυνατότητα εισαγωγής / εξαγωγής των ονομάτων ετικετών σε άλλες συσκευές εξαλείφει τα σφάλματα που προκύπτουν κατά την εισαγωγή πληροφοριών σε κάθε συσκευή από χέρι.[1], [3], [4]

Καθώς εξελίχθηκε η λειτουργικότητα των PLC (Porgrammable Logic Controller), οι συσκευές προγραμματισμού και οι επικοινωνίες σημείωσαν επίσης ραγδαία ανάπτυξη. Αργότερα, οι φορητές συσκευές προγραμματισμού μπήκαν στην εικόνα, αλλά σύντομα αντικαταστάθηκαν με ιδιόκτητο λογισμικό προγραμματισμού που εκτελούνταν σε προσωπικό υπολογιστή. Το DirectSOFT της AutomationDirect, που αναπτύχθηκε από την Host Engineering, ήταν το πρώτο πακέτο λογισμικού προγραμματισμού PLC για Windows λειτουργικό. Έχοντας έναν υπολογιστή επικοινωνία με PLC παρείχε τη δυνατότητα όχι μόνο να προγραμματίσει, αλλά και επέτρεψε ευκολότερες δοκιμές και αντιμετώπιση προβλημάτων. Οι επικοινωνίες ξεκίνησαν με το πρωτόκολλο MODBUS χρησιμοποιώντας σειριακές επικοινωνίες RS-232. Ακολούθησε η προσθήκη διαφόρων πρωτοκόλλων αυτοματισμού που επικοινωνούν μέσω RS-485, DeviceNet, Profibus και άλλων αρχιτεκτονικών σειριακής επικοινωνίας. Η χρήση σειριακών επικοινωνιών και τα

διάφορα πρωτόκολλα PLC επέτρεψαν επίσης τα PLC να δικτυωθούν με άλλα PLC, όπως τα HMI. Πιο πρόσφατα, πρωτόκολλα όπως το TCP / IP που ενσωματώθηκε στα PLC πρόσθεσε τεράστια δημοτικότητα.[1], [2]

1.2 Κατασκευαστές συστημάτων PLC

Ένας από τους καλύτερους τρόπους για να κρίνουμε ποια PLC είναι πιο δημοφιλή είναι με το μερίδιο αγοράς. Υπήρξε μια μελέτη που πραγματοποιήθηκε από την Interact Analysis το 2019 για τον προσδιορισμό του μεριδίου αγοράς PLC διαφόρων κατασκευαστών θέλοντας να επισημάνει την διαδραστικότητα και την υπεροχή που έχει η νέα τεχνολογία σε βάθος χρόνου. Μερικοί από αυτούς θα αναφερθούν παρακάτω. **Εικόνα [1]**



Εικόνα 1 Top 4 Vendors & Dominant Share [Interact Analysis 2019]

1.2.1 Siemens

Ίσως το μεγαλύτερο όνομα στον κόσμο της αυτοματοποίησης και των PLC. Προσφέρει τη σειρά SIMATIC, δίνοντας στους χρήστες όλων των επιδόσεων μια επιλογή.

Οι ελεγκτές SIMATIC διαθέτουν, πολύ καλές λειτουργίες, όπως εύκολες συνδέσεις Ethernet TCP / IP και επικοινωνίες Profinet IO. Το Profibus περιλαμβάνεται ή προστίθεται εύκολα ως επιπλέον module.

Όσον αφορά το λογισμικό SIMATIC, η Siemens ισχυρίζεται ότι προσφέρουν τη μέγιστη απόδοση καθ' 'όλη τη διαδικασία αυτοματοποίησης. Το λογισμικό **SIMATIC STEP 7** επιτρέπει στους χρήστες να διαμορφώσουν, να προγραμματίσουν, να δοκιμάσουν και να

διαγνώσουν τους βασικούς, προχωρημένους και κατανεμημένους ελεγκτές της εταιρείας.

Οι προγραμματιστές και μηχανικοί από όλο τον κόσμο είναι πλήρως εξοικειωμένοι με την πλατφόρμα της Siemens, καθιστώντας την μια σταθερή επιλογή για την ναυτιλία. **Πίνακας [1]**

	Software	**Type**	**Τύπος PLC**
Siemens			
		Micro PLC	S7-200
			S7-1200
	Simatic		
		Modular PLC	S5-115U
			S7-300
			S7-400

Πίνακας 1 Κατασκευαστή Siemens για τους πιο γνωστούς PLC

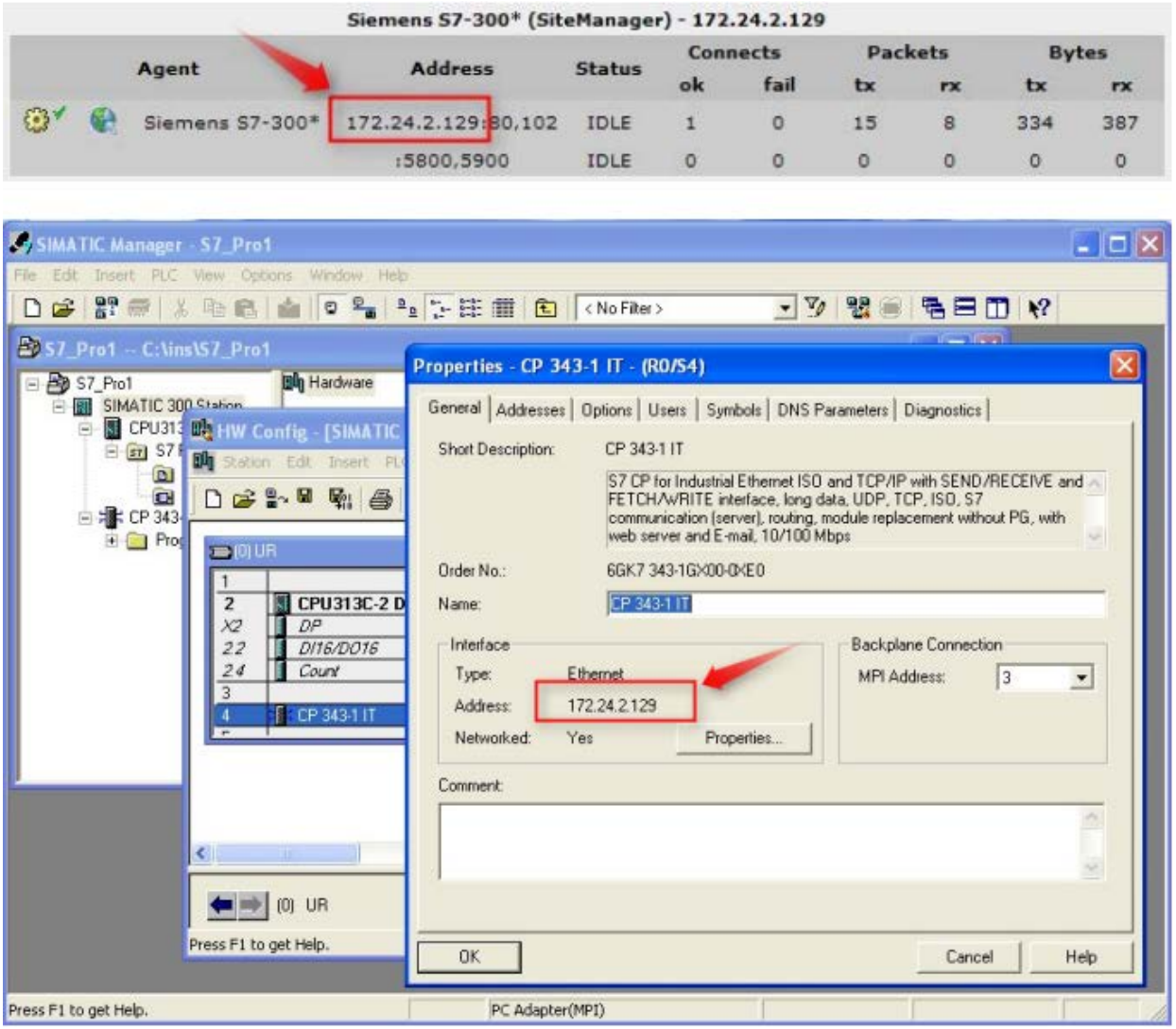
	Τύπος PLC	**Type**	**Εφαρμογές σε πλοία**
	S7-1200	Micro PLC	Αντλία υδροσυλλεκτών στο μηχανοστάσιο,
	S7-200	Micro PLC	βαλβίδες αεριού, λαδιού
Siemens			
	S5-115U	Modular PLC	φωτισμός, standby λειτουργία,
	S7-300	Modular PLC	έλεγχος βαλβίδας νερού και αέρα.
	S7-400	Modular PLC	

Πίνακας 2 Κατασκευαστή Siemens για εφαρμογές PLC στα πλοία.

Το λογισμικό SIMATIC STEP 7 της Siemens χρησιμοποιώντας το λογισμικό STEP 7, μπορεί να προγραμματίσει των PLC S7 σε ένα έργο.

Ο προγραμματιζόμενος ελεγκτής S7 αποτελείται από μονάδα τροφοδοσίας, CPU και είσοδο και μονάδες εξόδου (I/O modules).

Ο προγραμματιζόμενος λογικός ελεγκτής (PLC) παρακολουθεί και ελέγχει το μηχάνημά και το πρόγραμμα S7. Τα modules I/O εντοπίζονται στο πρόγραμμα S7 μέσω των ip διευθύνσεων. **Εικόνα [2]**



Εικόνα 2 Simatic Manager βρίσκει τον controller με την IP.

1.2.2 Rockwell Automation

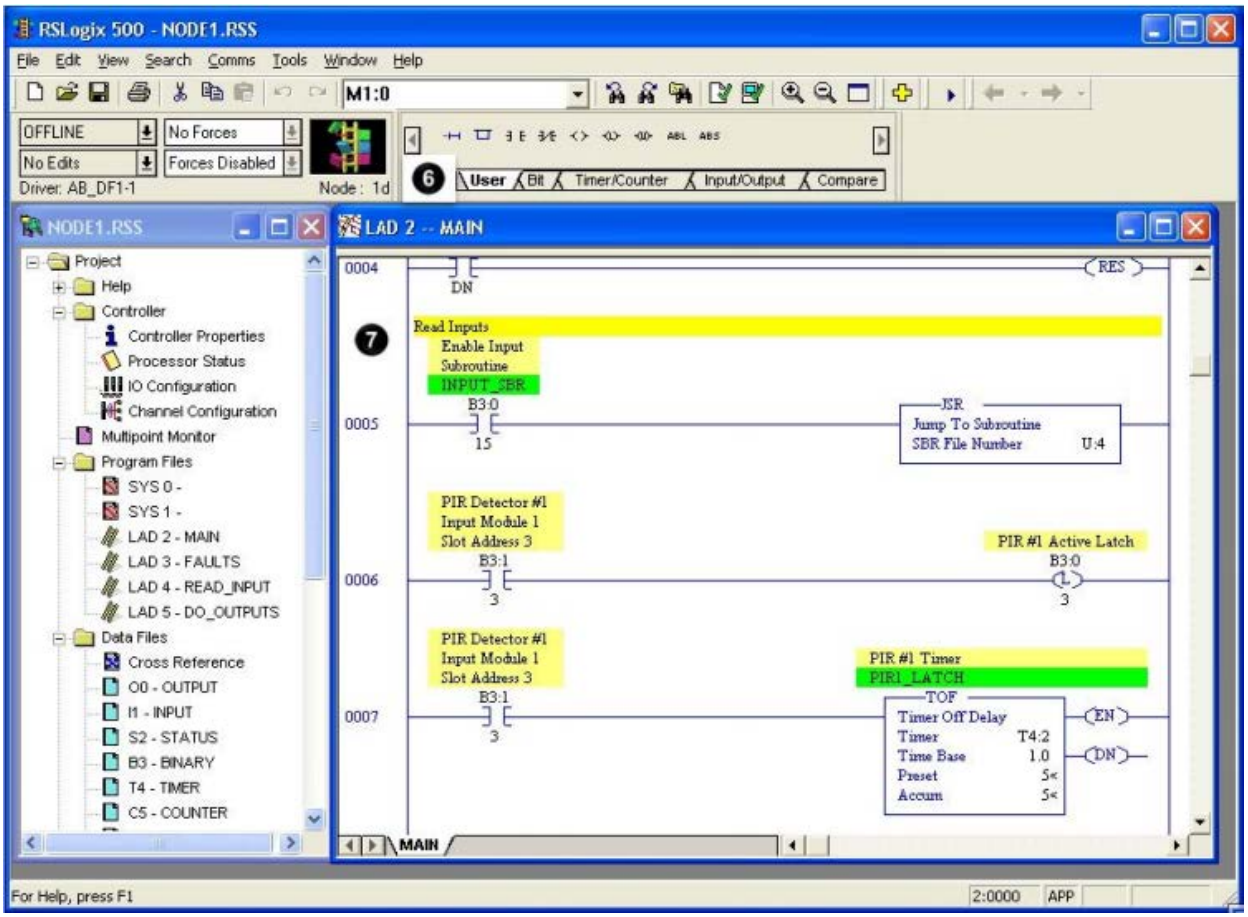
Από τους μεγαλύτερους κατασκευαστές PLC που χρησιμοποιείται στις Ηνωμένες Πολιτείες με την σειρά ελεγκτών Allen-Bradley.

Η Allen-Bradley προσφέρει ελεγκτές για έργα μεγάλου φάσματος. Τα μεγάλα συστήματα ελέγχου τους αναφέρονται ως προγραμματιζόμενοι αυτοματοποιημένοι ελεγκτές ή PAC. Αυτά κατασκευάζονται έχοντας κατά νου ένα ολοκληρωμένο αυτοματοποιημένο έργο.

Αυτό επιτυγχάνεται με το λογισμικό **ControlLogix**, το **GuardPLC** για συστήματα ασφαλείας και τη σουίτα λογισμικού **SoftLogix**.

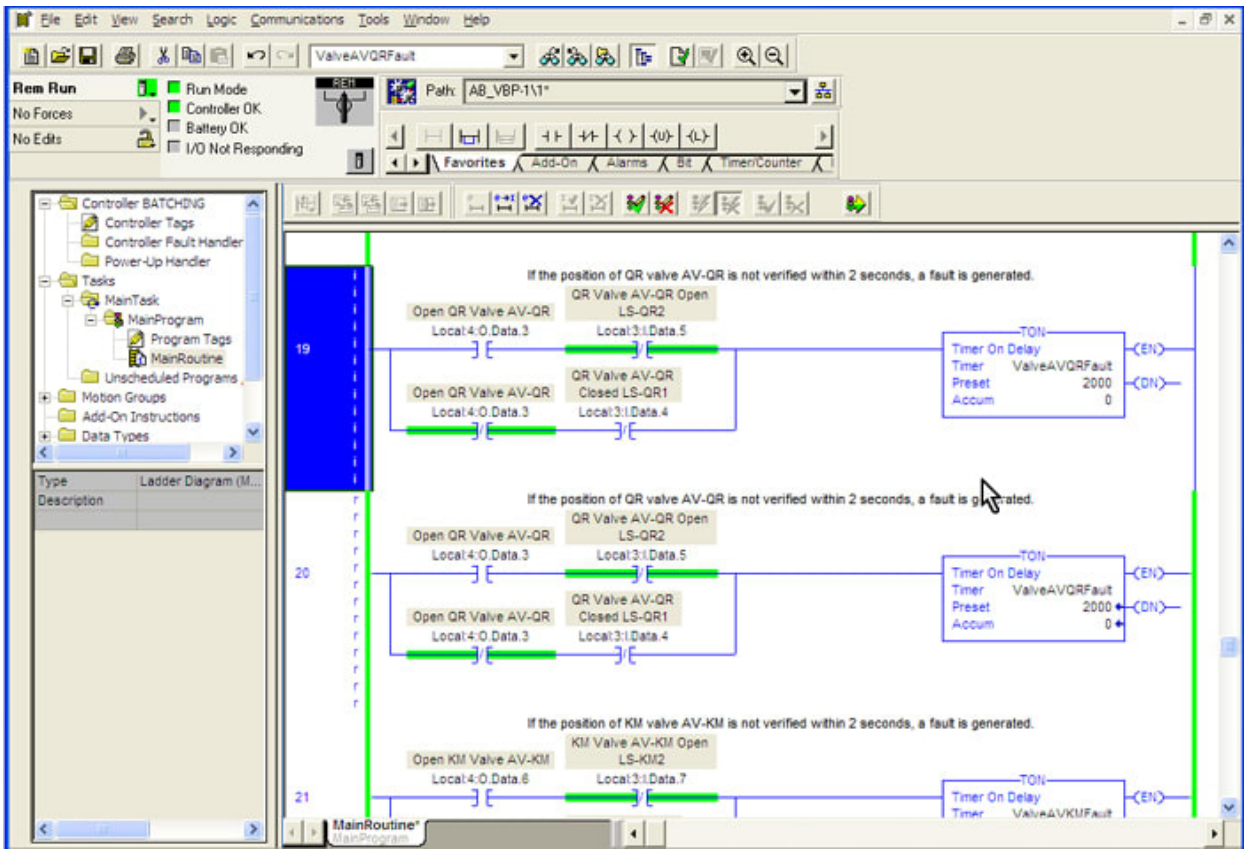
Η **Allen-Bradley** προσφέρει επίσης συστήματα για μικρότερες εφαρμογές. Τα πιο δημοφιλή είναι τα συστήματα **MicroLogix**, **SLC500** και **CompactLogix**.

Η σειρά λογισμικού προγραμματισμού **RSLogix** υπάρχει εδώ και πολλά χρόνια και έχει εξελιχθεί σε ένα εξαιρετικά ισχυρό εργαλείο αυτοματισμού. **Εικόνα [3]**



Εικόνα 3 RSI Logix 500 προγραμματισμός Ladder.

Ο προγραμματισμός για ελεγκτές **Allen-Bradley** έρχεται με τη μορφή **RSLogix 5000** και το νεότερο λογισμικό της εταιρείας το **Studio 5000**. **Εικόνα [4]**



Εικόνα 4 Simatic Manager βρίσκει τον controller με την IP

	Software	Type	Τύπος PLC
Allen Bradley		Logix-5 Family	PLC-5
	RS Logix	Logix-500 Family	SLC-500
			Micrologix
		Logix-5000 Family	ControlLogix
			CompactLogix
			FlexLogix

Πίνακας 3 Κατασκευαστή Rockwell για τους πιο γνωστούς PLC

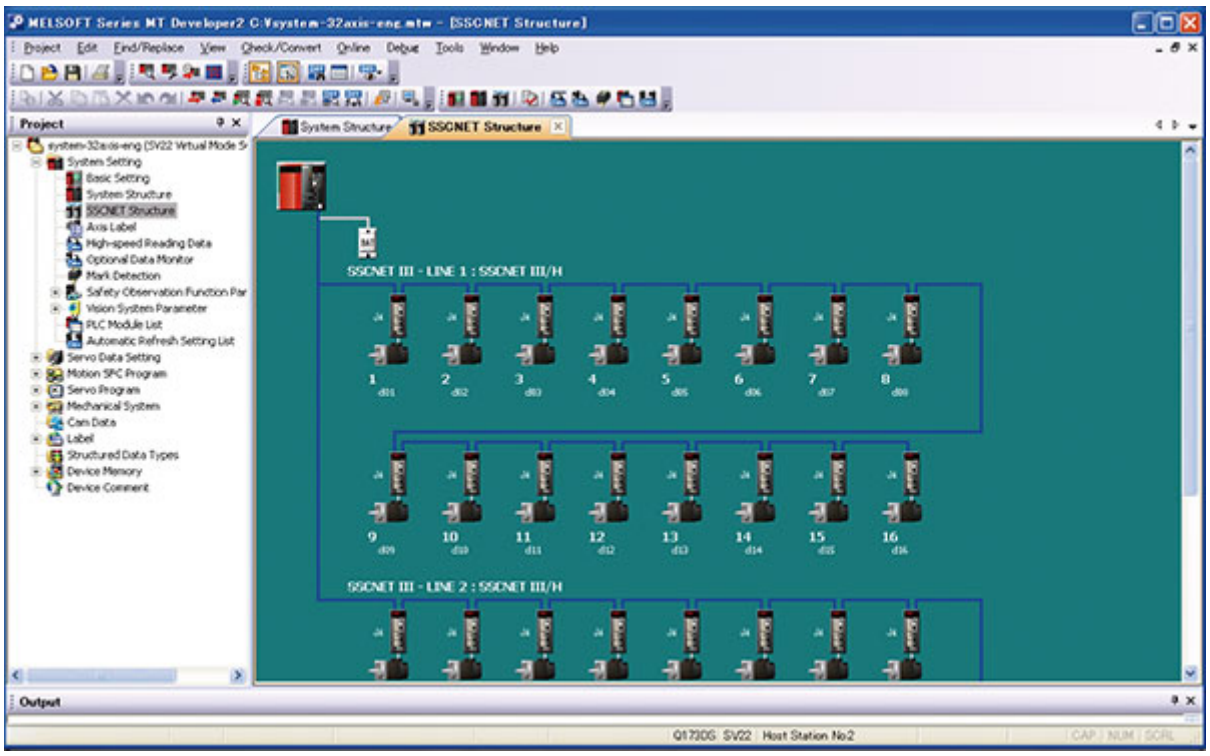
	Τύπος PLC	Type	Εφαρμογές σε πλοία
	PLC-5	Logix-5 Family	Ζύγιση φορτίων
	SLC-500	Logix-500 Family	Αισθητήρες νερού, έλεγχος δεξαμενών λυμάτων
Allen Bradley			
	ControlLogix	Logix-5000 Family	Έλεγχος αεριού, φωτιάς, έλεγχος καύσης μηχανής μηχανοστασίου
	CompactLogix		
	FlexLogix		

Πίνακας 4 Κατασκευαστή Rockwell για εφαρμογές PLC στα πλοία

1.2.3 Mitsubishi Electric

Ένας πολυεθνικός κατασκευαστής ηλεκτρικών και ηλεκτρονικών προϊόντων με έδρα το Τόκιο της Ιαπωνίας. Σήμερα η Mitsubishi Electric προσφέρει μεγάλη γκάμα από μικροελεγκτές.

Οι κυριότεροι τύποι για συστήματα είναι η σειρά **Q-Series Q00UJCPU**. Ο προγραμματισμός των μικροελεγκτων της γίνεται μέσα από το πρόγραμμα **MELSOFT series**. **Εικόνα [5]**



Εικόνα 5 MELSOFT Series MT software PLC

	Software	Type	Τύπος PLC
Mitsubishi		Compact PLC	Melsec FX3UX
			Melsec FX3G
	MELSOFT series		Melsec FX1N
			Melsec FX1S
		Modular PLC	Q-Series Q00UJCPU
		Process Control	Q12PHCPU

Πίνακας 5 Κατασκευαστή Rockwell για τους πιο γνωστούς PLC

	Τύπος PLC	Type	Εφαρμογές σε πλοία
Mitsubishi	Melsec FX3UX		Έλεγχος θερμοκρασίας στα κοντέινερ , διαχείριση των μηχανών diesel, έλεγχος καπνού, εξαερισμός, διαχείριση λυμάτων
	Melsec FX3G	Compact PLC	
	Melsec FX1N		
	Melsec FX1S		
			Έλεγχος ποσίμου νερού, έλεγχος πηδάλιου
	Q-Series Q00UJCPU	Modular PLC	
	Q12PHCPU	Process Control	-

Πίνακας 6 Κατασκευαστή Rockwell για εφαρμογές PLC στα πλοία

1.2.4 Schneider Electric

Με έδρα τη Rueil-Malmaison στη Γαλλία η Schneider Electric είναι γνωστή για την κατασκευή του Modicon PLC.

Ένα τεράστιο πλεονέκτημα είναι ότι οι περισσότερες από τις λειτουργίες που απαιτούνται για την εργασία με το σύστημα ελέγχου είναι ήδη ενσωματωμένες.

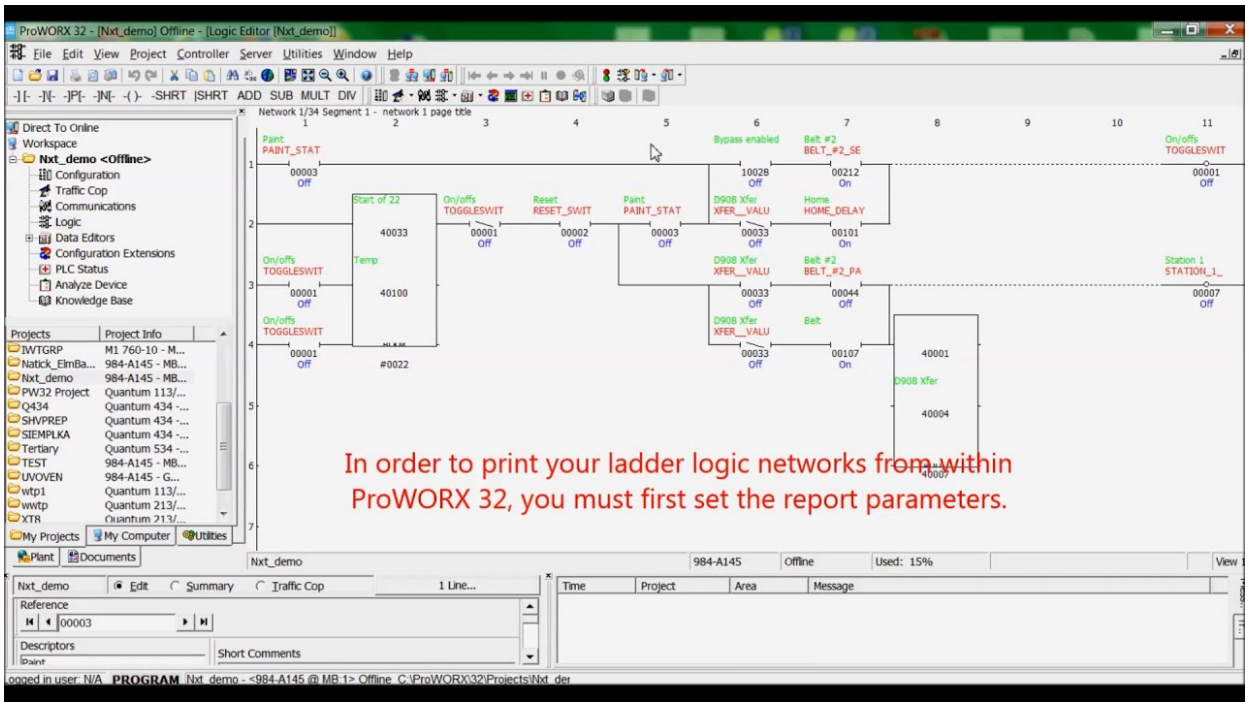
	Software	Type	Τύπος PLC
	PL7	Micro PLC	Modicon M340
Schneider			
	ProWORX	32Machine Control PLC	Modicon Premium
		Process Control PLC	Modicon Quantum
		Programmable Controller	Twido
		Smart Relay	Zelio

Πίνακας 7 Κατασκευαστή Schneider Electric για τους πιο γνωστούς PLC

	Τύπος PLC	Type	Εφαρμογές σε πλοία
	Modicon M340	Micro PLC	Έλεγχος και διαχείριση ποσίμου νερού
Schneider			
	Modicon Premium	32Machine Control PLC	-
	Modicon Quantum	Process Control PLC	Standby δίκτυο μέσω ethernet
	Twido	Programmable Controller	Έλεγχος επικοινωνιών plc
	Zelio	Smart Relay	Διαχείριση φωτισμού, πόρτες πλοίου, εξαερισμός κ έλεγχος θερμοκρασίας, έλεγχος θερμοκρασίας λεβητοστάσιου

Πίνακας 8 Κατασκευαστή Rockwell για εφαρμογές PLC στα πλοία

Κύρια λογισμικά για τα PLC της Schneider είναι το ProWorx και PL7. **Εικόνα [6]**



Εικόνα 6 MELSOFT Series MT software PLC

1.3 Λογισμικό συστημάτων PLC

Το λογισμικό για PLC είναι μια τεχνολογία που έχει σχεδιαστεί για να μετατρέψει έναν ενσωματωμένο υπολογιστή σε έναν πλήρως λειτουργικό και προγραμματιζόμενο PLC. Ως εκ τούτου, το λογισμικό προσφέρει μια αξιόπιστη και ανοιχτή πλατφόρμα αρχιτεκτονικής που επιτρέπει στους χρήστες να συνδεθούν σε ένα ευρύ φάσμα I/O συστημάτων και δίκτυών μεταξύ άλλων συσκευών.

Οι ερευνητές κατά το παρελθόν έχουν αποκαλύψει εύκολα εκμεταλλεύσιμες ευπάθειες στους καταλόγους (directories) που βρίσκονται στο λογισμικό βιομηχανικού συστήματος ελέγχου (ICS) για PLC. Κάποιες από αυτές σύμφωνα με τον ιστότοπο **cvedetails.com**. παρουσιάζονται επιγραμματικά παρακάτω από τους κατασκευαστές που έχουν δημιουργήσει το δικό τους λογισμικό.

