



KMITL
สถาบันเทคโนโลยี
พระจอมเกล้า
เจ้าคุณทหารลาดกระบัง



INDUSTRIAL CONTROL SYSTEMS

SEE-ED

inspiration starts here

รองศาสตราจารย์ ดร.มนตรี วิบูลย์รัตน์

คณะบริหารธุรกิจ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ผู้ช่วยศาสตราจารย์ ดร.อรรถพล ป้อมสถิตย์

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

แนวทางปฏิบัติสำหรับความปลอดภัยของ ระบบควบคุมทางอุตสาหกรรม (Guide to Industrial Control System (ICS) Security)

“รายได้หลังจากหักค่าใช้จ่ายทั้งหมดผู้เขียนขอมอบเพื่อร่วมสมทบทุน

ให้เพื่อสร้าง โรงพยาบาลพระจอมเกล้าเจ้าคุณทหาร”

SE-ED
inspiration starts here

รองศาสตราจารย์ ดร.มนตรี วิบูลย์รัตน์

คณะบริหารธุรกิจ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ผู้ช่วยศาสตราจารย์ ดร.อรรถพล ป้อมสถิตย์

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

แนวทางปฏิบัติสำหรับความปลอดภัยของระบบควบคุมทางอุตสาหกรรม (Guide to Industrial Control System (ICS) Security)

โดย

รองศาสตราจารย์ ดร.มนตรี วิบูลย์รัตน์

ผู้ช่วยศาสตราจารย์ ดร.อรรถพล ป้อมสถิตย์

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

มนตรี วิบูลย์รัตน์.

แนวทางปฏิบัติสำหรับความปลอดภัยของระบบควบคุมทางอุตสาหกรรม = Guide to Industrial Control System (ICS) security.-- กรุงเทพฯ : สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2567.233 หน้า.

1. การควบคุมกระบวนการผลิต--มาตรฐาน. I. อรรถพล ป้อมสถิตย์, ผู้แต่งร่วม. II. ชื่อเรื่อง.658.5

ISBN 978-616-338-201-6

สงวนลิขสิทธิ์ตามพระราชบัญญัติ

All right reserved and do not copy, excerpt, print and distribute

พิมพ์ครั้งที่ 1 วันที่ 2 กันยายน พ.ศ. 2567

ราคา 180 บาท

จัดทำโดย: คณะบริหารธุรกิจ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

1 ถ. ชลองกรุง แขวงลาดกระบัง เขตลาดกระบัง กรุงเทพฯ 10520

โทรศัพท์ 09 9459 5561 อีเมล montri.wi@kmitl.ac.th

จัดจำหน่ายในรูปแบบ e-book ที่ <https://se-ed.com/>

คำนำ

หนังสือแนวทางปฏิบัติสำหรับความปลอดภัยและของระบบควบคุมอุตสาหกรรมเล่มนี้ให้คำแนะนำเกี่ยวกับวิธีการรักษาความปลอดภัยระบบควบคุมอุตสาหกรรม Industrial Control Systems (ICS) Security รวมถึงระบบการควบคุมกำกับดูแลและเก็บข้อมูล หรือ Supervisory Control and Data Acquisition (SCADA) Systems ระบบควบคุมแบบกระจาย หรือ Distributed Control Systems (DCS) และการกำหนดค่าระบบควบคุมอื่น ๆ เช่น เครื่องควบคุมเชิงตรรกที่สามารถโปรแกรมได้ หรือ Programmable Logic Controllers (PLC) โดยมุ่งเน้นในการจัดการกับข้อกำหนดด้านประสิทธิภาพ ความน่าเชื่อถือ และข้อกำหนดด้านความปลอดภัยและหนังสือนี้ให้ภาพรวมของระบบควบคุมอุตสาหกรรม และโทโพโลยีของระบบทั่วไป การระบุภัยคุกคามและช่องโหว่ของระบบนอกจากนี้ยังเสนอมาตรการรับมือด้านความปลอดภัยที่แนะนำเพื่อลดความเสี่ยงที่เกี่ยวข้องกับระบบการผลิตและการจำหน่ายพลังงาน การจ่ายก๊าซและน้ำ ไปจนถึงระบบอัตโนมัติทางอุตสาหกรรม ระบบควบคุมการจราจร และการจัดการสิ่งอำนวยความสะดวกที่ล้ำสมัย ระบบควบคุมอุตสาหกรรมเหล่านี้เผชิญกับภัยคุกคามทางไซเบอร์แบบเดียวกับระบบไอทีทั่วไปมากขึ้นเรื่อย ๆ เนื่องจากความถี่ของเหตุการณ์ที่เพิ่มขึ้นและช่องโหว่ที่เพิ่งค้นพบ เจ้าของสินทรัพย์จำเป็นต้องแก้ไขปัญหาเหล่านี้อย่างเร่งด่วน ดังนั้น องค์กรต่าง ๆ จึงต้องพิจารณาความเสี่ยงและความเสียหายที่อาจเกิดขึ้นจากมัลแวร์ (Malware) การปฏิเสธการให้บริการแบบวงกว้าง Distributed Denial of Service (DDoS) หรือไวรัส ตลอดจนการโจมตีโครงสร้างพื้นฐาน ระบบควบคุมอุตสาหกรรมแบบกำหนดเป้าหมาย สิ่งนี้ใช้เจาะจงกับโครงสร้างพื้นฐานที่เชื่อมต่อโดยตรงกับอินเทอร์เน็ตตลอดจนโครงสร้างพื้นฐานที่สามารถตกเป็นเป้าหมายของการโจมตีทางไซเบอร์ทางอ้อมนอกจากนี้หนังสือคู่มือความปลอดภัยของระบบควบคุมอุตสาหกรรมเล่มนี้ยังนำเสนอ 11 กรณีศึกษาที่เกิดขึ้นจริงจากเหตุการณ์จริงที่มีการโจมตีในหลากหลายอุตสาหกรรมและนำเสนอโดยเป็นการรวบรวมข้อมูลและวิเคราะห์ตามหลักวิชาการและมาตรฐานนานาชาติ ถึงสาเหตุของปัญหาและปัจจัยอื่น ๆ เพื่อให้ผู้เรียนคิดวิเคราะห์หาเหตุผลและแนวทางในการตัดสินใจตามหลักวิชาการและหลักการที่อ้างอิงตามมาตรฐานนานาชาติไปสู่การสังเคราะห์เพื่อให้เกิดบูรณาภาพหรือปรากฏการณ์แนวทางการแก้ปัญหาใหม่ ๆ จากการผสมผสานความคิดหลังจากได้ศึกษาทั้ง 11 กรณีศึกษาของการโจมตีทางไซเบอร์

ผู้เขียนหวังเป็นอย่างยิ่งว่าหนังสือคู่มือความปลอดภัยและกรณีศึกษาของระบบควบคุมอุตสาหกรรมเล่มนี้จะเป็แนวทางในการสร้างเกราะป้องกันให้กับองค์กรของท่านในการบริหารความเสี่ยงด้วยความต่อเนื่อง เพิ่มประสิทธิภาพและผลผลิตอย่างต่อเนื่อง รวมทั้งสร้างความสามารถในการแข่งขันต่อไปในอนาคต

รองศาสตราจารย์ ดร.มนตรี วิบูลย์รัตน์

ผู้ช่วยศาสตราจารย์ ดร.อรรถพล ป้อมสถิตย์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

สารบัญ

บทสรุปผู้บริหาร	1
1. บทนำ	1-1
1.1 วัตถุประสงค์และขอบเขตงาน	1-1
1.2 บริบททางประวัติศาสตร์สำหรับอุตสาหกรรม 4.0	1-2
1.2.1 การปฏิวัติอุตสาหกรรมครั้งแรก	1-3
1.2.2 การปฏิวัติอุตสาหกรรมครั้งที่สอง	1-3
1.2.3 การปฏิวัติอุตสาหกรรมครั้งที่สาม	1-3
1.2.4 การปฏิวัติอุตสาหกรรมครั้งที่สี่	1-3
1.2.5 เทคโนโลยีอุตสาหกรรม 4.0 กำลังเปลี่ยนแปลงการผลิตอย่างไร	1-4
1.2.6 การรักษาความปลอดภัยทางไซเบอร์เป็นปัจจัยสำคัญในการนำไปใช้	1-5
1.3 ผู้อ่านและผู้ปฏิบัติ	1-6
1.4 โครงสร้างหนังสือคู่มือความปลอดภัยและกรณีศึกษาของระบบควบคุมอุตสาหกรรม	1-7
2. ภาพรวมของระบบควบคุมทางอุตสาหกรรม Industrial Control Systems (ICS)	2-1
2.1 วิวัฒนาการของระบบควบคุมทางอุตสาหกรรม	2-1
2.2 ภาคส่วนอุตสาหกรรมของ Industrial Control Systems (ICS) และความเกี่ยวพันกันของระบบ	2-2
2.2.1 อุตสาหกรรมการผลิต	2-2
2.2.2 อุตสาหกรรมการจัดจำหน่าย	2-2
2.2.3 ความแตกต่างระหว่าง ICS ของการผลิตและการจัดจำหน่าย	2-3
2.2.4 ICS และความเกี่ยวพันกันของโครงสร้างพื้นฐานที่สำคัญ	2-3
2.3 การดำเนินการและองค์ประกอบของ ICS	2-4
2.3.1 ข้อควรพิจารณาในการออกแบบระบบ ICS	2-5
2.3.2 การควบคุมดูแลและการรวบรวมข้อมูล Supervisory Control and Data Acquisition (SCADA)	2-6
2.3.3 ระบบควบคุมการจัดจำหน่าย Distributed Control Systems (DCS)	2-11
2.3.4 รูปแบบโครงข่าย Programmable Logic Controller (PLC)	2-13
2.4 เปรียบเทียบการรักษาความปลอดภัยระบบ ICS กับระบบ Information Technology (IT)	2-14
2.5 ระบบควบคุมประเภทอื่น ๆ	2-19
3. การจัดการและการประเมินความเสี่ยงของ ICS	3-1
3.1 การบริหารความเสี่ยง	3-1
3.2 ความรู้เบื้องต้นด้านกระบวนการบริหารความเสี่ยง	3-2
3.3 ข้อพิจารณาพิเศษสำหรับการประเมินความเสี่ยงของ ICS	3-4
3.3.1 ความปลอดภัยในการประเมินความเสี่ยงด้านความปลอดภัยข้อมูลของ ICS	3-5
3.3.2 ผลกระทบทางกายภาพที่อาจเกิดขึ้นจากอุบัติเหตุของ ICS	3-5
3.3.3 ผลกระทบจากการหยุดชะงักทางกายภาพของกระบวนการ ICS	3-6

3.3.4 การผสมรวมด้านที่ไม่ใช่ดิจิทัลของ ICS เข้ากับการประเมินผลกระทบ	3-6
3.3.5 การผสมรวมผลกระทบของระบบความปลอดภัย	3-7
3.3.6 การพิจารณาการแพร่กระจายของผลกระทบต่อระบบที่เชื่อมต่อกัน	3-8
4. การพัฒนาและการใช้งานโปรแกรมการรักษาความปลอดภัยระบบควบคุมทางอุตสาหกรรม (ICS)	4-1
4.1 เหตุผลทางธุรกิจสำหรับการรักษาความปลอดภัย	4-2
4.1.1 ประโยชน์	4-3
4.1.2 ผลลัพธ์ที่อาจเกิดขึ้นได้	4-3
4.1.3 แหล่งข้อมูลสำหรับการสร้างเหตุผลทางธุรกิจ	4-5
4.1.4 การนำเสนอเหตุผลทางธุรกิจต่อผู้บริหาร	4-5
4.2 การสร้างและฝึกอบรมทีมงานข้ามสายงาน	4-6
4.3 การกำหนดกฎระเบียบและขอบเขตงาน	4-6
4.4 การกำหนดนโยบายและวิธีการดำเนินการที่เกี่ยวข้องกับ ICS โดยเฉพาะ	4-7
4.5 การใช้กรอบงานการจัดการความเสี่ยง (Risk Management Framework) ด้านการรักษาความปลอดภัยของ ICS	4-7
4.5.1 การจัดประเภทระบบ ICS และสินทรัพย์เครือข่าย	4-8
4.5.2 การเลือกการควบคุมการรักษาความปลอดภัยของ ICS	4-9
4.5.3 ดำเนินการประเมินความเสี่ยง	4-10
4.5.4 การใช้งานระบบควบคุมการรักษาความปลอดภัย	4-10
5. สถาปัตยกรรมความปลอดภัยของ ICS	5-1
5.1 การแบ่งส่วนและการแบ่งแยกเครือข่าย	5-1
5.2 การป้องกันขอบเขต	5-3
5.3 ไฟร์วอลล์	5-5
5.4 เครือข่ายควบคุมที่แยกออกจากกันด้วยลอจิก	5-7
5.5 การแบ่งแยกเครือข่าย	5-8
5.5.1 คอมพิวเตอร์ที่เชื่อมต่อเครือข่ายได้แบบคู่/การ์ดเชื่อมต่อเครือข่าย Network Interface Card (NIC) แบบคู่	5-8
5.5.2 ไฟร์วอลล์ระหว่างเครือข่ายขององค์กรและเครือข่ายควบคุม	5-8
5.5.3 ไฟร์วอลล์และเราเตอร์ระหว่างเครือข่ายขององค์กรและเครือข่ายควบคุม	5-10
5.5.4 ไฟร์วอลล์ที่มี Demilitarized Zone (DMZ) ระหว่างเครือข่ายขององค์กรและเครือข่ายควบคุม	5-11
5.5.5 ไฟร์วอลล์ที่จับคู่ระหว่างเครือข่ายขององค์กรและเครือข่ายควบคุม	5-12
5.5.6 บทสรุปการแบ่งแยกเครือข่าย	5-14
5.6 สถาปัตยกรรมการป้องกันเชิงลึกที่แนะนำ	5-14
5.7 นโยบายทั่วไปเกี่ยวกับไฟร์วอลล์ของ ICS	5-15
5.8 กฎไฟร์วอลล์ที่แนะนำสำหรับบริการที่เฉพาะ	5-18
5.8.1 ระบบชื่อโดเมน Domain Name System (DNS)	5-18
5.8.2 โพรโตคอลขนส่งข้อความหลายมิติ Hypertext Transfer Protocol (HTTP)	5-18

