

แนวนับ IT

สำหรับอุตสาหกรรม

การผลิตไทย ปี 69

วิษณุศุภร์ เมระพงษ์

Development Team Leader & Senior system analyst
บริษัท student care จำกัด
และที่ปรึกษาการบริหาร IT องค์การภาครัฐ และเอกชน



5. ปฏิบัติการความปลอดภัยไซเบอร์แบบ Zero Trust

เมื่อโรงงานมีการเชื่อมต่ออินเทอร์เน็ตมากขึ้น ความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ก็สูงขึ้นตามไปด้วย ในปี 2569 อุตสาหกรรมไทยจะหันมาใช้แนวคิด Zero Trust Architecture (ไม่ไว้วางใจใครเลยจนกว่าจะตรวจสอบตัวตน) และการใช้ AI-driven Detection เพื่อตรวจจับความผิดปกติของระบบ OT (Operational Technology) ก่อนที่เครื่องจักรจะถูกระงับ

ข้อมูลเพิ่มเติมเกี่ยวกับ Zero Trust สำหรับโรงงานอุตสาหกรรม เพื่อให้เกิดความปลอดภัยสูงสุด ระบบ Zero Trust สำหรับโรงงานต้องครอบคลุม 3 องค์ประกอบหลัก ดังนี้

■ **Identity-First Security** คือ การยืนยันตัวตน ไม่ได้จำกัดแค่ “คน” แต่รวมถึง “เครื่องจักร” (Machine Identity) และแอปพลิเคชัน AI” ทุกตัวต้องมีใบรับรองดิจิทัลเพื่อยืนยันตัวตนก่อนเข้าถึงข้อมูล

■ **Least Privilege Access** คือ การมอบสิทธิ์การเข้าถึงให้น้อยที่สุดเท่าที่จำเป็น เช่น พนักงานซ่อมบำรุงจะมีสิทธิ์เข้าถึงเฉพาะพารามิเตอร์ หรือชุดข้อมูลเฉพาะในส่วนเครื่องจักรที่ตนรับผิดชอบ และสามารถเข้าถึงได้เฉพาะในช่วงเวลาที่กำลังปฏิบัติงานเท่านั้น

■ **Micro-segmentation** คือ การแบ่งเครือข่ายโรงงานออกเป็นส่วนย่อยๆ (Island) เพื่อจำกัดวงความเสียหายหากส่วนใดส่วนหนึ่งถูกโจมตี ระบบจะตัดการเชื่อมต่อไม่ให้มัลแวร์แพร่กระจายไปยังสายการผลิตอื่น

การประยุกต์ใช้ Zero Trust ในสายการผลิต

■ การป้องกันระบบ OT จากภัยคุกคามภายนอก

ระบบ Operational Technology (OT) เช่น PLC หรือ Scada มักเป็นระบบเก่าที่ไม่รองรับการติดตั้งแอนตี้ไวรัส การใช้ Zero Trust จะใช้วิธีสร้าง “อุโมงค์ที่ตรวจสอบได้” (Secure Tunnels) สำหรับการอัปเดตซอฟต์แวร์หรือการตรวจเช็คจาก Supplier ภายนอก โดยระบบจะตรวจสอบสิทธิ์ และพฤติกรรมตลอดเวลาที่เชื่อมต่อ

■ การตรวจสอบพฤติกรรม AI (AI-Driven Monitoring)

เมื่อเราใช้ Agentic AI ในการสั่งการผลิต ระบบ Zero Trust จะใช้ AI อีกตัวหนึ่งทำหน้าที่เป็น “ผู้ตรวจการ” (Sentinel) เพื่อคอยเฝ้าดูว่า Agentic AI ตัวนั้นมีพฤติกรรมที่ผิดปกติหรือไม่ เช่น ตรวจพบว่ามีความพยายามที่จะแก้ไขพารามิเตอร์ความปลอดภัยของเครื่องจักรเกินขอบเขตที่กำหนด ระบบจะทำการระงับสิทธิ์ทันที

ประโยชน์ที่จะได้รับ

■ **ลดความเสี่ยงจากการหยุดชะงัก (Downtime)** ป้องกันการถูกโจมตีด้วย Ransomware ที่อาจทำให้สายการผลิตหยุดชะงัก ซึ่งมีมูลค่าความเสียหายมหาศาลต่อวัน

■ **ความเชื่อมั่นจากคู่ค้าสากล** การมีมาตรฐานความปลอดภัยระดับ ZTA ช่วยให้ผู้ประกอบการไทยผ่านเกณฑ์มาตรฐานความปลอดภัยสากล (เช่น NIST หรือ ISO 27001) ทำให้ได้รับความไว้วางใจในการผลิตสินค้าจากแบรนด์ระดับโลก

■ **รองรับการทำงานแบบ Hybrid** ช่วยให้วิศวกรสามารถตรวจสอบ และแก้ไขปัญหาจากที่บ้านได้อย่างปลอดภัยเสมือนนั่งอยู่ในโรงงาน

ขั้นตอนการเริ่มต้นสำหรับผู้ประกอบการ

■ **ทำบัญชีทรัพย์สินดิจิทัล (Asset Discovery)** สำรวจว่าในโรงงานมีอุปกรณ์ใดบ้างที่เชื่อมต่ออินเทอร์เน็ต ซึ่งรวมถึงอุปกรณ์ IoT ขนาดเล็กต่างๆ