1.3.1 Siemens Simatic Step 7

a. Επιτρέπει στους τοπικούς χρήστες να αποκτήσουν προνόμια μέσω ενός αρχείου Trojan horse. [5]
b. Πριν από 14 χρήσεις ο επιτιθέμενος χρησιμοποιεί μια ακατάλληλη μορφή για τη διαχείριση αρχείων έργου TIA κατά τη διάρκεια ενημερώσεων έκδοσης, γεγονός που διευκολύνει τους τοπικούς χρήστες να λαμβάνουν ευαίσθητες πληροφορίες διαμόρφωσης μέσω μη καθορισμένων διανυσμάτων. [5]
c. Αποθηκεύει εσφαλμένα δεδομένα κοινόχρηστου κλειδιού σε αρχεία έργου TIA, γεγονός που διευκολύνει τους τοπικούς χρήστες να αποκτήσουν ευαίσθητες πληροφορίες, αξιοποιώντας την πρόσβαση σε ένα αρχείο και πραγματοποιώντας μια επίθεση ωμής βίας.
d. Τα δικαιώματα του χρήστη με βάση τα πεδία αρχείων έργου που δεν διαθέτουν προστασία ακεραιότητας, το οποίο επιτρέπει στους απομακρυσμένους εισβολείς να καθιερώσουν αυθαίρετα δεδομένα εξουσιοδότησης μέσω ενός τροποποιημένου αρχείου.
e. Επιτρέπει στους τοπικούς χρήστες να αποκτήσουν προνόμια μέσω ενός Trojan horse DLL σε ένα φάκελο έργου STEP7. [5]
f. Ο κωδικός κατακερματισμού με ανεπαρκή υπολογιστική προσπάθεια θα μπορούσε να επιτρέψει σε έναν εισβολέα να αποκτήσει πρόσβαση στους τοπικούς

χρήστες να αποκτήσουν προνόμια μέσω ενός Trojan horse DLL σε ένα φάκελο έργου STEP7. Ένα αρχείο έργου και να ανακατασκευάσει κωδικούς πρόσβασης. Αυτή η ευπάθεια θα μπορούσε να επιτρέψει στον εισβολέα να αποκτήσει ορισμένους κωδικούς πρόσβασης από το έργο. [5]

1.3.2 Rockwell Allen Bradley Control Logic, Gerd PLC & SoftLogix

a. Το κακόβουλο αρχείο Arena που άνοιξε ένας ανυποψίαστος χρήστης μπορεί να έχει ως αποτέλεσμα τη χρήση ενός δείκτη που δεν έχει αρχικοποιηθεί.[6]

b. Ένα κακόβουλο αρχείο Arena που άνοιξε ένας ανυποψίαστος χρήστης μπορεί να έχει ως αποτέλεσμα την περιορισμένη έκθεση των πληροφοριών που σχετίζονται με τον στοχευμένο σταθμό εργασίας.[6]

c. Ένα κακόβουλα δημιουργημένο αρχείο Arena που άνοιξε ένας ανυποψίαστος χρήστης μπορεί να οδηγήσει σε διακοπή της εφαρμογής ή στην εκτέλεση αυθαίρετου κώδικα.[6]

d. Μια ανοιχτή ευπάθεια ανακατεύθυνσης θα μπορούσε να επιτρέψει σε έναν απομακρυσμένο μη εξουσιοδοτημένο εισβολέα να εισάγει έναν κακόβουλο σύνδεσμο για να ανακατευθύνει τους χρήστες σε έναν κακόβουλο ιστότοπο που θα μπορούσε να εκτελέσει ή να κατεβάσει αυθαίρετο κακόβουλο λογισμικό στη μηχανή χρηστών.[6]

e. Επιτρέψτε σε απομακρυσμένους εισβολείς να προκαλέσουν άρνηση υπηρεσίας συντρίβοντας τη στοίβα δικτύου Common Industrial Protocol (CIP). Η ευπάθεια επιτρέπει στον εισβολέα να συντρίψει το CIP με τρόπο που δεν δέχεται νέες συνδέσεις, αλλά διατηρεί τις τρέχουσες συνδέσεις ενεργές, οι οποίες μπορούν να αποτρέψουν τους νόμιμους χρήστες από την ανάκτηση ελέγχου.[6]

f. Ένας απομακρυσμένος εισβολέας θα μπορούσε να στείλει ένα επεξεργασμένο πακέτο UDP στην υπηρεσία SNMP προκαλώντας μια κατάσταση άρνησης υπηρεσίας μέχρι την επανεκκίνηση του επηρεαζόμενου προϊόντος .[6]

g. Ένας απομακρυσμένος μη εξουσιοδοτημένος εισβολέας θα μπορούσε να στείλει πολυάριθμα κατασκευασμένα πακέτα σε θύρες εξυπηρέτησης με αποτέλεσμα την κατανάλωση μνήμης που θα μπορούσε να οδηγήσει σε μερική ή πλήρη κατάσταση άρνησης υπηρεσίας στις επηρεαζόμενες υπηρεσίες.[6]

h. Ο απομακρυσμένος παράγοντας απειλής θα μπορούσε να στείλει ένα αίτημα σύνδεσης CIP σε μια επηρεαζόμενη συσκευή και μετά την επιτυχή σύνδεση, να στείλει μια νέα διαμόρφωση IP στην επηρεαζόμενη συσκευή, ακόμη και αν ο ελεγκτής του συστήματος έχει ρυθμιστεί σε λειτουργία Hard RUN. Όταν η επηρεαζόμενη συσκευή αποδέχεται αυτήν τη νέα διαμόρφωση IP, συμβαίνει απώλεια επικοινωνίας μεταξύ της συσκευής και του υπόλοιπου συστήματος, καθώς η κίνηση του συστήματος προσπαθεί να επικοινωνήσει με τη συσκευή μέσω της αντικατασταθείσας διεύθυνσης IP .[6]

i. Ένα ειδικά κατασκευασμένο πακέτο μπορεί να προκαλέσει λειτουργία ανάγνωσης ή εγγραφής με αποτέλεσμα την αποκάλυψη ευαίσθητων πληροφοριών, τροποποίηση ρυθμίσεων ή τροποποίηση λογικής σκάλας. Ένας εισβολέας μπορεί να στείλει πακέτα χωρίς έλεγχο ταυτότητας για να προκαλέσει αυτήν την ευπάθεια. Απαιτούμενη κατάσταση Keyswitch: REMOTE ή PROG Περιγραφή: Ο τύπος αρχείου 0x03 επιτρέπει στους χρήστες πρόσβαση εγγραφής, επιτρέποντας τη δυνατότητα αντικατάστασης της τιμής κύριου κωδικού πρόσβασης που είναι αποθηκευμένη στο αρχείο. .[6]

j. Ένα ειδικά κατασκευασμένο πακέτο μπορεί να προκαλέσει λειτουργία ανάγνωσης ή εγγραφής με αποτέλεσμα την αποκάλυψη ευαίσθητων πληροφοριών, τροποποίηση ρυθμίσεων ή τροποποίηση λογικής σκάλας. Ένας εισβολέας μπορεί να στείλει πακέτα χωρίς έλεγχο ταυτότητας για να προκαλέσει αυτήν την ευπάθεια. Απαιτούμενη κατάσταση Keyswitch: REMOTE ή PROG (επίσης RUN για ορισμένους) Περιγραφή: Επιτρέπει σε έναν εισβολέα να ενεργοποιήσει SNMP, Modbus, DNP και οποιεσδήποτε άλλες δυνατότητες στη διαμόρφωση του καναλιού. Επιτρέπει επίσης στους εισβολείς να αλλάζουν παραμέτρους δικτύου, όπως διεύθυνση IP, διακομιστή ονομάτων και όνομα τομέα.[6]

1.3.3 Mitsubishi Melsoft series

a. Επιτρέπει στους απομακρυσμένους εισβολείς να προκαλέσουν άρνηση υπηρεσίας (διακοπή της συσκευής) μέσω μιας μακράς παραμέτρου. [7]

b. Επιτρέπει σε έναν απομακρυσμένο εισβολέα να συνδεθεί στο PLC μέσω της θύρας 5002 / TCP και να προκαλέσει άρνηση υπηρεσίας, απαιτώντας την επαναφορά του PLC για να συνεχίσει τη λειτουργία. Αυτό προκαλείται από μια απεριόριστη εξωτερική πρόσβαση. [7]

1.3.4 Schneider Electric ProWorx, PL7

a. Επιτρέπει σε απομακρυσμένους εισβολείς να εκτελέσουν αυθαίρετο κώδικα μέσω μιας μεγάλης τιμής μεγέθους buffer σε ένα Modbus. [8]

b. Επιτρέπει στους τοπικούς χρήστες, και πιθανώς στους απομακρυσμένους εισβολείς, να εκτελέσουν αυθαίρετο κώδικα μέσω μιας μη καθορισμένης παραμέτρου συστήματος.[8]

1.4 Βιομηχανικό πρωτόκολλο Modbus

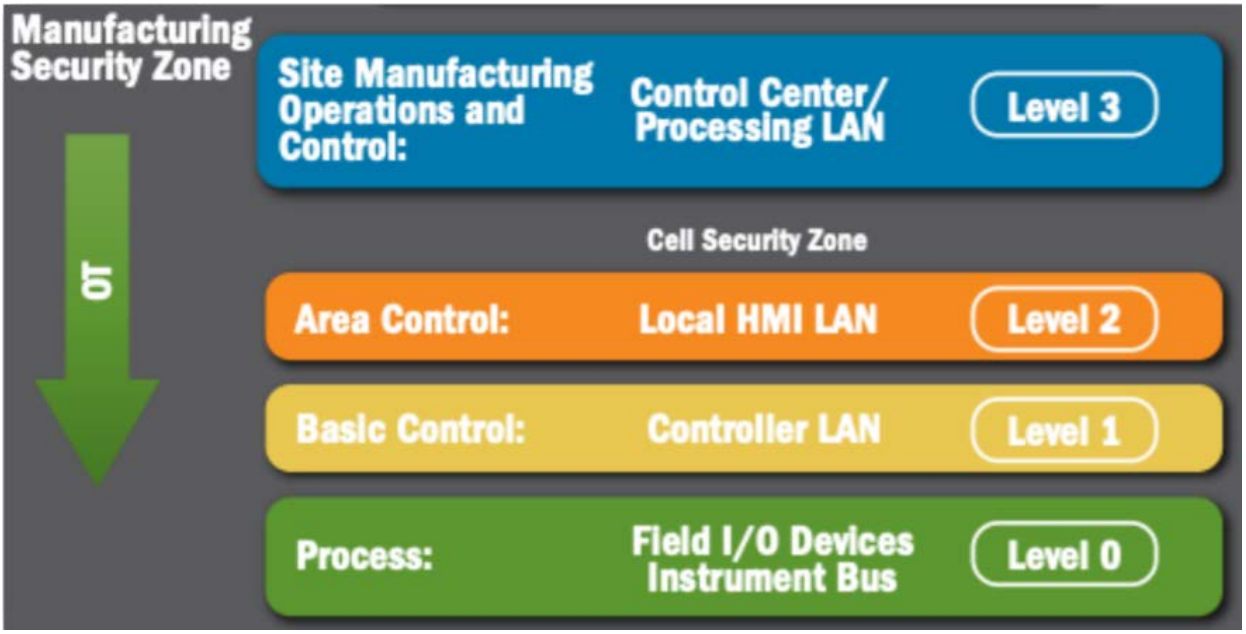
Το βιομηχανικό πρωτόκολλο Modbus που χρησιμοποιείτε για την επικοινωνία μεταξύ server και client χρησιμοποιείτε πάνω από 40 χρονιά και ακόμα είναι ευρέως διαδεδομένο και σε νέα συστήματα ICS. Το Modbus μπορεί να χρησιμοποιήσει σειριακές όπως την RS232 και την RS485 ή μπορεί τροποποιηθεί για IEEE 802.3 TCP τμήμα. Μέσα στο TCP, η τυπική εφαρμογή του είναι μια μονάδα απομακρυσμένου τερματικού Modbus (RTU) που περιέχεται στο επίπεδο εφαρμογής TCP / IP, το οποίο μπορούμε εύκολα να δούμε στο Wireshark . Το Modbus χρησιμοποιεί μια απλή λειτουργία κλήσης σε συνδυασμό με αιτήματα εύρους δεδομένων για ανάγνωση και εγγραφή των bit, τα οποία ονομάζονται πηνία (coils). Όταν οι μηχανικοί κατάφεραν να ενσωματώσουν το Modbus στο TCP, οι ανησυχίες για την ασφάλεια στον κυβερνοχώρο ήταν ανύπαρκτες και γι' αυτό το Modbus RTU δεν διαθέτει ενσωματωμένους μηχανισμούς ασφαλείας (Rinaldi).

Από άποψη ασφάλειας για τα ICS συστήματα , το Modbus είναι γεμάτο με ευπάθειες και υπόκειται σε πληθώρα ευπαθειών όπως : έλεγχο, σάρωση, πλημμύρα, παράκαμψη ελέγχου ταυτότητας, πλαστογράφηση, υποκλοπή, εσφαλμένη κατεύθυνση, ανάγνωση / αντιγραφή, τερματισμός, εκτέλεση, τροποποίηση και επιθέσεων διαγράφης (Draias, Serhrouchni & Vogel, 2015). [9]

1.4.1 Modbus που βρίσκεται συνήθως

Σε ένα περιβάλλον από PLC συστήματα το πρωτόκολλο Modbus TCP συνήθως βρίσκεται κοντά σε φυσικές λειτουργίες. Όπως φαίνεται και στην **εικόνα [7]** υπάρχουν πολλές

συσκευές στο πεδίο μιας παραγωγής στο επίπεδο 0, όπως αισθητήρες ροής αναλυτές οργάνων κ.α., που μπορεί να έχουν Modbus TCP συμβατότητα.



Εικόνα 7 Επίπεδα Ζωνών από ICS/PLC (SCIA ,2016)

Τέλος μπορούμε να παρατηρήσουμε ότι βάση της **εικόνα [7]** το Modbus πρωτόκολλο καλύπτει τα επίπεδα από 0 έως 2 εκεί βρίσκονται και συσκευές που σχετίζονται με επικοινωνία μεταξύ των συσκευών όπως Open Platform Communication (OPC).

Αν και το πρωτόκολλο Modbus έχει πολλές ευπάθειες και είναι εύκολο να το εκμεταλλευτούμε, η δυσκολία διεξαγωγής επιθέσεων σε συστήματα ICS έγκειται στη χαλαρή σχέση μεταξύ του πρωτοκόλλου Modbus και της προγραμματιστικής λογικής της συσκευής ICS.

Το Modbus δεν συσχετίζει δεδομένα σε ένα μοντέλο πληροφοριών όπως άλλα πρωτόκολλα ή frameworks (OPC Foundation, 2020). Έτσι περιορισμένες πληροφορίες περιβάλλοντος ενός αρχείου PLC είναι διαθέσιμες στον εισβολέα χωρίς σημαντικό χρόνο παραμονής του ιδίου στο σύστημα, με ευκαιρία την παρακολούθηση. Τα μητρώα Modbus μπορούν να αντιπροσωπεύουν μια γκάμα μεταβλητών διεργασίας ή ελέγχου. Αυτά μπορεί να περιλαμβάνουν το επίπεδο δεξαμενής, ρυθμό ροής, θερμοκρασία, πίεση, τάση, σημείο ρύθμισης ή έξοδος ελέγχου. Τα πηνία Modbus, από την άλλη πλευρά, προσφέρουν λιγότερες πληροφορίες και είναι πιο δύσκολο να αποκρυπτογραφηθούν: μια τιμή 0 ή 1, για παράδειγμα, μπορεί να υποδηλώνει κατάσταση αντλίας, θέση

διακόπτη, θέση βαλβίδας ή μπορεί να χρησιμοποιηθεί για τον έλεγχο αυτών των αντικειμένων.[10], [11]

Παρά τη δυσκολία κατανόησης της διαδικασίας και του συστήματος ελέγχου, το 2014 το Γερμανικό Steel Mill Cyber Attack ανέδειξε ότι έμαθαν επαρκείς λεπτομέρειες για το περιβάλλον, αξιοποιώντας εξειδικευμένες γνώσεις πάνω στο ICS και προκαλώντας πολλαπλές αστοχίες στο σύστημα ελέγχου που τελικά οδηγούσαν σε διακοπή λειτουργίας με επακόλουθο φυσικά τη ζημιά του εξοπλισμού (Lee, Assante, & Conway, 2014).

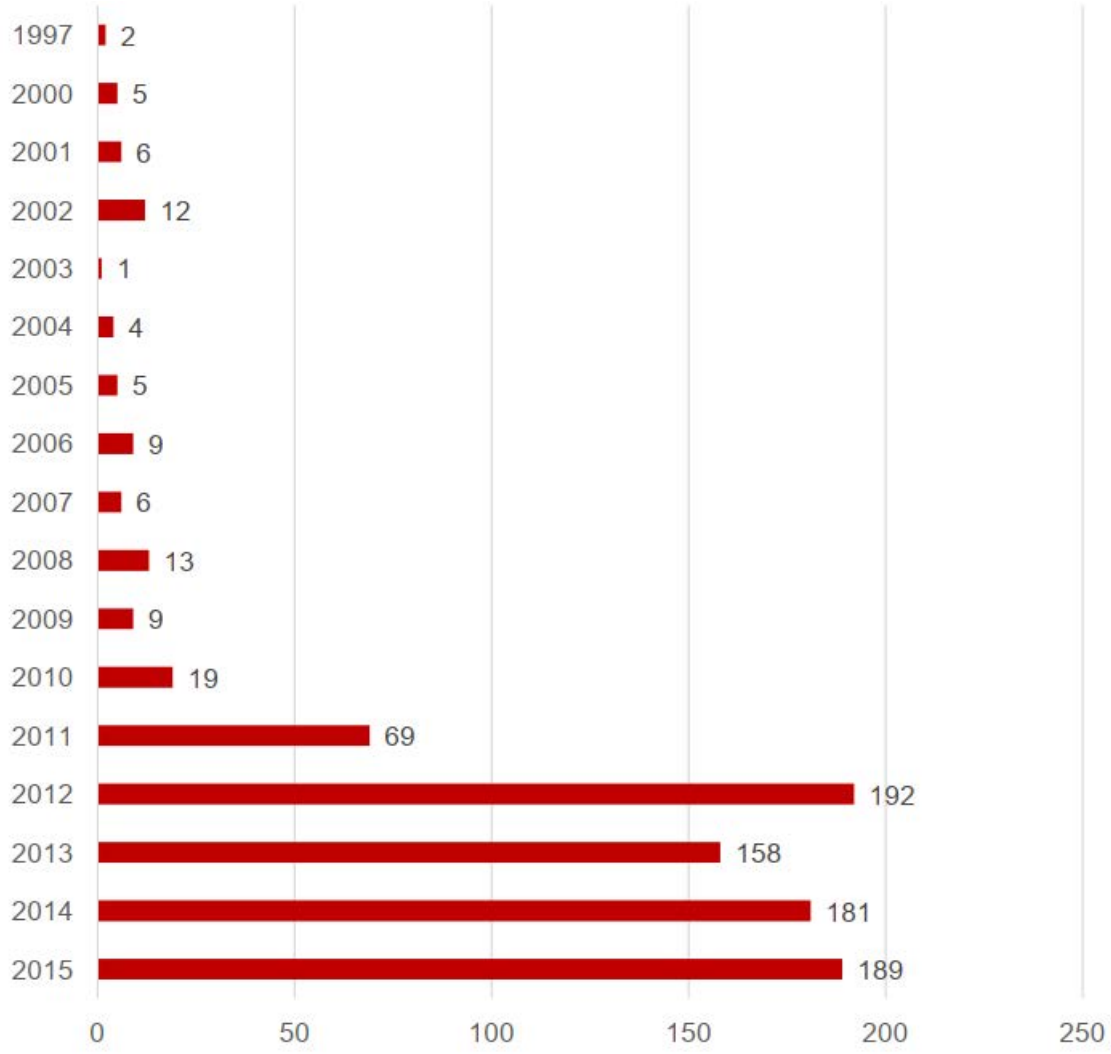
Το δίκτυο ηλεκτρικής ενέργειας της Ουκρανίας το 2015 είναι ένα ακόμη παράδειγμα που επιτιθέμενοι μαθαίνουν το περιβάλλον και αξιοποιούν τις επικοινωνίες για να προκαλέσουν διακοπή ηλεκτρικού δικτύου.

Η δεύτερη επίθεση στην Ουκρανία στο δίκτυο τροφοδοσίας, συνέβη το 2016, χρησιμοποιήθηκε κακόβουλου λογισμικό ICS γνωστό ως **CRASHOVERRIDE**. Το κακόβουλο λογισμικό περιείχε μια ενότητα πρωτοκόλλου IEC104, μεταξύ άλλων και αξιοποίησε τις δυνατότητες αυτές για να τραβήξει διαμορφώσεις RTU από το ICS περιβάλλον. Στη συνέχεια, το IEC104 χρησιμοποίησε αυτήν τη γνώση εφαρμογής για να χειριστεί τις θέσεις του διακόπτη, οδηγώντας σε διακοπή ρεύματος (Lee R. M., 2017).

Όπως ο Joe Slowik παρατήρησε το 2019 , οι επιθέσεις σε συστήματα PLC και ICS φαίνεται να αυξάνονται τόσο σε σχετική συχνότητα όσο και σε σοβαρότητα. Επομένως, όταν εξετάζουμε την αυξανόμενη απειλή για το περιβάλλοντα αυτά, καθίσταται επιτακτική ανάγκη για τους ιδιοκτήτες και τους χειριστές να αξιοποιήσουν τη σωστή διαμόρφωση στη συσκευή τους.

1.4.2 Αυξητική τάση των επιθέσεων σε PLC

Αξιοποιώντας τα στοιχεία που αναφερθήκαμε στο κεφάλαιο 6 καθώς και παραπάνω παρατηρούμε μια αυξητική τάση των επιθέσεων σε συστήματα PLC. Οι πρώτες αναφορές έγιναν γνωστές το 1997 όπου και αναφέρθηκαν μόλις 2 ευπάθειες . Από τότε η εκθετική αύξηση των ευπαθειών ανά περίοδο χρόνου είναι σημαντική. Κάθε χρόνο πάνω 150 ευπάθειες αναφέρονται σύμφωνα με την έρευνα της Kaspersky. **Γράφημα [1]**



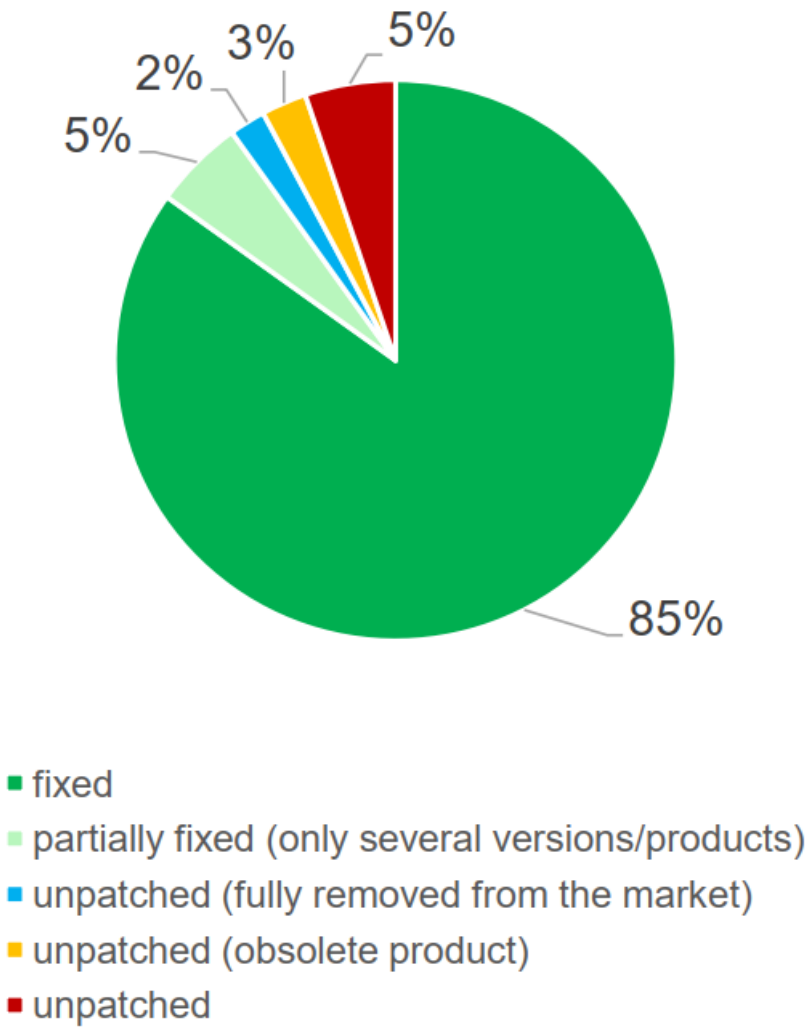
Γράφημα 1 Ευπάθειες σε σύστημα ICS/PLC ανά χρόνο [Kaspersky]

1.4.3 Διορθώσεις Σφαλμάτων

Υπάρχουν πολλές ευπάθειες ήδη γνωστές στους κατασκευαστές, αλλά παρασχέθηκαν στους ιδίους μέσω ιδιωτικής έρευνας. Τέτοιες ευπάθειες δεν δημοσιεύονται αυτή τη στιγμή επειδή οι αντίστοιχες διορθώσεις σφαλμάτων δεν έχουν ακόμη κυκλοφορήσει. Εκτός αυτού, ορισμένα ελαττώματα ασφαλείας δεν αναγνωρίζονται επίσημα από τους κατασκευαστές ως τρωτά σημεία, ωστόσο αυτές οι ιδιαιτερότητες θα μπορούσαν ακόμα να χρησιμοποιηθούν από τους επιτιθέμενους.

Αν λάβουμε υπόψιν τα δεδομένα από την ICS-CERT, οι κατασκευαστές μπορέσαν να αναπτύξουν νέες διορθώσεις σφαλμάτων και νέα υλικολογισμικό για μόλις το 85% τον δημοσιευμένων ευπαθειών. Εδώ πρέπει να τονίσουμε το 5% αυτού του ποσοστού δεν

είχε πλήρως διορθωθεί. Οι διορθώσεις σφαλμάτων αφορούσαν συγκεκριμένες εκδόσεις υλικολογισμικού και συγκεκριμένα προϊόντα. **Γράφημα [2]**



Γράφημα 2 Διορθώσεις σφαλμάτων σε σύστημα ICS/PLC [Kaspersky]

Κεφάλαιο 2
SCADA

2.1 Συνοπτική Αναφορά στα SCADA

Στη σύντομη ιστορία των συστημάτων SCADA κατασκευάστηκαν για πρώτη φορά στα τέλη της δεκαετίας του 1950, πολλές από τις σημερινές λειτουργίες τους δεν ήταν δυνατές ή ήταν πολύ περιορισμένες.

Μία από τις βασικές διαδικασίες των SCADA είναι η δυνατότητα παρακολούθησης ενός ολόκληρου συστήματος σε πραγματικό χρόνο. Αυτό συμβαίνει μέσω απόκτησης δεδομένων (**data collection**). Έπειτα τα συλλεγόμενα δεδομένα κοινοποιούνται σε χρονικά διαστήματα ανάλογα με το σύστημα που έχουν συλλεχθεί οι πληροφορίες.