5.8.3 File Transfer Protocol (FTP) และโปรโตคอลการถ่ายโอนไฟล์ขนาดเล็ก Trivial File Transfer Protocol (TFTP)	5-19
5.8.4 โปรโตคอลเครือข่ายแบบเทเลเน็ต	5-19
5.8.5 โปรโตคอลตั้งค่าแม่ข่ายแบบพลวัต Dynamic Host Configuration Protocol (DHCP)	5-19
5.8.6 โปรโตคอลเข้ารหัสแบบซีเคียวเชลล์ Secure Shell (SSH)	5-19
5.8.7 โปรโตคอลเข้าใช้งานอ็อบเจกต์อย่างง่าย Simple Object Access Protocol (SOAP)	5-20
5.8.8 โปรโตคอลการถ่ายโอนจดหมายอย่างง่าย Simple Mail Transfer Protocol (SMTP)	5-20
5.8.9 โปรโตคอลการจัดการเครือข่ายอย่างง่าย Simple Network Management Protocol (SNMP)	5-20
5.8.10 แบบจำลองส่วนประกอบวัตถุแบบกระจาย Distributed Component Object Model (DCOM)	5-20
5.8.11 SCADA และโปรโตคอลในอุตสาหกรรม	5-21
5.9 การแปลที่อยู่เครือข่าย Network Address Translation (NAT)	5-21
5.10 ปัญหาเกี่ยวกับไฟร์วอลล์ ICS โดยเฉพาะ	5-22
5.10.1 ฐานข้อมูลกลาง (Data Historians)	5-22
5.10.2 การเข้าใช้งานการสนับสนุนระยะไกล	5-22
5.10.3 การจราจรข้อมูลที่ส่งไปยังปลายทางหลายแห่งพร้อมกัน	5-22
5.11 เกตเวย์ทิศทางเดียว	5-23
5.12 จุดเดียวของความล้มเหลว (Single Points of Failure)	5-23
5.13 การทำระบบควบคุมและการทนทานต่อความบกพร่อง	5-24
5.14 การป้องกันการโจมตีแบบดักกลางทาง	5-24
5.15 การยืนยันตัวตนและการอนุญาต	5-26
5.15.1 ข้อพิจารณาการใช้ ICS	5-27
5.16 การตรวจดู การบันทึก และการตรวจสอบ	5-27
5.17 การตรวจจับเหตุ การตอบสนอง และการกู้คืนระบบ	5-27
6. การประยุกต์ใช้การควบคุมความปลอดภัยกับ ICS	6-1
6.1 การดำเนินการงานกรอบการจัดการความเสี่ยงสำหรับระบบการควบคุมทางอุตสาหกรรม	6-1
6.1.1 ขั้นตอนที่ 1: จัดประเภทระบบข้อมูล	6-2
6.1.2 ขั้นตอนที่ 2: เลือกการควบคุมความปลอดภัย	6-4
6.1.3 ขั้นตอนที่ 3: ดำเนินการควบคุมความปลอดภัย	6-5
6.1.4 ขั้นตอนที่ 4: ประเมินการควบคุมความปลอดภัย	6-6
6.1.5 ขั้นตอนที่ 5: อนุมัติระบบข้อมูล	6-6
6.1.6 ขั้นตอน 6: ติดตามตรวจสอบการควบคุมความปลอดภัย	6-6
6.2 คำแนะนำเกี่ยวกับการประยุกต์ใช้การควบคุมความปลอดภัยกับ ICS	6-6
6.2.1 ควบคุมการเข้าใช้งาน	6-9
6.2.2 การให้ความรู้และฝึกอบรม	6-14

6.2.3 การตรวจสอบและความรับผิดชอบ	6-14
6.2.4 การประเมินและการอนุมัติด้านความปลอดภัย	6-16
6.2.5 การจัดการการกำหนดค่า	6-16
6.2.6 แผนรองรับสถานการณ์ฉุกเฉิน	6-17
6.2.7 การระบุตัวตนและการพิสูจน์ตัวตน	6-20
6.2.8 การรับมือภัยคุกคาม	6-26
6.2.9 การบำรุงรักษา	6-28
6.2.10 การป้องกันสื่อ	6-28
6.2.11 การป้องกันทางกายภาพและสภาพแวดล้อม	6-29
6.2.12 การวางแผน	6-33
6.2.13 การรักษาความปลอดภัยบุคลากร	6-33
6.2.14 การประเมินความเสี่ยง	6-34
6.2.15 การจัดการระบบและบริการ	6-35
6.2.16 การป้องกันระบบและการสื่อสาร	6-36
6.2.17 ความมั่นคงของระบบและข้อมูล	6-40
6.2.18 การบริหารโครงการ	6-43
6.2.19 การควบคุมการรักษาความเป็นส่วนตัว	6-43
7. เพอร์ดูโมเดลและกรณีศึกษา (Purdue Model and Case Studies).....	7-1
7.1 กรณีศึกษา การโจมตีโรงงานบำบัดน้ำ Oldsmar.....	7-8
7.2 กรณีศึกษา การโจมตี Sandworm ต่อระบบส่งไฟฟ้าของยูเครน.....	7-14
7.3 กรณีศึกษา การโจมตีท่อส่งน้ำมัน Colonial Pipeline.....	7-21
7.4 กรณีศึกษา การโจมตี DigiNotar.....	7-28
7.5 กรณีศึกษา การโจมตีบริษัทประกันสุขภาพ Anthem.....	7-36
7.6 กรณีศึกษาการโจมตีประเทศคอซอวอ.....	7-41
7.7 กรณีศึกษา การโจมตีด้วยแรนซัมแวร์โจมตีระบบการดูแลสุขภาพของโรมาเนีย.....	7-47
7.8 กรณีศึกษา การที่ Cisco ถูกโจมตีโดยกลุ่มแรนซัมแวร์ Yanluowang.....	7-54
7.9 กรณีศึกษา การโจมตี Rackspace.....	7-59
7.10 กรณีศึกษา การโจมตีผู้ให้บริการท่าเรือรายใหญ่ที่สุดของออสเตรเลีย.....	7-65
7.11 กรณีศึกษา การโจมตีโรงไฟฟ้าชีวมวลทางภาคใต้ของประเทศไทย.....	7-75
เอกสารอ้างอิง.....	8-1

รายการรูป

รูปที่ 1-1 แบบจำลองทางทฤษฎีของการบูรณาการ IT และ OT	1-6
รูปที่ 1-2 การบรรจบกันอย่างเป็นค่อยเป็นค่อยไปเมื่อเวลาผ่านไปด้วยการใช้เทคโนโลยีสารสนเทศในระบบอุตสาหกรรม.....	1-7
รูปที่ 2-1 การทำงานของ ICS	2-4
รูปที่ 2-2 เค้าโครงทั่วไปของการควบคุมดูแลและการรวบรวมข้อมูล SCADA	2-7
รูปที่ 2-3 รูปแบบโครงข่ายการสื่อสาร SCADA ขั้นพื้นฐาน.....	2-8
รูปที่ 2-4 รูปแบบโครงข่ายการสื่อสาร SCADA ขนาดใหญ่	2-9
รูปที่ 2-5 ตัวอย่างการใช้งานการควบคุมดูแลและการรวบรวมข้อมูล SCADA (การตรวจดูและควบคุมการจำหน่าย)	2-10
รูปที่ 2-6 ตัวอย่างการใช้งานการควบคุมดูแลและการรวบรวมข้อมูล SCADA (การตรวจดูและควบคุมราง)	2-11
รูปที่ 2-7 ตัวอย่างการใช้งาน DCS	2-13
รูปที่ 2-8 ตัวอย่างการใช้งานระบบควบคุม PLC	2-14
รูปที่ 3-1 กระบวนการบริหารความเสี่ยงที่ใช้ในทุกระดับ.....	3-2
รูปที่ 5-1 ไฟร์วอลล์ระหว่างเครือข่ายขององค์กรและเครือข่ายควบคุม.....	5-9
รูปที่ 5-2 ไฟร์วอลล์และเราเตอร์ระหว่างเครือข่ายขององค์กรและเครือข่ายควบคุม.....	5-10
รูปที่ 5-3 ไฟร์วอลล์ที่มี DMZ ระหว่างเครือข่ายขององค์กรและเครือข่ายควบคุม.....	5-11
รูปที่ 5-4 ไฟร์วอลล์ที่จับคู่ระหว่างเครือข่ายขององค์กรและเครือข่ายควบคุม.....	5-13
รูปที่ 5-5 สถาปัตยกรรมการป้องกันเชิงลึกที่แนะนำโดย CSSP	5-15
รูปที่ 6-1 กรอบงานการบริหารความเสี่ยง.....	6-2
รูปที่ 7-1 แสดงระดับเครือข่ายทั้ง 6 ระดับของเพอร์ดูโมเดล	7-1
รูปที่ 7-2 มาตรฐาน IEC 62443 การแยกภัยคุกคามตามโซนและการเชื่อมต่อทางกายภาพ.....	7-6
รูปที่ 7-3 มาตรฐาน IEC 62443 การกำหนดระดับความปลอดภัย Security Level (SL).....	7-7
รูปที่ 7-4 แสกออร์พยายามปนเปื้อนโซเดียมไฮดรอกไซด์ในแหล่งน้ำ.....	7-8
รูปที่ 7-5 การเชื่อมต่อจากผู้ใช้งานจากระยะไกลแบบเดิม.....	7-9
รูปที่ 7-6 การเข้าถึงเครือข่ายแบบ Zero Trust สำหรับ OT.....	7-10
รูปที่ 7-7 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 3.5 ของเพอร์ดูโมเดล.....	7-13
รูปที่ 7-8 รูปแบบการทำงานของกรีนสคริปต์มัลแวร์อัตโนมัติ.....	7-16
รูปที่ 7-9 การบันทึกเหตุการณ์โจมตีของรัสเซียส่งผลกระทบต่อระบบ OT ในช่วงปี 2014-2022.....	7-18
รูปที่ 7-10 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 2 ของเพอร์ดูโมเดล.....	7-20
รูปที่ 7-11 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 4 ของเพอร์ดูโมเดล.....	7-27
รูปที่ 7-12 หน่วยงานออกใบรับรอง (CA) ดำเนินการอย่างไร.....	7-29
รูปที่ 7-13 ใบรับรองปลอมแทรกซึมเข้าไปได้อย่างไร.....	7-31
รูปที่ 7-14 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 4-5 ของเพอร์ดูโมเดล.....	7-35
รูปที่ 7-15 ประวัติการละเมิดในอุตสาหกรรมการดูแลสุขภาพ.....	7-37
รูปที่ 7-16 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 4 ของเพอร์ดูโมเดล.....	7-40

