5 ขั้นตอน เพื่อเพิ่มความปลอดภัยในกระบวนการทางอุตสาหกรรมผ่านทาง IIoT และการแปลงเป็นรูปแบบดิจิทัล

โดย สตีฟ เจ. เอลเลียต
ผู้อำนวยการฝ่ายการตลาดอาวุโสของ ชไนเดอร์ อิเล็คทริค

สรุปสาระสังเขป

เทคโนโลยีและแนวความคิดของ Industrial Internet of Things (IIoT) สามารถเปลี่ยนแปลงและเพิ่มความปลอดภัยในกระบวนการได้หากนำมาประยุกต์ใช้อย่างเหมาะสม ในอดีตนั้น ความสำเร็จหรือความล้มเหลวของความปลอดภัยในอุตสาหกรรมต่างต้องอาศัยโมเดลที่มีความโน้มเอียงโดยอิงจากข้อมูลในอดีต IIoT เปิดประตูสู่มุมมองการคาดการณ์ล่วงหน้าเกี่ยวกับความปลอดภัยที่คาดการณ์ได้อย่างแม่นยำเมื่อปัจจัยเสี่ยงด้านความปลอดภัยเกินเกณฑ์ที่จะยอมรับได้ บทความนี้เป็นแนวทางสำหรับการใช้ประโยชน์จากเครื่องมือและเทคนิค IIoT เพื่อสร้างความปลอดภัยทางอุตสาหกรรมในลักษณะที่ทำกำไรได้

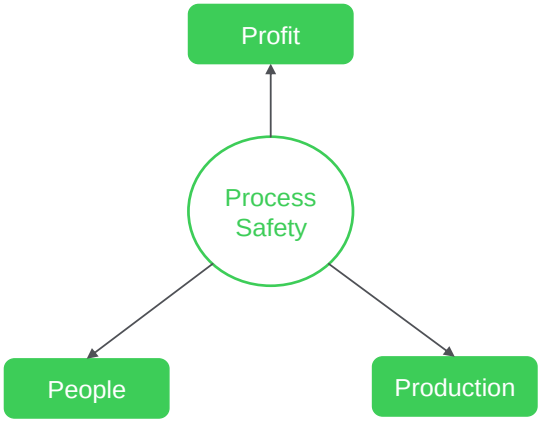
บทนำ

ความต้องการของตลาดใหม่โดยเฉพาะอย่างยิ่งช่วงการผลิตสั้นๆ กำลังกระตุ้นการแผ่ขยายของอุตสาหกรรมอินเทอร์เน็ตในทุกสิ่ง (IIoT) ที่เกี่ยวข้องกับเทคโนโลยีในอุตสาหกรรมต่างๆ การหลั่งไหลของเทคโนโลยีนี้ได้เปลี่ยนแปลงกระบวนการดำเนินงานของภาคอุตสาหกรรมซึ่งอาจจำเป็นต้องมีการปรับเปลี่ยนวิธีการจัดการความปลอดภัยโดยเฉพาะอย่างยิ่งในอุตสาหกรรมที่มีความเสี่ยงสูง ในสภาพแวดล้อมที่เคลื่อนที่เร็วเช่นนี้จำเป็นต้องมีระเบียบวินัยสูงและการผสมผสานระหว่างเทคโนโลยีที่เหมาะสมเพื่อรักษามาตรฐานความปลอดภัยที่สูง

เทคโนโลยี IIoT ทำให้สามารถรวบรวมข้อมูลและวิเคราะห์ข้อมูลได้อย่างรวดเร็วส่งผลให้เกิดการตัดสินใจที่รวดเร็วและแม่นยำสูง ความสามารถดังกล่าวเหมาะสมอย่างยิ่งสำหรับการเพิ่มความปลอดภัยในกระบวนการผลิตในแต่ละอุตสาหกรรม เมื่อผลิตภัณฑ์ถูกเก็บ "ในท่อ" แทนที่จะเก็บบนพื้นหรือในอากาศ การจัดการความเสี่ยงก็จะประสบความสำเร็จ IIoT ช่วยลดความเสี่ยงโดยการปรับปรุงประสิทธิภาพด้านความปลอดภัยของกระบวนการโดยหลีกเลี่ยงความผิดพลาดที่อาจเกิดขึ้นได้และการหยุดทำงานโดยไม่คาดคิด

อัลกอริทึมที่ขับเคลื่อนด้วย IIoT และการวิเคราะห์เชิงคาดการณ์สามารถกำหนดค่าเพื่อระบุภัยคุกคามที่ปรากฏขึ้นต่อความปลอดภัยของอุปกรณ์ได้ ขั้นตอนการปรับใช้การวิเคราะห์เชิงคาดการณ์ ได้แก่ การรวบรวมข้อมูลสินทรัพย์ของอุปกรณ์และการสร้างแบบจำลองทางคณิตศาสตร์ที่สะท้อนถึงโหมดการทำงานที่แตกต่างกันของอุปกรณ์ดังกล่าว จากนั้นจะรวมกับเซ็นเซอร์ที่รวบรวมข้อมูลแบบสดเพื่อสร้างโปรไฟล์บนอุปกรณ์ชิ้นหนึ่ง

เมื่อมีการกำหนดโปรไฟล์หรือซิกเนเจอร์ของอุปกรณ์ดังกล่าวแล้ว ก็จะสามารถกำหนดแนวทางสำหรับอุปกรณ์ชิ้นนี้ได้ ข้อมูลดังกล่าวถูกวางไว้แบบออนไลน์และพื้นที่เก็บข้อมูลมีการสร้างขึ้นเพื่อเปรียบเทียบประสิทธิภาพจริงกับประสิทธิภาพที่คาดไว้ หากมีความคลาดเคลื่อนเกินกว่าที่คาดไว้ระหว่างประสิทธิภาพที่คาดหวังและประสิทธิภาพจริง ระบบก็จะส่งการแจ้งเตือนไปยังทีมดูแลความปลอดภัยและบำรุงรักษาซึ่งสามารถจัดการกับความเสี่ยงที่เกิดขึ้นได้



รูปภาพที่ 1

การปรับปรุงความปลอดภัยของกระบวนการต้องมีความสมดุลที่ละเอียดอ่อนระหว่างผลกำไร การผลิต และการลดข้อผิดพลาดของมนุษย์