Τα πρώτα συστήματα SCADA είχαν γρήγορα υψηλή ζήτηση από κατασκευαστές σε διάφορες βιομηχανίες όπως η ναυτιλία. Ωστόσο, καθώς τα SCADA υιοθετήθηκαν ευρύτερα, οι κατασκευαστές άρχισαν να πιέζουν τους προμηθευτές RTU για να βελτιώσουν τα πρωτόκολλα επικοινωνίας των συστημάτων τους. Αυτή η ώθηση για βελτιώσεις οδήγησε στην εξέλιξη των SCADA και εγκαινίασε τις επόμενες γενιές εξέλιξης που θα δούμε παρακάτω.[12]

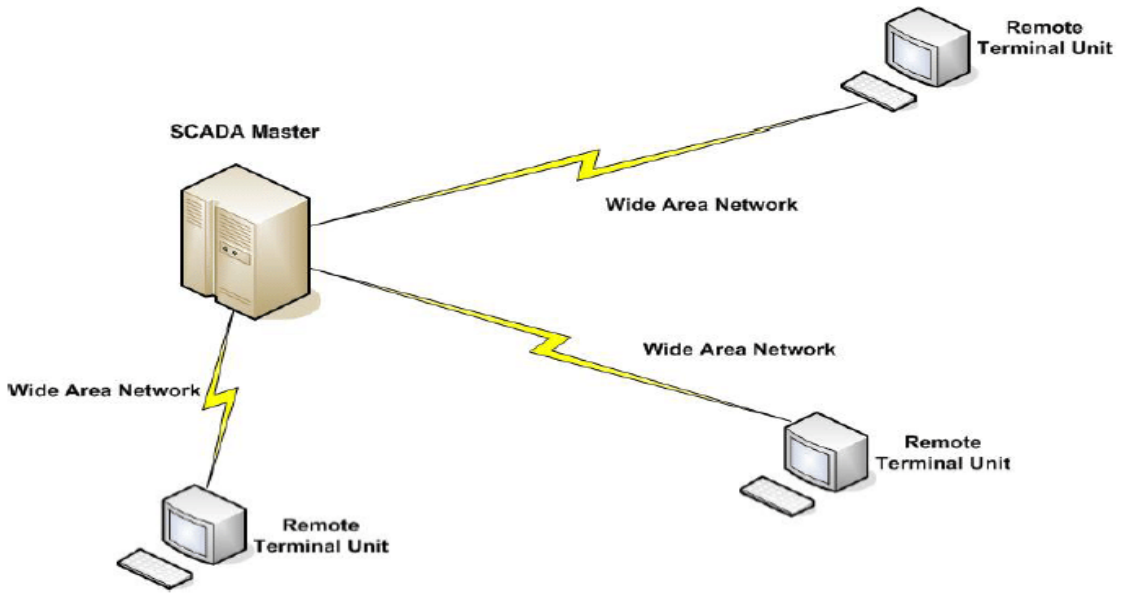
2.1.1 Πρώτη γενιά - Monolithic SCADA

Το αρχικό σύστημα SCADA δημιουργήθηκε σε μια εποχή όπου δεν υπήρχαν δίκτυα και τα πρώτα συστήματα SCADA δεν είχαν σχεδιαστεί για σύνδεση με άλλα συστήματα.

Τα πρώτα SCADA βασίστηκαν σε συστήματα mainframe, τα οποία δεν είχαν καθόλου δυνατότητες δικτύωσης. Λόγω των περιορισμένων δυνατοτήτων δικτύωσης, η πρώτη γενιά συστημάτων SCADA δεν μπόρεσε να διασυνδεθεί μεταξύ τους, καθιστώντας τα, αυτόνομα συστήματα.

Εκείνη τη χρονική στιγμή, τα πρωτόκολλα που χρησιμοποιούμε σήμερα για τα δίκτυα WAN δεν ήταν διαθέσιμα, ωστόσο, τα πρωτόκολλα επικοινωνίας ήταν διαθέσιμα και αναπτύχθηκαν από διάφορους κατασκευαστές RTUs που όμως μπορούσαν να χρησιμοποιηθούν από τους δικούς τους υπολογιστές. [13], [14]

Τέλος, τα πρωτόκολλα ήταν σε θέση μόνο να επιτρέπουν σάρωση, έλεγχο και ανταλλαγή δεδομένων μεταξύ του κυρίου υπολογιστή (master computer) και των αισθητήρων και των εισόδων RTU. **Εικόνα [8]**



Εικόνα 8 Αναπαράσταση Πρώτης γενιάς Scada-Monolithic

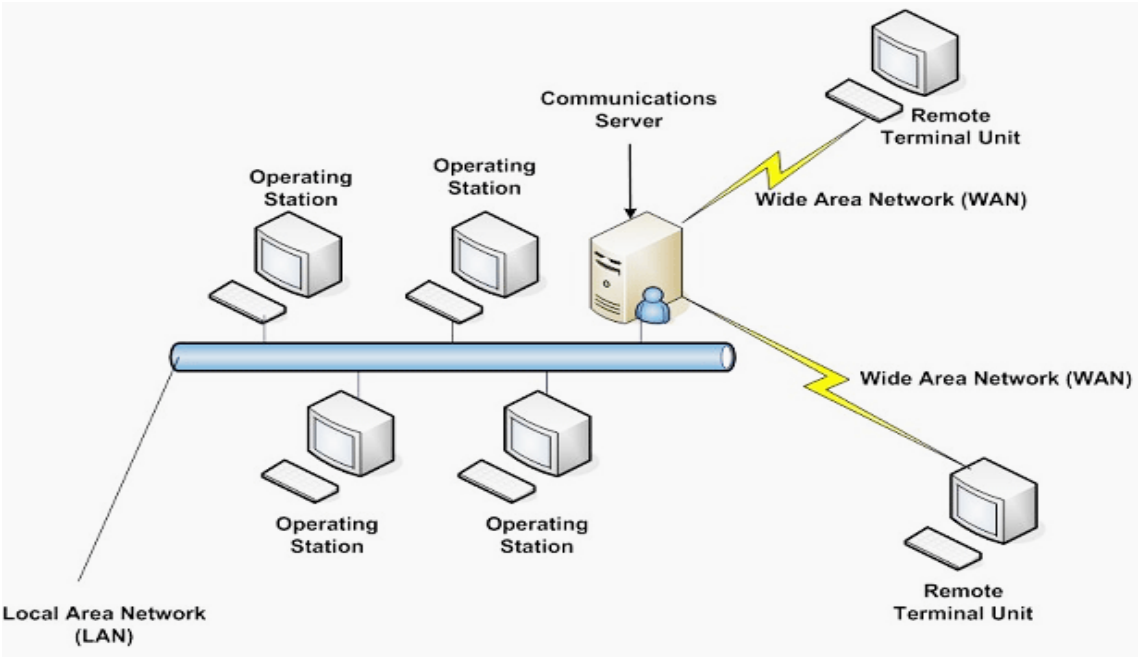
2.1.2 Δεύτερη γενιά - Distributed SCADA

Η επόμενη γενιά συστημάτων SCADA εκμεταλλεύτηκε τις εξελίξεις και τη βελτίωση των συστημάτων καθώς και της τεχνολογίας (LAN). Διαφορετικοί σταθμοί, ο καθένας με διαφορετικές λειτουργίες , συνδέθηκαν σε ένα LAN και μοιράστηκαν πληροφορίες μεταξύ τους σε πραγματικό χρόνο.

Η κατανομή μεμονωμένων λειτουργιών SCADA σε πολλά συστήματα παρείχε περισσότερη ισχύ επεξεργασίας στο σύνολό του συστήματος από ό,τι θα ήταν σε μεμονωμένο. Τα δίκτυα που συνέδεαν αυτά τα μεμονωμένα συστήματα βασίζονταν γενικά σε πρωτόκολλα LAN και δεν ήταν σε θέση να φτάσουν πέρα από τα όρια του τοπικού περιβάλλοντος. [13], [14]

Μερικά από τα πρωτόκολλα LAN που χρησιμοποιήθηκαν ήταν ιδιόκτητου χαρακτήρα, όπου ο κατασκευαστής δημιούργησε δικό του πρωτόκολλο δικτύου. Αυτό επέτρεψε στον κατασκευαστή ναι μεν να βελτιστοποιήσει το πρωτόκολλο LAN για κίνηση σε

πραγματικό χρόνο (real time traffic), αλλά περιόρισε ουσιαστικά τη σύνδεση δικτύου με άλλους κατασκευαστές SCADA (συμβατότητα μεταξύ των συσκευών). **Εικόνα [9]**



Εικόνα 9 Αναπαράσταση Δεύτερης Γενιάς Scada- Distributed

2.1.3 Τρίτη γενιά - Network SCADA

Η τρίτη γενιά αρχιτεκτονικής SCADA σχετίζεται στενά με αυτήν της δεύτερης γενιάς, με την κύρια διαφορά να είναι αυτή της αρχιτεκτονικής ανοιχτού συστήματος και όχι ενός ελεγχόμενου περιβάλλοντος «χτισμένο» από τους κατασκευαστές.

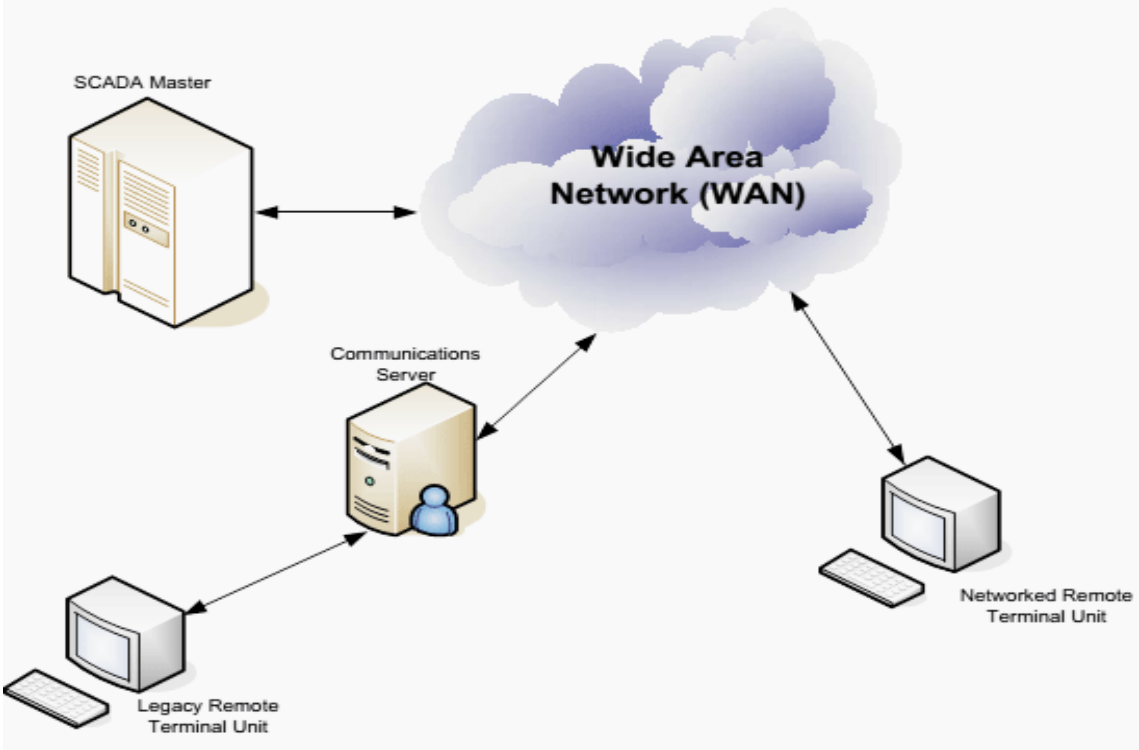
Η σημαντική βελτίωση της τρίτης γενιάς είναι αυτή του ανοιχτού συστήματος, χρησιμοποιώντας ανοιχτά πρότυπα και πρωτόκολλα και καθιστώντας δυνατή, τη διανομή της λειτουργικότητας SCADA πλέον σε WAN και όχι μόνο σε ένα LAN.

Τα ανοιχτά πρότυπα εξαλείφουν έναν αριθμό από τους περιορισμούς των προηγούμενων γενεών συστημάτων SCADA. Η χρήση συστημάτων εκτός του κατασκευαστή διευκολύνει τον χρήστη στο συνδέει περιφερειακές συσκευές τρίτων (όπως οθόνες, εκτυπωτές, μονάδες δίσκου, μονάδες ταινιών κ.λπ.) στο σύστημα και στο δίκτυο. [13], [14]

Αφού πλέον έχουν μετακινηθεί σε συστήματα «ανοιχτού» τύπου οι κατασκευαστές των SCADA σταδιακά αποχώρησαν από την επιχείρηση ανάπτυξης υλικού και την ανάθεσή

τους ανάλαβαν εταιρείες όπως, Compaq, Hewlett-Packard και Sun Microsystems λόγω της εμπειρίας τους, στην ανάπτυξη λογισμικού λειτουργικού.

Η σημαντική βελτίωση στα συστήματα SCADA τρίτης γενιάς προέρχεται από τη χρήση πρωτοκόλλων WAN όπως το Πρωτόκολλο Διαδικτύου (IP) για την επικοινωνία μεταξύ του κύριου σταθμού και του υπόλοιπου εξοπλισμού. **Εικόνα [10]**



Εικόνα 10 Αναπαράσταση Τρίτης Γενιάς Scada- Network

Υπάρχουν δύο τύποι κίνησης IP: Το Πρωτόκολλο ελέγχου Μετάδοσης (TCP) και Πρωτόκολλο Δεδομένων Χρήστη (UDP). Από τα δύο, το TCP είναι το πιο συχνά χρησιμοποιούμενο πρωτόκολλο για συστήματα SCADA. Ο λόγος για αυτό είναι το TCP προσφέρει διόρθωση σφαλμάτων. Όπου το πρωτόκολλο TCP χρησιμοποιείται υπάρχει «εγγυημένη παράδοση». Αυτό οφείλεται εν μέρει σε μια μέθοδο που ονομάζεται «έλεγχος ροής» που καθορίζει πότε πρέπει να σταλούν ξανά τα δεδομένα και σταματά τη ροή δεδομένων έως ότου τα προηγούμενα πακέτα έχουν μεταφερθεί με επιτυχία. Εάν αποστέλλεται για παράδειγμα ένα πακέτο δεδομένων, μπορεί να συμβεί ¨σύγκρουση¨ ή σφάλμα στις επικοινωνίες. Όταν συμβαίνει αυτό, το RTU / Client ζητά ξανά το πακέτο από τον κεντρικό υπολογιστή / διακομιστή μέχρι ολόκληρο το πακέτο να είναι πλήρες και ίδιο με το πρωτότυπο. [13], [14]

Το UDP από την άλλη είναι ένα πρωτόκολλο που χρησιμοποιείται και αυτό στο διαδίκτυο. Ωστόσο, το UDP δεν πρέπει να χρησιμοποιείται αποστολή σημαντικών δεδομένων, όπως Custody Transfer Δεδομένα μέτρησης, πληροφορίες βάσης δεδομένων, κ.λπ. Το UDP είναι το πιο κατάλληλο για ροή ήχου και βίντεο. Μέσα ροής όπως JPEGS, Windows Media αρχεία ήχου (.WMA), Real Player (.RM) και άλλα χρησιμοποιήστε το UDP επειδή προσφέρει την επιθυμητή μετάδοση ταχύτητες. Το UDP είναι ταχύτερο από το TCP επειδή υπάρχει καμία μορφή ελέγχου ροής ή διόρθωσης σφαλμάτων. Ωστόσο, τα δεδομένα που αποστέλλονται μέσω του Διαδικτύου θα επηρεαστούν από συγκρούσεις και θα εμφανιστούν σφάλματα. Θυμηθείτε ότι το UDP αφορά μόνο την ταχύτητα και όχι την ποιότητα. Αυτό είναι κυρίως γιατί τα μέσα ροής δεν είναι υψηλής ποιότητας. **Πίνακας [4]**

TCP vs UDP

Attributes	TCP	UDP
Acronym For	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Packet ordering	TCP rearranges data packets in the order specified.	UDP does not order packets. If ordering is required, it has to be managed by the application layer.
Error-checking	Yes	No
Header size	20 bytes	8 bytes
Usage	Non time-critical applications	Fast transmission of data: This is great for Streaming video or pushing JPEGs
Function	As a message makes its way across the Internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.
'Weight'	Three packets required to set up a socket connection before any user data can be sent. TCP handles reliability and congestion control.	Lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
Streaming of Data	Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.	Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.
Speed of Transfer	TCP is slower than UDP	UDP is faster because there is no error-checking for packets.
Data Reliability	There is an absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent will reach at all.

Πίνακας 4 Διαφορών TCP vs UDP

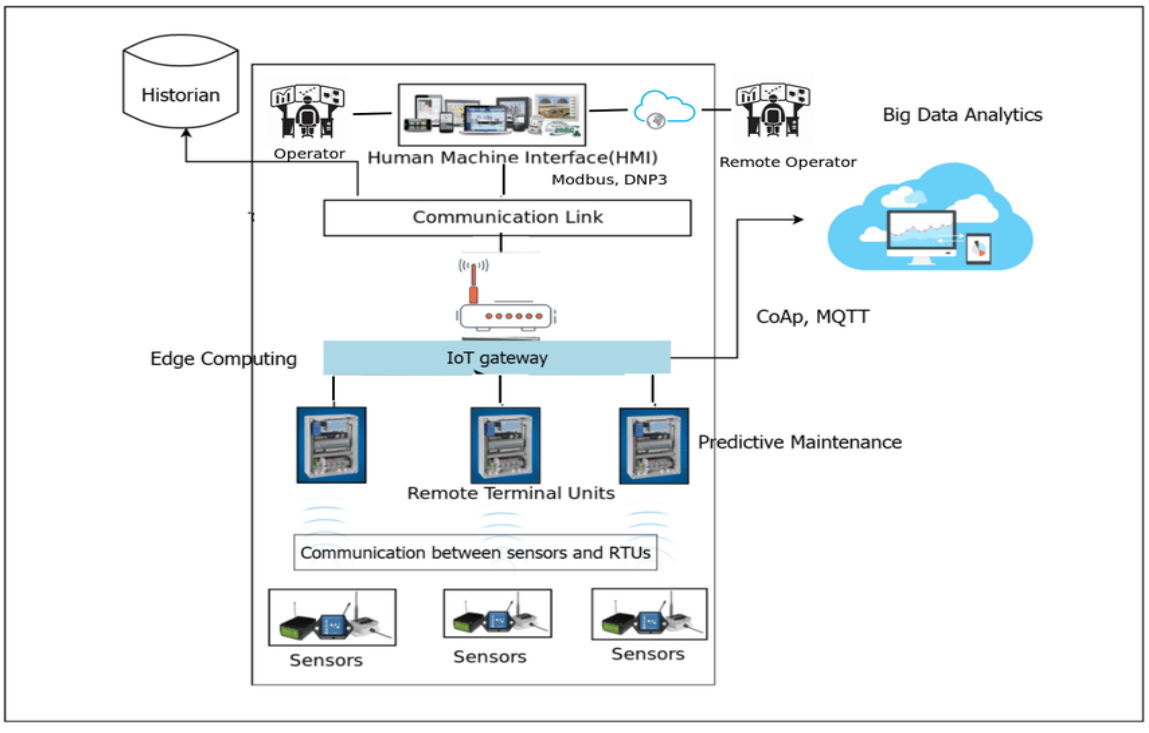
2.1.4 Τέταρτη γενιά – Internet of Things (IOT) SCADA

Η τέταρτη γενιά συστημάτων ελέγχου και απόκτησης δεδομένων εποπτείας (SCADA) οφείλεται κυρίως στην πρόοδο του cloud computing και στη συνεχή ανάπτυξη του Internet of Things (IoT). Χρησιμοποιώντας τεχνολογίες IoT και cloud computing όπως το

Web HMI και HTML5, τα συστήματα SCADA τέταρτης γενιάς μπορούν να αναφέρουν την κατάσταση σε πραγματικό χρόνο από απομακρυσμένους ιστιοτόπους που εξαπλώνονται σε μεγάλες αποστάσεις, καθώς και να εκμεταλλευτούν το cloud computing για την εφαρμογή πολύ πιο προηγμένων αλγορίθμων ελέγχου. Η ασφάλεια για τα συστήματα SCADA έλαβε επίσης τεράστια αύξηση, χάρη στις ανησυχίες ασφάλειας για το Διαδίκτυο των πραγμάτων (IoT) και του cloud computing. Αυτό με τη σειρά του έχει δει πολλούς κατασκευαστές να υιοθετούν μια προσέγγιση «ασφαλείας-σχεδιασμού» στα συστήματα SCADA. [13], [14]

Το IOT προσθέτει αξία και επεκτείνει τα SCADA και την αλυσίδα αξίας του κάνοντας τις επιχειρήσεις πιο προβλέψιμες, μειώνοντας το κόστος, την σπατάλη και βελτιώντας την κερδοφορία. Πληροφορίες που δημιουργήθηκαν από το SCADA κάνουν τα συστήματα να ενεργούν ως μία από τις πηγές δεδομένων για το IoT. Το SCADA επικεντρώνεται στην παρακολούθηση και τον έλεγχο ενώ με την εστίαση στο IoT παρέχετε σταθερότητα στην Ανάλυση δεδομένων για τη βελτίωση της παραγωγικότητας της επιχείρησης.

Σε τυπικά συστήματα μη-IoT SCADA, τα δεδομένα αποθηκεύονται σε συγκεκριμένες προγραμματιζόμενες διευθύνσεις μνήμης. Ωστόσο, όταν χρησιμοποιούνται τα συστήματα SCADA με ενσωματωμένες τεχνολογίες IoT, τα δεδομένα ενδέχεται να προέρχονται από ένα πλήθος διαφορετικών αισθητήρων, βάσεων δεδομένων και ελεγκτών. **Εικόνα [11]**



Εικόνα 11 Αναπαράσταση Τρίτης Γενιάς Scada- Internet Of Things (IOT)

Εάν κάποιος ρίξει μια πιο προσεκτική ματιά στον τρόπο εφαρμογής και λειτουργίας του SCADA, μπορούμε να δούμε κάποια στοιχεία του IoT – όπως ο εποπτικός έλεγχος και η απόκτηση δεδομένων. Μπορούμε να πούμε με ασφάλεια ότι το SCADA αντιπροσωπεύει μερικούς από τους πυλώνες στους οποίους το Διαδίκτυο των πραγμάτων έχει κατασκευαστεί. Ωστόσο, σε κάθε νέο στάδιο μετάβασης, πρέπει να γνωρίζουμε τις δυνατότητες και τους περιορισμούς των SCADA: [15]

a) Τα συστήματα SCADA δεν είναι κλιμακούμενα. Το Διαδίκτυο των πραγμάτων έχει τη δυνατότητα να φέρει και να επεξεργάζεται μεγάλες ποσότητες δεδομένα από πράγματα και μηχανές. Το IoT επιτρέπει σε οποιαδήποτε εταιρεία να συνδέσει οποιαδήποτε συσκευή και υπηρεσίες τρίτων. Όλα τα δεδομένα συλλέγονται σε μια πλατφόρμα IoT, προσβάσιμα με ασφάλεια με διαπιστευτήρια σύνδεσης. Αρκετά άτομα από εταιρείες και οι βιομηχανίες μπορούν να έχουν πρόσβαση στα δεδομένα (ή σε ΄να υποσύνολο δεδομένων ή υποσύνολο συσκευών). Ακόμα και στο cloud, μπορούν να δημιουργηθούν και να χρησιμοποιηθούν νέοι πόροι.

b) Τα SCADA είναι συστήματα που χρησιμοποιούνται για καθημερινές λειτουργίες σε μια αίθουσα ελέγχου ή παρόμοια. Ωστόσο, δεν υπάρχουν δεδομένα ανάλυσης για έλεγχο της απόδοσης, ενσωμάτωση αυτών με CRM ή ERP λογισμικό από την άλλη πλευρά, το IoT προσφέρει την ανάλυση δεδομένων, την επεξεργασία Big Data δεδομένων, όπως αλγόριθμοι AI, ML και προγνωστικά.

c) Πρωτόκολλα όπως OPC, OPC-UA και άλλα είναι τα πρότυπα σήμερα στον κλάδο. Επιπλέον, στο IoT υπάρχουν δεκάδες άλλα πρωτόκολλα που μπορούν να βοηθήσουν τις βιομηχανίες να συνδεθούν ή να λαμβάνουν ειδοποιήσεις σε πραγματικό χρόνο. Τα MQTTS, HTTPS ή CoaP με TLS μπορούν να βοηθήσουν τις βιομηχανίες να δημιουργήσουν ένα επίπεδο ασφαλείας που απαιτείται για την κρυπτογράφηση των μηνυμάτων και των πληροφορίων.

d) Η ενοποίηση μεταξύ συσκευών και κατασκευαστών δεν είναι εύκολη στα συστήματα SCADA. Συνήθως στον οικιακό αυτοματισμό, οι οργανισμοί πρέπει να

διαθέτουν συσκευές από τον ίδιο κατασκευαστή με την ίδια έκδοση όπως είχαμε πει ότι ίσχυε στις προηγούμενες γενιές. Εάν αυτό δεν συμβεί, συνήθως είναι σχεδόν αδύνατο να ενσωματώσουμε εύκολα συσκευές στο τρέχον SCADA. Δηλαδή δεν υπάρχει παρουσία οριζόντιας πλατφόρμας που λειτουργεί σε όλες τις συσκευές. Από την άλλη πλευρά, στο IoT αυτό είναι ένα από τα πιο ευεργετικά χαρακτηριστικά για μια βιομηχανία. Τα τυπικά πρωτόκολλα όπως το MQTT επιτρέπουν στις πλατφόρμες να επικοινωνούν μεταξύ τους ακόμα και αν υπάρχει διαφορετικός προμηθευτής.

e) Τέλος, το IoT φέρνει επανάσταση στο SCADA προσφέροντας περισσότερη τυποποίηση και διαφάνεια. Το IoT παρέχει επίσης επεκτασιμότητα, διαλειτουργικότητα και βελτιωμένη ασφάλεια εισάγοντας την ιδέα της πλατφόρμας IoT. Ουσιαστικά, χρησιμοποιούνται και οι δύο πλατφόρμες να αυξάνοντας τη συνολική παραγωγικότητα ενσωματώνοντας την ¨έξυπνη συντήρηση¨ εξασφαλίζοντας , την αύξηση της αποτελεσματικότητας, την μείωση του χρόνου διακοπής λειτουργίας και της παράτασης της διάρκειας ζωής του εξοπλισμού.