รูปที่ 7-17 สหรัฐอเมริกาจะจ่ายเงินรางวัลสูงถึง 10 ล้านดอลลาร์สหรัฐ สำหรับข้อมูลที่น่าไปสู่การระบุตัวตนของสมาชิกแก๊งค์ แรนซัมแวร์ Conti.....	7-43
รูปที่ 7-18 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 0 ของเพอร์ดูโมเดล.....	7-46
รูปที่ 7-19 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 0, 4 และ 5 ของเพอร์ดูโมเดล.....	7-52
รูปที่ 7-20 เอกสารพิสูจน์การละเมิดของ Cisco (BleepingComputer).....	7-56
รูปที่ 7-21 อีเมลแสดงรายการไอดีเร็กทอรีของข้อมูล Box ที่รั่วไหลออกมา.....	7-57
รูปที่ 7-22 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 4 และ 5 ของเพอร์ดูโมเดล.....	7-58
รูปที่ 7-23 Log4Shell ทำงานอย่างไร.....	7-62
รูปที่ 7-24 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 4 และ 5 ของเพอร์ดูโมเดล.....	7-64
รูปที่ 7-25 LockBit ประกาศขอกู้ยืมที่โจมตีท่าเรือที่ใหญ่ที่สุดของออสเตรเลีย.....	7-66
รูปที่ 7-26 LockBit อ้างการโจมตีท่าเรือลิบบอน.....	7-68
รูปที่ 7-27 การโจมตีเกิดจากช่องโหว่ใน ระดับที่ 3, 4 และ 5 ของเพอร์ดูโมเดล.....	7-73
รูปที่ 7-28 แนวโน้มการโจมตีทางไซเบอร์ทั่วโลกปี 2020.....	7-75
รูปที่ 7-29 กระบวนการผลิตไฟฟ้าชีวมวล.....	7-76
รูปที่ 7-30 แสดง Ovation highway ช่วงวันเกิดเหตุ.....	7-77
รูปที่ 7-31 แสดง Ovation highway ช่วงทดสอบระบบ.....	7-78
รูปที่ 7-32 แสดงการเกิด Broadcast storm (เส้นสีแดง).....	7-80
รูปที่ 7-33 แสดงการถอดการเชื่อมต่อที่ทำให้เกิด Network loop.....	7-82
รูปที่ 7-34 ตัวอย่างการกำหนด Network segmentation ด้วย VLAN.....	7-83
รูปที่ 7-35 IEC 62443 เป็นมาตรฐานโดยพฤตินัยสำหรับความปลอดภัยของกรอบงานระบบควบคุมอุตสาหกรรม (ICS).....	7-84
รูปที่ 7-36 สี่ขั้นตอนของการบูรณาการความปลอดภัยทางไซเบอร์ด้าน IT และ OT.....	7-86
รูปที่ 7-37 การออกแบบความปลอดภัยทางไซเบอร์ด้าน IT และ OT เพื่อการป้องกัน.....	7-87
รูปที่ 7-38 Spectrum Security – SL2.....	7-88
รูปที่ 7-39 Spectrum Security – SL4.....	7-89

รายการตาราง

ตารางที่ 2-1	สรุปข้อแตกต่างของระบบ IT และ ICS	2-17
ตารางที่ 3-1	หมวดหมู่ของส่วนประกอบการควบคุม ICS ที่ไม่ใช่ดิจิทัล.....	3-6
ตารางที่ 6-1	คำจำกัดความที่เป็นไปได้สำหรับระดับผลกระทบ ICS ตาม ISA 99	6-3
ตารางที่ 6-2	คำจำกัดความที่เป็นไปได้สำหรับระดับผลกระทบ ICS ขึ้นอยู่กับผลิตภัณฑ์ที่ผลิต อุตสาหกรรม และประเด็นด้านความปลอดภัย	6-4
ตารางที่ 7-1	โรงไฟฟ้าชีวมวลจากเชื้อเพลิงประเภทต่าง ๆ.....	7-85

SE-ED
inspiration starts here

บทสรุปผู้บริหาร

หนังสือคู่มือความปลอดภัยและกรณีศึกษาของระบบควบคุมอุตสาหกรรมนี้ให้แนวทางในการสร้างความปลอดภัยให้ระบบควบคุมทางอุตสาหกรรม (ICS) โดย ICS นี้ประกอบด้วยระบบการควบคุมดูแลและการเก็บข้อมูล (SCADA) ระบบควบคุมการจัดจำหน่าย (DCS) และการตั้งคาระบบควบคุมอื่น ๆ เช่น โปรแกรมเมเบิลลอจิกคอนโทรลเลอร์ (PLC) ที่มักจะพบได้บ่อยในภาคการควบคุมทางอุตสาหกรรม โดยทั่วไปจะใช้ ICS ในอุตสาหกรรมต่าง ๆ เช่น ไฟฟ้า น้ำและน้ำเสีย น้ำมันและแก๊สธรรมชาติ การขนส่ง เคมีภัณฑ์ เกล็ดหิน ย่อยและกระดาษ อาหารและเครื่องดื่ม และการผลิตแบบแยกส่วน (เช่น ยานยนต์ การบินและอวกาศ และสินค้าที่ต้องใช้เวลานาน) โดยทั่วไปการควบคุมดูแลและการรวบรวมข้อมูล SCADA จะใช้เพื่อควบคุมสินทรัพย์ที่กระจายโดยการใช้การรวบรวมข้อมูลแบบรวมศูนย์และการควบคุมดูแล โดยทั่วไป DCS จะใช้ในการควบคุมระบบการผลิตภายในพื้นที่ เช่น โรงงาน โดยการใช้การกำกับดูแลและการควบคุมตามกฎระเบียบ โดยทั่วไป PLC จะใช้สำหรับการควบคุมแบบแยกส่วนสำหรับการใช้งานเฉพาะและมักจะให้การควบคุมกฎระเบียบ ระบบควบคุมนี้มีความสำคัญต่อการดำเนินงานของโครงสร้างพื้นฐานที่สำคัญในสหรัฐอเมริกาซึ่งมักจะเชื่อมโยงถึงกันในระดับสูงและเป็นระบบที่ต้องเกี่ยวพันกัน สิ่งสำคัญที่ต้องทราบก็คือประมาณร้อยละ 90 ของโครงสร้างพื้นฐานที่สำคัญของประเทศเป็นของเอกชนและดำเนินการโดยเอกชน หน่วยงานรัฐบาลกลางยังคงดำเนินการ ICS ดังกล่าวข้างต้นอยู่หลายรายการ ตัวอย่างต่าง ๆ ได้แก่ การควบคุมการจราจรทางอากาศและการจัดการวัสดุ (เช่น การส่งจดหมายของบริการไปรษณีย์) เอกสารนี้ได้ให้ภาพรวมของ ICS นี้และรูปแบบโครงข่ายของระบบทั่วไป ระบุถึงภัยคุกคามและช่องโหว่ทั่วไปต่อระบบนี้ และให้มาตรการรับมือการรักษาความปลอดภัยตามที่แนะนำเพื่อลดความเสี่ยงที่เกี่ยวข้อง

ในช่วงแรกเริ่ม ICS มีความคล้ายคลึงกับระบบเทคโนโลยีสารสนเทศ (IT) แบบดั้งเดิมเพียงเล็กน้อย โดยที่ ICS เป็นระบบแยกเดี่ยวที่ใช้โปรโตคอลควบคุมที่เป็นกรรมสิทธิ์เฉพาะโดยใช้ฮาร์ดแวร์และซอฟต์แวร์เฉพาะทาง ส่วนประกอบต่างๆ ของ ICS อยู่ในบริเวณที่มีการรักษาความปลอดภัยทางกายภาพและส่วนประกอบดังกล่าวไม่ได้เชื่อมต่อกับเครือข่ายหรือระบบ IT ปัจจุบันนี้อุปกรณ์อินเทอร์เน็ตโปรโตคอล Internet Protocol (IP) ราคาถูกที่มีจำหน่ายกันอย่างแพร่หลายกำลังเข้ามาแทนที่วิธีการเดิมที่เป็นกรรมสิทธิ์เฉพาะ ซึ่งเพิ่มโอกาสเกิดช่องโหว่และเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ เนื่องจาก ICS กำลังใช้ระบบ IT เพื่อสนับสนุนการเชื่อมต่อระบบธุรกิจขององค์กรและความสามารถในการใช้งานจากระยะไกล และได้รับการออกแบบและใช้งานด้วยคอมพิวเตอร์ ระบบปฏิบัติการ Operating System (OS) และโปรโตคอลเครือข่ายที่เป็นมาตรฐานอุตสาหกรรม สิ่งนี้จึงเริ่มคล้ายกับระบบ IT การบูรณาการนี้รองรับความสามารถด้าน IT ใหม่ ๆ แต่จะแยก ICS ออกจากโลกภายนอกน้อยกว่ระบบรุ่นก่อนอย่างชัดเจน ทำให้เกิดความต้องการรักษาความปลอดภัยระบบนี้มากขึ้น การใช้เครือข่ายไร้สายที่เพิ่มขึ้นทำให้การใช้งานของ ICS มีความเสี่ยงมากขึ้นจากผู้ไม่หวังดีที่อยู่ใกล้เคียงแต่ไม่สามารถเข้าใช้งานอุปกรณ์ได้โดยตรง แม้ว่าวิธีดำเนินการด้านความปลอดภัยจะได้รับการออกแบบมาเพื่อจัดการกับปัญหาด้านความปลอดภัยนี้ในระบบ IT ทั่วไป แต่ก็ต้องใช้ความระมัดระวังเป็นพิเศษเมื่อนำวิธีการดำเนินการเดียวกันนี้ไปใช้กับสภาพแวดล้อมของ ICS ในบางกรณีอาจจำเป็นต้องมีวิธีดำเนินการในการรักษาความปลอดภัยใหม่ ๆ ที่ปรับให้เหมาะกับสภาพแวดล้อมของ ICS ด้วย

ถึงแม้ลักษณะบางประการจะคล้ายคลึงกัน แต่ ICS ก็มีลักษณะที่แตกต่างจากระบบประมวลผลข้อมูลแบบเดิมด้วย ความแตกต่างในหลายประการนี้เกิดจากการที่ลอจิกใน ICS มีผลโดยตรงต่อโลกทางกายภาพ ลักษณะบางประการนี้ประกอบด้วยความเสี่ยงที่มีความสำคัญต่อสุขภาพและความปลอดภัยของชีวิตมนุษย์และความเสียหายร้ายแรงต่อสิ่งแวดล้อม ตลอดจนปัญหาทางการเงินที่ร้ายแรง เช่น การสูญเสียในการผลิต ผลกระทบด้านลบต่อเศรษฐกิจของประเทศ และความหกล้มในข้อมูลกรรมสิทธิ์ ซึ่ง ICS มีข้อกำหนดด้านประสิทธิภาพและความน่าเชื่อถือที่เป็นเอกลักษณ์และมักใช้ระบบปฏิบัติการและ

แอปพลิเคชันที่แหวกแนวไปจากบุคลากรด้าน IT โดยทั่วไป นอกจากนี้เป้าหมายด้านความปลอดภัยและประสิทธิภาพในบางครั้งก็ขัดแย้งกับความปลอดภัยในการออกแบบและการทำงานของระบบควบคุมด้วย

โปรแกรมการรักษาความปลอดภัยทางไซเบอร์ของ ICS ควรเป็นส่วนหนึ่งของโปรแกรมการรักษาความปลอดภัยและเชื่อถือได้ของ ICS ที่ใช้กันในวงกว้าง ทั้งโปรแกรมในโรงงานอุตสาหกรรมและโปรแกรมการรักษาความปลอดภัยทางไซเบอร์ขององค์กร ด้วย เนื่องจากความปลอดภัยทางไซเบอร์มีความสำคัญต่อการดำเนินงานอย่างปลอดภัยและเชื่อถือได้สำหรับกระบวนการทางอุตสาหกรรมสมัยใหม่ ภัยคุกคามต่อระบบควบคุมมาจากหลายแหล่ง ได้แก่ การไม่ยอมรับของรัฐบาล กลุ่มก่อการร้าย พนักงานที่ไม่พึงพอใจ ผู้บุกรุกที่มุ่งอันตราย ความซับซ้อน อุบัติเหตุ และภัยพิบัติทางธรรมชาติ ตลอดจนการกระทำที่มุ่งอันตรายหรือพลาดพลังโดยบุคคลภายใน โดยทั่วไปวัตถุประสงค์ด้านความปลอดภัยของ ICS จะเป็นไปตามลำดับความสำคัญของความพร้อมใช้งานและความสมบูรณ์ ตามมาด้วยการรักษาความลับ