หน่วยแจ้งเตือนจะแจ้งให้ทีมงานทราบว่าน่าจะมีปัญหาเกิดขึ้นในอนาคตอันใกล้นี้และการดำเนินการดังกล่าวควรได้รับการวางแผนเพื่อหลีกเลี่ยงการหยุดการทำงานในอนาคตที่คาดไม่ถึงและปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นได้ การพิจารณาถังเก็บซึ่งมีการควบคุมความดันภายในอยู่เป็นการเริ่มแสดงสัญญาณของความล้มเหลวและความเสี่ยงต่อการระเบิดที่เพิ่มขึ้น เมื่อพิจารณาถึงลำดับความล้มเหลวในช่วงต้นของปัญหาที่อาจเกิดขึ้น อุปกรณ์ชิ้นนี้สามารถใช้งานแบบออฟไลน์ได้ในสถานการณ์ที่ไม่ฉุกเฉินโดยเสียค่าใช้จ่ายน้อยกว่าและสามารถแก้ไขปัญหาได้ก่อนที่สินทรัพย์จะประสบกับความล้มเหลวอย่างรุนแรง

ความปลอดภัยต้องเสียค่าใช้จ่ายเป็นเงิน (เป็นผลจากการลงทุนหลายอย่างที่จำเป็นเพื่อให้มั่นใจในความปลอดภัยระดับสูง) เช่นเดียวกับการซื้อประกัน แต่ความปลอดภัยยังช่วยเพิ่มความสามารถในการทำกำไรให้แก่ขององค์กร (โดยการเพิ่มช่วงเวลาให้บริการของกระบวนการ) และลดความเสี่ยงที่อาจเกิดขึ้นได้ด้วย (โดยการลดโอกาสของความล้มเหลวในด้านความปลอดภัยที่เกี่ยวข้องกับค่าใช้จ่ายทางกฎหมายและค่าใช้จ่ายด้านภาพลักษณ์ของบริษัท) บทความนี้อธิบายขั้นตอนห้าขั้นสำหรับการบูรณาการเทคโนโลยี IIoT ใหม่เพื่อจัดการกับความเสี่ยงและอันตรายให้ดียิ่งขึ้นเพื่อหลีกเลี่ยงการหยุดทำงานของสินทรัพย์แบบที่ไม่ได้คาดคิดซึ่งต้องเสียค่าใช้จ่ายอีก

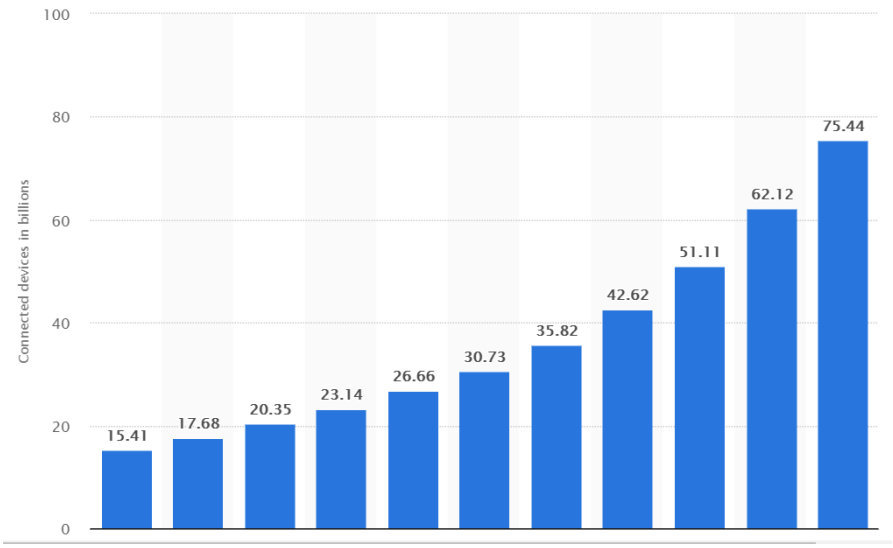
ภูมิหลังและบริบทของ IIoT

จำนวนของ "สิ่งต่างๆ" หรืออุปกรณ์อัจฉริยะที่เชื่อมต่อกับอินเทอร์เน็ตนั้นคาดว่าจะเติบโตขึ้นเป็นเกือบ 31 พันล้านทั่วโลกภายในปี 2563 (ดูรูปภาพที่ 2) เนื่องจากค่าใช้จ่ายในการเปิดใช้งาน IP อยู่ในระดับต่ำ อุปกรณ์ทุกประเภทจึงมีอิสระที่จะเข้าร่วมเครือข่าย IP แบบเปิดกว้างได้มากขึ้น การเปลี่ยนพฤติกรรมของมนุษย์ (เช่น การใช้โทรศัพท์มือถือ / สมาร์ทโฟนอย่างกว้างขวาง) และแรงงานที่กำลังเปลี่ยนแผลงไป (จากผู้เกษียณอายุยุค baby boomers ไปเป็นผู้ที่มีความรู้ความเข้าใจในสังคมออนไลน์มากขึ้นและมีความ "เชื่อมต่อกัน") อีกทั้งยังช่วยผลักดันการใช้เทคโนโลยี IIoT เพิ่มขึ้นด้วยความปรารถนาในการที่จะวัดและเปรียบเทียบประสิทธิผลของวัตถุที่มนุษย์มีปฏิสัมพันธ์กันนำไปสู่การเร่งความเร็วในการสร้างข้อมูลและการเปิดเผยข้อมูลนั้นมากขึ้น ตัวอย่างเช่น ผู้จัดการโรงงานสามารถเข้าถึงข้อมูลเกี่ยวกับโรงงานของเขาได้มากถึง 10 เท่าเมื่อเทียบกับที่เขาเคยทำได้เมื่อ 20 ปีก่อน

สำหรับผู้มีส่วนได้เสียด้านความปลอดภัยในภาคอุตสาหกรรมที่หวังจะตักตวงผลประโยชน์จากโอกาสที่มีข้อมูลท่วมท้นอยู่นี้ ความสำเร็จจะขึ้นอยู่กับความสามารถในการผสานรวมเครื่องมือซอฟต์แวร์ที่เหมาะสมซึ่งจะนำไปสู่ประโยชน์ของชุดข้อมูลขนาดใหญ่

ความปลอดภัยขั้นสูงหมายถึงการใช้ข้อมูลขนาดใหญ่จากสินทรัพย์ชั้นการผลิต จากทีมซ่อมบำรุงที่ใช้งานระบบดิจิทัลเพื่อเพิ่มเทคนิคการบำรุงรักษาเชิงคาดการณ์และจากทีม

วิเคราะห์ที่ใช้ข้อมูลกระบวนการที่มีรายละเอียดมากขึ้นเพื่อเพิ่มประสิทธิภาพและเพิ่มความเร็วในการตัดสินใจ