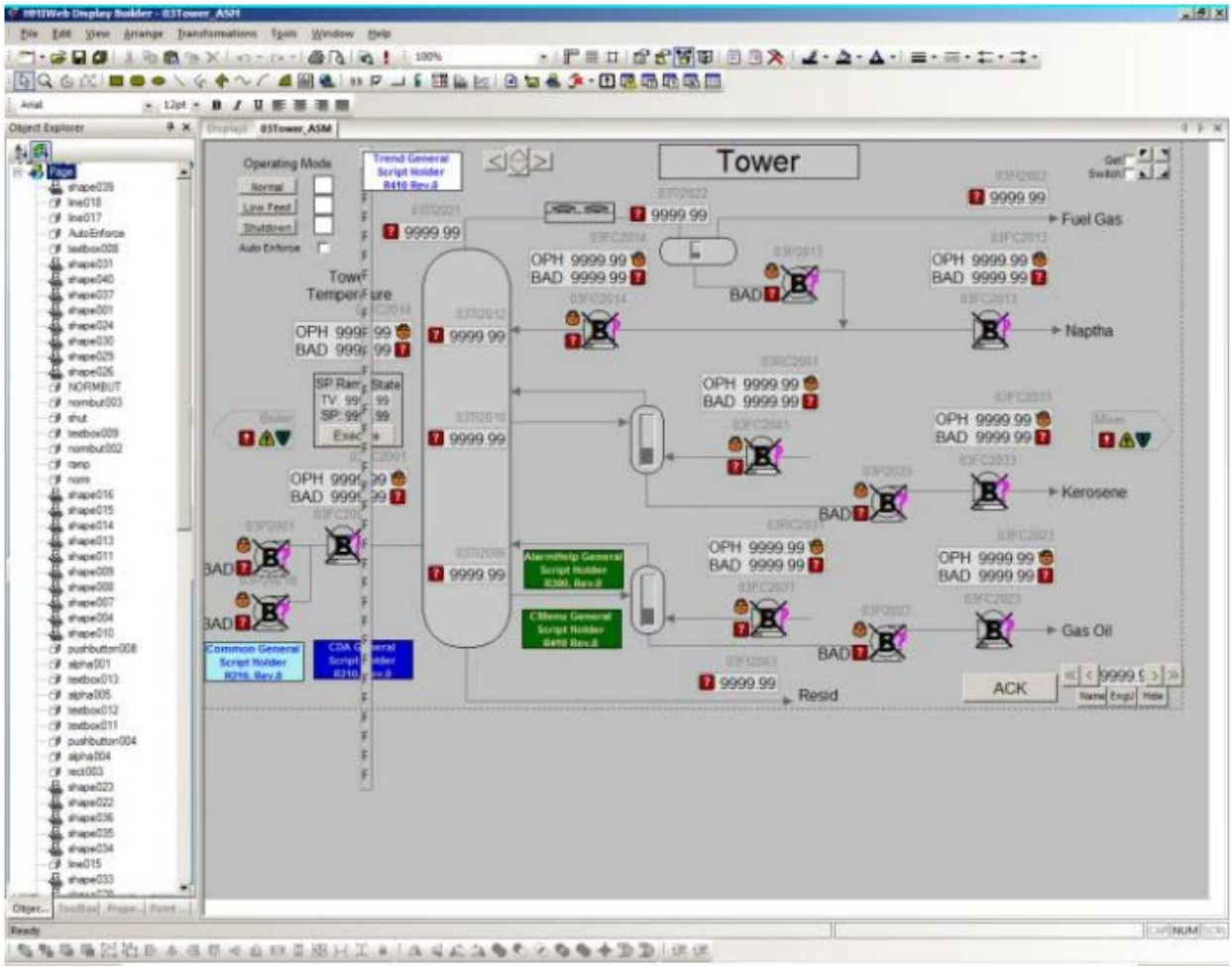
2.2 Κατασκευαστές συστημάτων SCADA

Το παγκόσμιο μέγεθος της αγοράς SCADA εκτιμήθηκε στα 27.900 εκατομμύρια δολάρια το 2016 και αναμένεται να φθάσει τα 41.603 εκατομμύρια δολάρια έως το 2023, αυξάνοντας το CAGR (Compound Annual Growth Rate) σε 6,00% από το 2017 έως το 2023. Οι συνεχιζόμενες τεχνολογικές εξελίξεις στο SCADA λόγω καινοτόμων προσπαθειών από τους παράγοντες της αγοράς έχουν βελτιώσει περαιτέρω την αποτελεσματικότητα του συστήματος, το οποίο είναι ευκαιριακό για την αγορά. Παρακάτω είναι τέσσερεις από τους βασικούς vendors της αγοράς SCADA. [16]

2.2.1 Honeywell

Το **Experion** SCADA, μια διαισθητική και επεκτάσιμη λύση, βρίσκεται στο επίκεντρο των συστημάτων ελέγχου και απόκτησης δεδομένων (SCADA) της Honeywell. Με εντυπωσιακές ενσωματωμένες δυνατότητες, η λύση εξασφαλίζει αξιοπιστία, ασφάλεια και προστασία. Μαζί με το **Experion** SCADA, ο ελεγκτής παρέχει μια ολοκληρωμένη λύση

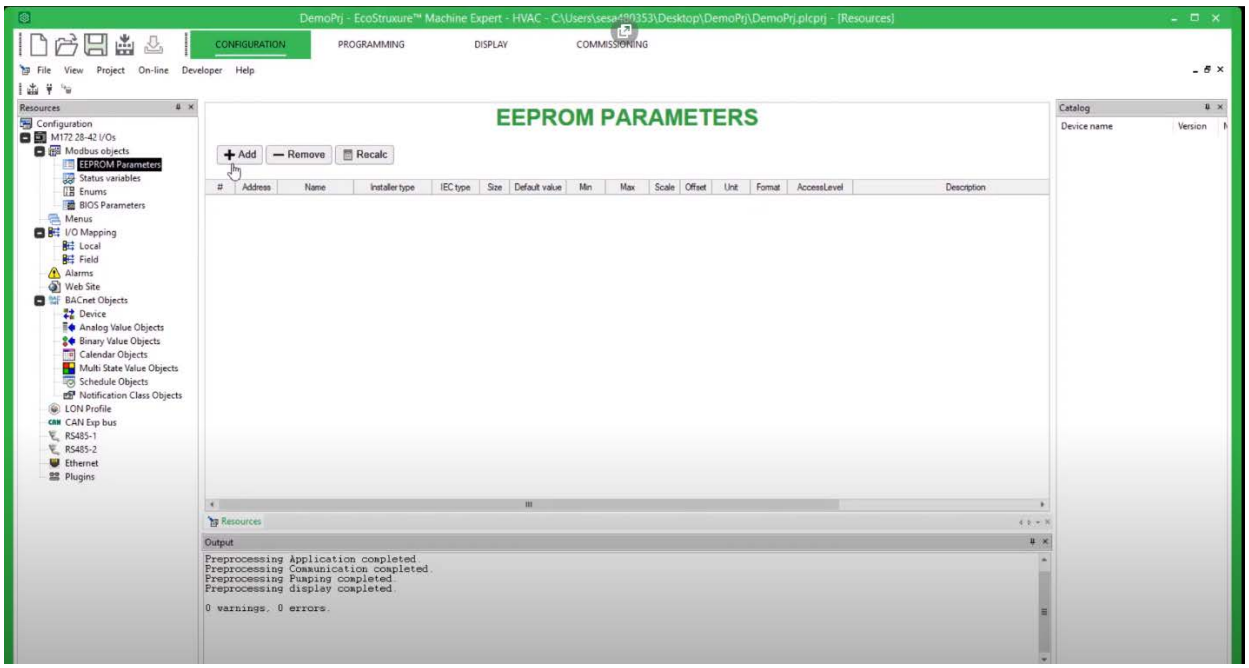
για την επίλυση σύνθετων απαιτήσεων απομακρυσμένου αυτοματισμού, ειδικά εκείνων που βρίσκονται στη βιομηχανία της ναυτιλίας και του πετρελαίου. Έτσι βελτιώνει την ασφάλεια και την αξιοπιστία της επιχείρησης, παρέχει διαισθητικό έλεγχο, βελτιώνει την αποτελεσματικότητα του χειριστή και διασφαλίζει τη βέλτιστη ευελιξία με το DSA. προσφέροντας βελτιωμένη αποτελεσματικότητα στο χειριστή. **Εικόνα [12]**



Εικόνα 12 HMIWeb Display Builder μέσω του EXPERION

2.2.2 Schneider Electric

Η Schneider Electric παρέχει ψηφιακές λύσεις ενέργειας και αυτοματισμού για αποδοτικότητα και βιωσιμότητα. Συνδυάζουν ενεργειακές τεχνολογίες, αυτοματισμό σε πραγματικό χρόνο, λογισμικό και υπηρεσίες σε ολοκληρωμένες λύσεις για σπίτια, κτίρια, κέντρα δεδομένων, υποδομές και βιομηχανίες. Το **Ecostracture** δίνει την δυνατότητα να αξιοποιήσει ο χρηστής όλες τις συνδεδεμένες συσκευές, να συλλέξει πληροφορίες και να αποθηκεύσει δεδομένα καθώς και να έχει κα την δυνατότητα να κάνει τοπική ανάλυση της συσκευής. **Εικόνα [13]**



Εικόνα 13 Ecostacrure Demo Display Options

2.2.3 ABB & Hitachi

Έπειτα από ένωση των Hitachi και ABB το 2020 στον τομέα της ενέργειας παρουσιάζει αξιομίμητα καινοτομικά στοιχεία . Ο συνδυασμός των δυο εταιρειών με πάνω από ένα αιώνα καινοτομίας τους δίνει ένα προβάδισμα στην παγκόσμια αγορά. Η σειρά **MicroscadaX** παρέχει ένα ισχυρό, μοντέρνα αποτελεσματική εμπειρία για το έλεγχο δικτύου και διαχείριση διανομής. Το **MicroSCADA X** κρατά τον έλεγχο του
Σύστηματος διανομής οπουδήποτε και οποτεδήποτε. Παρέχει ευέλικτη λειτουργικότητα SCADA και σύγχρονο σύστημα διαχείρισης διανομής (DMS) ενσωματωμένη στο ίδιο σύστημα. Μπορεί ο χρήστης να ελέγξει τη διαδικασία , να διαχειριστεί τα πληρώματά και παρέχετε εξυπηρέτηση με ένα μόνο σύστημα. **Εικόνα [14]**

Εικόνα 14 MicroScada X monitoring solar panels.

2.2.4 Siemens

Η Siemens και με **το SIMATIC WinCC**, επιλέγει ένα καινοτόμο, επεκτάσιμο σύστημα οπτικοποίησης των διαδικασιών με λειτουργίες υψηλής απόδοσης για την παρακολούθηση αυτοματοποιημένων διαδικασιών. Είτε σε ένα σύστημα ενός χρήστη είτε σε ένα κατανεμημένο σύστημα πολλαπλών χρηστών με περιττούς διακομιστές και επωφελείται από ένα ανοιχτό σύστημα που προσφέρει πλήρη λειτουργικότητα για όλους τους κλάδους και για πολύπλοκες εργασίες οπτικοποίησης. Η λειτουργικότητα των συστημάτων μπορεί να επεκταθεί περαιτέρω με τη χρήση επιλογών και πρόσθετων για επιλογές **WinCC** ή πολλαπλών SCADA**.** **Εικόνα [15]**

Εικόνα 15 Simatic WinCC Open Architecture Demo.

2.3 Λογισμικό συστημάτων SCADA

Τα συστήματα SCADA βρίσκονται στο επίκεντρο των διαδικασιών και χρησιμοποιούνται και την βιομηχανία της ναυτιλίας, για τον έλεγχο μηχανημάτων και μηχανών. Επειδή τα συστήματα SCADA παίζουν σημαντικούς ρόλους σε πολύ κρίσιμες διαδικασίες, μια ανεξέλεγκτη αδυναμία θα μπορούσε να προκαλέσει σοβαρές συνέπειες. Παρακάτω παραθέτουμε μερικές από αυτές τις ευπάθειες, ανά κατασκευαστή SCADA όπως επιγραμματικά αναφέρονται στον ιστότοπο **cvedetails.com** καθώς και το λογισμικό των κατασκευαστών αυτών θέλοντας να επισημάνουμε, ότι συστήματα όπως τα SCADA μαστίζονται από ανασφαλή ανάπτυξη και αργή διόρθωση.

2.3.1 Honeywell Exprerion

a. Επιτρέπει σε απομακρυσμένους, μη εξουσιοδοτημένους εισβολείς να εκτελούν αυθαίρετο κώδικα σε ένα ευάλωτο σύστημα. [16]
b. Υπάρχει μια αυθαίρετη ευπάθεια εγγραφής μνήμης στη μονάδα dual_onsrv.exe που θα μπορούσε να οδηγήσει σε πιθανή εκτέλεση απομακρυσμένου κώδικα ή άρνηση υπηρεσίας. [16]

c. Υπάρχει μια ευπάθεια διασταύρωσης καταλόγου στη μονάδα confd.exe, η οποία θα μπορούσε να οδηγήσει σε πιθανή αποκάλυψη πληροφοριών. [16]

d. Υπάρχει μια ευπάθεια συμπερίληψης αρχείων στη μονάδα confd.exe, η οποία θα μπορούσε να οδηγήσει στην αποδοχή αυθαίρετου αρχείου στη συνάρτηση και πιθανή αποκάλυψη πληροφοριών ή απομακρυσμένη εκτέλεση κώδικα.[16]

2.3.2 Schneider Electric EcoStruxure

a. Τα προϊόντα λογισμικού βρέθηκαν να έχουν ευπάθειες.

b. Θα μπορούσε ενδεχομένως να επιτρέψει μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς ή απομακρυσμένη εκτέλεση κώδικα. [17]

c. Ο επιτιθέμενος πρέπει να κάνει έναν χρήστη να ανοίξει ένα μολυσμένο αρχείο έργου για να εκμεταλλευτεί αυτήν την ευπάθεια. [17]

d. Ένας απομακρυσμένος εισβολέας μπορεί να εξαπατήσει έναν χρήστη να ανοίξει ένα ειδικά κατασκευασμένο αρχείο έργου. Στη συνέχεια, ο εισβολέας αποκτά μη εξουσιοδοτημένη πρόσβαση εγγραφής στο σύστημα προορισμού. [17]

e. Οι επιτιθέμενοι πρέπει να κάνουν τους χρήστες να επισκέπτονται μια κακόβουλη ιστοσελίδα ή να ανοίγουν ένα κακόβουλο αρχείο. [17]

f. Μπορεί να οδηγήσει σε αυθαίρετη εκτέλεση εφαρμογών κατά την εκκίνηση του υπολογιστή. [17]

2.3.3 ABB MicroSCADA X

a. Ορισμένοι ελεγκτές είναι επιρρεπείς σε επίθεση άρνησης υπηρεσίας λόγω μιας πλημμύρας πακέτων δικτύου. [18]

2.3.4 Siemens WinCC

a. Ένας εισβολέας πρέπει να πιστοποιηθεί με έναν έγκυρο λογαριασμό χρήστη. Η ευπάθεια ισχύει μόνο για σενάρια όπου η πρόσβαση μέσω της διεπαφής Ιστού είναι εφικτή για έναν εισβολέα ενώ η πρόσβαση στη δομή καταλόγου δεν είναι. [19]

b. Το ελάττωμα θα μπορούσε να επιτρέψει απομακρυσμένη εκτέλεση κώδικα για μη εξουσιοδοτημένους χρήστες, εάν αποστέλλονται ειδικά πακέτα στον διακομιστή WinCC. [19]

c. Θα μπορούσε να επιτρέψει σε έναν μη εξουσιοδοτημένο εισβολέα να εξαγάγει αυθαίρετα αρχεία από τον διακομιστή WinCC στέλνοντας ειδικά κατασκευασμένα πακέτα στον διακομιστή. Ωστόσο, για να εκμεταλλευτεί αυτό το ελάττωμα, ο εισβολέας πρέπει να έχει πρόσβαση στο δίκτυο στο επηρεαζόμενο σύστημα.[19]

2.3.5 Trend Micro έρευνα SCADA

Όπως είδαμε και παραπάνω οι επιθέσεις σε συστήματα SCADA έχουν τη δυνατότητα να επηρεάσουν ένα ευρύ φάσμα συστημάτων και πολλά κομμάτια κρίσιμης υποδομής. Αξιόλογη έρευνα που πρέπει να αναφέρουμε είναι από την Trend Micro με πολλά και ενδιαφέροντα στοιχεία. [20]

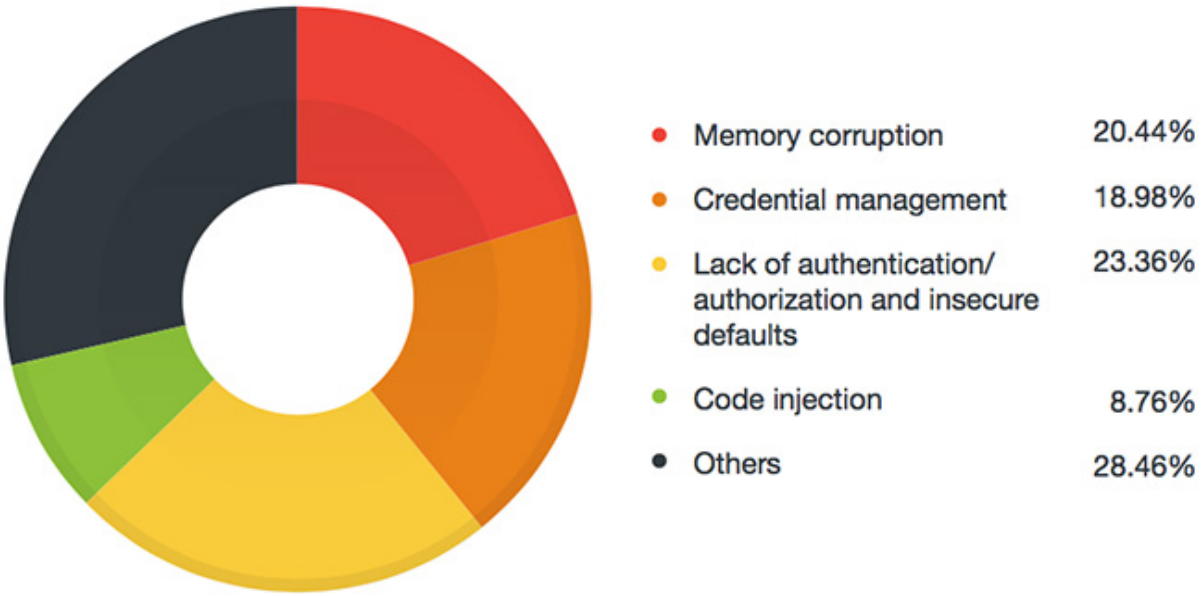
Οι ερευνητές της Trend Micro εξέτασαν τις συμβουλές του ICS-CERT από το 2015 και το 2016 που ασχολούνταν με τις ευπάθειες των HMI και έχουν καταγράψει πάνω από 250 επιθέσεις zero day που αποκτήθηκαν μέσω τους προγράμματος ZDI. Σε αυτήν την έρευνα βρήκαν ότι: [20]

i. Περίπου το 20% των αναγνωρισμένων τρωτών σημείων είναι ζητήματα αλλοίωσης μνήμης (ζητήματα ασφαλείας κώδικα όπως υπερχείλιση buffer που βασίζονται σε στοίβα και σωρούς και ευπάθειες ανάγνωσης / εγγραφής εκτός ορίου).

ii. Το 19% είναι ζητήματα διαχείρισης διαπιστευτηρίων (κωδικοποιημένοι κωδικοί πρόσβασης, κωδικοί πρόσβασης αποθηκευμένοι σε καθαρό κείμενο- clear text , κρυμμένοι λογαριασμοί υποστήριξης με πλήρη δικαιώματα κ.λπ.).

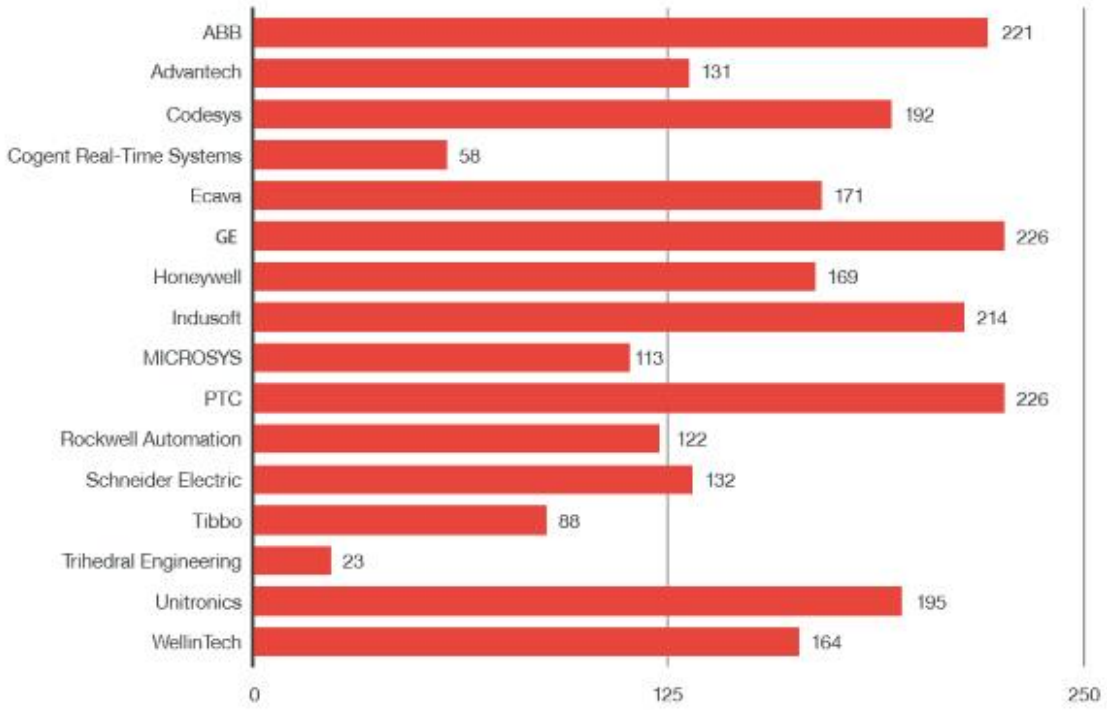
iii. Το 23% είναι ζητήματα που συνδέονται με την έλλειψη ελέγχου ταυτότητας / εξουσιοδότησης και μη ασφαλών προεπιλογών (ανασφαλείς προεπιλεγμένες διαμορφώσεις, μετάδοση ευαίσθητων πληροφοριών σαφούς κειμένου κ.λπ.)

iv. Το 9% είναι ζητήματα έγχυσης κώδικα που ανοίγουν συστήματα HMI τόσο σε κοινούς τύπους έγχυσης όσο και σε συγκεκριμένους τομείς. **Γράφημα [3]**



Γράφημα 3 Ευπαθειών ανά κατηγορίες [Trend Micro 2017]

Σύμφωνα με την Trend Micro, ο μέσος χρόνος μεταξύ της αποκάλυψης ενός σφάλματος σε έναν κατασκευαστή SCADA έως την κυκλοφορία μιας οποιασδήποτε ενημέρωσης φτάνει τις 150 ημέρες. Από τη μία πλευρά, αυτό είναι καλύτερο από τον μέσο χρόνο που απαιτούν οι κορυφαίες εταιρείες λογισμικού για να ‘‘κλείσουν τρύπες’’, λέει η έκθεση. Από την άλλη πλευρά, διαρκεί κατά μέσο όρο 30 ημέρες περισσότερο από ό, τι συνήθως χρειάζεται η Microsoft ή η Adobe για να κυκλοφορήσει μια ενημερωμένη έκδοση του λογισμικού της. **Γράφημα [4]**



Γράφημα 4 Χρόνος σε μέρες για την κυκλοφορία ενημέρωσης από τον κατασκευαστή [Trend Micro, 2017]

Αλλά ένας από τους τρόπους με τους οποίους οι επιτιθέμενοι θέτουν σε κίνδυνο τα συστήματα SCADA είναι εξοικειωμένοι με το CISO λογισμικό. Οι λεγόμενες διεπαφές ανθρώπινου μηχανήματος (HMI) - συχνά βασίζονται σε Windows - όπου οι εργαζόμενοι εισάγουν εντολές σε μηχανήματα που συνδέονται με το δίκτυο. Το πρόβλημα είναι αρκετά σοβαρό και η Trend Micro το ονομάζει διεπαφή μηχανής χάκερ.

Μια ανάλυση δύο ετών αποκαλύπτει τα τρωτά σημεία από την Πρωτοβουλία Zero Day δείχνει ότι το 23,6 τοις εκατό αντιμετώπισε την έλλειψη ελέγχου ταυτότητας / εξουσιοδότησης και ανασφαλών προεπιλογών (όπως ανασφαλείς προεπιλογές, μετάδοση ευαίσθητων πληροφοριών με σαφή κείμενο, κρυπτογράφηση που λείπει και μη ασφαλή στοιχεία ελέγχου ActiveX που σημειώνονται ασφαλές για δέσμες ενεργειών), 20 τοις εκατό με καταστροφή μνήμης και 19 τοις εκατό με διαχείριση διαπιστευτηρίων (συμπεριλαμβανομένων των κωδικοποιημένων κωδικών πρόσβασης και των κωδικών πρόσβασης που είναι αποθηκευμένα σε καθαρό κείμενο).

Η δυσκολία είναι ότι ορισμένοι κατασκευαστές εξοπλισμού επικεντρώνονται στο υλικό και όχι στο λογισμικό. Στην πραγματικότητα, λέει η έκθεση, πολλά HMI μπορούν να ληφθούν δωρεάν.

Η πλειονότητα των προγραμματιστών λογισμικού δεν χρησιμοποιεί βασικά μέτρα άμυνας σε βάθος, όπως η τυχαιοποίηση διάταξης χώρου διευθύνσεων (ASLR -Address space layout randomization), SafeSEH έκδοσης 9 και 10 ή στοίβας cookie, λέει η έκθεση. «Αυτό μπορεί να σχετίζεται με τη λανθασμένη πεποίθηση ότι αυτές οι λύσεις θα λειτουργούν σε ένα εντελώς απομονωμένο περιβάλλον. Οι προγραμματιστές λύσεων SCADA έχουν συχνά μικρή εμπειρία όσον αφορά την κατασκευή διεπαφών χρήστη. Αυτό συνδυάζεται με το γεγονός ότι οι προγραμματιστές δεν γνωρίζουν πώς θα είναι το τελικό περιβάλλον λειτουργίας για τα συστήματα. Αυτό προκαλεί τους προγραμματιστές να κάνουν υποθέσεις, που συχνά είναι λανθασμένες. Χωρίς ένα ώριμο πρόγραμμα κύκλου ζωής ανάπτυξης για να τους καθοδηγήσει, οι προγραμματιστές SCADA πιθανότατα θα συνεχίσουν να κάνουν τα ίδια λάθη με αυτά που έκαναν οι προγραμματιστές λειτουργικών συστημάτων πριν από μια δεκαετία.

2.3.6 Ζητήματα Διαχείρισης Διαπιστευτηρίων

Τα θέματα διαχείρισης διαπιστευτηρίων όπως είπαμε και παραπάνω αντιπροσωπεύουν το 19% των τρωτών σημείων που εντοπίστηκαν. Οι ευπάθειες στη κατηγορία αυτή αντιπροσωπεύουν περιπτώσεις όπως η χρήση κωδικοποιημένων κωδικών πρόσβασης, η αποθήκευση κωδικών πρόσβασης με δυνατότητα ανάκτησης (π.χ. clear text) και μη επαρκή προστασία διαπιστευτηρίων. **Γράφημα [5]**

Γράφημα 5 που σχετίζεται με ζητήματα διαχείρισης διαπιστευτηρίων [Trend Micro, 2017]

i. Οι εταιρείες τρίτων και οι κατασκευαστές συχνά έχουν απομακρυσμένη πρόσβαση στα ICS / SCADA συστήματα, απομακρύνοντας τον έλεγχο ασφαλείας από την εταιρεία και τον πελάτη. Ο εξοπλισμός του κατασκευαστή δεν ρυθμίζεται από την τελική εταιρεία-πελάτη και ενδέχεται να μην είναι ασφαλής. Οι παραβιάσεις που προκαλούνται από την αποτυχία ασφάλειας του κατασκευαστή θα μπορούσαν να διαταράξουν τις επιχειρηματικές υπηρεσίες, να σταματήσουν τις βιομηχανικές διαδικασίες, να συλλέξουν ζωτικής σημασίας πληροφορίες ή να θέσουν σε κίνδυνο την κρίσιμη υποδομή της επιχείρησης.

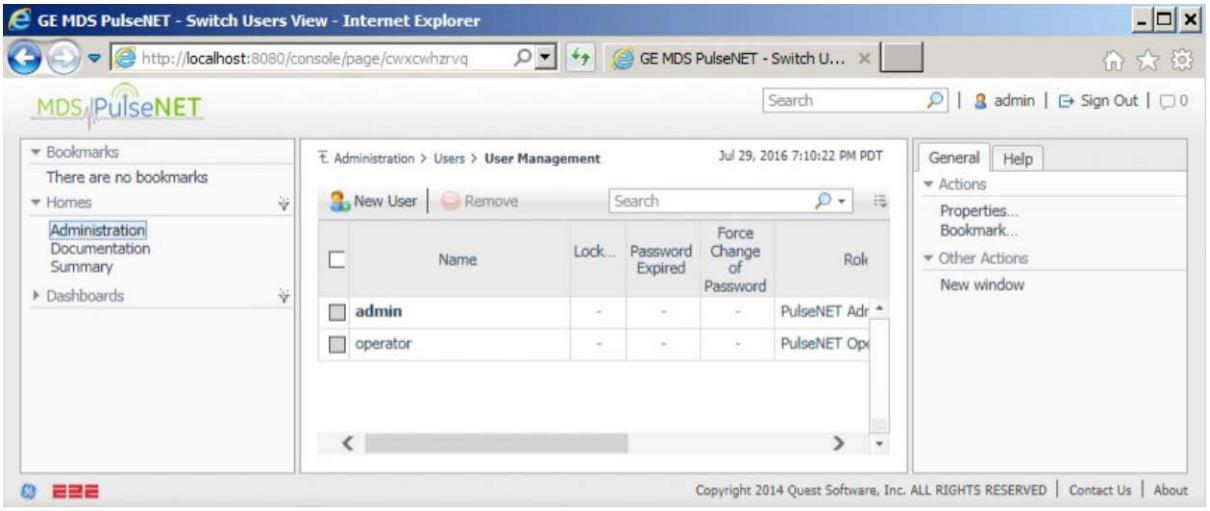
ii. Τα συστήματα ICS / SCADA έχουν γενικά κωδικούς πρόσβασης κωδικοποιημένους στο σύστημα τους κατά τη διάρκεια της κατασκευής τους. Οι περισσότερες επιχειρήσεις και οργανισμοί δεν ασχολούνται όμως με την αλλαγή των κωδικών πρόσβασης από το προεπιλεγμένο σύνολο που υπάρχει. Ένας εισβολέας με μια λίστα προεπιλεγμένων κωδικών πρόσβασης θα μπορούσε εύκολα να αποκτήσει απεριόριστη πρόσβαση σε ευαίσθητες πληροφορίες και δεδομένα.

iii. Αυτά τα συστήματα συνδέονται επίσης με παραδοσιακά συστήματα πληροφορικής, υψηλής αξίας περιουσιακά στοιχεία και φιλοξενούν συσκευές Industrial Internet of Things (IIoT). Τα συστήματα SCADA που συνδέονται με συστήματα πληροφορικής και με επιχειρηματικά περιουσιακά στοιχεία αποτελούν σημαντικό κίνδυνο για την ασφάλεια. Μια παραβίαση των συστημάτων ICS / SCADA εκθέτει επίσης άλλα κρίσιμα επιχειρηματικά στοιχεία και συστήματα.

iv. Ένα μη λειτουργικό σύστημα SCADA μπορεί και διαταράσσει τις επιχειρηματικές δραστηριότητες ενός πλοίου. Τα συστήματα ICS είναι κρίσιμα για την επίτευξη της επιχειρηματικής αποστολής και κάθε κακόβουλο λογισμικό ή απειλή που αποκτά πρόσβαση σε αυτά τα συστήματα μπορεί να διαταράξει αυτές τις επιχειρηματικές δραστηριότητες.