อุบัติการณ์ที่ ICS อาจต้องเผชิญ มีดังต่อไปนี้:

- การส่งข้อมูลผ่านเครือข่าย ICS โดนปิดกั้นหรือหน่วง ซึ่งอาจขัดขวางการทำงานของ ICS ได้
- การเปลี่ยนแปลงโดยไม่ได้รับอนุญาตต่อคำแนะนำ คำสั่ง หรือเกณฑ์เริ่มการแจ้งเตือน ซึ่งอาจสร้างความเสียหาย ปิดการใช้งาน หรือปิดอุปกรณ์ สร้างผลกระทบต่อสิ่งแวดล้อม และ/หรือเป็นอันตรายต่อชีวิตมนุษย์ได้
- การส่งข้อมูลที่ไม่ถูกต้องไปยังผู้ปฏิบัติงานระบบ ไม่ว่าจะเป็นการปิดบังการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตหรือเป็นสาเหตุที่ทำให้ผู้ปฏิบัติงานเริ่มกระทำการที่ไม่ถูกต้อง ซึ่งอาจส่งผลเสียต่าง ๆ ได้
- การแก้ไขซอฟต์แวร์ ICS หรือการตั้งค่ากำหนด หรือซอฟต์แวร์ ICS ตัดมีลแวร์ซึ่งอาจทำได้มีผลเสียต่าง ๆ ได้
- การรบกวนการทำงานของระบบป้องกันอุปกรณ์ ซึ่งอาจมุ่งอันตรายต่ออุปกรณ์ที่มีราคาสูงและเปลี่ยนทดแทนได้ยาก
- การรบกวนการทำงานของระบบความปลอดภัย ซึ่งอาจมุ่งอันตรายต่อชีวิตมนุษย์

วัตถุประสงค์ด้านความปลอดภัยที่สำคัญสำหรับการใช้ ICS ควรมีดังต่อไปนี้:

- การจำกัดการเข้าใช้งานเครือข่าย ICS และกิจกรรมเครือข่ายแบบบล็อก โดยอาจรวมถึงการใช้เกตเวย์แบบทิศทางเดียว ซึ่งเป็นสถาปัตยกรรมเครือข่ายที่อนุญาตให้เข้าใช้งานได้ผ่านทางอินเทอร์เน็ต (DMZ) ที่มีไฟร์วอลล์ป้องกันการรับส่งข้อมูลเครือข่ายจากการผ่านโดยตรงระหว่างเครือข่ายขององค์กรและเครือข่าย ICS และมีกลไกการรับรองความถูกต้องและรับรองข้อมูลแยกออกจากกันสำหรับผู้ใช้งานเครือข่ายขององค์กรและ ICS โดย ICS ควรใช้รูปแบบโครงข่ายเครือข่ายแบบหลายชั้นที่มีการสื่อสารที่สำคัญอยู่ในชั้นที่ปลอดภัยและเชื่อถือได้มากที่สุด
- การจำกัดการเข้าใช้งานทางกายภาพสำหรับเครือข่ายและอุปกรณ์ของ ICS การเข้าใช้งานทางกายภาพโดยไม่ได้รับอนุญาตไปยังส่วนต่าง ๆ อาจทำให้การทำงานของ ICS หยุดชะงักขั้นรุนแรง ควรใช้การควบคุมการเข้าใช้งานทางกายภาพแบบผสมผสานกัน เช่น ล็อกกุญแจ เครื่องอ่านบัตร และ/หรือผู้ดูแลป้องกัน
- การป้องกัน ICS ในแต่ละส่วนจากการเจาะระบบ ซึ่งรวมถึงการใช้การปรับแต่งเสริมเพื่อรักษาความปลอดภัยอย่างรวดเร็วด้วยวิธีที่เป็นไปได้หลังจากทดสอบในหน่วยปฏิบัติงานแล้ว [32] [77] ปิดการใช้งานพอร์ตทั้งหมดที่ไม่ได้ใช้และบริการต่างๆ แล้วตรวจสอบให้แน่ใจว่ายังคงปิดการใช้งานอยู่ จำกัดสิทธิ์ผู้ใช้งาน ICS ไว้เฉพาะหน้าที่จำเป็นเท่านั้น การติดตามและตรวจสอบการตรวจสอบที่ดำเนินการ และใช้การควบคุมความปลอดภัย เช่น ซอฟต์แวร์ป้องกันไวรัสและซอฟต์แวร์ตรวจสอบความสมบูรณ์ของไฟล์ เมื่อมีความเป็นไปได้ในทางเทคนิคที่จะป้องกัน ยับยั้ง ตรวจสอบ และบรรเทาผลกระทบจากมัลแวร์

- **การจำกัดการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต** ซึ่งรวมถึงข้อมูลที่อยู่ในระหว่างการส่ง (ที่ข้ามขอบเขตเครือข่ายเป็นอย่างน้อย) และที่เก็บพักไว้
- **การตรวจจับเหตุการณ์และอุบัติการณ์ด้านความปลอดภัย** การตรวจจับเหตุการณ์ด้านความปลอดภัยที่ยังไม่ได้ยกระดับเป็นอุบัติการณ์ ช่วยให้ฝ่ายป้องกันสามารถทำลายห่วงโซ่การโจมตีก่อนที่ผู้โจมตีจะบรรลุวัตถุประสงค์ได้ รวมไปถึงความสามารถในการตรวจจับส่วนประกอบของ ICS ที่ทำงานล้มเหลว บริการที่ไม่พร้อมใช้งาน และทรัพยากรที่หมดไปแล้วซึ่งมีความสำคัญต่อการทำงานอย่างถูกต้องและปลอดภัยของ ICS
- **การรักษาฟังก์ชันการทำงานในสถานะที่ไม่เอื้ออำนวย** ซึ่งเกี่ยวกับการออกแบบ ICS ให้องค์ประกอบสำคัญแต่ละส่วนมีการทำงานสำรองแบบควบคู่กัน นอกจากนี้หากมีส่วนประกอบที่ทำงานล้มเหลวก็ควรจะเป็นความล้มเหลวในลักษณะที่ไม่ก่อให้เกิดการรับส่งข้อมูลที่ไม่จำเป็นบน ICS หรือเครือข่ายต่าง ๆ หรือไม่ก่อให้เกิดปัญหาในที่อื่นได้อีก เช่น เหตุการณ์ที่ส่งผลกระทบต่อการทำงานในระบบอื่น นอกจากนี้ ICS ก็ควรสามารถทำงานได้ในสถานะเสื่อมสภาพ เช่น การเปลี่ยนจาก “การทำงานปกติ” ด้วยระบบอัตโนมัติเต็มรูปแบบมาเป็น “การทำงานฉุกเฉิน” โดยอาศัยผู้ปฏิบัติงานมากขึ้นและลดการใช้ระบบอัตโนมัติเป็น “ดำเนินการด้วยตนเอง” โดยไม่มีระบบอัตโนมัติ
- **การกู้คืนระบบหลังเกิดอุบัติการณ์** อุบัติการณ์เป็นสิ่งที่หลีกเลี่ยงไม่ได้และการมีแผนรับมืออุบัติการณ์นั้นก็เป็นเรื่องจำเป็น ซึ่งลักษณะที่สำคัญของโปรแกรมรักษาความปลอดภัยที่ดีคือความรวดเร็วในการกู้คืนระบบหลังเกิดอุบัติการณ์

ในการกำหนดความปลอดภัยของ ICS อย่างถูกต้อง ทีมงานรักษาความปลอดภัยทางไซเบอร์แบบข้ามสายงานจึงจำเป็นต้องแบ่งปันความรู้และประสบการณ์กันอย่างหลากหลายในการประเมินและลดความเสี่ยงต่อ ICS ทีมงานความปลอดภัยทางไซเบอร์ควรประกอบไปด้วยสมาชิกของเจ้าหน้าที่ IT ขององค์กร วิศวกรควบคุม ผู้ดำเนินงานระบบควบคุม ผู้เชี่ยวชาญด้านความปลอดภัยเครือข่ายและระบบ สมาชิกของเจ้าหน้าที่ฝ่ายบริหาร และเจ้าหน้าที่ความปลอดภัยทางกายภาพเป็นอย่างน้อย เพื่อให้มีความต่อเนื่องและครบถ้วน ทีมงานความปลอดภัยทางไซเบอร์ควรปรึกษากับผู้จำหน่ายระบบ ควบคุมและ/หรือผู้วางระบบด้วย ทีมรักษาความปลอดภัยทางไซเบอร์ควรประสานงานอย่างใกล้ชิดกับฝ่ายบริหารสถานที่ (เช่น ผู้ดูแลอาคารสถานที่) และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง Chief Information Officer (CIO) หรือผู้บริหารด้านการรักษาความปลอดภัยระดับสูง Chief Security Officer (CSO) ของบริษัท ซึ่งในทางกลับกันก็เป็นผู้ที่ต้องยอมรับความรับผิดชอบและภาระหน้าที่ทั้งหมดสำหรับความปลอดภัยทางไซเบอร์ของ ICS และสำหรับอุบัติการณ์ด้านความปลอดภัย อุบัติการณ์ในด้านความน่าเชื่อถือ หรือความเสียหายของอุปกรณ์ที่เกิดจากอุบัติการณ์ทางไซเบอร์ทั้งทางตรงและทางอ้อมต่าง ๆ โปรแกรมรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพสำหรับ ICS ควรใช้กลยุทธ์ที่เรียกว่า “การป้องกันแบบเจาะลึก” โดยวางกลไกการรักษาความปลอดภัยเป็นชั้น เพื่อให้ผลกระทบของความล้มเหลวในโลกไคโดกลไกหนึ่งลดลง องค์กรไม่ควรพึ่งพาอาศัย “ความปลอดภัยที่คลุมเครือ”

ใน ICS แบบทั่วไป ความหมายของกลยุทธ์การป้องกันเชิงลึกมีดังนี้:

- การพัฒนานโยบาย ขั้นตอน การฝึกอบรม และสื่อการศึกษาความปลอดภัยที่ใช้ให้กับ ICS โดยเฉพาะ
- พิจารณานโยบายและขั้นตอนการรักษาความปลอดภัยของ ICS ตามแนวทางของระบบที่รักษาความมั่นคงแห่งมาตุภูมิ ระดับภัยคุกคาม โดยปรับใช้มาตรการรักษาความปลอดภัยที่เพิ่มมากขึ้นเมื่อระดับภัยคุกคามเพิ่มขึ้น