รูปภาพที่ 2

การเติบโตที่คาดการณ์ไว้ของอุปกรณ์ *Internet of Things (IoT)* ***ในหน่วยพันล้าน*** *(courtesy of Statista)*

ในความเป็นจริงนั้น จากมุมมองของวิศวกรด้านความปลอดภัย การปรับปรุงความน่าเชื่อถือของกระบวนการขับเคลื่อนด้วยระบบดิจิทัลจะช่วยปรับปรุงความปลอดภัยในขณะที่สินทรัพย์เกิดความล้มเหลวน้อยลง ซึ่งหมายความว่าการมีส่วนร่วมของมนุษย์จะน้อยลงและลดความเสี่ยงต่อความผิดพลาดของมนุษย์ด้วย เนื่องจากผู้ให้บริการอาจได้รับสิทธิ์ให้เข้าถึงข้อมูลการดำเนินงานแบบเรียลไทม์พร้อมกับการควบคุมกระบวนการและข้อมูลความเสี่ยงที่น่าเชื่อถือแบบเรียลไทม์ การตัดสินใจของพวกเขาจึงสามารถสร้างความปลอดภัยและผลกำไรได้โดยตรง ผู้ประกอบการจะสามารถปรับจุดกำหนดและเห็นผลกระทบที่การปรับตัวของพวกเขามีต่อความปลอดภัยในกระบวนการความสามารถในการทำกำไรและความน่าเชื่อถือของสินทรัพย์

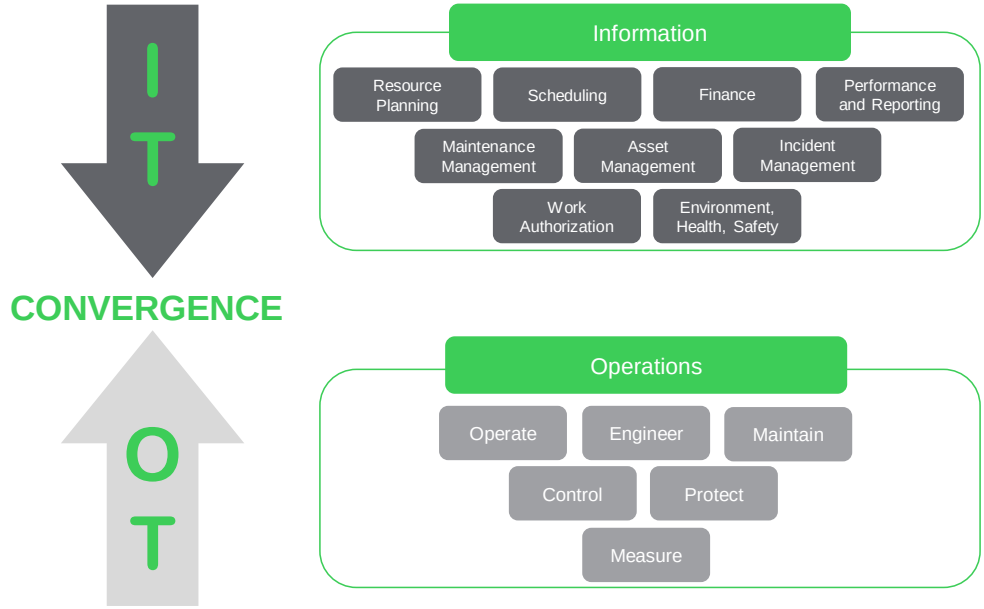
เหตุการณ์ความปลอดภัยในภาคอุตสาหกรรมส่วนใหญ่มักเกิดจากเหตุการณ์เดี่ยวบ่อยครั้งที่มันเป็นผลรวมของเหตุการณ์เล็กๆ ที่ดูไม่เหมือนกันซึ่ง เมื่อรวมกันได้ส่งผลให้เกิดเหตุการณ์หนึ่งขึ้น เครื่องมือการวิเคราะห์ใหม่จะช่วยให้สามารถกำหนดแนวโน้มพฤติกรรมทางด้านสินทรัพย์ได้อย่างแม่นยำมากขึ้น ในยุคใหม่ของการแปลงข้อมูลดิจิทัลขั้นสูงนี้ วิศวกรด้านความปลอดภัยจะต้องมีเครื่องมือวิเคราะห์ดังกล่าวเพื่อทำความเข้าใจเกี่ยวกับความสัมพันธ์และการพึ่งพาระหว่างจุดข้อมูล รูปแบบข้อมูลประสิทธิภาพของสินทรัพย์สามารถเริ่มปรากฏเร็วกว่าที่เป็นไปได้ก่อนหน้านี้ ด้วยวิธีนี้ผู้ประกอบการและผู้เชี่ยวชาญด้านความปลอดภัยสามารถรับรู้สัญญาณเบื้องต้นของอันตรายที่จะเกิดขึ้นก่อนที่สถานการณ์นั้นจะหมุนวนออกจากการควบคุม

การเข้าใจในความแตกต่างระหว่าง IT / OT

แนวโน้มของ IIoT เกิดขึ้นเนื่องจากการรวมกันของทีมเทคโนโลยีสารสนเทศ (IT) และเทคโนโลยีการดำเนินงาน (OT) "โลก" ทั้งสองนี้มีความแตกต่างกันในด้านการประยุกต์ใช้ สถาปัตยกรรมและการปกครอง ผู้เชี่ยวชาญด้านข้อมูลที่ชำนาญในด้าน IT

มักไม่ค่อยชำนาญในด้านความปลอดภัยของกระบวนการเกี่ยวกับ OT และในทางกลับกัน

IT และ OT มีวิวัฒนาการไปในทิศทางและช่วงเวลาที่แตกต่างกันโดยมักใช้ข้อมูลประเภทต่างๆ และโครงสร้างข้อมูลที่แตกต่างกัน ทั้งหมดนี้มีความแตกต่างกันโดยสิ้นเชิงในวัตถุประสงค์และลักษณะเพื่อก่อให้เกิดอุปสรรคที่ทำให้เข้ากันได้ทั้งการรวมสังเคราะห์และแลกเปลี่ยนข้อมูลระหว่างกัน



รูปภาพที่ 3

การหลอมรวมโลก: การเชื่อมต่อขั้นสูงจะผสานรวม IT เข้ากับโครงสร้างพื้นฐานทางกายภาพขององค์กร