Έρευνα που πραγματοποιήθηκε στην General Electric μέσω του **MDS PulseNet** που χρησιμοποιείτο στο να διαχειρίζεστε συσκευές και βιομηχανικά δίκτια επικοινωνιών και έχει εφαρμογή στο χώρο της ενέργειας και της ναυτιλίας . Το λογισμικό **ZDI** έλαβε αναφορά από ευπάθεια που δήλωνε ότι “The affected products contain a hard-coded support account with full privileges.”, ‘’Τα επηρεαζόμενα προϊόντα περιέχουν έναν λογαριασμό κωδικοποίησης υποστήριξης με πλήρη προνόμια.’’. Η πλήρης ερευνά βάση

της Trend Micro είχε αποτέλεσμα με βαθμό 9.0 (Common Vulverability Scroning System) στην κλίμακα ευπαθειών. **Εικόνα [16]**



Εικόνα 16 MDS PulseNet control panel [Trend Micro, 2017]

Πιο κάτω μπορούμε να δούμε ότι χρησιμοποιώντας το λογισμικό HeidiSQL για να εξάγουμε πληροφορίες από την βάση μας δίνετε η δυνατότητα να δούμε το password HASH του λογαριασμού. Που αυτό έπειτα μπορεί να μεταφραστεί στον κωδικό εισόδου στο MDS PulseNet. **Εικόνα [17]**

Εικόνα 17 Χρησιμοποιώντας HediSQL μετά από είσοδο στο MDS PulseNet control panel [Trend Micro, 2017]

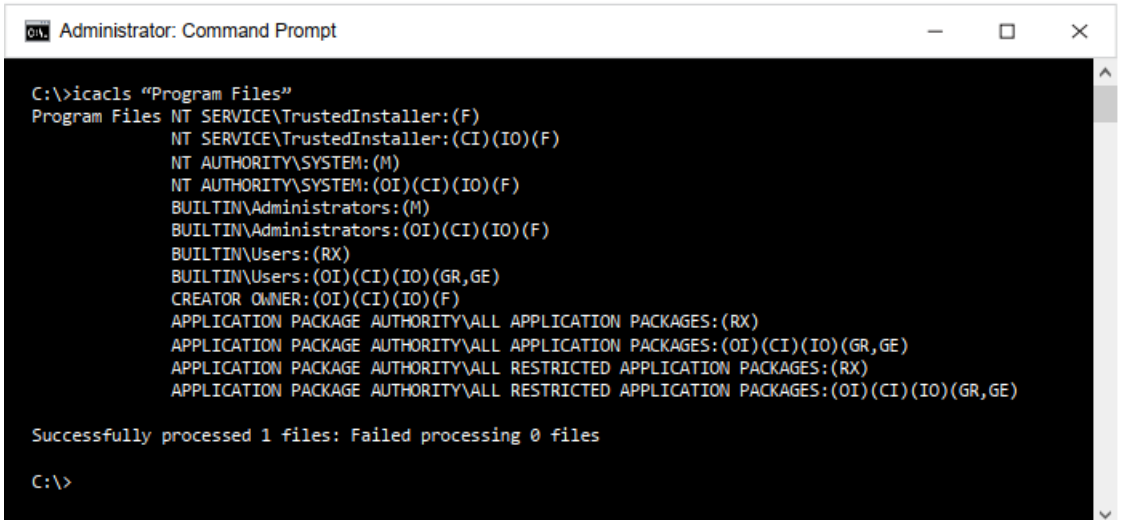
2.3.7 Έλλειψη ελέγχου ταυτότητας / εξουσιοδότησης

Όπως αναφερθήκαμε στην αρχή του κεφαλαίου αυτή η κατηγορία αντιπροσωπεύει το 23% των ευπαθειών σε συστήματα SCADA. Περιλαμβάνει πολλές ανασφαλείς προεπιλογές, clear text, μετάδοση ευαίσθητων πληροφοριών, ελλιπής κρυπτογράφηση και μη ασφαλή στοιχεία ελέγχου ActiveX που χαρακτηρίζονται ως ασφαλή για την εκτέλεση διαφόρων σεναρίων. **Γράφημα [6]**

Γράφημα 6 που σχετίζεται με έλλειψη ελέγχου ταυτότητα [Trend Micro, 2017]

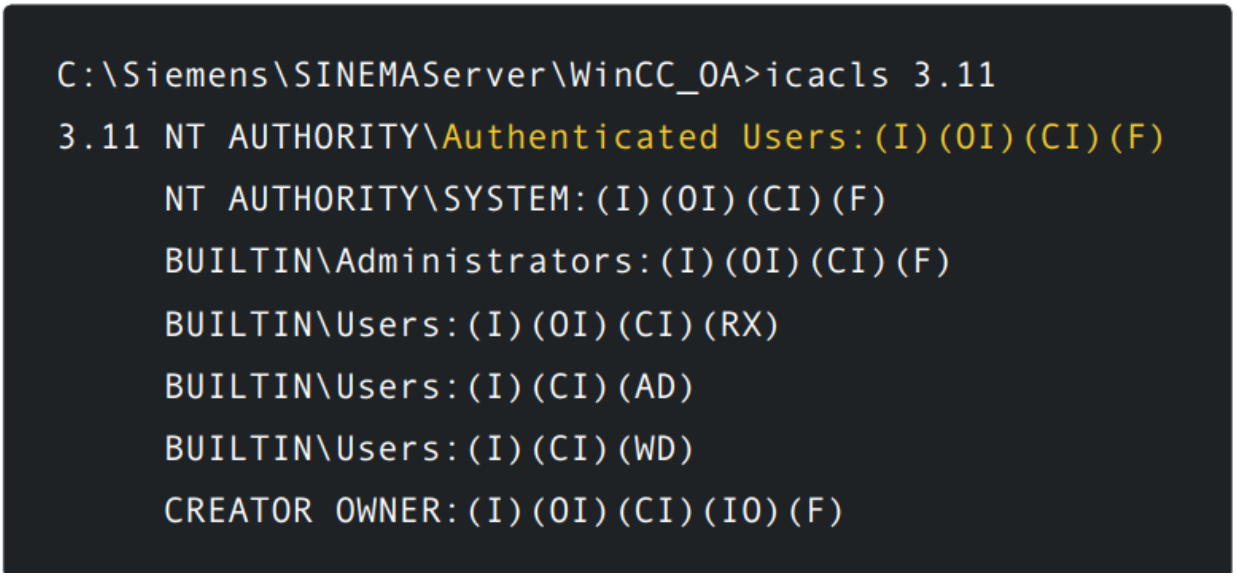
Έρευνα που πραγματοποιήθηκε στη Siemens και συγκεκριμένα στο SINEMA Server είναι χαρακτηριστικό παράδειγμα όταν μια εσφαλμένη διαμόρφωση σε HMI προϊόντα που συμβαίνει συχνά, εταιρείες αποφασίζουν να δημιουργήσουν τις δίκες τους Access Control Lists (ACLs) με διαφορετικό κατάλογο αναβαθμισμένου επιπέδου αντί να χρησιμοποιήσουν τον προεπιλεγμένο κατάλογο των Windows Program Files. Αντί να είναι καταλλήλως προστατευμένοι αυτοί οι αναβαθμισμένοι κατάλογοι, από προεπιλογή δίνουν την δυνατότητα πλήρους εγγραφής. Αυτό επιτρέπει σε κάθε τοπικό χρήστη να κάνει νέα

δυαδικά αρχεία που θα εκτελεστούν ως υπηρεσία συστήματος στον κατάλογο. Όπως παρατηρούμε το προϊόν εγκαθίσταται σε έναν κατάλογο με αδύναμή ACL σε αντίθεση με τον κατάλογο της Microsoft Program Files που δίνει πιο ασφαλής λίστες ACL **Εικόνα [18]**



Εικόνα 18 που σχετίζεται με έλλειψη ελέγχου ταυτότητα [Trend Micro, 2017]

Όπως παρατηρείτε οι χρήστες που έχουν πιστοποιηθεί έχουν πλήρη δικαίωμα και έλεγχο. Για να μπορέσουν να έχουν αυτά τα δικαιώματα αρκεί μόνο να εισέλθουν στα Windows Domain. Αυτό πρακτικά σημαίνει ότι όσοι χρήστες έχουν εισέλθει στο Domain έχουν πάρει και το δικαίωμα αυτό. **Εικόνα [19]**



Εικόνα 19 χρήστες έχουν πλήρη δικαιώματα στο SINEMAServer. [Trend Micro, 2017]

2.3.8 Ζητήματα εγχύσεων κώδικα – Code Injections

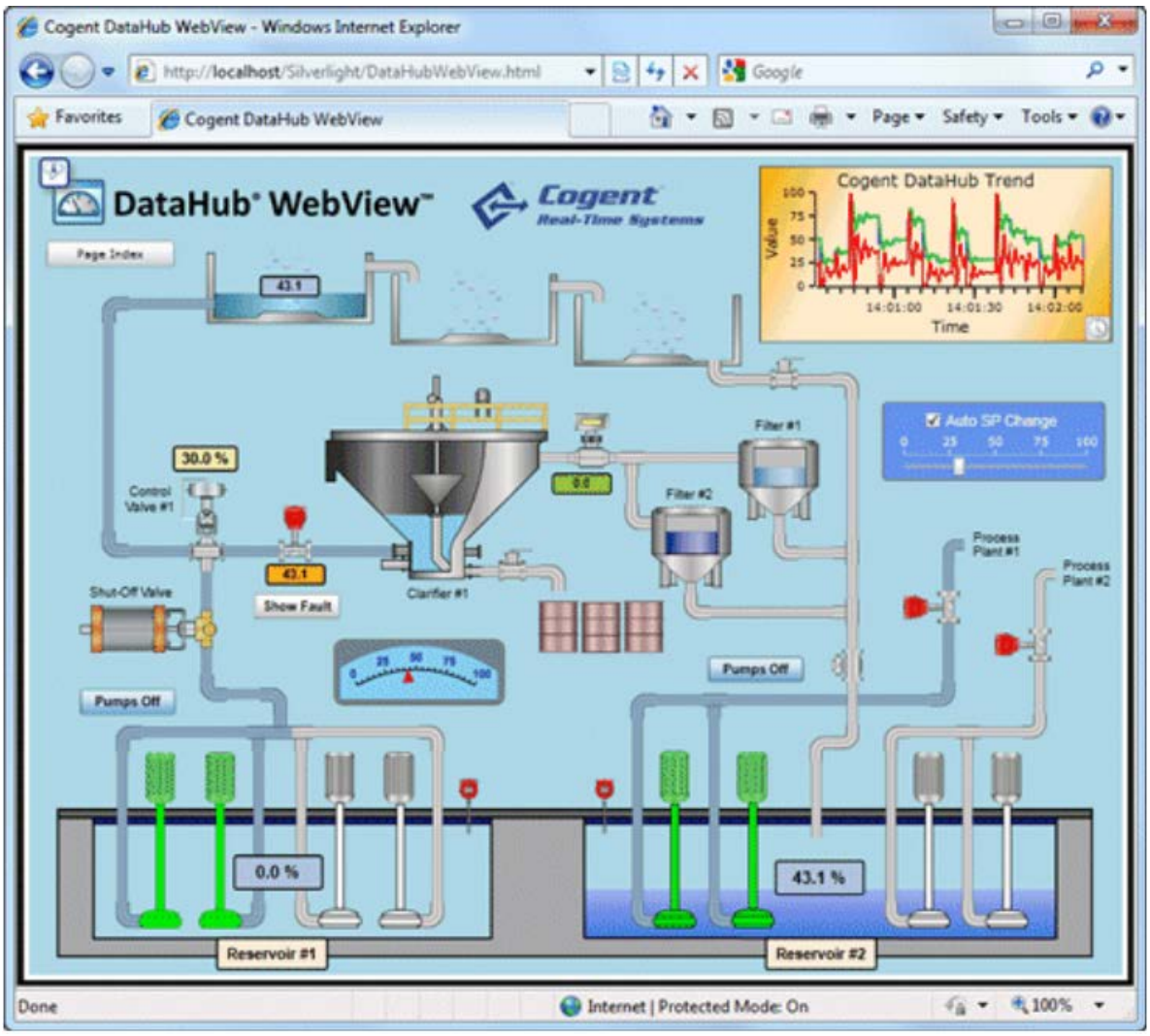
Όπως σε πολλές υπηρεσίες που χρησιμοποιούν σύνδεση με ίντερνετ, έτσι το code injection υπάρχει στο "βασίλειο" των HMI. Τέτοιους είδους προβλήματα αντιπροσωπεύουν όπως είπαμε και στην αρχή του κεφαλαίου το 9% από τις αναγνωρίσιμες ευπάθειες. Ενώ έχοντας υπόψη της συνήθης επιθέσεις έκχυσης SQL , command και OS που εξακολουθούν να συμβαίνουν, υπάρχει μια ξεχωριστή κατηγορία που φέρνουν σε κίνδυνο τα SCADA συστήματα. Μια από αυτές τις γλώσσες που χρησιμοποιούνται για να εισβάλλουν σε τέτοιου είδους συστήματα αναφέρεται και ως **Gamma script injection**. **Γράφημα [7]**

Γράφημα 7 που σχετίζεται με την έγχυση κώδικα [Trend Micro, 2017]

Η γλώσσα που χρησιμοποιείτε με την ονομασία Gamma είναι προϊόν της Cogent DataHub. Σύμφωνα με τους κατασκευαστές η Gamma είναι μια δυναμική προγραμματιστική γλώσσα ειδικά σχεδιασμένη να επιτρέπει την ταχεία ανάπτυξη του ελέγχου και των εφαρμογών UI. Η Gamma βασίζεται πάνω στη C και C++ γλώσσα, άλλα με περισσότερα στοιχεία που την κάνει καλύτερη στην ανάπτυξη πιο εκλεπτυσμένων συστημάτων σε πραγματικό χρόνο.

Σύμφωνα με τη Trend Micro ο κατασκευαστής Cogent DataHub δημιούργησε ένα προϊόν που έχει μια βάση σε πραγματικό που δρούσε ως κεντρικό σημείο διανομής (hub) δίνοντας γρήγορα και αξιόπιστα δεδομένα, συγκεντρώνοντας τα. Το λογισμικό ZDI έλαβε δεδομένα για ένα τρωτό σημείο που δίνει την δυνατότητα σε έναν εισβολέα να ανοίξει την λειτουργία επεξεργασίας στον ίντερνετ με αποτέλεσμα να στέλνει αυθαίρετα σενάρια στον server και να τα εκτελεί.

Όπως βλέπετε και παρακάτω το Cogent DataHub παρέχει πληροφορίες σε πραγματικό χρόνο σε συστήματα SCADA που απαιτείται απεικόνιση. **Εικόνα [20]**



Εικόνα 20 Cogent DataHub WebView

Σε αυτή την περίπτωση ο επιτιθέμενος αξιοποιεί το ελάττωμα μέσω του EvalExpression με Gamma σενάριο και εκτελεί ελεγχόμενη επίθεση στο σύστημα. Η μέθοδος αυτή είναι διαθέσιμη απομακρυσμένα μέσω Ajax ακούγοντας στην πόρτα TCP 80. Δίνοντας στο στόχο συγκεκριμένα Gamma σενάρια δίνει την δυνατότητα να εκτελέσει αυθαίρετες εντολές στο σύστημα.

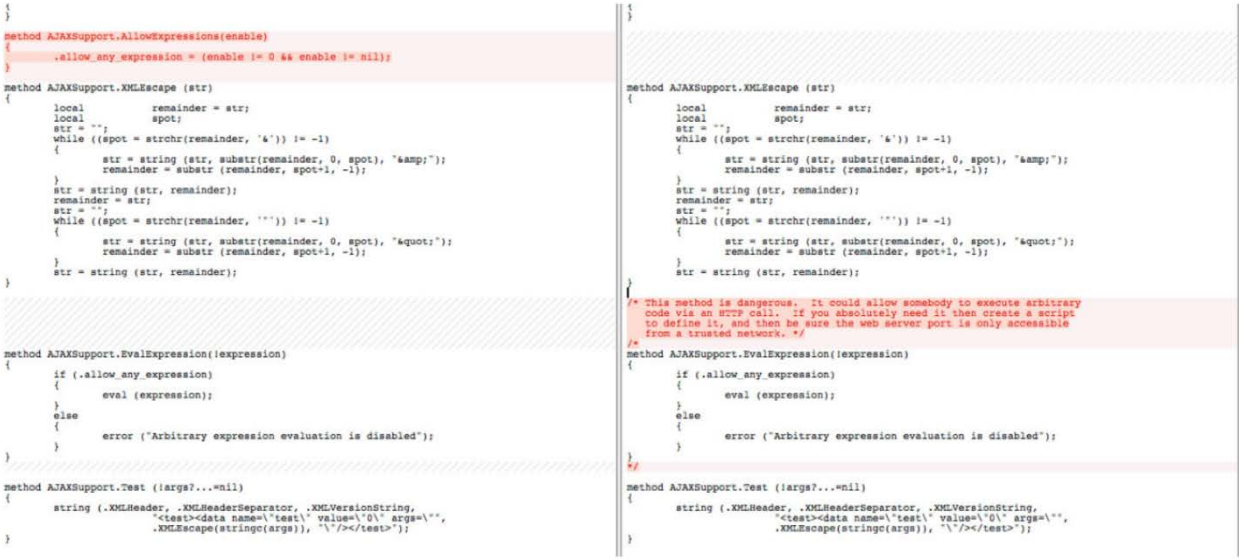
Το μαρκαρισμένο σφάλμα που βλέπουμε στην παρακάτω εικόνα ελέγχει ένα τα flag για να προσδιορίσει αν το σύστημα είναι ικανό για να εκτέλεση την εντολή. Αν ο έλεγχος που γίνει είναι αληθής τότε εκτελείτε η εντολή ανεξαρτήτως το τι περιέχει. Ο επιτιθέμενος έπειτα πρέπει να ξεγελάσει το σύστημα φορτώνοντας τις απαραίτητες βιβλιοθήκες και αλλάζοντας τις τιμές τους διασφαλίζοντας έτσι, ότι το σύστημα θα ‘’γυρνάει’’ πάντα σε κατάσταση αλήθειας για να μπορεί να εκτελείτε η εντολή. **Εικόνα [21]**

```
Method AJAXSupport.EvalExpression(!expression)
{
        if (.allow_any_expression)
        {
                eval (expression); << Bug here
        }
        else
        {
                error ("Arbitrary expressions evaluation is disabled");
        }
}
```

Εικόνα 21 Μέθοδος Ajax expression εκτέλεση [Trend Micro, 2017]

Για να μπορέσει να ολοκληρωθεί το exploit ο επιτιθέμενος πρέπει πρώτα να στείλει HTTP αίτημα σε οποιοδήποτε Gamma σενάριο που φορτώνει τις απαραίτητες βιβλιοθήκες, Όπως αναφερθήκαμε και στην αρχή όσο οι προγραμματιστές θα νομίζουν ότι το σύστημα λειτουργεί σε απομονωμένο περιβάλλον αυτό στην πραγματικότητα δεν θα ισχύει. Ο επιτιθέμενος καλεί μέσω του αιτήματος που έκανε το AJAXSupport.EvalExpression βάζοντας την εντολή οποιαδήποτε φράση να είναι αληθής (allow any expression).

Τέλος βλέποντας τις διαφορές μεταξύ των ενημερώσεων που κυκλοφόρησε η εταιρεία συνειδητοποιούμε ότι έχει προσθέσει ένα κείμενο προειδοποίησης χωρίς να αφαιρέσει τελείως το EvalExpressions. **Εικόνα [22]**



Εικόνα 22 Διάφορες μεταξύ νέου και παλιού κώδικα με κόκκινη επισήμανση στο δεύτερο μισό [Trend Micro, 2017]

Κεφάλαιο 3
Δέκα αδυναμίες ασφάλειας

3.1 Συνοπτική αναφορά στις ευπάθειες

Ενώ η παγκόσμια αγορά IoT αναμένεται να φτάσει τα 1,1 τρισεκατομμύρια δολάρια έως το 2026, η εταιρεία Gartner προβλέπει ότι θα υπάρχουν 25 δισεκατομμύρια συνδεδεμένες συσκευές μέσα στον επόμενο χρόνο - ένας τρομακτικός αριθμός λαμβάνοντας υπόψη τις ευπάθειες IoT που υπάρχουν σε αυτές τις συσκευές.[21]–[23]

Οι τεχνολογίες IoT βρίσκονται γύρω μας, και χωρίς την κατάλληλη προστασία, αφήνουν ευαίσθητα δεδομένα και προσωπικές πληροφορίες ευάλωτες σε εγκληματίες στον κυβερνοχώρο.

Οι ζωές μας γίνονται ευκολότερες καθημερινά με τις καινοτομίες στην τεχνολογία και το Διαδίκτυο των πραγμάτων (IoT-Internet of things) είναι μόνο μια τέτοια πρόοδος που μας φέρνει πολλά υπέροχα προνόμια όπως να έχουμε μια έξυπνες συσκευές στο σπίτι μας. Αλλά αυτές οι ευκολίες συχνά κοστίζουν την ασφάλειά μας και μας αφήνουν ανοιχτούς σε μια μεγάλη ποικιλία επιθέσεων στον κυβερνοχώρο. [21]–[23]

Δεν αποτελεί έκπληξη το γεγονός ότι η ασφάλεια θεωρείται κορυφαία ανησυχία για πολλούς καταναλωτές. Στην πραγματικότητα, τα δεδομένα από μια πρόσφατη έρευνα στο Ηνωμένο Βασίλειο δείχνουν ότι η ασφάλεια είναι η τρίτη πιο σημαντική πληροφορία για τους καταναλωτές που λαμβάνουν αποφάσεις αγοράς. Επιπλέον, τα δεδομένα δείχνουν ότι μεταξύ εκείνων που δεν κατατάσσουν την «ασφάλεια» ως κορυφαία προτίμηση στην επιλογή συσκευής, το 72% είπε ότι αυτό οφείλεται στο γεγονός ότι περίμεναν ότι η ασφάλεια θα έχει ήδη ενσωματωθεί σε συσκευές που ήταν ήδη στην αγορά.

Ακόμα κι αν η βιομηχανία λογισμικού ασχολείται με ζητήματα ασφαλείας από τότε που δημιουργήθηκε ο παγκόσμιος ιστός (web). Το OWASP σήκωσε τον πήχη και ενθάρρυνε τους κατασκευαστές για να κατασκευάσουν τις συσκευές τους έχοντας κατά νου την ασφάλεια και να αποφύγουν να επαναλάβουν τα ίδια λάθη στην βιομηχανία της πληροφορικής ασχολείται με μερικές δεκαετίες. [21]–[23]

Ωστόσο, η διασυνδεδεμένη και ανεξάρτητη φύση των αντικειμένων, καθώς και οι περιορισμένες δυνατότητές τους σχετικά με τους υπολογιστικούς πόρους καθιστούν αδύνατη την εφαρμογή των συμβατικών μηχανισμών ασφαλείας. Επιπλέον, η ετερογένεια διαφόρων τεχνολογιών που συνδυάζει το IoT αυξάνει την πολυπλοκότητα των διαδικασιών ασφαλείας, καθώς κάθε τεχνολογία χαρακτηρίζεται από διαφορετικά τρωτά σημεία. Επιπλέον, οι τεράστιες ποσότητες δεδομένων που παράγονται από τις πολλαπλές αλληλεπιδράσεις μεταξύ των χρηστών και των αντικειμένων ή μεταξύ των αντικειμένων δυσχεραίνουν τη διαχείριση και τη λειτουργικότητα των συστημάτων ελέγχου πρόσβασης. [21]–[23]

3.1.1 Διαχείριση προσβάσεων και συνδέσεων.

Οι αδύναμοι, προεπιλεγμένοι και παλαιοί κωδικοί πρόσβασης είναι εύκολη λεία για τους χάκερ που θέλουν να επιτεθούν και να αναπτύξουν μεγάλα **botnets** και άλλα κακόβουλα προγράμματα. Η διαχείριση κωδικών πρόσβασης συσκευών σε κλίμακα είναι τρομακτική ευθύνη, επειδή συνήθως οι συσκευές IoT δεν έχουν ανθρώπινους χειριστές για να υποκινήσουν την αλλαγή κωδικού πρόσβασης.

Οι κωδικοί πρόσβασης είναι ιδιαίτερα επικίνδυνοι, διότι είναι εύκολοι στόχοι επιτρέποντας σε χάκερ και κακόβουλα προγράμματα να εισβάλλουν σε, συστήματα και λογισμικό. Ο ίδιος κωδικός πρόσβασης , χρησιμοποιείται συχνά σε όλες τις εφαρμογές και πολλές απαιτούν αυξημένα δικαιώματα διαχείρισης. Έτσι, όταν ένας χάκερ γνωρίζει τον προεπιλεγμένο κωδικό πρόσβασης, μπορεί ενδεχομένως να έχει πρόσβαση σε όλες τις παρόμοιες συσκευές ή παρουσίες εφαρμογών. Αυτό το είδος εκμετάλλευσης είχε ως αποτέλεσμα μαζικές επιθέσεις οι οποίες προκαλούν μαζικές παραβιάσεις ασφάλειας, κίνδυνο κρίσιμης υποδομής.

Η ερευνητική ομάδα SCADA StrangeLove δημοσίευσε μια λίστα προεπιλεγμένων κωδικών πρόσβασης που σχετίζονται με προϊόντα βιομηχανικού συστήματος ελέγχου (ICS) από διάφορους προμηθευτές.

Η λίστα, που ονομάζεται "**SCADAPASS**", περιέχει προεπιλεγμένα διαπιστευτήρια για βιομηχανικούς δρομολογητές, προγραμματιζόμενους ελεγκτές λογικής (PLC), ασύρματες πύλες, διακομιστές και λειτουργικές μονάδες δικτύου από προμηθευτές όπως ABB, B&B Electronics, Digi, Emerson, eWON, Hirschmann, Moxa, Netcomm Wireless , Rockwell Automation, Samsung, Schneider Electric, Siemens και Yokogawa.

Ο ανεξάρτητος ερευνητής για SCADA που ανήκει στην StrangeLove, Sergey Gordeychik πιστεύει ότι οι περισσότεροι προμηθευτές δεν βλέπουν τους προεπιλεγμένους κωδικούς πρόσβασης ως ευπάθεια. Ο ειδικός λέει ότι οι αδύναμοι ή καθόλου κωδικοί πρόσβασης είναι αποδεκτοί για συστήματα που είναι φυσικά προστατευμένα και είναι προσβάσιμα μόνο σε τοπικό επίπεδο, αλλά μπορεί να ενέχουν σοβαρό κίνδυνο για συστήματα που θα μπορούσαν να έχουν πρόσβαση από απόσταση. **Εικόνα [23]**

Εικόνα 23 απεικόνιση των επικρατέστερων κωδίκων. [networkworld.com]

3.1.2 Μη ασφαλείς υπηρεσίες δικτύου.

Όταν προσπαθείτε να θέσετε σε κίνδυνο ένα συνδεδεμένο τελικό σημείο IoT, μία από τις πρώτες και απλούστερες επιφάνειες επίθεσης εντοπίζει αδυναμίες στο μοντέλο

επικοινωνίας δικτύου και στις υπηρεσίες δικτύου που εκτελούνται στη συσκευή. Οι επιτιθέμενοι θα στοχεύουν στην εκμετάλλευση ορισμένων ευπαθειών για τη λήψη διαπιστευτηρίων σύνδεσης, διακριτικών επικοινωνίας ή άλλων αναγνωριστικών που θα χρησιμοποιήσει το Service Ecosystem για τον προσδιορισμό του τελικού σημείου. Είναι επιτακτική ανάγκη να διασφαλιστεί το τελικό σημείο με τις βέλτιστες πρακτικές της βιομηχανίας. [21]–[23]

Οι υπηρεσίες δικτύου μπορούν να τεθούν σε κίνδυνο μέσω υπερχείλισης buffer (**buffer overflows**), **fuzzing**, **DDoS** και άλλων μορφών επιθέσεων. **Εικόνα [24]**

Εικόνα 24 απεικόνιση των επικρατέστερων κωδίκων [Cloudflare.com]

3.1.3 Μη ασφαλείς Διεπαφές.

Για την αντιμετώπιση μη ασφαλών διασυνδέσεων ιστού, backend API, cloud ή κινητών συσκευών στο οικοσύστημα εκτός της συσκευής IoT, πρέπει να υπάρχει ένας τακτικός ισχυρός μηχανισμός για τον έλεγχο ταυτότητας και την εξουσιοδότηση της συσκευής. [21]–[23]

3.1.4 Έλλειψη μηχανισμού ασφαλών ενημερώσεων.