- จัดการกับความปลอดภัยตลอดอายุการทำงานของ ICS ตั้งแต่การออกแบบสถาปัตยกรรมไปจนถึงการจัดซื้อจัดจ้าง การติดตั้ง การบำรุงรักษา จนถึงการรื้อถอน
- การใช้รูปแบบโครงข่ายเครือข่ายไปสำหรับ ICS ที่มีหลายชั้น โดยให้การสื่อสารที่สำคัญที่สุดอยู่ในชั้นที่ปลอดภัยและเชื่อถือได้มากที่สุด
- ให้การแบ่งแยกออกจากกันด้วยลอจิกระหว่างเครือข่ายขององค์กรและเครือข่าย ICS (เช่น ไฟร์วอลล์ที่ตรวจสอบสถานะระหว่างเครือข่าย เกตเวย์ทิศทางเดียว)
- การใช้สถาปัตยกรรมเครือข่าย DMZ (เช่น ป้องกันการรับส่งข้อมูลโดยตรง ระหว่างองค์กรและเครือข่าย ICS)
- ตรวจสอบให้แน่ใจว่ามีส่วนประกอบที่สำคัญสองชุดและมีเครือข่ายสำรอง
- การออกแบบระบบที่สำคัญให้สามารถทำงานได้ในสภาวะรองรับต่อความผิดพลาดได้ (ทนต่อความผิดพลาด) เพื่อป้องกันการเกิดเหตุการณ์ความล้มเหลวแบบเรียงซ้อนตามลำดับซึ่งมีมูลค่าความเสียหายสูง
- การปิดใช้งานพอร์ตและบริการที่ไม่ได้ใช้แล้วบนอุปกรณ์ ICS ภายหลังการทดสอบ เพื่อให้มั่นใจว่าจะไม่ส่งผลกระทบต่อการทำงานของ ICS
- การจำกัดการเข้าถึงงานทางกายภาพสำหรับเครือข่ายและอุปกรณ์ของ ICS
- การจำกัดสิทธิผู้ใช้งาน ICS เฉพาะที่จำเป็นต่อการปฏิบัติงานของแต่ละคนเท่านั้น (ได้แก่ การสร้างการควบคุมการเข้าถึงงานตามบทบาทและการกำหนดค่าแต่ละบทบาทตามหลักการให้สิทธิขั้นต่ำ) [28]
- การใช้กลไกการรับรองความถูกต้องและข้อมูลรับรองแยกออกจากกันสำหรับผู้ใช้งานเครือข่าย ICS และเครือข่ายขององค์กร (เช่น บัญชีเครือข่าย ICS ไม่สามารถใช้บัญชีผู้ใช้งานเครือข่ายขององค์กร)
- ใช้เทคโนโลยีที่ทันสมัย เช่น สมาร์ทการ์ดเพื่อการยืนยันตัวตนบุคคล Personal Identity Verification (PIV)
- การใช้การควบคุมความปลอดภัย เช่น ซอฟต์แวร์ตรวจจับการบุกรุก ซอฟต์แวร์ป้องกันไวรัส และซอฟต์แวร์ตรวจสอบความสมบูรณ์ไฟล์ ในกรณีที่เป็นไปได้ทางเทคนิค เพื่อป้องกัน ขัดขวาง ตรวจจับ และบรรเทาผลกระทบของการนำพา การเผชิญ และการแพร่กระจายซอฟต์แวร์ที่เป็นอันตรายไปยัง โหนด และจาก ICS
- การใช้เทคนิคการรักษาความปลอดภัย เช่น การเข้ารหัสและ/หรือแฮชการเข้ารหัสเพื่อจัดเก็บข้อมูลและการสื่อสารตามที่เห็นสมควร
- ปรับใช้การปรับแต่งเพื่อรักษาความปลอดภัยอย่างรวดเร็วหลังจากทดสอบการปรับแต่งทั้งหมดภายใต้สภาวะการทดสอบในหน่วยปฏิบัติงานหากเป็นไปได้ ก่อนทำการติดตั้งบน ICS
- ติดตามและตรวจดูเส้นทางการตรวจสอบในพื้นที่สำคัญของ ICS
- ใช้โปรโตคอลและบริการเครือข่ายที่เชื่อถือได้และปลอดภัยหากเป็นไปได้

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ National Institute of Standards and Technology (NIST) ร่วมกับชุมชน ICS ในภาคส่วนรัฐและเอกชน ได้พัฒนาแนวปฏิบัติเฉพาะเกี่ยวกับการประยุกต์ใช้การควบคุมความปลอดภัยในบทความฉบับพิเศษ (SP) 800 - 53 แก์ครั้งที่ 4 ของ NIST การควบคุมความปลอดภัยและการรักษาความเป็นส่วนตัวสำหรับระบบข้อมูลและองค์กรรัฐบาลกลาง [22] ให้กับ ICS

ในขณะที่ส่วนควบคุมต่าง ๆ ของ NIST SP 800 - 53 สามารถใช้ได้กับ ICS ตามที่เขียนไว้ แต่ส่วนควบคุมหลายส่วนต้องมีการตีความที่เฉพาะสำหรับ ICS และ/หรือเสริมโดยเพิ่มข้อใดข้อหนึ่งต่อไปนี้อยู่ในส่วนควบคุม:

- แนวทางปฏิบัติเสริมของ ICS ให้ข้อมูลเพิ่มเติมแก่องค์กรเกี่ยวกับการประยุกต์ใช้การควบคุมการรักษาความปลอดภัย และการเพิ่มประสิทธิภาพการควบคุมของ NIST SP 800 - 53 สำหรับ ICS และสภาพแวดล้อมที่ระบบเฉพาะทางนี้ทำงาน นอกจากนี้แนวทางปฏิบัติเสริมยังให้ข้อมูลด้วยว่าทำไมจึงต้องมีการควบคุมหรือควบคุมความปลอดภัยโดยเฉพาะ การปรับปรุง อาจไม่สามารถใช้ได้กับสภาพแวดล้อมของ ICS บางลักษณะและอาจใช้เป็นตัวเลือกสำหรับการปรับแต่ง (ได้แก่ การใช้เป็น แนวทางกำหนดขอบเขตงาน และ/หรือ ควบคุมการชดเชย) ซึ่งแนวทางปฏิบัติเสริมของ ICS ไม่ได้มาแทนที่แนวทางของ NIST SP 800 - 53 [22]
- การเพิ่มประสิทธิภาพ ICS (หนึ่งหรือมากกว่า) ที่ให้การเสริมประสิทธิภาพจากการควบคุมดั้งเดิมที่อาจจำเป็นสำหรับ ICS บางอย่าง
- แนวทางปฏิบัติเสริมของการเพิ่มประสิทธิภาพ ICS ที่ให้คำแนะนำเกี่ยวกับวิธีการเพิ่มประสิทธิภาพการควบคุมที่ใช้หรือไม่ ใช้ในสภาพแวดล้อมของ ICS

วิธีที่ประสบความสำเร็จมากที่สุดในการรักษาความปลอดภัยของ ICS คือการรวบรวมแนวทางปฏิบัติที่แนะนำใน อุตสาหกรรมและมีส่วนร่วมในความพยายามเชิงรุกและการทำงานร่วมกันระหว่างฝ่ายบริหาร วิศวกรควบคุม และ ผู้ปฏิบัติงาน องค์กรด้าน IT และที่ปรึกษาระบบอัตโนมัติที่เชื่อถือได้ ทีมนี้ควรจะต้องหาความสมบูรณ์ของข้อมูลที่ได้รับจาก รัฐบาลกลาง กลุ่มอุตสาหกรรม ผู้จำหน่าย และกิจกรรมองค์กรมาตรฐานที่กำลังดำเนินอยู่

SE-ED
inspiration starts here

1. บทนำ

1.1 วัตถุประสงค์และขอบเขตงาน

วัตถุประสงค์ของหนังสือแนวทางปฏิบัติสำหรับความปลอดภัยของระบบควบคุมทางอุตสาหกรรม (ICS) เพื่อใช้เป็นคู่มือแนวทางปฏิบัติสำหรับความปลอดภัย รวมทั้งกรณีศึกษาของทั้ง 11 เหตุการณ์ที่เกิดขึ้นจริงกับระบบควบคุมอุตสาหกรรม ซึ่งเหตุการณ์ที่เกิดขึ้นจะเกี่ยวข้องกับระบบใดระบบหนึ่งในระบบควบคุมทางอุตสาหกรรม เช่น ระบบการควบคุมดูแลและการรับข้อมูล (SCADA) ระบบควบคุมการจัดจำหน่าย (DCS) และระบบอื่น ๆ ที่ทำหน้าที่ควบคุม ซึ่งเอกสารนี้จะให้ภาพโดยรวมของ ICS ทบทวนรูปแบบโครงสร้างของระบบและสถาปัตยกรรม ระบุภัยคุกคามและช่องโหว่ที่ทราบต่อระบบนี้ และมีคำแนะนำมาตรการรับมือด้านความปลอดภัยเพื่อบรรเทาความเสี่ยงที่เกี่ยวข้อง นอกจากนี้ยังนำเสนอการซ้อนทับการควบคุมความปลอดภัยของ ICS ที่ออกแบบไว้โดยเฉพาะ โดยอ้างอิงตาม NIST SP 800 - 53 แก์ครั้งที่ 4 [22] เพื่อปรับแต่งการควบคุมตามที่ต้องการใช้กับลักษณะเฉพาะของ โดเมน ICS เนื้อหาของเอกสารให้บริบทสำหรับการซ้อนทับแต่การซ้อนทับนั้นไม่จุดประสงค์เพื่อให้ทำงานแยกเดี่ยวได้

ICS พบได้ในหลายอุตสาหกรรม เช่น ไฟฟ้า น้ำและน้ำเสีย น้ำมันและแก๊สธรรมชาติ สารเคมี ยา เยื่อและกระดาษ อาหารและเครื่องดื่ม และการผลิตแบบแยกส่วน (เช่น ยานยนต์ การบินและอวกาศ สินค้าคงทน) เนื่องจาก ICS มีหลายประเภทซึ่งมีระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้นได้แตกต่างกัน และมีการวิวัฒนาการตามการปฏิวัติอุตสาหกรรม มีเอกสารนำเสนอรายการเกี่ยวกับวิธีการต่าง ๆ มากมายและเทคนิคการรักษาความปลอดภัยของ ICS แต่ไม่ควรใช้เอกสารเป็นรายการตรวจสอบเพื่อรักษาความปลอดภัยระบบเฉพาะเพียงอย่างเดียวเท่านั้น ขอสนับสนุนให้ผู้เข้าอบรมดำเนินการประเมินความเสี่ยงระบบตนเองและปรับแต่งแนวทางและการแก้ไขที่แนะนำเพื่อให้ตรงตามข้อกำหนดด้านความปลอดภัย ธุรกิจ และการปฏิบัติงานที่เฉพาะ การใช้งานต่าง ๆ ตามแนวคิดพื้นฐานสำหรับการรักษาความปลอดภัยระบบควบคุมที่นำเสนอในเอกสารนี้ ยังคงมีเพิ่มขึ้นอย่างต่อเนื่อง

แนวโน้มของการโจมตีทางไซเบอร์ในบริบทของอุตสาหกรรม 4.0 (Industrial 4.0) มีลักษณะพิเศษคือความซับซ้อน ความถี่ และผลกระทบที่เพิ่มขึ้น เมื่อระบบอุตสาหกรรมเชื่อมโยงและบูรณาการกันมากขึ้น ลักษณะและขนาดของภัยคุกคามทางไซเบอร์ก็ยังคงพัฒนาต่อไป ความท้าทายด้านความปลอดภัยทางไซเบอร์ในอุตสาหกรรม 4.0 โดยเฉพาะการผลิตเป็นอุตสาหกรรมที่ถูกโจมตีมากเป็นอันดับสอง แต่ภาคการผลิตยังคงล่าช้าในเรื่องการป้องกันภัยจากการโจมตีทางไซเบอร์ โรงงานอัจฉริยะอาจตกอยู่ภายใต้ช่องโหว่ มัลแวร์ การปฏิเสธการบริการ (DoS) การแฮ็กอุปกรณ์ และวิธีการโจมตีทั่วไปอื่น ๆ ที่เครือข่ายอุตสาหกรรมต้องเผชิญ และวงในการโจมตีทางไซเบอร์ที่ขยายใหญ่ขึ้นของโรงงานอัจฉริยะทำให้ผู้ผลิตตรวจจับและป้องกันการโจมตีทางไซเบอร์ได้ยากเป็นพิเศษ ขณะนี้ภัยคุกคามเหล่านี้ทำงานในระดับใหม่ทั้งหมดพร้อมกับ การขยายตัวด้านการสื่อสารผ่านระบบ IoT อาจส่งผลให้เกิดผลกระทบทางกายภาพที่ร้ายแรง โดยเฉพาะอย่างยิ่งในขอบเขตของ IoT ต่อไปนี้เป็นความท้าทายด้านความปลอดภัยใหม่ ๆ ที่องค์กรต่าง ๆ เผชิญในยุคอุตสาหกรรม 4.0

- อุปกรณ์ที่เชื่อมต่อทุกเครื่องแสดงถึงความเสี่ยงที่อาจเกิดขึ้น
- ระบบการผลิต เช่น ระบบควบคุมอุตสาหกรรม (ICS) มีช่องโหว่เฉพาะที่ทำให้เสี่ยงต่อการโจมตีทางไซเบอร์เป็นพิเศษ
- อุตสาหกรรม 4.0 เชื่อมต่อกับระบบที่แยกออกจากกันก่อนหน้านี้ ซึ่งเพิ่มพื้นที่การโจมตี
- การอัปเดตมักจะได้รับการติดตั้งที่ละน้อยเนื่องจากระบบมีความซับซ้อนมาก
- การผลิตมีมาตรฐานการปฏิบัติตามกฎระเบียบน้อยกว่าภาคส่วนอื่น ๆ มาก