IT มีวิวัฒนาการมาจากบนลงล่างโดยมุ่งเน้นไปที่ความต้องการทางธุรกิจเป็นหลัก (เช่น การดำเนินงานขององค์กรและระบบที่จำเป็นต่อการจัดการธุรกิจโดยส่วนใหญ่มาจากมุมมองทางการเงิน) อีกทั้งยังถือว่า IT เป็นนัยยะสำคัญของ "ผู้บริโภค" เนื่องจากระบบ IT มีอยู่ทั้งในคอมพิวเตอร์สำหรับใช้ในบ้านและคอมพิวเตอร์สำหรับใช้ในธุรกิจหลายล้านเครื่อง ระบบไอทีเป็นไปตามมาตรฐานที่ได้รับการยอมรับซึ่งสามารถรองรับการรวมและจัดการข้อมูลจำนวนมากทั่วทั้งองค์กรได้

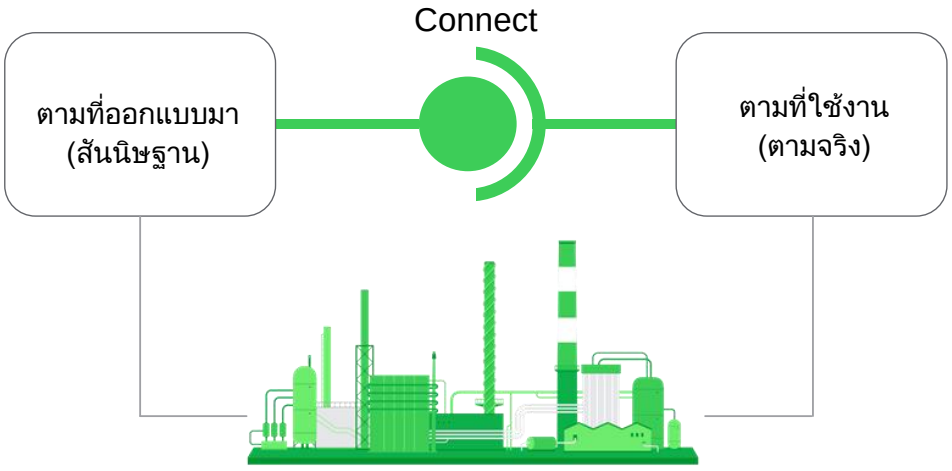
ในทางกลับกัน ระบบ OT ได้เติบโตขึ้นจากด้านล่างสู่ด้านบน โดยมีระบบที่เป็นกรรมสิทธิ์ซึ่งแตกต่างกันไปและมักเป็นระบบซึ่งได้รับการออกแบบโดยผู้ผลิตรายอื่นเพื่อควบคุมกระบวนการและอุปกรณ์ที่เฉพาะเจาะจงในสภาพแวดล้อมแบบเรียลไทม์ เทคโนโลยี OT มักใช้งานในสภาพแวดล้อมที่รุนแรงและโดยทั่วไปมักมีความทนทานต่ำต่อความล้มเหลวและความต้องการที่สำคัญสำหรับการกู้คืนและความซ้ำซ้อน สภาพแวดล้อมของ OT มีรูปแบบการกำกับดูแลที่เน้นในกระบวนการที่มีการปรับให้เข้ากับบริบทอย่างสูง บริษัทต่างๆ เช่น Schneider Electric ได้พัฒนาความเชี่ยวชาญทั้งในโดเมนเหล่านี้และมีตำแหน่งที่ดีเพื่อช่วยให้อุตสาหกรรมได้ใช้เทคโนโลยี IIoT ได้ ซึ่งรวมถึงการสนับสนุนการเพิ่มประสิทธิภาพด้านความปลอดภัยของกระบวนการความ

ปลอดภัยด้วย และท้ายที่สุดคือการได้รับผลกำไรเพิ่มเติมจากมาตรการด้านความปลอดภัยที่ขับเคลื่อนด้วย IIoT

ขั้นตอนที่ 1: ทำให้เป็นดิจิทัลและเชื่อมต่อ

หนึ่งในเป้าหมายระดับสูงของการควบคุม IIoT และผลประโยชน์ที่เกี่ยวข้องกับการแปลงข้อมูลคือ การเพิ่มความปลอดภัยในอุตสาหกรรมให้คุ้มค่าใช้จ่าย ขั้นตอนแรกในกระบวนการคือการจับข้อมูลที่หลั่งไหลออกจากเครื่องมือต่างๆ เกี่ยวกับความปลอดภัย เช่น Safety Instrumented Systems (SIS), Safety Instrumented Functions (SIF), Layer of Protection Analysis systems (LOPA), Process Hazards Analysis tools (PHA) และ Hazard and Operability tools (HazOp) ข้อมูลนี้ควรรวมเข้าไว้ในฐานข้อมูลดิจิทัลเพื่อช่วยให้ข้อมูลการออกแบบด้านความปลอดภัยที่สำคัญนี้มีความสอดคล้องรวดเร็วในการเข้าถึงและใช้งานง่าย

เครื่องมือความปลอดภัยแบบดั้งเดิมเหล่านี้ได้รับการออกแบบเพื่อตอบสนองพารามิเตอร์ด้านความปลอดภัยโดยเฉพาะ อย่างไรก็ตามวิธีใช้งานนั้นอาจแตกต่างจากจุดประสงค์ของการออกแบบดั้งเดิม ดังนั้นข้อมูล "ตามที่ได้รับการออกแบบ" (เช่น อัตราความต้องการ ช่วงการทดสอบเวลาในการบายพาส) จึงควรเชื่อมต่อแบบดิจิทัลกับข้อมูล "ขณะทำงาน" เพื่อให้ความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นจากความเสื่อมของระบบนั้นสามารถประเมินได้ในแบบเรียลไทม์ (ตัวอย่างเช่น การระบุช่องว่างที่อาจเกิดขึ้นใน Instrument Protection Layers และการมองเห็นว่าผลกระทบในโลกความเป็นจริงมีความปลอดภัยในการปฏิบัติงานอย่างไร) ในการเชื่อมต่อแบบดิจิทัลกับระบบที่มีอยู่และแหล่งข้อมูลนั้น จำเป็นที่จะต้องมีการรวบรวมข้อมูลด้วยตนเอง การจัดการข้อมูลจะลดลงและข้อมูลเรียลไทม์ใหม่ๆ จะสามารถเติมเต็มข้อมูลด้านความปลอดภัยที่รวบรวมได้จากรายงานที่มีอยู่ การแปลงข้อมูลดิจิทัลนี้ให้บริบทที่มีความหมายมากกว่าการวิเคราะห์ดั้งเดิมของ KPI ของความปลอดภัยซึ่งช่วยให้บุคลากรสามารถมองเห็นสิ่งที่กำลังเกิดขึ้นแทนที่จะวิเคราะห์เหตุการณ์หลังจากข้อเท็จจริงนั้น