Μη εξουσιοδοτημένες ενημερώσεις λογισμικού και υλικολογισμικού είναι ένας σημαντικός φορέας απειλών για διαδικτυακές επιθέσεις IoT. Οι παραβιάσεις IoT μπορεί να έχουν φυσικές συνέπειες που έχουν ως αποτέλεσμα την απώλεια δεδομένων και επίσης εισάγουν ουσιαστική νομική ευθύνη και διαβρώνουν τη φήμη της μάρκας.
Υπάρχουν τρεις κρίσιμες απαιτήσεις ασφαλείας για την ασφαλή παράδοση ενημερώσεων σε συσκευές IoT:

I. Εξασφάλιση πρόσβασης στις ενημερώσεις

II. Επαλήθευση της πηγής των ενημερώσεων
III. Επαλήθευση της ακεραιότητας των ενημερώσεων

3.1.5 Χρήση ανασφαλών ή ξεπερασμένων στοιχείων.

Η ασφάλεια των πληροφοριών είναι ένας συνεχής αγώνας για να παραμείνετε στην κορυφή των ευπαθειών που ανακαλύφθηκαν πρόσφατα στις διάφορες βιβλιοθήκες λογισμικού που αξιοποιούνται από ένα δεδομένο προϊόν ή υπηρεσία. Κάποιος πρέπει να σκεφτεί μόνο τις σημαντικές ευπάθειες όπως το Heartbleed (OpenSSL, 2014) και το Shellshock (Bash, 2014) για να θυμηθεί πόσο γρήγορη πρέπει να είναι η επιδιόρθωση των ευπαθών συστατικών. [21]–[23]

3.1.6 Ανεπαρκής προστασία απορρήτου.

Η προσέγγιση της Αρχής Συσκευών για το απόρρητο των καταναλωτών και τα προσωπικά στοιχεία ξεκινά με την παροχή ασφάλειας από την αρχή. Αυτό σημαίνει παροχή ασφάλειας δεδομένων από την ίδια τη συσκευή του τελικού σημείου. Για να διασφαλιστεί ότι η συσκευή μπορεί να είναι αξιόπιστη, η συσκευή πρέπει να είναι ενεργοποιημένη με την τεχνολογία ασφαλείας και να παρέχει έλεγχο ταυτότητας. Μετά από αυτό, η συσκευή μπορεί να είναι αξιόπιστη για την αποστολή ευαίσθητων δεδομένων στο δίκτυο. [21]–[23]

3.1.7 Μη ασφαλής μεταφορά αποθήκευσης δεδομένων.

Η προστασία των δεδομένων IoT είναι υψίστης σημασίας για την ακεραιότητα των εφαρμογών IoT. Οι εφαρμογές τροφοδοσίας δεδομένων IoT οδηγούν σε αυτοματοποιημένες ενέργειες και ελέγχους που μπορεί να έχουν επικίνδυνες φυσικές συνέπειες. Είναι σημαντικό τόσο η πηγή όσο και το περιεχόμενο των δεδομένων που δημιουργούνται από συσκευές IoT να προστατεύονται και να επαληθεύονται. Ωστόσο, τα δεδομένα πρέπει να κρυπτογραφούνται από τη δημιουργία έως την αποστολή και να απαιτούν υψηλότερο επίπεδο ευελιξίας κρυπτογράφησης από ό, τι μπορεί να προσφέρει η παραδοσιακή μονόδρομη ασφάλεια Layer Security (TLS). [21]–[23]

3.1.8 Έλλειψη διαχείρισης συσκευών.

Δεν μπορούμε να ασφαλίσουμε συσκευές που δεν γνωρίζουμε ότι διαθέτουμε. Η διαχείριση συσκευών είναι μια θεμελιώδης, αλλά συνήθως παραβλέπετε πτυχή της ασφάλειας.

Πολλές συσκευές μεταφέρονται εκτός των επίσημων προγραμμάτων και τοποθετούνται σε δίκτυα με μη διαχειριζόμενο τρόπο.

Είναι σημαντικό να κατανοήσουμε τα νέα οικοσυστήματα IoT που κατασκευάζονται και πώς θα διαχειρίζονται οι συσκευές IoT όχι μόνο από την αρχική εγκατάσταση αλλά και καθ' 'όλη τη διάρκεια του κύκλου ζωής τους. Καθώς οι υπηρεσίες IoT αυξάνονται και ο αριθμός των αναπτύξεων αυξάνεται με αυτό, η τεράστια κλίμακα και το μέγεθος της διαχείρισης αυτών των συσκευών δεν μπορούν να υποτιμηθούν. Είναι απαραίτητο να οικοδομήσουμε ασφάλεια από την αρχή. Το Device Authority μπορεί να βοηθήσει τους οργανισμούς με τη στρατηγική τους για την ασφάλεια IoT και να εφαρμόσουν μια προσέγγιση «Secure by Design» από την αρχή. [21]–[23]

3.1.9 Μη ασφαλείς προεπιλεγμένες ρυθμίσεις.

Πολλές συσκευές αποστέλλονται με μια σειρά υπερβολικά ανεκτικών ρυθμίσεων για τη μείωση της τριβής ανάπτυξης. Υπηρεσίες και λογισμικό που λειτουργούν ως root, για παράδειγμα. Επιπλέον, ενδέχεται να επιτρέπουν στους τοπικά συνδεδεμένους χρήστες να απενεργοποιούν ορισμένες λειτουργίες ασφαλείας και να κάνουν τις συσκευές λιγότερο ασφαλείς από ό, τι όταν έφτασαν, έτσι έχουμε έναν απλό χρήστη (user) με δικαιώματα όμως διαχειριστή (administrator). [21]–[23]

3.1.10 Έλλειψη φυσικής πρόσβασης.

Εάν ένας εισβολέας έχει φυσική πρόσβαση στον στόχο του, έχει ήδη παραβιαστεί.

Οι άνθρωποι θέλουν να αποκτήσουν μια εικόνα για το τι συμβαίνει σε μια δεδομένη συσκευή. Για αυτόν τον λόγο, η φυσική πρόσβαση στο υλικό είναι μία από τις σημαντικότερες προκλήσεις ασφάλειας που πρέπει να ξεπεραστούν. [21]–[23]

Κεφάλαιο 4
Προτεινόμενα Αντίμετρα

4.1 Σκοπός της κυβερνοασφάλειας στα πλοία

Τα συστήματα PLC/SCADA βοηθούν ουσιαστικά την επίτευξη της μέγιστης απόδοσης στο πλοίο. Την ίδια στιγμή όμως είναι ευάλωτα σε κυβερνοεπίθεσης γιατί παρέχουν πληροφορίες σχετικές με τον έλεγχο των συστημάτων του πλοίου. Σκοπός των οδηγιών που ακολουθούν βάση των Cyber Security Onboard Ships Guidelines 2.0, 4.0 και των δέκα κορυφαίων ευπαθειών που έχουμε αναφέρει στο προηγούμενο **κεφάλαιο 3** είναι να παρέχει ένα ασφαλές περιβάλλον κατάλληλο για την εκτέλεση οποιοδήποτε διαδικασιών βασισμένων πάνω στην αξιολόγηση όλων των κινδύνων όπου έχουν εντοπιστεί για το πλοίο, για το προσωπικό του πλοίου και το περιβάλλον αυτού.

4.1.1 Ευαισθητοποίηση

Ένα πρώτο βήμα για τη βελτίωση της ασφάλειας των SCADA/PLC συστημάτων είναι απλώς η ευαισθητοποίηση σχετικά με τις τελευταίες απειλές και θέματα ασφάλειας. Η εγγραφή σε ένα ενημερωτικό δελτίο που βασίζεται σε τεχνολογία και παραδίδεται μέσω email είναι αποτελεσματική. Ένας εξαιρετικός πόρος είναι το US-CERT, το επιχειρησιακό σκέλος του Εθνικού τμήματος ασφάλειας στον κυβερνοχώρο στο Υπουργείο Εσωτερικής Ασφάλειας.

Αυτό το τμήμα συντονίζει την ανταλλαγή πληροφοριών, διαχειρίζεται προληπτικά τους κινδύνους στον κυβερνοχώρο και προσφέρει δωρεάν, έγκαιρη, ενεργή πληροφορία για να βοηθήσει τους χρήστες να ασφαλίσουν τα συστήματα υπολογιστών τους. Παρέχει επίσης έναν τρόπο για τους οργανισμούς να επικοινωνούν και να συντονίζονται

απευθείας με την κυβέρνηση των ΗΠΑ σχετικά με την ασφάλεια στον κυβερνοχώρο.

Η ένταξη σε ομάδες χρηστών ή η ανταλλαγή πληροφοριών με βοηθητικά προγράμματα παρόμοιας λειτουργίας και μεγέθους είναι ένας άλλος τρόπος για να αυξήσουμε την ευαισθητοποίηση και να μοιραστούμε τις γνώσεις και τα διδάγματα που αντλήθηκαν μέσα από ένα πρόβλημα. Επιπλέον, οι επαγγελματίες με γνώμονα την ασφάλεια πρέπει να προσέχουν τις τακτικές ενημερώσεις λειτουργικού συστήματος και εφαρμογών που παρέχονται από τη Microsoft και από οποιοδήποτε κατασκευαστή .

Πολλά συστήματα SCADA χρησιμοποιούν διεπαφή ανθρώπου-μηχανής (HMI) για την προβολή και τον έλεγχο διαδικασιών. Οι περισσότεροι εκτελούνται σε κάποια μορφή του λειτουργικού συστήματος των Windows, καθιστώντας τους στόχους για επιθέσεις. Οι υπολογιστές που έχουν τα SCADA συστήματα πρέπει να ενημερώνονται "θρησκευτικά" -"Patch Tuesday". [24]–[26]

4.1.2 Αντιμετώπιση στο πεδίο

Αφού αντιμετωπιστεί η υποδομή δικτύου, η εστίαση μπορεί να μετατοπιστεί στα στοιχεία του συστήματος, ειδικά στα PLC. Οι περισσότεροι κατασκευαστές ζητούν εγγραφή των προϊόντων τους στο site της εταιρείας. Αυτό μπορεί να φαίνεται σαν μια χειροκίνητη εργασία, αλλά οι περισσότεροι κατασκευαστές το ανταμείβουν παρέχοντας αυτοματοποιημένες ειδοποιήσεις όταν είναι διαθέσιμες νέες ενημερώσεις υλικολογισμικού ή λογισμικού.

Οι τομείς τεχνικής υποστήριξης αυτών των κατασκευαστών και τα διαδικτυακά φόρουμ μπορούν να προσφέρουν προτάσεις ή ανησυχίες σχετικά με τα ζητήματα που μπορεί να χάσει ένας μη εγγεγραμμένος χρήστης. Το λογισμικό PLC και το υλικολογισμικό πρέπει επίσης να ενημερώνονται τακτικά. Πέρα από τον νέο εξοπλισμό, τα βοηθητικά προγράμματα πρέπει να ενημερώνουν όλα τα στοιχεία του συστήματος SCADA. ". [24]–[26]

4.1.3 Καλύτερη Προετοιμασία

Όταν αντιμετωπίζουμε ζητήματα ασφάλειας στον κυβερνοχώρο που σχετίζονται με τα

SCADA συστήματα, τα τρία βασικά δεδομένα πρέπει να είναι ισορροπημένα: εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Αντιμετωπίζοντας αυτά τα ζητήματα, ένας οργανισμός θα γίνει καλύτερα προετοιμασμένος να ανταποκριθεί σε όλους τους τύπους καταστροφών, συμπεριλαμβανομένων των ανθρώπινων σφαλμάτων, της κυβερνο-τρομοκρατίας και των φυσικών καταστροφών. Η ολιστική προσέγγιση, ειδικά με την ανάλυση κινδύνου, μπορεί να κάνει κάθε οργανισμό πιο ανθεκτικό, βιώσιμο και αποτελεσματικό. **Εικόνα [25]**

Εικόνα 25 Θεμελιώδης Απατήσεις Ασφαλείας CIA [itgovernanceusa.com]

4.1.4 Μέτρα ασφάλειας

Για να βελτιωθεί και να ενισχυθεί η συνολική ασφάλεια του συστήματος SCADA, είναι απαραίτητο να ενισχυθούν τα χαρακτηριστικά ασφαλείας στα πρωτόκολλα SCADA. Είναι απαραίτητο να αναλύσουμε τα υπάρχοντα πρωτόκολλα όπως το Modbus και να κατανοήσουμε τις ευπάθειες που υπάρχουν στα πρωτόκολλα. Αυτό θα βοηθήσει στην ανάπτυξη μέτρησης ασφάλειας που μπορεί να προστεθεί στις προδιαγραφές του πρωτοκόλλου. Για την προστασία του Modbus RTU / ASCII, οι συστάσεις είναι οι

ακόλουθες:

i. Ανάπτυξη εντοπισμού εισβολής, είτε μέσω εμπορικών προϊόντων IDS, καταγραφής συναλλαγών ή παρακολούθησης κίνησης. Όλες οι πιθανές εξωτερικές συνδέσεις που αφήνουν την προστασία του φυσικού συστήματος θα πρέπει να θεωρούνται ανασφαλείς και οι συνδέσεις θα πρέπει να κρυπτογραφούνται όπου είναι δυνατόν.

ii. Όλες οι συνδέσεις με αξιόπιστα τρίτα μέρη πρέπει να θεωρούνται ανασφαλείς και πρέπει να αναπτυχθεί προστασία μέσω τείχους προστασίας ή εικονικών ιδιωτικών δικτύων (VPN).

iii. Όλες οι συσκευές πύλης που επικοινωνούν με συσκευές εκτός της άμεσης φυσικής προστασίας του φυσικού συστήματος είναι ευαίσθητες σε άμεσες επιθέσεις. Θα πρέπει να απομονωθούν από άλλες συσκευές SCADA.

Στο Modbus TCP, η διασύνδεση των δικτύων καλύπτει ολόκληρο τον κόσμο επιτρέποντας στο SCADA να εκμεταλλευτεί δυνητικά το σύστημα ανεξάρτητα από την τοποθεσία. Η μορφή κειμένου του πρωτοκόλλου το καθιστά ιδιαίτερα ευάλωτο. Η παρακολούθηση και η εισροή σημαντικών δεδομένων μπορούν να συλλεχθούν εύκολα και οι κωδικοί πρόσβασης μπορεί να συσσωρευτούν από τη μετάδοση. Για την παροχή μηχανισμών ασφάλειας και προστασίας, αυτό το πρωτόκολλο πρέπει να ενσωματώνει το μήνυμα μέσα σε ένα μέσο κρυπτογράφησης. Η σύνδεση VPN IPsec θα πρέπει να χρησιμοποιείται για την ενθυλάκωση της κυκλοφορίας όποτε ταξιδεύει σε ένα ευάλωτο μέσο. Μερικά παραδείγματα ευάλωτων μέσων περιλαμβάνουν μη SCADA και ασύρματα δίκτυα. Το IPsec περιλαμβάνει επίσης πρωτόκολλα για την καθιέρωση αμοιβαίου ελέγχου ταυτότητας μεταξύ παραγόντων στην αρχή αυτής της περιόδου και τη διαπραγμάτευση κρυπτογραφικών κλειδιών που θα χρησιμοποιηθούν κατά τη διάρκεια της συνεδρίας. Το IPsec μπορεί να χρησιμοποιηθεί για την προστασία ροών δεδομένων μεταξύ ενός ζεύγους κεντρικών υπολογιστών, μεταξύ ενός ζεύγους πυλών ασφαλείας ή μεταξύ μιας πύλης ασφαλείας και ενός κεντρικού υπολογιστή.

Τα συστήματα SCADA εκτίθενται στις ίδιες απειλές στον κυβερνοχώρο με οποιοδήποτε επιχειρηματικό σύστημα επειδή μοιράζονται τις κοινές ευπάθειες με τα παραδοσιακά

συστήματα τεχνολογίας πληροφοριών. Ως εκ τούτου, είναι επωφελής η διαμόρφωση και η επιβολή προτύπων ασφαλείας για την ενίσχυση της ασφάλειας των δικτύων SCADA. Παρά τους πολλούς οργανισμούς που εμπλέκονται στην προσπάθεια τυποποίησης και βελτίωσης της ασφάλειας του δικτύου SCADA, χρειάζεται ακόμη μια ισχυρή προσπάθεια για την πραγματοποίηση ερευνών για την περαιτέρω ενίσχυση της ασφάλειας αυτών των συστημάτων, ιδίως στα πρότυπα που χρησιμοποιούνται. ". [24]–[26]

Το ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) ενθαρρύνει τους ιδιοκτήτες τέτοιων στοιχείων να λάβουν επιπρόσθετα μέτρα για την προστασία έναντι αυτού και άλλων κινδύνων στην κυβερνοασφάλεια, παραθέτοντας μερικές συμβουλές:

i. Ελαχιστοποιήστε την έκθεση στο δίκτυο για όλες τις συσκευές ή / και τα συστήματα ελέγχου και βεβαιωθείτε ότι δεν είναι προσβάσιμα από το Διαδίκτυο.

ii. Εντοπίστε δίκτυα συστήματος ελέγχου (control systems networks) και απομακρυσμένες συσκευές πίσω από τείχη προστασίας και απομονώστε τα από το επιχειρηματικό δίκτυο.

iii. Όταν απαιτείται απομακρυσμένη πρόσβαση, χρησιμοποιήστε ασφαλείς μεθόδους, όπως εικονικά ιδιωτικά δίκτυα (VPN), αναγνωρίζοντας ότι τα VPN ενδέχεται να έχουν ευπάθειες και θα πρέπει να ενημερώνονται στην πιο πρόσφατη διαθέσιμη έκδοση. Επίσης αναγνωρίστε ότι το VPN είναι τόσο ασφαλές όσο οι συνδεδεμένες συσκευές.

4.1.5 Διαμόρφωση συσκευών δικτύου

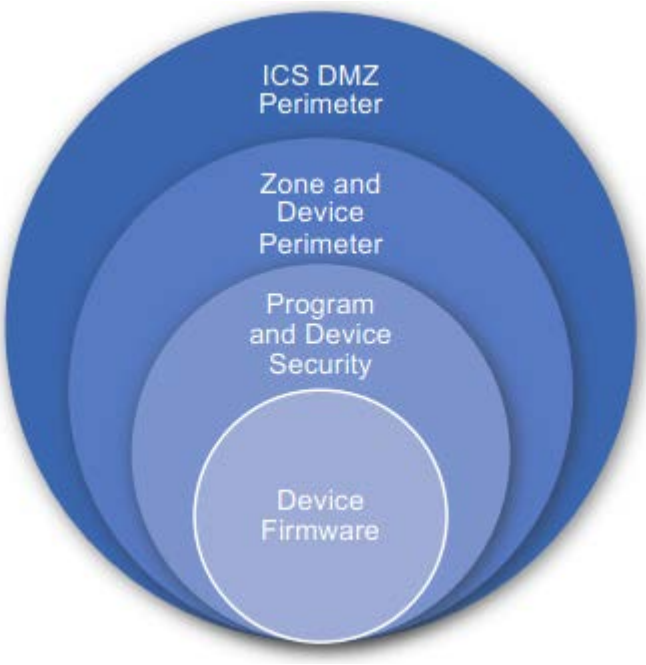
Πρέπει να προσδιοριστεί ποια συστήματα πρέπει να συνδέονται με ελεγχόμενα ή μη ελεγχόμενα δίκτυα. Τα ελεγχόμενα δίκτυα έχουν σχεδιαστεί για να αποτρέπουν τυχόν κινδύνους ασφαλείας από συνδεδεμένες συσκευές με χρήση τείχους προστασίας, πυλών ασφαλείας, δρομολογητών και διακοπτών. Τα μη ελεγχόμενα δίκτυα ενδέχεται να ενέχουν κινδύνους λόγω έλλειψης ελέγχου της κυκλοφορίας δεδομένων και θα πρέπει να απομονωθούν από τα ελεγχόμενα δίκτυα, γιατί ως άμεση σύνδεση στο Διαδίκτυο τα καθιστά πολύ επιρρεπείς σε διείσδυση από κακόβουλο λογισμικό. [24]–[26] Για παράδειγμα:

i. Τα δίκτυα που είναι κρίσιμα για τη λειτουργία του ίδιου του πλοίου, πρέπει να ελέγχονται. Είναι επιτακτική ανάγκη αυτά τα συστήματα - να έχουν υψηλό επίπεδο ασφάλειας.

ii. Δίκτυα που παρέχουν στους προμηθευτές απομακρυσμένη πρόσβαση στην πλοήγηση καθώς και σε άλλα σύστημα ΟΤ το λογισμικό στον εξοπλισμό επί του πλοίου, πρέπει επίσης να ελέγχεται. Αυτά τα δίκτυα μπορεί να είναι απαραίτητα για τους κατασκευαστές επιτρέποντάς τους τη μεταφόρτωση αναβαθμίσεων στα συστήματα ή να εκτελούν απομακρυσμένη συντήρηση. Τα εξωτερικά σημεία πρόσβασης τέτοιων συνδέσεων πρέπει να ασφαλίζονται για να αποφεύγετε η μη εξουσιοδοτημένη πρόσβαση. **Εικόνα [26]**

iii. Άλλα δίκτυα, όπως τα δίκτυα πρόσβασης επισκεπτών, μπορεί να είναι ανεξέλεγκτα, για παράδειγμα αυτά που σχετίζονται με δραστηριότητες αναψυχής επιβατών ή η ιδιωτική πρόσβαση στο Διαδίκτυο για το πλήρωμα. Κανονικά, οποιοδήποτε ασύρματο δίκτυο θα πρέπει να θεωρείται ανεξέλεγκτο.

Τα ενσωματωμένα δίκτυα πρέπει να διαχωρίζονται από τείχη προστασίας για τη δημιουργία ασφαλών ζωνών. Όσο λιγότεροι σύνδεσμοι επικοινωνίας και συσκευές σε μια ζώνη, τόσο πιο ασφαλή είναι τα συστήματα και τα δεδομένα σε αυτή τη ζώνη. Τα κρίσιμα συστήματα ασφάλειας και ασφάλειας πρέπει να βρίσκονται στην πιο προστατευμένη ζώνη.



Εικόνα 26 Πεδία για την προστασία των συσκευών [SANS Institute 2020]

4.1.6 Φυσική Ασφάλεια

Ο κρίσιμος εξοπλισμός ασφαλείας και οι διαδρομές καλωδίων πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Η φυσική ασφάλεια είναι μια κεντρική πτυχή της ασφάλειας στον κυβερνοχώρο.

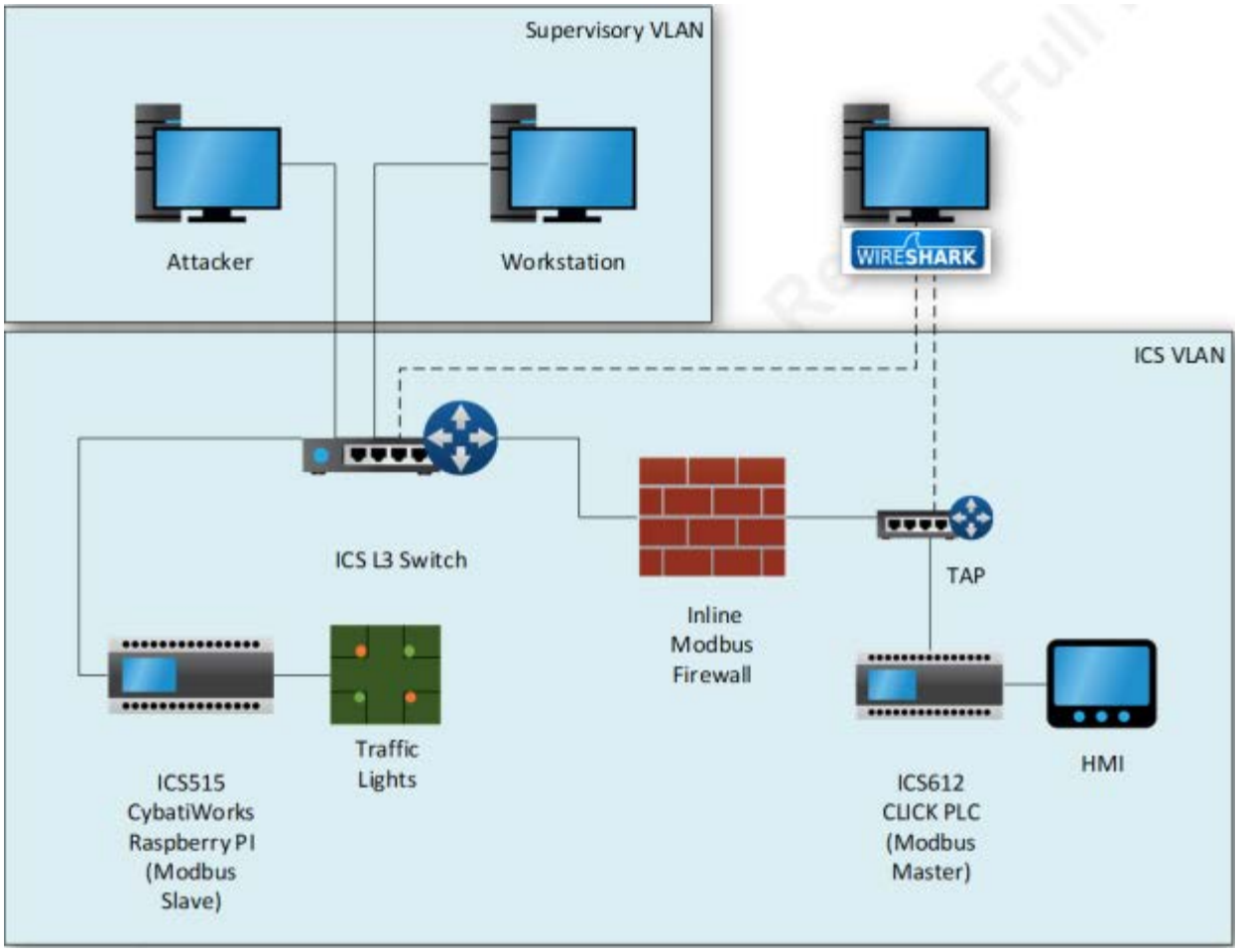
4.1.7 Εντοπισμός και ειδοποιήσεις

Ο εντοπισμός των επιτιθέμενων καθώς και των μολύνσεων αποτελεί ζωτικό μέρος των ελέγχων. Ένα βασικό σημείο του δικτύου λειτουργιών είναι να καθοριστούν οι αναμενόμενες ροές δεδομένων για τους χρήστες και τα συστήματα καθώς θα πρέπει να τα διαχειριστούν έτσι ώστε να καθοριστούν οι απαραίτητες προειδοποιήσεις για τα συμβάντα.

Επιπλέον, μια εταιρεία μπορεί να επιλέξει στο πλοίο της να ενσωματώσει ένα σύστημα εντοπισμού εισβολής (IDS) ή ένα σύστημα πρόληψης εισβολής (IPS) στο δίκτυο ή ως ένα μέρος του τείχους προστασίας. Ορισμένες από τις κύριες λειτουργίες τους περιλαμβάνουν την αναγνώριση απειλών, την κακόβουλη δραστηριότητα, και στη συνέχεια η καταγραφή, και αναφορά για απόπειρα αποκλεισμού. [24]–[26]

Τέλος πρέπει να διασφαλιστεί ότι το αφοσιωμένο προσωπικό επί του πλοίου μπορεί να

κατανοήσει τις ειδοποιήσεις και τις επιπτώσεις τους. Συμβάντα που ανιχνεύονται θα πρέπει να απευθύνονται στο ανώτερο άτομο, ο οποίος είναι υπεύθυνο για τέτοιου είδους προειδοποιήσεις. **Εικόνα [27]**



Εικόνα 27 Προσημείωση εργαστήριου για διαμόρφωση εσωτερικής ασφαλείας [SANS Institute 2020]

4.1.8 Δορυφορική και ραδιοεπικοινωνία

Η ασφάλεια στον κυβερνοχώρο της ραδιοφωνικής και δορυφορικής σύνδεσης θα πρέπει να εξεταστεί σε συνεργασία με τους παρόχους υπηρεσιών (ISPs). Στο πλαίσιο αυτό, πρέπει να ληφθεί υπόψη η προδιαγραφή του δορυφορικού συνδέσμου κατά τον καθορισμό των απαιτήσεων για την προστασία δικτύου επί του πλοίου.

Όταν δημιουργείτε μια σύνδεση ανερχόμενης ζεύξης για συστήματα πλοήγησης και ελέγχου πλοίων, θα πρέπει να δοθεί προσοχή στον τρόπο αποφυγής της απόκτησης παράνομων συνδέσεων στη πρόσβαση στα ενσωματωμένα συστήματα.