- ทศนวิสัยและการบูรณาการไม่ดีในระบบที่แยกจากกันและสภาพแวดล้อมที่แยกออกไป

นอกจากนี้การโจมตีทางไซเบอร์นั้นความรุนแรงหรือผลกระทบที่ตามมาแต่ละองค์กรย่อมไม่เท่ากันอย่างแน่นอน แม้ว่าองค์กรต่าง ๆ จะต้องปกป้องเทคโนโลยีจำนวนมากบนระบบ IT และ OT ที่การโจมตีที่มีขนาดใหญ่มาก ผู้โจมตีต้องการเพียงระบุจุดอ่อนที่สุดเท่านั้น ในท้ายที่สุด แนวทางปฏิบัติด้านความปลอดภัยจะเป็นกุญแจสู่ความสำเร็จของอุตสาหกรรม 4.0 ภาคการผลิตจำเป็นต้องนำกรอบความคิดด้านความปลอดภัยที่อิงตามความเสี่ยงมาใช้ (ผู้วิกฤตทางธุรกิจเข้ากับกลยุทธ์การป้องกัน) จัดเก็บรายการสินทรัพย์ OT ทั้งหมดที่แม่นยำในแบบเรียลไทม์ ผสมผสานสิ่งที่ดีที่สุดใน IT และ OT เข้าด้วยกันเป็นกลยุทธ์การป้องกันแบบบูรณาการในทุกๆ ระบบที่มีโอกาสในการโจมตี ระบบและแก้ไขระบบที่ล้าสมัย ช่องโหว่ที่ยังไม่ได้แพตช์หรือปรับปรุง และไฟล์ที่มีความปลอดภัยต่ำ ใช้แนวทางการรักษาความปลอดภัยเป็นอันดับแรกในการปรับใช้ระบบที่เชื่อมต่อใหม่ รมิตระวังอยู่เสมอเพื่อระบุภัยคุกคามที่อาจเกิดขึ้นด้วยการประเมินช่องโหว่แบบเรียลไทม์และการจัดลำดับความสำคัญตามความเสี่ยง ตรวจสอบให้แน่ใจว่าซัพพลายเออร์เทคโนโลยีและผู้ผลิตอุปกรณ์ที่เชื่อมต่อมุ่งมั่นที่จะรักษาความปลอดภัยและแพตช์ซอฟต์แวร์และการตรวจสอบเป็นประจำ ข้อมูลภัยคุกคามรวมถึงการตรวจสอบเว็บมีดก็สามารถดำเนินการได้เช่นกัน เป็นระบบเตือนภัยล่วงหน้าเพื่อเปิดเผยการโจมตีที่วางแผนไว้ ดังนั้นองค์กรจึงสามารถป้องกันการละเมิดและดำเนินการทันทีเพื่อปกป้องทรัพย์สินดิจิทัลขององค์กรและโครงสร้างพื้นฐานทางกายภาพ

การเข้าใจในบริบทด้านประวัติศาสตร์สำหรับอุตสาหกรรมจะทำให้ผู้ปฏิบัติทราบถึงกระบวนการในการผลิตและเทคโนโลยีที่ประยุกต์ใช้ในแต่ละช่วงของการปฏิวัติอุตสาหกรรม เพื่อเป็นพื้นฐานในการวิเคราะห์ปัญหาและแนวทางในการแก้ไขปัญหาโดยเทคโนโลยี และผลของสภาพแวดล้อมจากปฏิวัติอุตสาหกรรม ในภูมิภาคทางเทคโนโลยีที่พัฒนาอย่างรวดเร็วในปัจจุบัน IT และ OT มักจะดำเนินการเป็นโดเมนที่แตกต่างกัน IT เกี่ยวข้องกับการจัดการข้อมูล ความปลอดภัยทางไซเบอร์ และโครงสร้างพื้นฐานเครือข่าย โดยมุ่งเน้นที่ด้านการคำนวณของการดำเนินธุรกิจ ในทางกลับกัน OT มุ่งเน้นไปที่การตรวจสอบและควบคุมกระบวนการทางกายภาพ ระบบ และเครื่องจักร ซึ่งมีบทบาทสำคัญในอุตสาหกรรมต่าง ๆ เช่น การผลิตพลังงาน และการขนส่ง นอกจากนี้ การปฏิบัติตามกฎระเบียบและมาตรฐานอุตสาหกรรมมีบทบาทสำคัญในการจัดการความแตกต่างด้าน IT และ OT การปฏิบัติตามมาตรฐานเหล่านี้ช่วยให้มั่นใจว่าระบบมีความปลอดภัย ยืดหยุ่น และสามารถตอบสนองความต้องการในการปฏิบัติงานได้ หน่วยงานกำกับดูแลกำลังตระหนักมากขึ้นถึงความจำเป็นในการใช้เฟรมเวิร์กบูรณาการที่ครอบคลุมทั้งไอทีและ OT โดยส่งเสริมแนวทางปฏิบัติที่ดีที่สุดและกำหนดเกณฑ์มาตรฐานด้านความปลอดภัยและประสิทธิภาพ

1.2 บริบททางประวัติศาสตร์สำหรับอุตสาหกรรม 4.0

ในทุกภาคอุตสาหกรรม เครื่องจักรแบบไดนามิกและใช้งานง่ายกำลังเปลี่ยนแปลงวิธีดำเนินธุรกิจ ต่างจากเทคโนโลยีที่อิงรูปแบบดั้งเดิม เครื่องจักรและกระบวนการที่ยืดหยุ่นเหล่านี้จะปรับให้เข้ากับสภาพแวดล้อมแบบไดนามิกและตัวแปรที่เปลี่ยนแปลง ลองนึกภาพสายการผลิตที่แขนหุ่นยนต์ติดตั้งชิ้นส่วนไฟฟ้าในเครื่องจักร โดยทั่วไปแล้ว แขนจะต้องหยุดชั่วคราวหากชิ้นส่วนไม่ได้รับการจัดวางอย่างถูกต้องในสายการผลิต แต่ด้วยเทคโนโลยีแบบไดนามิกและปรับเปลี่ยนได้ แขนจะสามารถปรับการเคลื่อนไหวเพื่อให้ติดตั้งชิ้นส่วนได้ง่ายไม่ว่าจะอยู่ในตำแหน่งใดก็ตาม นี่ไม่ใช่เทคโนโลยีจากอนาคตอันไกลโพ้น มีตัวอย่างเทคโนโลยีอัจฉริยะมากมายที่ส่งผลกระทบต่อโลกในปัจจุบัน ตั้งแต่โดรนที่ตรวจสอบท่อส่งก๊าซอย่างอิสระไปจนถึง

โรงงานที่เพิ่มประสิทธิภาพด้วยตนเอง เช่นเดียวกับการผลิตไอน้ำและไฟฟ้าที่เพิ่มขึ้นร้อยละ 17-20 จากผู้ผลิตที่ใช้ระบบอัจฉริยะ ซึ่งเป็นการปฏิวัติอุตสาหกรรมเมื่อศตวรรษก่อน เทคโนโลยีที่ใช้ปัญญาประดิษฐ์ หรือ Artificial Intelligence (AI) กำลังกระตุ้นการปฏิวัติอุตสาหกรรมครั้งที่สี่หรืออุตสาหกรรม 4.0

1.2.1 การปฏิวัติอุตสาหกรรมครั้งแรก

เริ่มต้นในช่วงปลายศตวรรษที่ 18 ในอังกฤษ การปฏิวัติอุตสาหกรรมครั้งแรกช่วยให้เกิดการผลิตจำนวนมากโดยใช้พลังงานน้ำและไอน้ำ แทนที่จะเป็นพลังของมนุษย์และสัตว์ล้วน ๆ สินค้าสำเร็จรูปถูกสร้างขึ้นด้วยเครื่องจักรแทนที่จะผลิตด้วยมืออย่างอุตสาหกรรม

1.2.2 การปฏิวัติอุตสาหกรรมครั้งที่สอง

หนึ่งศตวรรษต่อมา การปฏิวัติอุตสาหกรรมครั้งที่สองทำให้เกิดสายการผลิตและการใช้น้ำมัน ก๊าซ และพลังงานไฟฟ้า แหล่งพลังงานใหม่เหล่านี้ พร้อมด้วยการสื่อสารขั้นสูงผ่านทางโทรศัพท์และโทรเลข ได้นำการผลิตจำนวนมากและระบบอัตโนมัติในระดับหนึ่งมาสู่กระบวนการผลิต

1.2.3 การปฏิวัติอุตสาหกรรมครั้งที่สาม

การปฏิวัติอุตสาหกรรมครั้งที่สามซึ่งเริ่มขึ้นในกลางศตวรรษที่ 20 ได้เพิ่มคอมพิวเตอร์ โทรคมนาคมขั้นสูง และการวิเคราะห์ข้อมูลในกระบวนการผลิต การแปลงโรงงานเป็นดิจิทัลเริ่มต้นด้วยการฝังตัวควบคุมลอจิกแบบโปรแกรมได้ (PLC) ไว้ในเครื่องจักรเพื่อช่วยให้กระบวนการบางอย่างเป็นอัตโนมัติและรวบรวมและแบ่งปันข้อมูล

1.2.4 การปฏิวัติอุตสาหกรรมครั้งที่สี่

ขณะนี้เราอยู่ในการปฏิวัติอุตสาหกรรมครั้งที่ 4 หรือที่เรียกว่าอุตสาหกรรม 4.0 โดดเด่นด้วยการเพิ่มระบบอัตโนมัติและการใช้งานเครื่องจักรอัจฉริยะและโรงงานอัจฉริยะ ข้อมูลที่ได้รับแจ้งช่วยในการผลิตสินค้าได้อย่างมีประสิทธิภาพและประสิทธิภาพมากขึ้นตลอดห่วงโซ่คุณค่า ความยืดหยุ่นได้รับการปรับปรุงเพื่อให้ผู้ผลิตสามารถตอบสนองความต้องการของลูกค้าได้ดียิ่งขึ้นโดยใช้การปรับแต่งจำนวนมาก ซึ่งในท้ายที่สุดแล้ว พยายามที่จะบรรลุประสิทธิภาพด้วยขนาดจำนวนมากในหลายๆ กรณีด้วยการรวบรวมข้อมูลเพิ่มเติมจากพื้นที่โรงงานและผสมผสานกับข้อมูลการดำเนินงานอื่น ๆ ขององค์กร โรงงานอัจฉริยะจึงสามารถบรรลุถึงความโปร่งใสของข้อมูลและการตัดสินใจที่ดีขึ้น

อุตสาหกรรม 4.0 เป็นแนวคิดใหม่ ดังนั้นการประเมินความเสี่ยงจึงมีความจำเป็น มีการเสนอวิธีการประเมินความเสี่ยงหลายวิธีสำหรับระบบควบคุมอุตสาหกรรม หรือ Industrial Control Systems (ICS) และอุตสาหกรรม 4.0 อย่างไรก็ตาม เป็นการยากที่จะระบุผลกระทบต่องานทางกายภาพที่เกิดจากการโจมตีทางไซเบอร์ต่อ ICS เนื่องจากหลายวิธีเหล่านี้ขึ้นอยู่กับการวิเคราะห์บนโต๊ะหรือการจำลองซอฟต์แวร์ ดังนั้นเราจึงมุ่งเน้นไปที่การประเมินความเสี่ยงโดยใช้เครื่องจักรจริงในการทดสอบซึ่งสามารถช่วยแก้ไขปัญหาล่วงหน้าได้ ในอุตสาหกรรม 4.0 ระบบไซเบอร์ทางกายภาพจำเป็นต้องมีการตัดสินใจและการดำเนินการอัตโนมัติ โดยขึ้นอยู่กับทางเลือกเปลี่ยนข้อมูลโดยใช้ปัญญาประดิษฐ์ (AI) และเทคโนโลยีคลาวด์ ในการวิจัยนี้ เราประเมินความเสี่ยงทางไซเบอร์ผ่านการโจมตี ICS ด้วย AI และระบบคลาวด์โดยใช้การทดสอบหรือการจำลองการโจมตีทางระบบไซเบอร์ (ICS Testbed) วิธีการที่นำเสนอสามารถชี้แจงความเสี่ยงทางไซเบอร์และผลกระทบต่อโลกแห่งความเป็นจริงและมาตรการรับมือที่เกี่ยวข้อง