รูปภาพที่ 4

การทำให้เป็นดิจิทัลช่วยให้สามารถระบุช่องว่างด้านความปลอดภัยได้เนื่องจากชั้นการป้องกันที่เป็นอิสระจะเปลี่ยนจากการออกแบบไปสู่การทำงานจริง

ขั้นตอนที่ 2: ใช้การวิเคราะห์เพื่อระบุแนวโน้ม

เมื่อข้อมูลด้านความปลอดภัยถูกรวบรวมจากส่วนกลางแล้ว ส่วนที่สำคัญอีกประการหนึ่งสำหรับการใช้ประโยชน์จาก IIoT คือการใช้การวิเคราะห์เพื่อให้ได้ข้อมูลเชิงลึกที่มีความหมายและสามารถดำเนินการได้จากข้อมูลและระบบที่แตกต่างกัน ก่อนที่จะใช้เครื่องมือวิเคราะห์ใด ๆ อย่างไรก็ตามต้องกำหนดประเภทของการวิเคราะห์ที่จำเป็นด้วย

ด้านล่างนี้เป็นรายการประเภทของการวิเคราะห์ความปลอดภัยที่เกี่ยวข้องซึ่งควรได้รับการพิจารณา:

- **การวิเคราะห์เชิงพรรณนา** – การวิเคราะห์เหล่านี้แสดงให้เห็นถึงสิ่งที่เกิดขึ้นโดยรอบเหตุการณ์ความปลอดภัยเฉพาะและตอบคำถามเกี่ยวกับอุปกรณ์ที่ล้มเหลวและเวลาที่ใช้

- **การวิเคราะห์ข้อมูลเพื่อวินิจฉัย** – จุดข้อมูลเหล่านี้จะอธิบายเหตุผลของการที่มีเหตุการณ์ด้านความปลอดภัยเกิดขึ้นและจะระบุสาเหตุหลักของความล้มเหลวในการบ่งชี้ว่าเกิดความสัมพันธ์ใดขึ้นระหว่างอัตราความล้มเหลวที่ไม่ซ้ำกันหรือไม่

- **การวิเคราะห์เชิงคาดการณ์** – ข้อมูลประเภทนี้จะคาดการณ์ว่าเหตุการณ์ความปลอดภัยประเภทใดที่น่าจะเกิดขึ้นในอนาคตอันใกล้และอนาคตที่ห่างออกไป การคาดการณ์ที่มีขึ้นจะเชื่อมโยงกับการตัดสินใจทางธุรกิจ (เช่น เมื่อทำการบำรุงรักษา) เครื่องมือวิเคราะห์จะใช้กฎตามเงื่อนไขที่แท้จริงหรือรูปแบบพฤติกรรมและตัวชี้วัดชั้นนำเพื่อระบุว่าชิ้นส่วนหรืออุปกรณ์ใดมีแนวโน้มที่จะล้มเหลว

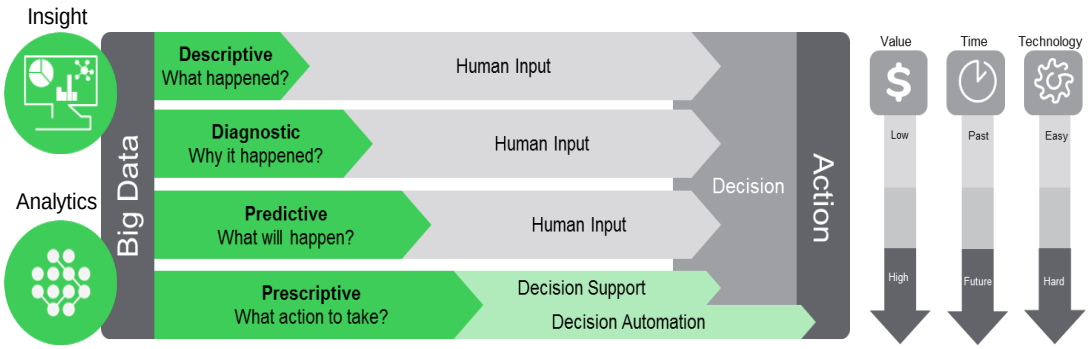
- **การวิเคราะห์แบบกำหนดไว้ล่วงหน้า** - การวิเคราะห์เหล่านี้ใช้เพื่อแจ้งให้เจ้าหน้าที่ด้านความปลอดภัยทราบถึงการดำเนินการที่จะมีขึ้น เครื่องมือเหล่านี้รวมแหล่งข้อมูลภายนอกเช่นการติดตามบุคลากรและสภาวะแวดล้อมเพื่อสร้างขีดความสามารถที่กำหนดไว้

การวิเคราะห์ข้อมูลนี้จะช่วยให้บุคลากรของโรงงานสามารถกำหนดกิจกรรมการผลิตและการบำรุงรักษาที่เหมาะสมที่สุดในหลายๆ สินทรัพย์เพื่อลดความเสี่ยงสะสมและเพื่อลดการหยุดชะงักได้

จากมุมมองด้านความปลอดภัยนี้ ข้อมูลที่รวบรวมจะเป็นประโยชน์สำหรับบริษัทที่ทำงานร่วมกับหน่วยงานกำกับดูแลอุตสาหกรรมเพื่อช่วยรับรองระดับความปลอดภัยของโรงงานของตน

รูปภาพที่ 5

ใช้เครื่องมือและเทคนิคในการวิเคราะห์เพื่อสร้างความเข้าใจที่มีความหมายและสามารถดำเนินการได้



การใช้โซลูชันการวิเคราะห์สามารถเปิดเผยความสัมพันธ์ระหว่างระบบต่างๆเน้นองค์ประกอบด้านความปลอดภัยและคำนวณผลสะสมของการเบี่ยงเบนหลาย ๆ สภาวะหรือสภาวะที่เสื่อมโทรม นอกจากนี้ ด้วยการรวมปัจจัยต่างๆ และการเปรียบเทียบเงื่อนไขในอดีตและรูปแบบประสิทธิภาพแล้ว แนวโน้มสำหรับสถานการณ์ที่ไม่คำนึงถึงก็อาจเกิดขึ้นได้ เงื่อนไขอาจบานปลายไปยังสถานะที่ไม่ปลอดภัยหากยังไม่ได้รับการจัดการอย่างถูกต้อง