Η διασύνδεση πρόσβασης είναι ευθύνη του συνεργάτη διανομής. Η τελική δρομολόγηση

της κίνησης των χρηστών από το σημείο πρόσβασης στο Διαδίκτυο έως τον τελικό προορισμό του («τελευταίο μίλι») , είναι η ευθύνη του εφοπλιστή. Η κίνηση των χρηστών κατευθύνεται μέσω του εξοπλισμού επικοινωνίας για μετάδοση επί του πλοίου. Στο σημείο πρόσβασης για αυτήν την κίνηση, είναι απαραίτητο να παρέχεται ασφάλεια δεδομένων, τείχος προστασίας και μια αποκλειστική σύνδεση "τελευταίου μιλίου".

Όταν χρησιμοποιείτε ένα Εικονικό Ιδιωτικό Δίκτυο (VPN) όπως είπαμε και παραπάνω, η κίνηση δεδομένων πρέπει να είναι κρυπτογραφημένη σε αποδεκτό Διεθνές πρότυπο. Επιπλέον, ένα τείχος προστασίας μπροστά από τους διακομιστές και τους υπολογιστές που είναι συνδεδεμένα τα δίκτυα (στην ξηρά ή επί του πλοίου) πρέπει να αναπτυχθούν. Ο συνεργάτης διανομής θα πρέπει να υποδεικνύει τη δρομολόγηση και τον τύπο σύνδεσης που ταιριάζει περισσότερο σε συγκεκριμένη κίνηση. Το χερσαίο φιλτράρισμα (επιθεώρηση / αποκλεισμός) της κυκλοφορίας είναι επίσης θέμα μεταξύ ενός πλοιοκτήτη και του συνεργάτη διανομής. Ωστόσο, δεν αρκεί να υπάρχει είτε φιλτράρισμα κίνησης στην ξηρά είτε τείχος προστασίας / ασφάλεια επιθεώρηση / αποκλεισμός πυλών στο πλοίο, χρειάζονται και οι δύο τύποι και να συμπληρώνουν ο καθένας τον άλλο για να επιτευχθεί έτσι ένα επαρκές επίπεδο προστασίας. [24]–[26]

Οι παραγωγοί δορυφορικών τερματικών επικοινωνίας και άλλου εξοπλισμού επικοινωνίας μπορούν να παρέχουν διασυνδέσεις διαχείρισης με λογισμικό ελέγχου ασφαλείας που είναι προσβάσιμα μέσω του δικτύου. Αυτά παρέχονται κυρίως με τη μορφή Ιστοσελίδας μέσω του διαδικτύου. Η προστασία τέτοιων διασαφών πρέπει να λαμβάνετε υπόψιν κατά την αξιολόγηση της ασφάλειας της εγκατάστασης ενός πλοίου.

4.1.9 Τυποποίηση

Μέσα από την τυποποίηση, διαδικασιών ασφάλειας δομών θα υπάρξει μεγαλύτερη ασφάλεια από τις κυβερνοεπιθέσεις.. Ο στόχος είναι η αύξηση της συμβατότητας και, συνεπώς, η βελτιστοποίηση των πόρων.

4.1.10 Σκοπός των οδηγιών στα πρότυπα

Στην ανάπτυξη νέων συστημάτων, οι δυνατότητες τυποποίησης χρησιμοποιούνται μόνο σε μερικές περιπτώσεις σήμερα. Τα έργα PLC και SCADA αντιγράφονται συχνά χειροκίνητα μαζί από έργα υπαρχόντων μηχανημάτων και προσαρμόζονται αναλόγως.

Υπάρχει μια πολύ μεγάλη ποικιλία στυλ προγραμματισμού και διαλέκτων γλωσσών προγραμματισμού. Ο οδηγός τυποποίησης μας δείχνει πώς μπορούμε να διαμορφώσουμε τις μηχανές και τα συστήματά μας. Μας δίνει συστάσεις και συμβουλές για δομημένο και τυποποιημένο προγραμματισμό λύσεων του αυτοματισμού μας. Ένα βασικό στοιχείο για την ανάπτυξη και την κατασκευή ενός προτύπου είναι ο ορισμός διεπαφής των ενοτήτων (interfaces modules). Προκειμένου οι μονάδες να χρησιμοποιούνται με ευελιξία, οι διεπαφές πρέπει να είναι όσο το δυνατόν πιο ανεξάρτητες από τις ειδικές απαιτήσεις των πελατών και της αντίστοιχης μονάδας. [27]

4.1.11 Ανάπτυξη εκτίμησης ασφάλειας στο κυβερνοχώρο (CSA)

Ο σκοπός της αξιολόγησης της ασφάλειας στον κυβερνοχώρο είναι να υιοθέτηση μιας προσέγγισης διαχείρισης κινδύνων που έχει ως στόχο την αξιολόγηση και τον μετριασμό των κινδύνων που συνδέονται με τους παράγοντες απειλής που σχετίζονται με το πλοίο ή τα πλοία που αξιολογούνται. Τα οφέλη αυτής της υιοθέτησης αποσκοπούν στην προσέγγιση ότι οι κίνδυνοι ασφάλειας στον κυβερνοχώρο μπορεί να έχουν προτεραιότητα, επιτρέποντας κατάλληλες επενδύσεις εκεί που πρέπει να γίνουν και τον μετριασμό αυτών, που δυνητικά θα είχαν μεγαλύτερο αντίκτυπο στο πλοίο.

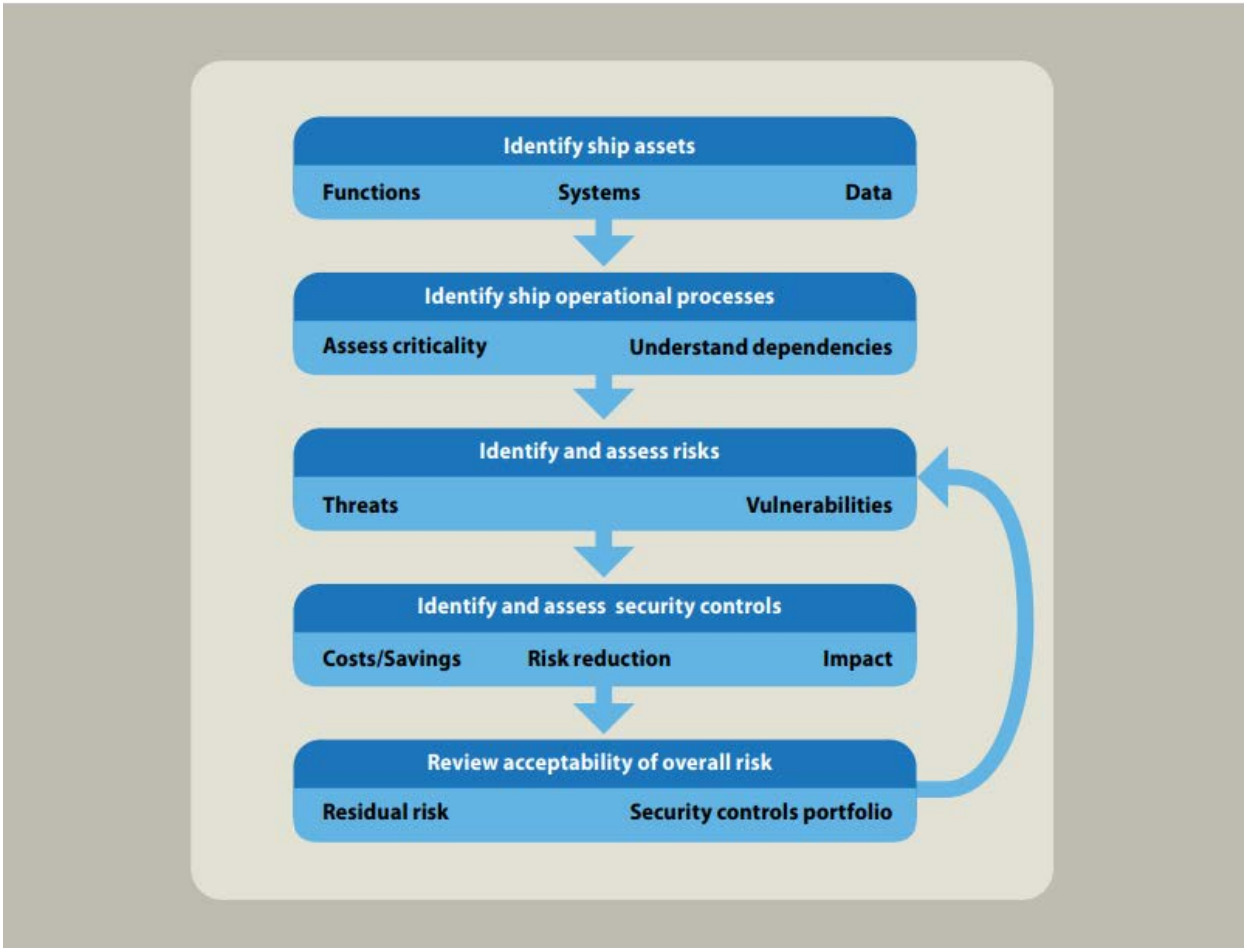
Οι αξιολογήσεις ασφάλειας διενεργούνται σύμφωνα με τα πρότυπα ασφάλειας του πλοίου. Ο σκοπός αυτών των αξιολογήσεων είναι κυρίως ο εντοπισμός τρωτών σημείων σε φυσικό επίπεδο καθώς και τα μέτρα ασφαλείας για το προσωπικό και τις επιχειρηματικές διαδικασίες της Εταιρείας / πλοίου που μπορεί οδηγήσουν σε περιστατικό ασφαλείας, ενδείκνυται να δημιουργηθεί το CSA (Cyber Security assessment) βάσει των υφιστάμενων αξιολογήσεων ασφαλείας. [24]–[26]

Όπως ορίζονται τα πρότυπα ασφάλειας του πλοίου όπως απεικονίζεται στο **Γράφημα [8]**, αυτές οι αξιολογήσεις θα πρέπει να περιλάβουν το πλοίο ως ένα πλήρες σύστημα φυσικής κυβερνομηχανής που θα περιλαμβάνει:

a) Τον προσδιορισμό και αξιολόγηση βασικών ή ευαίσθητων στοιχείων και υποδομών (για παράδειγμα, εγκαταστάσεις, συστήματα και δεδομένα) που θεωρούνται σημαντικά για την προστασία του πλοίου, και τα εξωτερικά συστήματα υποδομής από τα οποία εξαρτώνται.

b) Τον προσδιορισμό των επιχειρηματικών διαδικασιών του πλοίου χρησιμοποιώντας τα στοιχεία και την υποδομή, έτσι ώστε να αξιολογείται η κρίσιμη σημασία των στοιχείων και να κατανοούνται τυχόν εσωτερικά και εξωτερικά ζητήματα.

c) Τον προσδιορισμό , την αξιολόγηση, την επιλογή και την ιεράρχηση των ελέγχων ασφαλείας και αλλαγές στην διαδικασία, με βάση το κόστος τους, το επίπεδο αποτελεσματικότητας στη μείωση των κίνδυνων και την οποιαδήποτε επίπτωση μπορεί να έχουν στις εργασίες του πλοίου.



Γράφημα 8 Γενική Εικόνα Λειτουργίας του CSA

4.1.12 Αναπτύσσοντας σχέδιο αποτροπής κυβερνοεπίθεσης (CSP)

Οι αξιολογήσεις ασφάλειας ενός πλοίου αποτελούν τη βάση των σχεδίων ασφαλείας για το πλοίο. Αυτά τα σχέδια πρέπει να αντιμετωπίζουν τα κυρίως φυσικά και προσωπικά

ζητήματα που προσδιορίζονται στη σχετική αξιολόγηση μέσω της θέσπισης κατάλληλων μέτρων ασφαλείας που έχουν σχεδιαστεί για να ελαχιστοποιηθεί η πιθανότητα παραβίασης της ασφάλειας με συνέπειες πιθανούς κινδύνους. Προβλέπεται ότι, όπου ενδείκνυται, το CSP (Cyber Security Plan) θα βασίζεται στο υφιστάμενο σχέδιο ασφάλειας πλοίου (SSP – Ship Security Plan) και μπορεί να αποτελεί παράρτημά του. Έτσι, τα μέτρα στοχεύουν στη μείωση του κινδύνου μη εξουσιοδοτημένης πρόσβασης στο πλοίο που θα πρέπει επίσης να δώσει ένα βαθμό προστασίας στα φυσικά του συστήματα.

Ένα CSP θα πρέπει να εκτελεί την ίδια λειτουργία και για τα ζητήματα που εντοπίζονται στο CSA (Cyber Security Assessment) λαμβάνοντας υπόψη τον αντίκτυπο των μέτρων που ορίζονται στο σχέδιο ασφαλείας για το πλοίο και τα συστήματά του. [24]–[26]
Κατά την ανάπτυξη του CSP, είναι απαραίτητο να υιοθετηθεί μια ολιστική προσέγγιση, η οποία να καλύπτει το άτομα, τις διαδικασίες, τις φυσικές και τεχνολογικές πτυχές του πλοίου. Με την προοπτική ασφάλειας στον κυβερνοχώρο, το CSP πρέπει να περιέχει ή να αναφέρεται:

a) στις πολιτικές που καθορίζουν τους επιχειρηματικούς κανόνες που σχετίζονται με την ασφάλεια και προέρχονται από το SSP.

b) στις διαδικασίες που προέρχονται από τις πολιτικές ασφαλείας και παρέχουν οδηγίες για τη συνεπή εφαρμογή τους καθ’ όλη τη διάρκεια του κύκλου ζωής και της χρήσης του πλοίου.

c) στις διαδικασίες που περιλαμβάνουν τις λεπτομερείς οδηγίες εργασίας σχετικά με επαναλαμβανόμενους μηχανισμούς για την υλοποίηση των επιχειρησιακών διαδικασιών.

Με ένα μεγάλο ποσοστό παραβιάσεων ασφαλείας που προκαλούνται από ανθρώπους και κακές διαδικασίες, είναι απαραίτητο το προσωπικό, οι διαδικασίες να σχετίζονται άμεσα με τα τεχνολογικά συστήματα για τα οποία απαιτούνται μέτρα ασφάλειας στον κυβερνοχώρο, λαμβάνονται επίσης υπόψη και τα κατάλληλα μέτρα. Για παράδειγμα, ευαίσθητα συστήματα πλοίων μπορεί να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση ως εξής:

a) Σε φυσικό επίπεδο - το σύστημα και τα στοιχεία του ενδέχεται να βρίσκονται σε περιορισμένη προσβάσιμη περιοχή, στην οποία επιτρέπεται μόνο το προσωπικό που έχει λάβει άδεια πρόσβασης για μη επιτηρούμενη πρόσβαση, έτσι διατηρείται αρχείο καταγραφής όλου του εξουσιοδοτημένου προσωπικού και ενημερώνεται τακτικά.

b) Σε επιπέδου προσωπικού – το προσωπικό που έχει προνομιακή (διοικητικό, μηχανικών ή τεχνική υποστήριξη) πρόσβαση στα συστήματα υπόκειται σε έλεγχο πριν από την απασχόληση τους καθώς και περιοδικοί έλεγχοι ιστορικού.

c) Σε τεχνικό επίπεδο – πρέπει να υπάρχουν μέτρα για τον έλεγχο τυχόν αφαιρούμενων μέσων ή φορητών συσκευών που θα συνδεθούν στο σύστημα για κακόβουλο λογισμικό (για παράδειγμα, λογισμικό ενημερώσεις σε USB stick ή διαγνωστικό λογισμικό σε φορητούς υπολογιστές ή tablet συσκευές). Η πρόσβαση σε κονσόλες συστημάτων, οθόνες κ.λπ. θα πρέπει προστατεύεται με κωδικό πρόσβασης.

Εδώ πρέπει να σημειωθεί ότι τα μέτρα που απαιτούνται σε κάθε μία από τις πτυχές αυτές θα εξαρτώνται επίσης από το επίπεδο ανθεκτικότητας που μπορεί να έχει το πλοίο.

Τέλος πρέπει να καθιερωθεί τακτική εκπαίδευση και αξιολόγηση για όλους εκείνους που τους χορηγούνται «εξουσιοδοτημένη» πρόσβαση σε συστήματα και υποσυστήματα για να διασφαλιστεί έτσι μια κατάλληλη ‘’υγιεινή’’ στον κυβερνοχώρο κατά την πρόσβαση σε συστήματα για οποιονδήποτε λόγο. [24]–[26]

Κεφάλαιο 5
Συμπεράσματα

5.1 Συμπεράσματα

Με τις μεταβαλλόμενες και αναδυόμενες απειλές για τα SCADA και τα συστήματα ελέγχου διεργασιών, οι ιδιοκτήτες και οι χειριστές αυτών των συστημάτων θα πρέπει να ρίξουν μια πιο προσεκτική ματιά στους ελέγχους πρόσβασης στον κυβερνοχώρο που χρησιμοποιούνται επί του παρόντος για την υπεράσπιση αυτών των συστημάτων από εξωτερικές και εσωτερικές απειλές. Η βιομηχανία των επικοινωνιών Ethernet TCP / IP στα τέλη της δεκαετίας του 1990 εισήγαγε στα SCADA και στα συστήματα ελέγχου διεργασιών στην αγορά εξαρτήματα με δυνατότητες επικοινωνίας Ethernet. Τώρα είναι πολύ συνηθισμένο να βρίσκονται επικοινωνίες IP σε όλο το περιβάλλον συστημάτων ελέγχου SCADA/PLC. Η τάση συνεχίζεται με τους κατασκευαστές και τους χειριστές συστημάτων SCADA/PLC να παρέχουν μόνο μία περιμετρική λύση στην κυβερνοάμυνα κατά τη σύνδεση μεταξύ των δικτύων SCADA και IT. Αυτή η αμυντική λύση, όπως ένα τείχος προστασίας, είναι μια καλή αρχή, αλλά αφήνει το εσωτερικό του περιβάλλοντος SCADA/PLC ανασφαλές και ευάλωτο. Αυτή η επίπεδη σχεδίαση δικτύου στο περιβάλλον SCADA/PLC επιτρέπει τόσο εξωτερικές όσο και εσωτερικές απειλές να διαδίδουν και να επηρεάζουν τις τελικές συσκευές που ελέγχουν τον φυσικό εξοπλισμό. Αρκετές νέες και καινοτόμες τεχνικές είναι διαθέσιμες για χρήση για τη διασφάλιση του εσωτερικού του περιβάλλοντος SCADA, καθώς και για την παροχή ασφαλούς απομακρυσμένης πρόσβασης σε αυτό. Γνωρίζοντας τι ευπάθειες βρίσκονται στα SCADA/PLC συστήματα και στα Συστήματα Ελέγχου Διαδικασίας, οι εξωτερικές και οι εσωτερικές απειλές μπορούν να επωφεληθούν από αυτές τις ευπάθειες και το να γνωρίζουμε πώς να

εφαρμόζουμε νέες αμυντικές λύσεις για την αποτροπή, την υπεράσπιση και τον εντοπισμό των απειλών στον κυβερνοχώρο είναι το κλειδί για την προστασία αυτών των κρίσιμων συστημάτων.

Ένα σημείο που πρέπει να σημειωθεί είναι ότι ορισμένες ευπάθειες είναι δύσκολο να εντοπιστούν χωρίς να εξεταστούν από ειδικούς ασφαλείας. Μια έρευνα διαπίστωσε ότι η αποτυχία που προέκυψε λόγω της αύξησης της κυκλοφορίας δεδομένων του δικτύου - που μοιάζει με μια κακόβουλη επίθεση άρνησης υπηρεσίας (denial-of-service attack)- που προήλθε από ένα δυσλειτουργικό PLC. Περαιτέρω έρευνα αποκάλυψε ότι οι συσκευές στο δίκτυο ήταν ευάλωτες σε τέτοιου είδους προβλήματα εν μέρει επειδή οι κατασκευαστές τους δεν είχαν δοκιμάσει ποτέ τη συμπεριφορά τους κατά το χειρισμό κακών δεδομένων.

Το κλειδί για την αποκάλυψη δυσκολιών όπως αυτές του Brown's Ferry plant έγκειται στο να εκτελέσουμε αυτό που λέγεται σάρωση ευπάθειας και διείσδυσης (vulnerability and penetration scans). Οι αξιολογήσεις ευπάθειας γενικά χρησιμοποιούν ένα πακέτο λογισμικού, όπως το Nessus ή το OpenVas, για τη σάρωση μιας σειράς διευθύνσεων IP για γνωστά τρωτά σημεία. Στη συνέχεια, το λογισμικό παράγει μια αναφορά που παραθέτει τις ευπάθειες που εντοπίστηκαν και, ανάλογα με το λογισμικό, θα δείξει τη σοβαρότητα της ευπάθειας και τα βασικά βήματα αποκατάστασης. Συγκεκριμένα, αυτοί οι σαρωτές χρησιμοποιούν μια λίστα γνωστών τρωτών σημείων - δηλαδή εκείνων που είναι ήδη γνωστοί στην κοινότητα ασφαλείας, τους χάκερ και τους προμηθευτές λογισμικού. Δεν θα βρουν ευπάθειες που δεν έχουν ακόμη ανακαλυφθεί από την κοινότητα ασφαλείας.

Μια δοκιμή διείσδυσης μοιάζει με σάρωση ευπάθειας αλλά πηγαίνει βαθύτερα. Όταν εντοπίσει μια ευπάθεια, προσπαθεί να ανακαλύψει το βάθος του προβλήματος και να ανακαλύψει ακριβώς τι είδους πληροφορίες θα μπορούσαν να αποκαλυφθούν εάν αξιοποιηθούν. Τα αποτελέσματα ταξινομούνται συνήθως κατά σοβαρότητα με τα βήματα αποκατάστασης που παρέχονται. Υπάρχουν εμπορικά εργαλεία για δοκιμές διείσδυσης, αλλά πολλές εταιρείες ασφαλείας γράφουν τις δικές τους.

Με πλήρη σάρωση ευπάθειας και διείσδυσης, το συνηθισμένο επόμενο βήμα είναι μια ανάλυση κινδύνου. Η ιδέα είναι να καθίσουμε και να εξετάσουμε κάθε συγκεκριμένη ευπάθεια, όπως ένα εύρημα από ένα τεστ διείσδυσης, και να εξακριβώσουμε τον κίνδυνο

εάν πρέπει να αξιοποιηθεί η ευπάθεια. Για παράδειγμα, στην περίπτωση PLC, μια ανάλυση κινδύνου μπορεί να εξετάσει πού βρίσκεται το PLC στην υποδομή δικτύου, τα δεδομένα που αποθηκεύει και τις εργασίες που χειρίζεται. Ένα PLC που διαχειρίζεται μια γραμμή συναρμολόγησης μπορεί να έχει μια πολύ διαφορετική στάση κινδύνου από εκείνη που τρέχει έναν χειριστή αέρα.

Στη συνέχεια, η ανάλυση να μπορεί να εξετάσει τις απειλές που ενδέχεται να εκμεταλλευτούν κάθε ευπάθεια - όπως χάκερ, θυμωμένους υπαλλήλους ή δυσλειτουργικό υλικό - και δημιουργεί ένα προφίλ δυνατοτήτων, κινήτρων και στόχων. Στη συνέχεια, η ανάλυση αυξάνει τον αντίκτυπο στην εταιρεία κάθε ευπάθειας. Το αποτέλεσμα της ανάλυσης κινδύνου είναι μια αξιολόγηση κινδύνου με προτεινόμενες μεθόδους για περαιτέρω μείωση κάθε κινδύνου. Οι διαχειριστές μπορούν στη συνέχεια να αποφασίσουν εάν θα εφαρμόσουν τις προτεινόμενες αλλαγές.

Τέλος, όταν συμβαίνει παραβίαση ασφαλείας, ο χρόνος είναι ουσιαστικός. Τα άτομα που έχουν πρόσβαση στο περιβάλλον του συστήματος ελέγχου πρέπει να είναι αξιόπιστα. Όποιος εργάζεται με το σύστημα ελέγχου πρέπει να είναι καλά καταρτισμένος και ενημερωμένος με την ομάδα ή / και την εταιρεία του. Για αυτό το λόγο όλες οι εταιρείες αυτού του τομέα είναι σημαντικό να λάβουν τα απαραίτητα μέτρα , επενδύοντας στα κατάλληλα συστήματα, μειώνοντας τους κινδύνους και τις απειλές από το κυβερνοχώρο.

Βιβλιογραφία

[1] European Network and Information Security Agency ., *Window of exposure… a real problem for SCADA systems?: recommendations for Europe on SCADA patching*. LU: Publications Office, 2013. Accessed: Apr. 07, 2021. [Online]. Available: https://data.europa.eu/doi/10.2824/25757

[2] "What is SCADA?," *Inductive Automation*. https://inductiveautomation.com/resources/article/what-is-scada (accessed Apr. 07, 2021).

[3] "What is SCADA Security? Protecting SCADA Networks | Forcepoint." https://www.forcepoint.com/cyber-edu/scada-security (accessed Apr. 07, 2021).

[4] "What is SCADA Security," *Forcepoint*, Aug. 09, 2018. https://www.forcepoint.com/cyber-edu/scada-security (accessed Apr. 07, 2021).

[5] "What Are PLCs and Why Are They Important? | Fine Line Marine Electric." https://www.finelinemarineelectric.com/blog/what-are-plcs-and-why-are-they-important/ (accessed Apr. 07, 2021).

[6] M. Hoffman, "Vulnerabilities on the Wire: Mitigations for Insecure ICS Device Communication." Feb. 06, 2020.

[7] "Vulnerabilities in Siemens' most secure industrial PLCs can lead to industrial havoc," *Help Net Security*, Aug. 09, 2019. https://www.helpnetsecurity.com/2019/08/09/siemens-plc-vulnerabilities/ (accessed Apr. 07, 2021).

[8] R. J. Robles, M. Choi, E. Cho, S. Kim, G. Park, and S.-S. Yeo, "Vulnerabilities in SCADA and Critical Infrastructure Systems," p. 6.

[9] "Top IoT security vulnerabilities: 2020 and beyond." https://www.perle.com/articles/top-iot-security-vulnerabilities-2020-and-beyond-40189357.shtml (accessed Apr. 07, 2021).

[10] Sivaranjith, "Top 15 PLC brands," *Instrumentation and Control Engineering*, Aug. 09, 2019. https://automationforum.co/plc-learning-series-10-top-15-plc-brands/ (accessed Apr. 07, 2021).

[11] F. Paul, "Top 10 IoT vulnerabilities," *Network World*, Jan. 14, 2019. https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html (accessed Apr. 07, 2021).

[12] "Top 10 Critical Infrastracture and SCADA/ICS Cybersecurity Vulnerabilities and Threats." Checkpoint.

[13] "To make better decisions, you need to see the big picture.," *IHS Markit*. https://ihsmarkit.com/products/maritime-shipping-intelligence.html (accessed Apr. 07, 2021).

[14] C. Null, "The state of IoT security: OWASP Top Ten highlights challenges," *TechBeacon*. https://techbeacon.com/security/state-iot-security-owasp-top-ten-highlights-challenges (accessed Apr. 07, 2021).

[15] "Strong Password Protection." https://www.nortonlifelockpartner.com/security-center/strong-password.html (accessed Apr. 07, 2021).