■ **กำหนดนโยบายการเข้าถึง (Access Policy)** ระบุว่าใคร (หรือเครื่องจักรเครื่องไหน) มีสิทธิ์ทำอะไร กับข้อมูลส่วนไหนบ้าง

■ **เลือกใช้โซลูชันที่เหมาะสม** เริ่มจากการติดตั้งระบบ Multi-Factor Authentication (MFA) และการทำ Micro-segmentation ในส่วนที่สำคัญที่สุดก่อน

ตาราง สรุปประโยชน์ของแนวโน้มเทคโนโลยีอุตสาหกรรมการผลิต ปี 69

เทคโนโลยี	ประโยชน์ต่อโรงงาน
Agentic AI	ลดการพึ่งพาแรงงานทักษะต่ำ และลดข้อผิดพลาดจากการตัดสินใจของมนุษย์
Digital Twin	คาดการณ์ความเสียหายของเครื่องจักร (Predictive Maintenance) ลด Downtime
Green IT	เพิ่มขีดความสามารถในการส่งออกสินค้าไปยังตลาดยุโรปและอเมริกา
Low-Code	สร้างนวัตกรรมภายในองค์กรได้รวดเร็ว (Agile Manufacturing)

ก้าวต่อไปสำหรับผู้ประกอบการ

หากองค์กรกำลังมองหาแนวทางการปรับตัวเพื่อรับมือกระแสเทคโนโลยีที่กำลังถาโถมเข้ามา สิ่งแรกที่เราควรเริ่มดำเนินการในปี 2569 ไม่ใช่การซื้อระบบ AI มาติดตั้ง แต่คือการสร้างฐานข้อมูลที่ “พร้อมใช้งาน” ผ่านกระบวนการ Data Consolidation หรือการรวบรวมข้อมูลจากเครื่องจักร และส่วนกลางให้มาอยู่ในที่เดียวกัน เพื่อเตรียมความพร้อมสำหรับการประยุกต์ใช้งาน AI เพื่อให้ระบบ AI สามารถ “มองเห็น” “วางแผน” และ “ลงมือทำ” ได้อย่างแม่นยำบนฐานข้อมูลชุดเดียวกัน

Data Consolidation คือ การรวบรวมข้อมูลอย่างเป็นระบบซึ่งไม่ใช่แค่เรื่องทางเทคนิคของฝ่าย IT แต่จะถูกใช้เป็นกลยุทธ์หลักในการสร้างความได้เปรียบทางการแข่งขัน เพราะข้อมูลจะอยู่ในสถานะของเชื้อเพลิงที่ใช้ในการขับเคลื่อน อุตสาหกรรมยุค 5.0 ที่กำลังจะมาถึง

1. ความท้าทาย และแนวทางการปรับตัวสำหรับโรงงานผู้ผลิตของไทย การทำ Data Consolidation สำหรับประเทศไทยยังคงมีอุปสรรคสำคัญที่ต้องเร่งดำเนินการ

2. เครื่องจักรเก่า (Legacy Machinery) เครื่องจักรในโรงงานไทยจำนวนมากไม่มีระบบเชื่อมต่อดิจิทัล แนวทางแก้ไขคือการติดตั้งอุปกรณ์ IoT Gateway เพื่อดึงสัญญาณพื้นฐานออกมา

3. วัฒนธรรมการทำงานแบบแยกส่วน (Departmental Silos) ฝ่ายผลิตมักไม่แชร์หรือแบ่งปันข้อมูลกับฝ่าย Supply Chain การทำ Data Consolidation จึงต้องเริ่มจากนโยบายการบริหารระดับสูงที่กำหนดให้ “ข้อมูลเป็นทรัพย์สินส่วนกลาง”

4. ความปลอดภัยไซเบอร์ (Security) การรวบรวมข้อมูลไว้ที่จุดเดียวเพิ่มความเสี่ยงหากระบบถูกเจาะ การใช้โครงสร้างแบบดังที่กล่าวถึง จึงเป็นสิ่งที่ต้องทำควบคู่กันไป

การรวบรวมข้อมูล (Data Consolidation) ไม่ใช่เพียงขั้นตอนการเตรียมความพร้อมทาง IT แต่คือจุดเริ่มต้นของการสร้างระบบนิเวศการผลิตที่ชาญฉลาดในปี 2569 โรงงานผู้ผลิตของไทยที่สามารถบูรณาการข้อมูลจากทุกส่วนเข้าด้วยกันได้สำเร็จจะเป็นกลุ่มแรกที่สามารถเปลี่ยนผ่านไปสู่การใช้งาน Agentic AI และ Physical AI ได้อย่างเต็มรูปแบบ ซึ่งจะส่งผลให้เกิดการผลิตที่ยืดหยุ่น ลดต้นทุน และสร้างความยั่งยืนในระยะยาวตามแนวทางอุตสาหกรรม 5.0 ต่อไป

ข้อมูลอ้างอิง

- techsauce.co ai trends 2026 agentic ai digital labor strategy
- nvidia.com: Agentic AI for Physical Operations
- openfabric.ai: Merging Agentic and Physical AI - The Future of Intelligent Systems
- co.bot
- universal-robots.com
- nvlpubs.nist.gov: NIST Special Publication - Zero Trust Architecture
- microsoft.com: security - what is zero trust architecture
- taxation-customs.ec.europa.eu: Carbon Border Adjustment Mechanism
- circularanalytics.com
- incentives.eeco.or.th