อินเทอร์เฟซที่ใช้กับเครื่องมือในการวิเคราะห์สามารถให้คำอธิบายภาพได้ตามบริบทที่ทำให้ผู้ปฏิบัติงานเข้าใจได้ง่ายและรวดเร็วในปัจจุบันและระบุปัญหาที่เป็นไปได้ก่อนที่จะเกิดขึ้น นอกจากนี้ยังสามารถเข้าถึงและแชร์ข้อมูลจากระยะไกลเพื่อให้การบริหารความปลอดภัยไม่ต้องยึดติดกับห้องควบคุมสำนักงานหรือพื้นที่ทางภูมิศาสตร์ที่เฉพาะเจาะจง

ขั้นตอนที่ 3: ใช้โซลูชันคลาวด์เพื่อควบคุมค่าใช้จ่าย

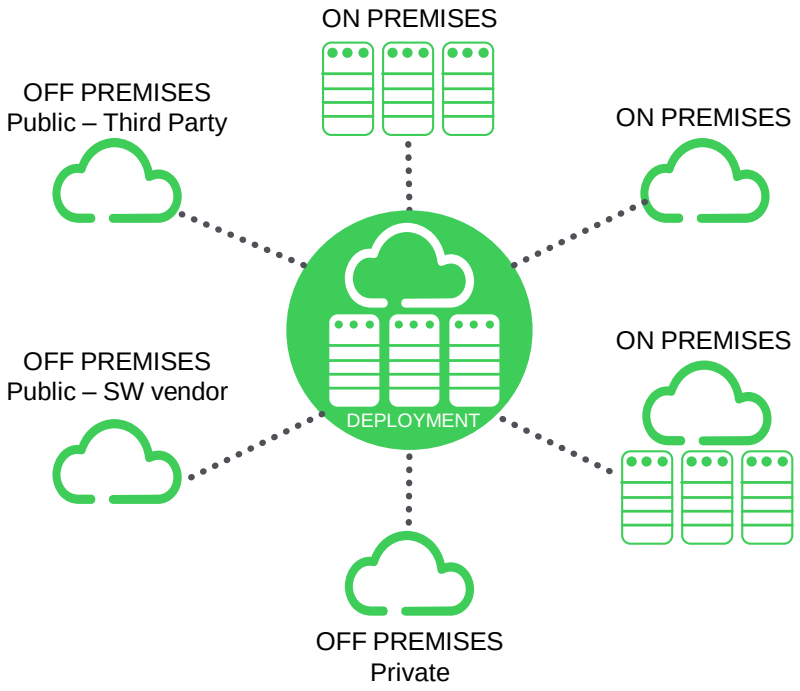
ข้อมูลดังกล่าวให้ความสำคัญกับผู้มีส่วนได้ส่วนเสีย เช่น การดำเนินงาน การบำรุงรักษา วิศวกรรม ความน่าเชื่อถือและความปลอดภัยของบุคลากร ด้วยความเข้าใจในระดับความเสี่ยงในการดำเนินงาน (เช่น ทำงานภายใต้สภาวะที่มีความเสี่ยงสูงกว่าที่คิดไว้) และเตือนผู้บริหารเกี่ยวกับสภาวะที่เบี่ยงเบนไป ความเสี่ยงที่เพิ่มขึ้นและความเสี่ยงสะสมจะรับรู้ก่อนที่จะมีการเปลี่ยนแปลงหรือมีข้อจำกัดเกิดขึ้นใน Instrument Protection Layer (IPL) ดังนั้นการบริหารความปลอดภัยที่ดีที่สุดจะเสียค่าใช้จ่ายน้อยกว่าและมีประสิทธิภาพมากขึ้น

Cloud computing และ / หรือ Software as a Service (SaaS) กำลังขับเคลื่อนการเปลี่ยนแปลงในอุตสาหกรรมกระบวนการ ในอดีต ผู้จัดการโรงงานอาจมีเพียงไม่กี่ตัวเลือกในการเสริมระบบความปลอดภัย การแก้ปัญหาคือการซื้อซอฟต์แวร์และฮาร์ดแวร์ จ้างผู้เชี่ยวชาญด้าน IT เพื่อจัดการโครงสร้างพื้นฐานและหวังว่าจะสามารถทำงานได้ทั้งหมด สิ่งเหล่าเสียค่าใช้จ่ายสูงมากโดยเฉพาะในอุตสาหกรรมที่มีอัตรากำไรต่ำ แต่ Cloud computing กำลังเสนอตัวเลือกที่เหมาะสมให้ ขณะนี้ผู้ให้บริการบุคคลที่สามสามารถเสนอโซลูชันผ่านค่าสมัครรายเดือนได้โดยไม่มีค่าธรรมเนียมล่วงหน้าสำหรับฮาร์ดแวร์และซอฟต์แวร์

คลาวด์นี้ถือได้ว่าเป็นจุดรวมศูนย์และมีวิธีลดค่าใช้จ่ายด้านโครงสร้างพื้นฐานและค่าใช้จ่ายในการใช้งานเครื่องมือด้านความปลอดภัย แอพพลิเคชั่นและข้อมูล (แต่เป็นเฉพาะในสถานที่และเวลาที่เหมาะสม) โมเดล Cloud computing / SaaS ช่วยให้สามารถนำข้อมูลด้านความปลอดภัยและบริบทไปใช้กับผู้เชี่ยวชาญทุกแห่งในโลกเพื่อให้สามารถวิเคราะห์ IPL แยกกันเพื่อให้การตัดสินใจด้านความปลอดภัยสอดคล้องกันมากขึ้น

รูปภาพที่ 6

พิจารณาคลาวด์เป็นจุดศูนย์รวม



การแก้ปัญหาดังกล่าวยังทำให้เกิดความโปร่งใสทั่วทั้งองค์กรและขจัดอุปสรรคดั้งเดิมภายในแผนก โครงสร้างการจัดการ สินทรัพย์และ / หรือส่วนของสินทรัพย์ การใช้คลาวด์เป็น "แหล่งความจริง" สำหรับการออกแบบ วิเคราะห์และตรวจสอบความปลอดภัยแบบดิจิทัลทำให้ทุกคนสามารถเข้าถึงได้อย่างง่ายดายทุกที่และทุกเวลา