อุตสาหกรรม 4.0 สร้างขึ้นบนระบบอัจฉริยะที่เชื่อมต่อกัน อุตสาหกรรม 4.0 ถูกกำหนดโดยการหลอมรวมความชาญฉลาด การเชื่อมต่อ และระบบอัตโนมัติเข้าสู่โลกทางกายภาพ การดำเนินงานที่ชาญฉลาด เชื่อมต่อกัน และคล่องตัวกำลังเปิดศักราชใหม่ของอุตสาหกรรมดิจิทัล นอกเหนือจากเทคโนโลยีแล้ว ยังหมายถึงระบบนิเวศแบบควบคุมทุกขั้นตอนที่มีเชื่อมต่อกัน กลยุทธ์ทางธุรกิจที่เป็นนวัตกรรมใหม่ พนักงานที่มีอำนาจในการบริหารแบบคล่องตัวเพื่อเพิ่มประสิทธิภาพ เช่นเดียวกับการเปลี่ยนแปลงทางอุตสาหกรรมครั้งก่อน ๆ อุตสาหกรรม 4.0 มีศักยภาพที่จะสร้างมูลค่ามหาศาลให้กับเกือบทุกองค์กร อุตสาหกรรม 4.0 โดดเด่นด้วยการบูรณาการเทคโนโลยีขั้นสูง เช่น IoT การวิเคราะห์ข้อมูลขนาดใหญ่ ปัญญาประดิษฐ์ (AI) หุ่นยนต์ และระบบทางกายภาพทางไซเบอร์ มอບโอกาสมากมายสำหรับบริษัทต่าง ๆ ในการเพิ่มผลกำไร โดยเทคโนโลยีอุตสาหกรรม 4.0 ขับเคลื่อนความสามารถในการทำกำไรโดยการเพิ่มประสิทธิภาพการดำเนินงาน ปรับปรุงคุณภาพผลิตภัณฑ์ เพิ่มความยืดหยุ่น เพิ่มประสิทธิภาพการจัดการห่วงโซ่อุปทาน ปรับปรุงประสบการณ์ของลูกค้า และสร้างแหล่งรายได้ใหม่ บริษัทที่ใช้เทคโนโลยีเหล่านี้อย่างมีประสิทธิภาพสามารถบรรลุความได้เปรียบทางการแข่งขันที่สำคัญและการเติบโตที่ยั่งยืน

1.2.5 เทคโนโลยีอุตสาหกรรม 4.0 กำลังเปลี่ยนแปลงการผลิตอย่างไร

อุตสาหกรรม 4.0 กำลังปฏิวัติวิธีที่บริษัทต่าง ๆ ผลิต ปรับปรุง และจัดจำหน่ายผลิตภัณฑ์ของตน ผู้ผลิตกำลังบูรณาการเทคโนโลยีใหม่ ๆ รวมถึง IoT การประมวลผลบนคลาวด์และการวิเคราะห์ ตลอดจน AI และการเรียนรู้ของเครื่องเข้ากับโรงงานผลิตและตลอดการดำเนินงาน โรงงานอัจฉริยะเหล่านี้ติดตั้งเซ็นเซอร์ขั้นสูง ซอฟต์แวร์ฝังตัว และหุ่นยนต์ที่รวบรวมและวิเคราะห์ข้อมูล และช่วยให้ตัดสินใจได้ดีขึ้น มูลค่าที่สูงขึ้นจะถูกสร้างขึ้นเมื่อข้อมูลจากการดำเนินการผลิตรวมกับข้อมูลการดำเนินงานจาก ERP ห่วงโซ่อุปทาน การบริการลูกค้า และระบบองค์กรอื่น ๆ เพื่อสร้างการมองเห็นและข้อมูลเชิงลึกในระดับใหม่ทั้งหมดจากข้อมูลที่จัดเก็บไว้ก่อนหน้านี้ เทคโนโลยีดิจิทัลนี้นำไปสู่การเพิ่มระบบอัตโนมัติ การบำรุงรักษาเชิงคาดการณ์ การเพิ่มประสิทธิภาพตนเองของการปรับปรุงกระบวนการ และเหนือสิ่งอื่นใด คือระดับใหม่ของประสิทธิภาพและการตอบสนองต่อลูกค้าที่ไม่เคยเป็นไปได้อีกก่อน

การพัฒนาโรงงานอัจฉริยะเป็นโอกาสอันเหลือเชื่อสำหรับอุตสาหกรรมการผลิตในการเข้าสู่การปฏิวัติอุตสาหกรรมครั้งที่สี่ การวิเคราะห์ข้อมูลขนาดใหญ่จำนวนมากที่รวบรวมจากเซ็นเซอร์ในโรงงานช่วยให้มั่นใจในการมองเห็นสินทรัพย์การผลิตแบบเรียลไทม์ และสามารถจัดหาเครื่องมือสำหรับดำเนินการบำรุงรักษาเชิงคาดการณ์เพื่อลดเวลาหยุดทำงานของอุปกรณ์ให้เหลือน้อยที่สุด การใช้อุปกรณ์ IoT ที่มีเทคโนโลยีสูงในโรงงานอัจฉริยะนำไปสู่ประสิทธิภาพการผลิตที่สูงขึ้นและคุณภาพที่ดีขึ้น การแทนที่โมเดลธุรกิจการตรวจสอบด้วยตนเองด้วยข้อมูลเชิงลึกด้วยภาพที่ขับเคลื่อนด้วย AI ช่วยลดข้อผิดพลาดในการผลิต และประหยัดเงินและเวลา ด้วยการลงทุนเพียงเล็กน้อย เจ้าหน้าที่ควบคุมคุณภาพสามารถตั้งค่าสมาร์ตโฟนที่เชื่อมต่อกับระบบคลาวด์เพื่อตรวจสอบกระบวนการผลิตได้จากทุกที่ ด้วยการใช้อัลกอริธึมการเรียนรู้ของเครื่องจักร ผู้ผลิตสามารถตรวจจับข้อผิดพลาดได้ทันที แทนที่จะตรวจพบในภายหลังเมื่องานซ่อมแซมมีราคาแพงกว่า แนวคิดและเทคโนโลยีอุตสาหกรรม 4.0 สามารถนำไปใช้กับบริษัทอุตสาหกรรมทุกประเภท รวมถึงการผลิตแบบแยกส่วนและแบบกระบวนการ เช่นเดียวกับน้ำมันและก๊าซ เหมืองแร่ และกลุ่มอุตสาหกรรมอื่น ๆ

ในการปฏิวัติอุตสาหกรรมครั้งที่สี่ หรือที่เรียกกันทั่วไปว่าอุตสาหกรรม 4.0 ระบบไซเบอร์-กายภาพ (CPS) ผสมผสานส่วนประกอบทางกายภาพและเครือข่ายดิจิทัล เพื่อเปลี่ยนวิธีที่บริษัทผู้ผลิตทำให้กระบวนการและการแบ่งปันข้อมูลเป็นแบบอัตโนมัติ อุตสาหกรรม 4.0 ได้รับการสนับสนุนจากอินเทอร์เน็ตของสรรพสิ่งทางอุตสาหกรรม (IIoT) การเรียนรู้ของเครื่องจักร

และข้อมูลขนาดใหญ่ ส่งเสริมการปรับปรุงที่สำคัญในการแลกเปลี่ยนข้อมูลและการควบคุมทางอุตสาหกรรมในอุตสาหกรรม การผลิต ดังที่รวมอยู่ในสิ่งที่เรียกว่า "โรงงานอัจฉริยะ" อย่างไรก็ตาม ขณะนี้เทคโนโลยีสารสนเทศ (IT) เทคโนโลยีการดำเนินงาน (OT) และทรัพย์สินทางปัญญา (IP) กำลังถูกรวมเข้าด้วยกัน ปัญหาด้านความปลอดภัยรูปแบบใหม่ทั้งหมดก็เกิดขึ้นเช่นกัน นอกจากนี้ ยังเป็นที่น่าสังเกตว่าเนื่องจากระบบควบคุมทางอุตสาหกรรม (ICS) จำนวนมาก เช่น ตัวควบคุมลอจิกที่ตั้งโปรแกรมได้ (PLC) พร้อมด้วยอินเทอร์เฟซระหว่างมนุษย์กับเครื่องจักร (HMI) ที่ใช้ร่วมกับระบบดังกล่าว ได้รับการออกแบบมาสำหรับสภาพแวดล้อมที่แยกออกจากกัน มาตรการรักษาความปลอดภัยทางไซเบอร์ที่เพียงพอจึงอาจไม่รวมอยู่ในนั้น สถานที่สำหรับพวกเขา สิ่งนี้ทำให้มีโอกาสที่ ICS จะถูกเปิดเผยบนอินเทอร์เน็ตอันเป็นผลมาจากการเชื่อมต่อที่เพิ่มขึ้นระหว่างเครือข่าย IT และ OT

1.2.6 การรักษาความปลอดภัยทางไซเบอร์เป็นปัจจัยสำคัญในการนำไปใช้

มีหลายสิ่งที่จะได้รับการนำเทคโนโลยีอุตสาหกรรม 4.0 มาใช้แล้วเหตุใดการนำไปใช้จึงไม่ก้าวทันความคาดหวังคำตอบนั้น ความยุ่งยากในการติดตั้งระบบ รวมทั้งผู้เชี่ยวชาญที่จะดูแลในระบบความปลอดภัยยังมีไม่เพียงพอ ขณะที่อุตสาหกรรม 4.0 ยังคงให้พื้นฐานอุตสาหกรรมการผลิตมาใช้ อุตสาหกรรมการผลิตก็กลายเป็นเป้าหมายที่น่าดึงดูดมากขึ้นสำหรับผู้โจมตี ซึ่งมีโอกาสเคลื่อนข้ามเครือข่ายการผลิตในแนวขวาง และกระโดดข้ามระบบ IT และ OT เพื่อหากิจกรรมที่เป็นอันตราย หากไม่มีการป้องกันที่เข้มงวด ผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์จากระบบสำหรับการจารกรรมทางอุตสาหกรรม การโจรกรรมทรัพย์สินทางปัญญา การรั่วไหลของ IP หรือแม้แต่ว่าการก่อวินาศกรรมในการผลิต

ความสัมพันธ์กับคำสั่งของประธานาธิบดีแห่งสหรัฐอเมริกา 13636 “ปรับปรุงโครงสร้างพื้นฐานที่สำคัญด้านความปลอดภัยทางไซเบอร์”

ด้วยความตระหนักว่า ความมั่นคงของชาติและเศรษฐกิจของสหรัฐอเมริกาขึ้นอยู่กับการทำงานที่เชื่อถือได้ของโครงสร้างพื้นฐานที่สำคัญ ประธานาธิบดีภายใต้คำสั่งประธานาธิบดี “ปรับปรุงโครงสร้างพื้นฐานที่สำคัญด้านความปลอดภัยทางไซเบอร์” [82] กำกับ NIST ให้ทำงานร่วมกับผู้มีส่วนได้ส่วนเสียเพื่อพัฒนากรอบความสนใจในการลดความเสี่ยงทางไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญ

กรอบการทำงานด้านความปลอดภัยทางไซเบอร์ Cybersecurity Framework (CSF) [83] [84] ประกอบด้วยมาตรฐานแนวทางปฏิบัติ และการปฏิบัติที่ดีที่สุดเพื่อส่งเสริมการคุ้มครองโครงสร้างพื้นฐานที่สำคัญ การจัดลำดับความสำคัญ ความยืดหยุ่น การทวนซ้ำได้ การอิงตามประสิทธิภาพ และความคุ้มค่าของกรอบการทำงานจะช่วยให้เจ้าของและผู้ปฏิบัติงานโครงสร้างพื้นฐานสำคัญสามารถจัดการความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ได้ ในขณะเดียวกันก็ป้องกันความล้มเหลวธุรกิจ การรักษาความเป็นส่วนตัวของบุคคล และเสรีภาพของพลเมืองด้วย ซึ่ง CSF ฉบับแรกเริ่มได้ตีพิมพ์เผยแพร่ในเดือนกุมภาพันธ์ 2557 ส่งผลให้มีกรอบการทำงานระดับชาติที่มีความยืดหยุ่นเพียงพอที่จะนำไปใช้ในหลายภาคส่วนและในสภาพแวดล้อมการปฏิบัติงานที่แตกต่างกัน โดย CSF ได้รับการพัฒนาตามข้อมูลของผู้มีส่วนได้ส่วนเสีย เพื่อช่วยให้แน่ใจได้ว่างานที่มีอยู่ในภาคส่วนต่าง ๆ นั้นสามารถนำไปใช้ภายในกรอบการทำงานได้ โดยมาตรฐาน แนวทางปฏิบัติ และการปฏิบัติด้านความปลอดภัยทางไซเบอร์ของระบบควบคุมทางอุตสาหกรรมนั้นสามารถนำไปใช้เพื่อจัดการกับหน้าที่ของ CSF ในบริบทของโปรแกรมการจัดการความเสี่ยงขององค์กรได้