[16] “Standardization Guideline.” Siemens.
[17] “SIMATIC SCADA systems Siemens prochure.” https://assets.new.siemens.com/siemens/assets/api/uuid:48100bcd-41c5-4594-9132-48611270ca7a/dffa-b10338-01-7600-simatic-scada-systems-broschuere-144.pdf (accessed Apr. 08, 2021).
[18] “SIMATIC SCADA Systems,” *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industry-software/automation-software/scada.html (accessed Apr. 08, 2021).
[19] “Siemens Simatic Step 7 : List of security vulnerabilities.” https://www.cvedetails.com/vulnerability-list/vendor_id-109/product_id-22699/Siemens-Simatic-Step-7.html (accessed Apr. 07, 2021).
[20] O. Mares, “Siemens PLC affected by exploitable vulnerabilities,” *Information Security Newspaper | Hacking News*, Feb. 12, 2020. https://www.securitynewspaper.com/2020/02/12/siemens-plc-scalance-simantic-siplus-affected-by-exploitable-vulnerabilities/ (accessed Apr. 07, 2021).
[21] H. Kim, “Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks,” *International Journal of Distributed Sensor Networks*, vol. 8, no. 11, p. 268478, Nov. 2012, doi: 10.1155/2012/268478.
[22] “Secure Scada Networks.”
[23] T. Yardley, “SCADA: issues, -vulnerabilities, and future directions,” vol. 33, no. 6, p. 7, 2008.
[24] “SCADA systems plagued by insecure development and slow patching,” *Help Net Security*, May 23, 2017. https://www.helpnetsecurity.com/2017/05/23/scada-systems-insecure/ (accessed May 09, 2021).
[25] “Scada systems and their vulnerabilities.” https://www.secpoint.com/scada-systems-their-vulnerabilities.html (accessed Apr. 07, 2021).
[26] “SCADA System Vulnerabilities to Cyber Attack,” *Electric Energy Online*. https://electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm (accessed Apr. 07, 2021).
[27] Yogesh Sahu, “SCADA system vulnerabilities and Threat to critical infrastructure.” Tata Power.
[28] “SCADA Market by Size, Share, and Industry Analysis - 2023,” *Allied Market Research*. https://www.alliedmarketresearch.com/scada-market (accessed May 07, 2021).
[29] “SCADA and Mobile Security in the IoT Era,” *IOActive*, Jan. 11, 2018. https://ioactive.com/scada-and-mobile-security-in-iot-era/ (accessed Apr. 07, 2021).
[30] “SCADA,” *Wikipedia*. Apr. 27, 2021. Accessed: May 05, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=SCADA&oldid=1020067574
[31] “Samsung Standardization Guideline.pdf.” Samsung.
[32] “Safety at Sea and BIMCO publish cyber security white paper.” https://www.bimco.org/news/priority-news/20190916-safety-at-sea-and-bimco-publish-cyber-security-white-paper (accessed Apr. 07, 2021).
[33] “Researchers find 147 vulnerabilities in 34 SCADA mobile applications,” *SC Media*, Jan. 11, 2018. https://www.scmagazine.com/home/security-news/network-security/researchers-find-147-vulnerabilities-in-34-scada-mobile-applications/ (accessed Apr. 07, 2021).
[34] R. Leszczyna, “Protecting Industrial Control Systems,” p. 72.
[35] M. H. Moradi and M. R. Katebi, “Predictive PID Control for Ship Autopilot Design,” *IFAC Proceedings Volumes*, vol. 34, no. 7, pp. 375–380, Jul. 2001, doi: 10.1016/S1474-6670(17)35111-X.
[36] N. Dahl, “PLCs in Marine Monitoring,” p. 8.
[37] “PLC’s and SCADA: Vulnerabilities and Security Issues,” *Online Technical Training*

Programs | George Brown College, Mar. 18, 2016. https://www.gbctechtraining.com/blog/plcs-scada-security-vulnerabilities (accessed Apr. 07, 2021).
[38] "PLC Timeline." http://www.plcdev.com/plc_timeline (accessed Apr. 08, 2021).
[39] "PLC security in the age of the IIoT," *Design World*, Apr. 25, 2018. https://www.designworldonline.com/plc-security-in-the-age-of-the-iiot/ (accessed Apr. 07, 2021).
[40] G. P. H. Sandaruwan, P. S. Ranaweera, and V. A. Oleshchuk, "PLC Security and Critical Infrastructure Protection," p. 7.
[41] c3controls, "PLC PROGRAMMING THEN & NOW: THE HISTORY OF PLC'S," *v2*. https://www.c3controls.com/white-paper/history-of-programmable-logic-controllers/ (accessed Apr. 08, 2021).
[42] Steven, "PLC Manufacturers: The Latest PLC Brands, Rankings & Revenues," *Ladder Logic World*, Jun. 20, 2020. https://ladderlogicworld.com/plc-manufacturers/ (accessed Apr. 07, 2021).
[43] "PLC History, Development, Functions & System Tools," *Technique Learning Solutions*, Sep. 24, 2014. https://learntechnique.com/plc-history-development-functions-system-tools/ (accessed Apr. 07, 2021).
[44] S. E. Valentine, "PLC Code Vulnerabilities Through SCADA Systems," p. 137.
[45] M. T. Jamsutkar, M. S. Gore, M. P. Patil, and A. Suryawanshi, "PLC BASED SYSTEM FOR CONTROLLING AND MONITORING PARAMETERS IN SHIP," vol. 3, no. 4, p. 5, 2014.
[46] Edward Amoroso and Andrew Ginter, "OT Security for IT Professionals Handbook." Waterfall.
[47] Dr. J.M. Ceron, Dr. J.J.Chromik, Dr. J.J.C. Santanna, and Prof. dr. ir. A. Pras, "Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands." Universiteit Twente.
[48] "One Flaw too Many: Vulnerabilities in SCADA Systems - Security News." https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems (accessed Apr. 07, 2021).
[49] S. H. H. Education Norwegian University of Science and Technology (NTNU); and Erik David Martin, Noroff, "More exploits: the great PLC hack," *Control Design*. https://www.controldesign.com/articles/2018/more-exploits-the-great-plc-hack/ (accessed Apr. 07, 2021).
[50] "MicroSCADA-X-NC-distribution-1MRS756253-A4.pdf."
[51] Lech Kobylinsky, "Marine Transport and the Fourth Industrial Revolution." Apr. 2016.
[52] E. A. Offiong, "Marine automation and impact on shipboard machinery," p. 319.
[53] "M5: Poor Authorization and Authentication | OWASP." https://owasp.org/www-project-mobile-top-10/2014-risks/m5-poor-authorization-and-authentication.html (accessed May 10, 2021).
[54] Dr. J.M. Ceron, Dr. J.J.Chromik, Dr. J.J.C. Santanna, and Prof. dr. ir. A. Pras, "ISC/SCADA Device Discoverability." Universiteit Twente.
[55] M. K. Rajeswar, "Industry 4.0 wave - Relevance of SCADA in an IOT world and journey towards a true digital enterprise," vol. 14, no. 3, p. 11, 2019.
[56] Stevan A. Milinkoviü and Ljubomir R. Laziü, "Industrial PLC security issues," p. 5.
[57] S. A. Milinkovic and L. R. Lazic, "Industrial PLC security issues," in *2012 20th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, Nov. 2012, pp. 1536–1539. doi: 10.1109/TELFOR.2012.6419513.
[58] Oxana Andreeva *et al.*, "Industrial Cotrol Systems Vulnerabilities Statistics." KASPERSKY.
[59] "Industrial Controls & Remote I/O – A focus on the PLC market." https://www.interactanalysis.com/industrial-controls-remote-i-o-a-focus-on-the-plcs-

market/ (accessed Apr. 07, 2021).
[60] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Tucson, AZ, USA, Sep. 2016, pp. 25–30. doi: 10.1109/ISI.2016.7745438.
[61] "ICS-CERT Monitor." ICS-CERT, Jul. 2011.
[62] "ICS vulnerabilities." Positive Technologies, 2018.
[63] G. Ward, "How your ship has probably been Cyber Attacked already," p. 5.
[64] "How to Choose a PLC: Pros and Cons of 3 Popular Vendors," *Affinity Energy*, Nov. 30, 2016. https://www.affinityenergy.com/how-to-choose-a-plc-next-controls-project/ (accessed Apr. 07, 2021).
[65] "Hitachi Completes Acquisition of ABB's Power Grids Business; Hitachi ABB Power Grids Begins Operation," p. 10.
[66] "History of the PLC | Library.AutomationDirect," *Library.Automationdirect.com*, Aug. 05, 2015. https://library.automationdirect.com/history-of-the-plc/ (accessed Apr. 07, 2021).
[67] "Hijacking a PLC Using its Own Network Features," *Dark Reading*. https://www.darkreading.com/vulnerabilities---threats/hijacking-a-plc-using-its-own-network-features/d/d-id/1333660 (accessed Apr. 07, 2021).
[68] "Hackers took 'full control' of container ship's navigation systems for 10 hours @AsketO." https://www.asket.co.uk/post/2017/11/26/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-asketoperati (accessed Apr. 07, 2021).
[69] Brian Gorenc and Fritz Sands, "Hacker Machine Interface: The State of SCADA HMI Vulnerabilities," *Trend Micro*, p. 30.
[70] "Guidelines on Cyber Security Onboard Ships V4."
[71] "Guidelines on Cyber Security Onboard Ships V2." Jul. 2017.
[72] "Getting Rid Of Weak Passwords To Improve Security," *Teamstack Blog*, Mar. 31, 2020. https://blog.teamstack.com/getting-rid-of-weak-passwords-to-improve-security/ (accessed Apr. 07, 2021).
[73] "Fairplay and BIMCO Maritime Cyber Security survey." Sep. 14, 2018.
[74] G. Tzokatziou, L. A. Maglaras, H. Janicke, and Y. He, "Exploiting SCADA vulnerabilities using a Human Interface Device," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 7, p. 8, 2015.
[75] A. Ujvarosi, "EVOLUTION OF SCADA SYSTEMS," vol. 9, no. 1, p. 6, 2016.
[76] D. Rutherford, "Ethernet for SCADA Systems Explained," p. 12.
[77] A. A. Farooq, J. Marquard, K. George, and T. Moyer, "Detecting Safety and Security Faults in PLC Systems with Data Provenance," *arXiv:1911.06304 [cs]*, Nov. 2019, Accessed: May 11, 2021. [Online]. Available: http://arxiv.org/abs/1911.06304
[78] J.-H. Huh, T. Koh, and K. Seo, "Design of a Shipboard Outside Communication Network and Its Testbed Using PLC: For Safety Management during the Ship Building Process," p. 21, 2018.
[79] "Cyber Risks in Shipping LP Briefing.pdf." The North of England P&I Association, Jul. 2017.
[80] Max J. Bobys, "Cyber Risks in Shipping LP Briefing." The North of England P&I Association.
[81] "Credential Management and Enforcement for ICS/SCADA environments," *Infosec Resources*. https://resources.infosecinstitute.com/topic/credential-management-and-enforcement-for-ics-scada-environments/ (accessed May 10, 2021).
[82] "Control Engineering | Future of the PLC," *Control Engineering*, Aug. 26, 2014. https://www.controleng.com/articles/future-of-the-plc/ (accessed Apr. 07, 2021).
[83] *Code of Practice Cyber Security for Ships*. 2017.
[84] "CERN Computer Security Information."

https://security.web.cern.ch/recommendations/en/password_alternatives.shtml (accessed Apr. 07, 2021).
[85] A. Pauna, “Can we learn from SCADA security incidents?,” p. 10, 2013.
[86] European Network and Information Security Agency., Rossella Mattioli, ENISA, and Konstantinos Moulinos, ENISA, *Analysis of ICS-SCADA cyber security maturity levels in critical sectors*. LU: Publications Office, 2015. Accessed: Apr. 07, 2021. [Online]. Available: https://data.europa.eu/doi/10.2824/835661
[87] C. Cimpanu, “All four of the world’s largest shipping companies have now been hit by cyber-attacks,” *ZDNet*. https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/ (accessed Apr. 07, 2021).
[88] “ABB named global leader in SCADA systems for the power sector.” https://new.abb.com/news/detail/2672/ABB-named-global-leader-in-scada-systems-for-the-power-sector (accessed Apr. 08, 2021).
[89] E.-M. Kalogeraki, S. Papastergiou, H. Mouratidis, and N. Polemi, “A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments,” *Applied Sciences*, vol. 8, no. 9, p. 1477, Aug. 2018, doi: 10.3390/app8091477.
[90] “A Brief History of the SCADA System,” *Process Solutions, Inc.*, Jul. 10, 2020. https://www.processsolutions.com/a-brief-history-of-the-scada-system/ (accessed Apr. 07, 2021).
[91] “21 Steps to Improve Cyber Security of SCADA Networks.” USA Departmnet of Energy.
[92] A. N. Koushik and R. Bs, “4th Generation SCADA Implementation for Automation,” vol. 5, no. 3, p. 4.
[93] E.-E. E. Portal, “3 generations of SCADA system architectures you should know about | EEP,” *EEP - Electrical Engineering Portal*, Apr. 22, 2013. https://electrical-engineering-portal.com/three-generations-of-scada-system-architectures (accessed Apr. 07, 2021).
[1] European Network and Information Security Agency ., *Window of exposure… a real problem for SCADA systems?: recommendations for Europe on SCADA patching*. LU: Publications Office, 2013. Accessed: Apr. 07, 2021. [Online]. Available: https://data.europa.eu/doi/10.2824/25757
[2] “What is SCADA?,” *Inductive Automation*. https://inductiveautomation.com/resources/article/what-is-scada (accessed Apr. 07, 2021).
[3] “What is SCADA Security? Protecting SCADA Networks | Forcepoint.” https://www.forcepoint.com/cyber-edu/scada-security (accessed Apr. 07, 2021).
[4] “What is SCADA Security,” *Forcepoint*, Aug. 09, 2018. https://www.forcepoint.com/cyber-edu/scada-security (accessed Apr. 07, 2021).
[5] “What Are PLCs and Why Are They Important? | Fine Line Marine Electric.” https://www.finelinemarineelectric.com/blog/what-are-plcs-and-why-are-they-important/ (accessed Apr. 07, 2021).
[6] M. Hoffman, “Vulnerabilities on the Wire: Mitigations for Insecure ICS Device Communication.” Feb. 06, 2020.
[7] “Vulnerabilities in Siemens’ most secure industrial PLCs can lead to industrial havoc,” *Help Net Security*, Aug. 09, 2019. https://www.helpnetsecurity.com/2019/08/09/siemens-plc-vulnerabilities/ (accessed Apr. 07, 2021).
[8] R. J. Robles, M. Choi, E. Cho, S. Kim, G. Park, and S.-S. Yeo, “Vulnerabilities in SCADA and Critical Infrastructure Systems,” p. 6.
[9] “Top IoT security vulnerabilities: 2020 and beyond.” https://www.perle.com/articles/top-iot-security-vulnerabilities-2020-and-beyond-40189357.shtml (accessed Apr. 07, 2021).
[10] Sivaranjith, “Top 15 PLC brands,” *Instrumentation and Control Engineering*, Aug. 09,

2019. https://automationforum.co/plc-learning-series-10-top-15-plc-brands/ (accessed Apr. 07, 2021).
[11] F. Paul, “Top 10 IoT vulnerabilities,” *Network World*, Jan. 14, 2019. https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html (accessed Apr. 07, 2021).
[12] “Top 10 Critical Infrastracture and SCADA/ICS Cybersecurity Vulnerabilities and Threats.” Checkpoint.
[13] “To make better decisions, you need to see the big picture.,” *IHS Markit*. https://ihsmarkit.com/products/maritime-shipping-intelligence.html (accessed Apr. 07, 2021).
[14] C. Null, “The state of IoT security: OWASP Top Ten highlights challenges,” *TechBeacon*. https://techbeacon.com/security/state-iot-security-owasp-top-ten-highlights-challenges (accessed Apr. 07, 2021).
[15] “Strong Password Protection.” https://www.nortonlifelockpartner.com/security-center/strong-password.html (accessed Apr. 07, 2021).
[16] “Standardization Guideline.” Siemens.
[17] “SIMATIC SCADA systems Siemens prochure.” https://assets.new.siemens.com/siemens/assets/api/uuid:48100bcd-41c5-4594-9132-48611270ca7a/dffa-b10338-01-7600-simatic-scada-systems-broschuere-144.pdf (accessed Apr. 08, 2021).
[18] “SIMATIC SCADA Systems,” *siemens.com Global Website*. https://new.siemens.com/global/en/products/automation/industry-software/automation-software/scada.html (accessed Apr. 08, 2021).
[19] “Siemens Simatic Wincc : List of security vulnerabilities.” https://www.cvedetails.com/vulnerability-list/vendor_id-109/product_id-19778/Siemens-Simatic-Wincc.html (accessed May 13, 2021).
[20] “Siemens Simatic Step 7 : List of security vulnerabilities.” https://www.cvedetails.com/vulnerability-list/vendor_id-109/product_id-22699/Siemens-Simatic-Step-7.html (accessed Apr. 07, 2021).
[21] O. Mares, “Siemens PLC affected by exploitable vulnerabilities,” *Information Security Newspaper | Hacking News*, Feb. 12, 2020. https://www.securitynewspaper.com/2020/02/12/siemens-plc-scalance-simantic-siplus-affected-by-exploitable-vulnerabilities/ (accessed Apr. 07, 2021).
[22] H. Kim, “Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks,” *International Journal of Distributed Sensor Networks*, vol. 8, no. 11, p. 268478, Nov. 2012, doi: 10.1155/2012/268478.
[23] “Secure Scada Networks.”
[24] “Schneider Electric : Security vulnerabilities.” https://www.cvedetails.com/vulnerability-list/vendor_id-15060/Schneider-Electric.html (accessed May 13, 2021).
[25] T. Yardley, “SCADA: issues, -vulnerabilities, and future directions,” vol. 33, no. 6, p. 7, 2008.
[26] “SCADA systems plagued by insecure development and slow patching,” *Help Net Security*, May 23, 2017. https://www.helpnetsecurity.com/2017/05/23/scada-systems-insecure/ (accessed May 09, 2021).
[27] “Scada systems and their vulnerabilities.” https://www.secpoint.com/scada-systems-their-vulnerabilities.html (accessed Apr. 07, 2021).
[28] “SCADA System Vulnerabilities to Cyber Attack,” *Electric Energy Online*. https://electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm (accessed Apr. 07, 2021).
[29] Yogesh Sahu, “SCADA system vulnerabilities and Threat to critical infrastructure.” Tata Power.

[30] “SCADA Market by Size, Share, and Industry Analysis - 2023,” *Allied Market Research*. https://www.alliedmarketresearch.com/scada-market (accessed May 07, 2021).
[31] “SCADA and Mobile Security in the IoT Era,” *IOActive*, Jan. 11, 2018. https://ioactive.com/scada-and-mobile-security-in-iot-era/ (accessed Apr. 07, 2021).
[32] “SCADA,” *Wikipedia*. Apr. 27, 2021. Accessed: May 05, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=SCADA&oldid=1020067574
[33] “Samsung Standardization Guideline.pdf.” Samsung.
[34] “Safety at Sea and BIMCO publish cyber security white paper.” https://www.bimco.org/news/priority-news/20190916-safety-at-sea-and-bimco-publish-cyber-security-white-paper (accessed Apr. 07, 2021).
[35] “Rockwellautomation : Security vulnerabilities.” https://www.cvedetails.com/vulnerability-list/vendor_id-9492/Rockwellautomation.html (accessed May 13, 2021).
[36] “Researchers find 147 vulnerabilities in 34 SCADA mobile applications,” *SC Media*, Jan. 11, 2018. https://www.scmagazine.com/home/security-news/network-security/researchers-find-147-vulnerabilities-in-34-scada-mobile-applications/ (accessed Apr. 07, 2021).
[37] R. Leszczyna, “Protecting Industrial Control Systems,” p. 72.
[38] M. H. Moradi and M. R. Katebi, “Predictive PID Control for Ship Autopilot Design,” *IFAC Proceedings Volumes*, vol. 34, no. 7, pp. 375–380, Jul. 2001, doi: 10.1016/S1474-6670(17)35111-X.
[39] N. Dahl, “PLCs in Marine Monitoring,” p. 8.
[40] “PLC’s and SCADA: Vulnerabilities and Security Issues,” *Online Technical Training Programs | George Brown College*, Mar. 18, 2016. https://www.gbctechtraining.com/blog/plcs-scada-security-vulnerabilities (accessed Apr. 07, 2021).
[41] “PLC Timeline.” http://www.plcdev.com/plc_timeline (accessed Apr. 08, 2021).
[42] “PLC security in the age of the IIoT,” *Design World*, Apr. 25, 2018. https://www.designworldonline.com/plc-security-in-the-age-of-the-iiot/ (accessed Apr. 07, 2021).
[43] G. P. H. Sandaruwan, P. S. Ranaweera, and V. A. Oleshchuk, “PLC Security and Critical Infrastructure Protection,” p. 7.
[44] c3controls, “PLC PROGRAMMING THEN & NOW: THE HISTORY OF PLC’S,” *v2*. https://www.c3controls.com/white-paper/history-of-programmable-logic-controllers/ (accessed Apr. 08, 2021).
[45] Steven, “PLC Manufacturers: The Latest PLC Brands, Rankings & Revenues,” *Ladder Logic World*, Jun. 20, 2020. https://ladderlogicworld.com/plc-manufacturers/ (accessed Apr. 07, 2021).
[46] “PLC History, Development, Functions & System Tools,” *Technique Learning Solutions*, Sep. 24, 2014. https://learntechnique.com/plc-history-development-functions-system-tools/ (accessed Apr. 07, 2021).
[47] S. E. Valentine, “PLC Code Vulnerabilities Through SCADA Systems,” p. 137.
[48] M. T. Jamsutkar, M. S. Gore, M. P. Patil, and A. Suryawanshi, “PLC BASED SYSTEM FOR CONTROLLING AND MONITORING PARAMETERS IN SHIP,” vol. 3, no. 4, p. 5, 2014.
[49] Edward Amoroso and Andrew Ginter, “OT Security for IT Professionals Handbook.” Waterfall.
[50] Dr. J.M. Ceron, Dr. J.J.Chromik, Dr. J.J.C. Santanna, and Prof. dr. ir. A. Pras, “Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands.” Universiteit Twente.
[51] “One Flaw too Many: Vulnerabilities in SCADA Systems - Security News.”

https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems (accessed Apr. 07, 2021).
[52] "Multiple Schneider Electric EcoStruxure Products CVE-2018-7797 Open Redirection Vulnerability." https://www.cvedetails.com/bugtraq-bid/106277/Multiple-Schneider-Electric-EcoStruxure-Products-CVE-2018-77.html (accessed May 13, 2021).
[53] S. H. H. Education Norwegian University of Science and Technology (NTNU); and Erik David Martin, Noroff, "More exploits: the great PLC hack," *Control Design*. https://www.controldesign.com/articles/2018/more-exploits-the-great-plc-hack/ (accessed Apr. 07, 2021).
[54] "Mitsubishielectric : Security vulnerabilities." https://www.cvedetails.com/vulnerability-list/vendor_id-13139/Mitsubishielectric.html (accessed May 13, 2021).
[55] "MicroSCADA-X-NC-distribution-1MRS756253-A4.pdf."
[56] Lech Kobylinsky, "Marine Transport and the Fourth Industrial Revolution." Apr. 2016.
[57] E. A. Offiong, "Marine automation and impact on shipboard machinery," p. 319.
[58] "M5: Poor Authorization and Authentication | OWASP." https://owasp.org/www-project-mobile-top-10/2014-risks/m5-poor-authorization-and-authentication.html (accessed May 10, 2021).
[59] Dr. J.M. Ceron, Dr. J.J.Chromik, Dr. J.J.C. Santanna, and Prof. dr. ir. A. Pras, "ISC/SCADA Device Discoverability." Universiteit Twente.
[60] M. K. Rajeswar, "Industry 4.0 wave - Relevance of SCADA in an IOT world and journey towards a true digital enterprise," vol. 14, no. 3, p. 11, 2019.
[61] Stevan A. Milinkoviü and Ljubomir R. Laziü, "Industrial PLC security issues," p. 5.
[62] S. A. Milinkovic and L. R. Lazic, "Industrial PLC security issues," in *2012 20th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, Nov. 2012, pp. 1536–1539. doi: 10.1109/TELFOR.2012.6419513.
[63] Oxana Andreeva *et al.*, "Industrial Cotrol Systems Vulnerabilities Statistics." KASPERSKY.
[64] "Industrial Controls & Remote I/O – A focus on the PLC market." https://www.interactanalysis.com/industrial-controls-remote-i-o-a-focus-on-the-plcs-market/ (accessed Apr. 07, 2021).
[65] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Tucson, AZ, USA, Sep. 2016, pp. 25–30. doi: 10.1109/ISI.2016.7745438.
[66] "ICS-CERT Monitor." ICS-CERT, Jul. 2011.
[67] "ICS vulnerabilities." Positive Technologies, 2018.
[68] G. Ward, "How your ship has probably been Cyber Attacked already," p. 5.
[69] "How to Choose a PLC: Pros and Cons of 3 Popular Vendors," *Affinity Energy*, Nov. 30, 2016. https://www.affinityenergy.com/how-to-choose-a-plc-next-controls-project/ (accessed Apr. 07, 2021).
[70] "Honeywellprocess Experion : List of security vulnerabilities." https://www.cvedetails.com/vulnerability-list/vendor_id-12270/product_id-23157/Honeywellprocess-Experion.html (accessed May 13, 2021).
[71] "Hitachi Completes Acquisition of ABB's Power Grids Business; Hitachi ABB Power Grids Begins Operation," p. 10.
[72] "History of the PLC | Library.AutomationDirect," *Library.Automationdirect.com*, Aug. 05, 2015. https://library.automationdirect.com/history-of-the-plc/ (accessed Apr. 07, 2021).
[73] "Hijacking a PLC Using its Own Network Features," *Dark Reading*. https://www.darkreading.com/vulnerabilities---threats/hijacking-a-plc-using-its-own-network-features/d/d-id/1333660 (accessed Apr. 07, 2021).

[74] “Hackers took ‘full control’ of container ship’s navigation systems for 10 hours @AsketO.” https://www.asket.co.uk/post/2017/11/26/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-asketoperati (accessed Apr. 07, 2021).
[75] Brian Gorenc and Fritz Sands, “Hacker Machine Interface: The State of SCADA HMI Vulnerabilities,” *Trend Micro*, p. 30.
[76] “Guidelines on Cyber Security Onboard Ships V4.”
[77] “Guidelines on Cyber Security Onboard Ships V2.” Jul. 2017.
[78] “Getting Rid Of Weak Passwords To Improve Security,” *Teamstack Blog*, Mar. 31, 2020. https://blog.teamstack.com/getting-rid-of-weak-passwords-to-improve-security/ (accessed Apr. 07, 2021).
[79] “Fairplay and BIMCO Maritime Cyber Security survey.” Sep. 14, 2018.
[80] G. Tzokatziou, L. A. Maglaras, H. Janicke, and Y. He, “Exploiting SCADA vulnerabilities using a Human Interface Device,” *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 7, p. 8, 2015.
[81] A. Ujvarosi, “EVOLUTION OF SCADA SYSTEMS,” vol. 9, no. 1, p. 6, 2016.
[82] D. Rutherford, “Ethernet for SCADA Systems Explained,” p. 12.
[83] A. A. Farooq, J. Marquard, K. George, and T. Moyer, “Detecting Safety and Security Faults in PLC Systems with Data Provenance,” *arXiv:1911.06304 [cs]*, Nov. 2019, Accessed: May 11, 2021. [Online]. Available: http://arxiv.org/abs/1911.06304
[84] J.-H. Huh, T. Koh, and K. Seo, “Design of a Shipboard Outside Communication Network and Its Testbed Using PLC: For Safety Management during the Ship Building Process,” p. 21, 2018.
[85] “Cyber Risks in Shipping LP Briefing.pdf.” The North of England P&I Association, Jul. 2017.
[86] Max J. Bobys, “Cyber Risks in Shipping LP Briefing.” The North of England P&I Association.
[87] “Credential Management and Enforcement for ICS/SCADA environments,” *Infosec Resources*. https://resources.infosecinstitute.com/topic/credential-management-and-enforcement-for-ics-scada-environments/ (accessed May 10, 2021).
[88] “Control Engineering | Future of the PLC,” *Control Engineering*, Aug. 26, 2014. https://www.controleng.com/articles/future-of-the-plc/ (accessed Apr. 07, 2021).
[89] *Code of Practice Cyber Security for Ships*. 2017.
[90] “CERN Computer Security Information.” https://security.web.cern.ch/recommendations/en/password_alternatives.shtml (accessed Apr. 07, 2021).
[91] A. Pauna, “Can we learn from SCADA security incidents?,” p. 10, 2013.
[92] European Network and Information Security Agency., Rossella Mattioli, ENISA, and Konstantinos Moulinos, ENISA, *Analysis of ICS-SCADA cyber security maturity levels in critical sectors*. LU: Publications Office, 2015. Accessed: Apr. 07, 2021. [Online]. Available: https://data.europa.eu/doi/10.2824/835661
[93] C. Cimpanu, “All four of the world’s largest shipping companies have now been hit by cyber-attacks,” *ZDNet*. https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/ (accessed Apr. 07, 2021).
[94] “ABB named global leader in SCADA systems for the power sector.” https://new.abb.com/news/detail/2672/ABB-named-global-leader-in-scada-systems-for-the-power-sector (accessed Apr. 08, 2021).
[95] “ABB : Security vulnerabilities.” https://www.cvedetails.com/vulnerability-list/vendor_id-8555/year-2018/ABB.html (accessed May 13, 2021).
[96] E.-M. Kalogeraki, S. Papastergiou, H. Mouratidis, and N. Polemi, “A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments,” *Applied Sciences*, vol. 8, no. 9, p. 1477, Aug. 2018, doi: 10.3390/app8091477.
[97] “A Brief History of the SCADA System,” *Process Solutions, Inc.*, Jul. 10, 2020.

https://www.processsolutions.com/a-brief-history-of-the-scada-system/ (accessed Apr. 07, 2021).
[98] “21 Steps to Improve Cyber Security of SCADA Networks.” USA Departmnet of Energy.
[99] A. N. Koushik and R. Bs, “4th Generation SCADA Implementation for Automation,” vol. 5, no. 3, p. 4.
[100] E.-E. E. Portal, “3 generations of SCADA system architectures you should know about | EEP,” *EEP - Electrical Engineering Portal*, Apr. 22, 2013. https://electrical-engineering-portal.com/three-generations-of-scada-system-architectures (accessed Apr. 07, 2021).