ขั้นตอนที่ 4: แนะนำการจำลองเพื่อเพิ่มความปลอดภัย

ระบบการฝึกอบรมผู้ประกอบการยุคใหม่ (OTS) ใช้เทคโนโลยีการจำลองแบบไดนามิกเพื่อสร้างระบบการประมวลผลอุตสาหกรรมที่มีความละเอียดสูงรวมถึงอุปกรณ์ กระบวนการและขั้นตอนการควบคุมแบบอัตโนมัติ เครื่องมือที่ทันสมัยจะรวบรวมข้อมูลเกี่ยวกับตัวแปรนับหมื่น ข้อมูลทั้งหมดนี้สามารถเข้าถึงได้เพื่อให้โมเดลสามารถปรับให้เข้ากับระบบควบคุมโรงงานได้ ดังนั้นเมื่อมีการเปลี่ยนแปลงแบบจำลองที่นำไปใช้กับระบบการผลิต การเปลี่ยนแปลงเหล่านี้ก็จะเป็นการเปลี่ยนแปลงที่ดีที่สุดสำหรับโรงงานจากมุมมองด้านความปลอดภัยประสิทธิภาพและประสิทธิผล

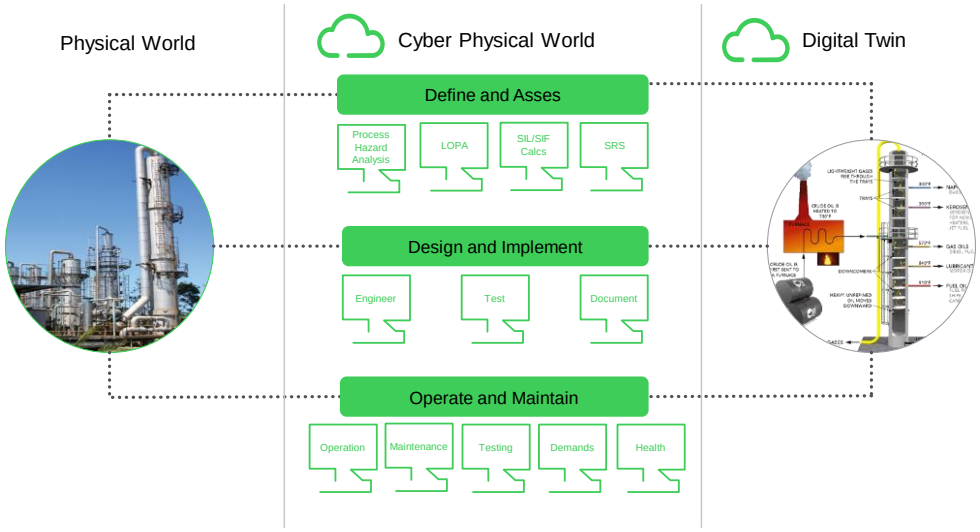
โมเดลเสมือนที่เรียกว่า "คู่ดิจิทัล" จะวิเคราะห์ข้อมูลที่รวบรวมแล้วนำไปใช้เพื่อจำลองผลการปฏิบัติงานและเปรียบเทียบประสิทธิภาพเพื่อช่วยให้ผู้ประกอบการโรงงานสามารถระบุตำแหน่งที่สามารถทำกำไรได้อย่างมีประสิทธิภาพ การจับคู่ทั้งโลกเสมือน

และโลกทางกายภาพ (ฝาแฝด) จะช่วยแก้ปัญหาได้ก่อนที่จะเกิดขึ้นเพื่อป้องกันอันตรายจากสถานการณ์ด้านความปลอดภัย

คู่ดิจิทัลสามารถนำมาใช้ได้ ตัวอย่างเช่น เพื่อตรวจสอบการออกแบบระบบความปลอดภัยก่อนที่จะมีการผลิตระบบทางกายภาพ โดยสามารถใช้งานในโหมด 'ออฟไลน์' เพื่อเรียกใช้สถานการณ์สมมติ "ได้ตามต้องการ" โดยพิจารณาจากระดับความเสี่ยงที่เพิ่มขึ้น ด้วยการใช้ในโหมด 'ออนไลน์' นี้ คู่ดิจิทัลสามารถให้โมเดลแบบไดนามิกของสินทรัพย์ที่ใช้งานได้ก่อนที่จะเกิดปัญหาขึ้นหรือเพื่อระบุสาเหตุของปัญหา

รูปภาพที่ 7

แบบจำลองเสมือนเช่นฝาคู่ดิจิทัลช่วยลดความเสี่ยงด้านความปลอดภัยในการใช้งานอุปกรณ์โรงงานได้



ขั้นตอนที่ 5: รวมกลยุทธ์ความปลอดภัยในโลกไซเบอร์

แม้ว่า IIoT และโครงการริเริ่มด้านดิจิทัลที่เกี่ยวข้องจะมีโอกาสมากมายในการปรับปรุงด้านความปลอดภัยในอุตสาหกรรม การเชื่อมต่อกับอินเทอร์เน็ตในวงกว้างยังก่อให้เกิดความเสี่ยงใหม่ในการนำระบบความปลอดภัยไปสู่การโจมตีทางไซเบอร์ด้วย เพื่อต่อต้านภัยคุกคามนี้ กลยุทธ์ด้านความปลอดภัยในโลกไซเบอร์ที่กำลังดำเนินการอยู่จะต้องมีการนำมาใช้เพื่อเติมเต็มกลยุทธ์ด้านความปลอดภัย

ในทุกกรณีนั้น ทีมรักษาความปลอดภัยในท้องถิ่นต้องตรวจสอบว่าการเชื่อมต่ออินเทอร์เน็ตของระบบความปลอดภัยนั้นเป็นไปได้หรือไม่และถ้าเป็นเช่นนั้น จะอยู่ภายใต้เงื่อนไขใด ในบางกรณี เครื่องมือเช่น นักประวัติศาสตร์โรงงานอาจต้องเข้าถึงข้อมูลที่เกี่ยวข้องกับความปลอดภัย อีกทั้งความเสี่ยงแบบดิจิทัลจะต้องได้รับการประเมินเป็นกรณีๆ ไป มาตรฐานที่เกี่ยวกับความปลอดภัยที่อัพเดตแล้วเช่น IEC61511 และ IEC62443 สามารถให้คำแนะนำเกี่ยวกับวิธีการคำนวณความเสี่ยงด้านความปลอดภัยในโลกไซเบอร์ได้

ผู้มีส่วนได้เสียที่ได้รับผลกระทบจะต้องรวมการปฏิบัติในปัจจุบันเพื่อปกป้อง "มนุษย์จากเครื่องจักร" (กล่าวคือ วิธีที่ระบบความปลอดภัยช่วยปกป้องแรงงานจากความเสี่ยงจากกระบวนการทางเคมีและทางจักรกล) ด้วยการปฏิบัติใหม่เพื่อปกป้อง "เครื่องจักรจากมนุษย์" (กล่าวคือ อุปกรณ์ได้รับการป้องกันจากการโจมตีทางอินเทอร์เน็ตภายนอก)