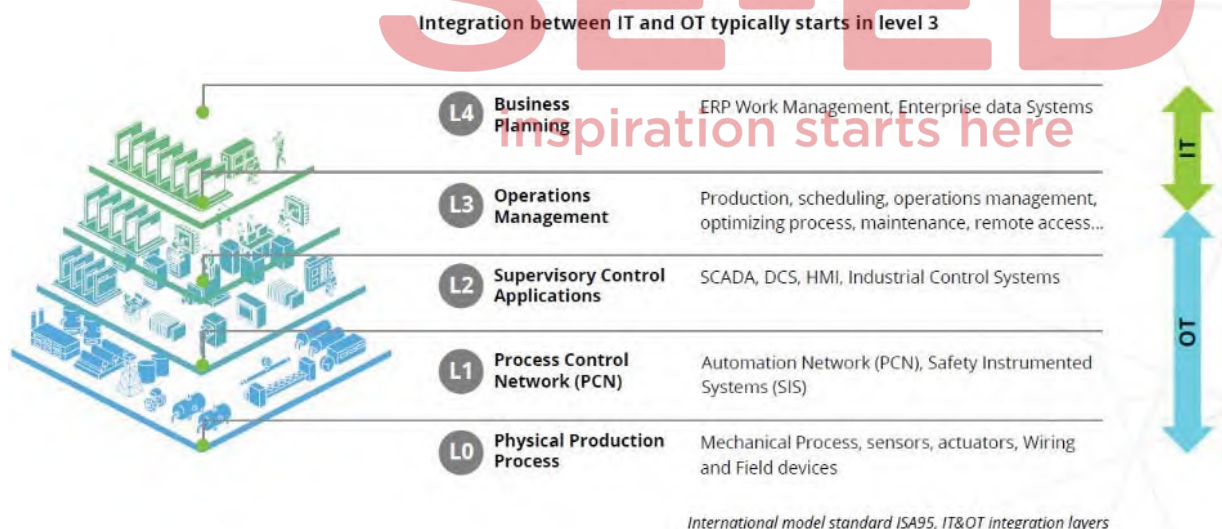
1.3 ผู้อ่านและผู้ปฏิบัติ

หนังสือกรณีศึกษาที่ครอบคลุมรายละเอียดเฉพาะของ ICS ผู้อ่าน ควรทำความเข้าใจกับแนวคิดด้านความปลอดภัยของคอมพิวเตอร์ทั่วไป และการสื่อสารโปรโตคอลต่าง ๆ เช่น ที่ใช้ในเครือข่าย เอกสารนี้มีลักษณะเป็นข้อมูลทางเทคนิค แต่อย่างไรก็ตาม ก็มีพื้นฐานที่จำเป็นในการทำความเข้าใจหัวข้อที่เกี่ยวข้องจะต้องอ่านเพิ่มเติมอีกด้วย

กลุ่มเป้าหมายผู้อ่านนั้นมีหลากหลายและยังรวมถึงบุคคลดังต่อไปนี้ด้วย:

- วิศวกรควบคุม ผู้วางระบบ และสถาปนิกที่ออกแบบหรือใช้งานการรักษาความปลอดภัย ICS
- ผู้ดูแลระบบ วิศวกร และผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ (IT) อื่น ๆ ที่ดูแล ปรับแต่ง หรือรักษาความปลอดภัย ICS
- ที่ปรึกษาด้านความปลอดภัยที่ดำเนินการประเมินความปลอดภัยและทดสอบการเจาะระบบของ ICS
- ผู้จัดการที่รับผิดชอบ ICS
- ผู้บริหารระดับสูงที่พยายามทำความเข้าใจผลกระทบและผลลัพธ์ที่ตามมาในกรณีที่ให้เหตุผลและใช้โปรแกรมการรักษาความปลอดภัยทางไซเบอร์ของ ICS เพื่อช่วยบรรเทาผลกระทบต่อการดำเนินงานของธุรกิจ
- นักวิจัยและนักวิเคราะห์ที่พยายามทำความเข้าใจความต้องการด้านความปลอดภัยเฉพาะของ ICS
- ผู้จำหน่ายที่กำลังพัฒนาผลิตภัณฑ์ที่จะนำไปใช้เป็นส่วนหนึ่งของ ICS

ระดับชั้นทางกายภาพของระบบควบคุมอุตสาหกรรมในองค์กรต่าง ๆ ได้รับการอธิบายอย่างเหมาะสมตามมาตรฐาน ISA-95 และแบบจำลอง Purdue ISA-95 [159] โดยมีห้าระดับตั้งแต่ ระดับ 0 ถึง ระดับ 4 ดังแสดงในรูปที่ 1-1 โดยที่ระดับต่าง ๆ ของควบคุมอุตสาหกรรมจะแสดงให้เห็นตามอัตราตามมาตรฐาน ISA-95 ด้านล่างนี้ บ่งชี้ถึงการแยกระดับของระบบ IT และ OT ออกจากกัน โดยจะมีการเชื่อมภายในชั้นการจัดการการดำเนินงาน (ระดับ 3) การแบ่งแยกทางทฤษฎีนี้มีความแตกต่างกันอย่างมากในแต่ละองค์กรและประเภทของอุตสาหกรรม และอาจเปลี่ยนแปลงได้ตลอดเวลาและเมื่อมีการบรรจบกัน [93]



รูปที่ 1-1 แบบจำลองทางทฤษฎีของการบูรณาการ IT และ OT [94]

เส้นเวลาในอดีตนั้นยาวนานเกือบ 2 ทศวรรษ และการปรับตำแหน่งของเทคโนโลยี IT และ OT ได้เริ่มที่จะมาบรรจบกันเป็นแพลตฟอร์มเทคโนโลยีทั่วไป การจัดวางเทคโนโลยี IT อย่างต่อเนื่องใน ICS ได้นำไปสู่การปรับองค์กรและระบบควบคุมอุตสาหกรรมที่เชื่อมต่อกันอย่างสมบูรณ์ การบูรณาการในแนวตั้งและแนวนอนของห่วงโซ่คุณค่าทั้งหมด [93] ดังแสดงในรูปที่ 1-2 โดยในบทที่ 2 จะเน้นไปยังการแสดงผลภาพรวมของระบบควบคุมทางอุตสาหกรรม Industrial Control Systems (ICS) ลงไปในแต่ละระบบโดยละเอียด



รูปที่ 1-2 การบรรจบกันอย่างค่อยเป็นค่อยไปเมื่อเวลาผ่านไปด้วยการใช้เทคโนโลยีสารสนเทศในระบบอุตสาหกรรม [94]

1.4 โครงสร้างของหนังสือคู่มือความปลอดภัยและกรณีศึกษาของระบบควบคุมอุตสาหกรรม

ส่วนที่เหลือของหนังสือเล่มนี้แบ่งออกเป็นส่วนหลักดังต่อไปนี้:

- ส่วนที่ 2 แสดงภาพรวมของ ICS รวมถึงการเปรียบเทียบระหว่าง ICS กับระบบ IT
- ส่วนที่ 3 เป็นการอภิปรายเกี่ยวกับการจัดการและการประเมินความเสี่ยงของ ICS
- ส่วนที่ 4 แสดงภาพรวมของการพัฒนาและการใช้งานโปรแกรมการรักษาความปลอดภัยระบบควบคุมทางอุตสาหกรรม (ICS) เพื่อลดความเสี่ยงของช่องโหว่ระบบ
- ส่วนที่ 5 แสดงคำแนะนำสำหรับการบูรณาการการรักษาความปลอดภัยเข้ากับสถาปัตยกรรมเครือข่ายที่มักพบใน ICS โดยเน้นที่แนวทางปฏิบัติในการแบ่งแยกเครือข่าย
- ส่วนที่ 6 แสดงข้อมูลสรุปของการควบคุมการจัดการ การปฏิบัติงาน และทางเทคนิคที่ระบุใน NIST บทความฉบับพิเศษ 800-53 การควบคุมความปลอดภัยและการรักษาความเป็นส่วนตัวสำหรับระบบข้อมูลของรัฐบาลกลางและองค์กร และให้คำแนะนำเบื้องต้นเกี่ยวกับวิธีการที่การควบคุมความปลอดภัยนี้นำไปใช้กับ ICS
- ส่วนที่ 7 แสดงภาพรวมของเพอร์ดูโมเดลและกรณีศึกษาของการถูกโจมตีทั้ง 11 กรณีศึกษาที่แตกต่างกันในแต่ละระดับของเพอร์ดูโมเดล และข้อแนะนำรวมทั้งแนวทางในการป้องกันจากการถูกโจมตี



รองศาสตราจารย์ ดร. มนตรี วิบูลย์รัตน์



การศึกษา

- ปริญญาตรีวิทยาศาสตร์ สาขาวิทยาการคอมพิวเตอร์และคณิตศาสตร์ประยุกต์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- ปริญญาโทด้านการบริหาร (MBA) มหาวิทยาลัยอัสสัมชัญ
- ปริญญาเอกด้านการบริหารจัดการด้านคอมพิวเตอร์และการบริหารวิศวกรรม มหาวิทยาลัยอัสสัมชัญ เกียรตินิยมเหรียญทองอันดับหนึ่ง

ประวัติย่อ

ประสบการณ์การทำงานกว่า 14 ปี ในบริษัทชั้นนำของโลก เช่น Chevron, Hewlett-Packard (HP), Celestica (Thailand), L'Oreal(Thailand), Lantro (Thailand) และประสบการณ์ในการสอน 14 ปี ใน มหาวิทยาลัยขอนแก่น, มหาวิทยาลัยธรรมศาสตร์ และ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ตำแหน่งกรรมการ และที่ปรึกษา

1. นายกสมาคมการค้าพลังงานขยะ: Waste to Energy Trade Association (WETA)
2. ประธานคณะกรรมการมาตรฐานดาตาเซ็นเตอร์ วิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (วสท.)
3. ประธานคณะกรรมการร่างมาตรฐานเมืองอัจฉริยะ (Smart City) วิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (วสท.)
4. รองประธาน คณะกรรมการวิชาการด้านมาตรฐานสถาบันประเมินและรับรองเทคโนโลยีดิจิทัล ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค)
5. รองผู้อำนวยการ สำนักวิจัยนวัตกรรมเมืองอัจฉริยะ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (สจล.)
6. อุปนายกสมาคมนักวิจัยชายแดนใต้
7. ที่ปรึกษานักบริหารข้อมูลดิจิทัลพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
8. ประธานคณะกรรมการประจำมาตรฐาน Data Center Mobile and Modular (DCMM) วิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (วสท.)
9. ที่ปรึกษาคณะกรรมการจัดทำมาตรฐาน Data Center Operations and Maintenance วิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (วสท.)
10. คณะกรรมการประจำมาตรฐาน Data Center Infrastructure Management (DCIM) วิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (วสท.)
11. คณะกรรมการ IEEE Power & Energy Society (PES) Thailand Section

ผู้ช่วยศาสตราจารย์ ดร.อรรถพล ป้อมสฤติย์



การศึกษา

- 2556 วิศวกรรมศาสตรดุษฎีบัณฑิต (วศ.ด.) สาขาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- 2548 วิศวกรรมศาสตรมหาบัณฑิต (วศ.ม.) สาขาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- 2544 วิศวกรรมศาสตรบัณฑิต (วศ.บ.) สาขาวิศวกรรมอิเล็กทรอนิกส์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- 2556 ตำแหน่ง ผู้ช่วยศาสตราจารย์ สาขา วิศวกรรมคอมพิวเตอร์

ผลงานทางวิชาการ

1. หนังสือ Computer and Information Security Theory ,ผู้เขียนอรรถพล ป้อมสฤติย์ , ISBN: 978-616-90849- 6-9, สำนักพิมพ์มหาวิทยาลัยราชภัฏสวนสุนันทา 2561
2. หนังสือ IT Security Concept ,ผู้เขียนอรรถพล ป้อมสฤติย์, ISBN:978-616-90849-1-4, สำนักพิมพ์เวลส์โนวัน เมษายน 2554
3. เอกสารคำสอน รายวิชาระบบฐานข้อมูล ISBN 978-974-421-870-4,ผู้เขียนอรรถพล ป้อมสฤติย์, ปี 2560
4. เอกสารประกอบการสอน รายวิชาการพัฒนาโปรแกรมเชิงพลวัต, ผู้เขียนอรรถพล ป้อมสฤติย์,ปี 2554

ประสบการณ์ทำงาน

ปัจจุบัน

- อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- หัวหน้าสาขาการจัดการความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยี
- อาจารย์ประจำ วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต
- ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพระนคร
- ผู้ช่วยผู้อำนวยการ วิทยาลัยนานาชาติพระนคร มหาวิทยาลัยราชภัฏพระนคร
- อาจารย์ประจำสาขาการสื่อสารผ่านสื่อใหม่ มหาวิทยาลัยราชภัฏพระนคร
- อาจารย์ประจำสาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ISBN 978-616-33-8201-6



9 786163 382016
180 บาท