แหล่งที่มาของภัยคุกคาม ได้แก่ แฮกเกอร์ที่ไม่เพียงแต่มองไม่เห็นซึ่งกำลังท่องอยู่ในอินเตอร์เน็ตเพื่อค้นหาเป้าหมายเท่านั้น แต่ยังรวมถึงพนักงานภายในและซัพพลายเออร์ภายนอกที่เข้ามาในพื้นที่เขตอุตสาหกรรมด้วย การเชื่อมโยงที่อ่อนแอที่สุดคือผู้ที่บริหารและใช้ระบบ การกระทำของพวกเขาโดยเจตนาหรือไม่เจตนาอาจเพิ่มความเสี่ยงด้านความปลอดภัยให้กับระบบขึ้น ดังนั้นการฝึกอบรมด้านการรักษาความปลอดภัยในโลกไซเบอร์ของพนักงานและซัพพลายเออร์ภายนอกจึงมีความสำคัญพอๆ กับการใช้โซลูชันซอฟต์แวร์ความปลอดภัยในโลกไซเบอร์

ผู้ผลิตระบบควบคุมที่มีความรับผิดชอบกำลังออกแบบระบบรักษาความปลอดภัยในโลกไซเบอร์ไว้ในทุกโมดูลที่พวกเขาสร้างและส่งมอบเพื่อให้ลูกค้าไม่ต้องกังวลกับการสร้างระบบรักษาความปลอดภัยในโลกไซเบอร์หลังจากที่ซื้อผลิตภัณฑ์ใหม่ไป

ตัวอย่างเช่น ผู้ผลิตอย่าง Schneider Electric ใช้แนวทาง Secure Development Life Cycle (SDL) เพื่อพัฒนาผลิตภัณฑ์ ภายใต้บริบทของ SDL การวิเคราะห์การออกแบบที่มีความปลอดภัยจะดำเนินการการสร้างแบบจำลองภัยคุกคามของการออกแบบการรักษาความปลอดภัยในแนวความคิดที่เกิดขึ้น มีการใช้กฎการเข้ารหัสที่ปลอดภัย เครื่องมือพิเศษที่ใช้ในการวิเคราะห์รหัสและการทดสอบความปลอดภัยของผลิตภัณฑ์จะได้รับการดำเนินการ การกระทำเหล่านี้ช่วยให้ผลิตภัณฑ์ 'แข็งแกร่ง' ทำให้มีความยืดหยุ่นมากขึ้นกับการโจมตีทางอินเทอร์เน็ตได้ทันทีที่เริ่มใช้งาน ด้วยวิธีนี้เมื่อผลิตภัณฑ์ใหม่เปลี่ยนไป ระบบทั้งหมดจะมีวิวัฒนาการเพื่อให้ปลอดภัยยิ่งขึ้นในโลกไซเบอร์ ตัวอย่างผลิตภัณฑ์ที่เกี่ยวข้องกับความปลอดภัยของ Schneider Electric ที่ผ่านการตรวจสอบแล้วและได้รับการรับรองระดับ Achilles Level 2 ได้แก่ ชุด Triconex (Tricon, Trident, Tri-GP) Modicon M580 control และ ePACs เพื่อความปลอดภัย

รูปภาพที่ 8

กระบวนการรักษาความปลอดภัยแบบไซเบอร์จะสอดคล้องกับความปลอดภัยของกระบวนการทางอุตสาหกรรม

บทสรุป

โลกแห่งความปลอดภัยของกระบวนการมีมานานหลายปีตามปรัชญาในการจัดการระบบความปลอดภัยซึ่งเป็นหน่วยงานแยกต่างหาก เป็นอิสระ ไม่เชื่อมต่อและแยกตัวออกจากอินเตอร์เน็ตอย่างมากที่สุดเท่าที่จะเป็นไปได้ แนวทางนี้กำลังเปลี่ยนแปลงไป ประโยชน์ที่ได้จากการแปลงเป็นข้อมูลดิจิทัลและการใช้ข้อมูลที่เกี่ยวข้องกับความปลอดภัยจะมีมากกว่าความเสี่ยงของการเชื่อมต่อที่เปิดกว้างมากขึ้น (หากว่ามีการใช้กลยุทธ์ด้านความปลอดภัยในโลกไซเบอร์แบบดิจิทัล) การปรากฏขึ้นของอินเตอร์เน็ตอุตสาหกรรมสิ่งต่างๆและเทคโนโลยีการแปลงข้อมูลที่เกี่ยวข้องช่วยให้ผู้เชี่ยวชาญด้านความปลอดภัยในอุตสาหกรรมสามารถวิเคราะห์ปัญหาด้านความปลอดภัยจากมุมมองในอดีต ปัจจุบันและในอนาคตได้ สิ่งนี้นำไปสู่การทำให้เข้าใจง่ายเกี่ยวกับความปลอดภัยในสองประเด็นหลักคือการจัดการความเสี่ยงและการจัดการการดำเนินงานและช่วยในการรวมทั้งสองอย่างในชีวิตประจำวันเข้าไว้ด้วยกัน

การใช้เครื่องมือและเทคนิค IIoT แสดงถึงศักยภาพที่ยิ่งใหญ่สำหรับการปฏิบัติตามหลักปฏิบัติด้านความปลอดภัยอย่างชาญฉลาดและรวดเร็วขึ้น เครื่องมือเหล่านี้สามารถช่วยให้พนักงานในภาคอุตสาหกรรมสามารถทราบข้อมูลการดำเนินงานและการตัดสินใจทางธุรกิจที่ดีขึ้นช่วยให้ดำเนินงานได้อย่างมีผลกำไรและปลอดภัย

เกี่ยวกับผู้เขียน

สตีฟ เอลเลียต เป็นผู้อำนวยการอาวุโสของชไนเดอร์ อิเล็คทริคฝ่ายกระบวนการทางการตลาดอัตโนมัติ รับหน้าที่ในการกำหนดทิศทางในอนาคตและกลยุทธ์นำเข้าสู่ตลาด เป็นวิศวกรด้านความปลอดภัยที่ได้รับการรับรองจาก TÜV พร้อมด้วยประสบการณ์มากกว่า 20 ปีในกระบวนการควบคุมและอุตสาหกรรมระบบอัตโนมัติ เขามีประสบการณ์มากมายในการออกแบบระบบความปลอดภัยและวงจรชีวิตความปลอดภัยในโรงงานอุตสาหกรรม