إدارة السلامة في بيئات العمل المعززة بالروبوتات والأتمتة

الإمارات العربية المتحدة - دبي

2026 / 04 /16 – 12

مقدمة:

في ظل التوجه الاستراتيجي نحو السيادة الرقمية وتطبيق مبدأ تصفير البيروقراطية، لم تعد الأتمتة مجرد وسيلة لزيادة الإنتاج، بل أصبحت شريكاً في بيئة العمل يتطلب إدارة سلامة فائقة الذكاء. تهدف هذه الدورة إلى تمكين القادة من أدوات إدارة المخاطر في البيئات التي تتفاعل فيها الروبوتات التشاركية (Cobots) مع العنصر البشري. يركز البرنامج على حوكمة الأنظمة المؤتمتة لضمان النزاهة المطلقة وحماية البيانات السيادية، مما يضمن ريادة المؤسسة وقدرتها على بناء "مصانع ومكاتب ذكية" معصومة من الحوادث وتدعم جودة الحياة المهنية.

أهداف الدورة:

- استيعاب مفاهيم **السلامة السيبرانية-المادية** وعلاقتها بالرشاقة المؤسسية وتصفير البيروقراطية التقنية.
- تطوير مهارات تقييم مخاطر الروبوتات (Robot Risk Assessment) وفق المعايير العالمية.(ISO 10218)
- إتقان فن هندسة مساحات العمل المشتركة بين البشر والآلات بنزاهة وشفافية مطلقة.
- حوكمة الخوارزميات المشغلة للأتمتة لضمان السيادة المعلوماتية والامتثال للقيم الوطنية.
- اكتساب مهارات **تصفير التداخل الخطِر** عبر أنظمة الرؤية الحاسوبية والمستشعرات الذكية.
- تعزيز السيادة الرقمية من خلال تأمين شيفرات الأتمتة ومنع التدخلات الخارجية في أنظمة التحكم.
- تطبيق استراتيجيات "الثقة المتبادلة بين الإنسان والآلة" لتعزيز الإنتاجية دون المساس بالسلامة.
- تطوير مهارات إدارة المعضلات الأخلاقية المرتبطة بقرار الآلة في حالات الطوارئ القصوى.
- صياغة خارطة طريق شاملة لتحويل الأتمتة إلى "درع وقائي" يدعم الريادة والتميز الحكومي.

محتويات الورشة:

اليوم الأول:

فلسفة الأتمتة في عصر السيادة الرقمية

من "الآلة المعزولة" إلى "الروبوت التشاركي والرشاقة"

- مفهوم السلامة في عصر الثورة الصناعية الرابعة: لماذا نحتاج لسيادة رقمية على قرارات الآلة؟
- مواءمة الأتمتة مع استراتيجية تصفير البيروقراطية: كيف نلغي عوائق الإنتاج عبر "التكامل الآمن"؟
- تحليل العلاقة بين "دقة الروبوت" وبين بناء الثقة والمصداقية الوطنية في جودة المخرجات.
- تمرين "هندسة التفاعل": تحديد نقاط الالتقاء بين الموظف والروبوت وتصفير مخاطرها بنزاهة.

النزاهة والسيادة في بناء "الأنظمة الموثوقة"

- مفهوم "السيادة الخوارزمية": حماية برمجيات الأتمتة الوطنية من التلاعب أو الاختراق.
- دور القائد في حماية سلامة الفريق عبر ممارسات النزاهة في برمجة معايير التوقف الطارئ.
- سيكولوجية "الأمان مع الآلة": بناء المصداقية عبر الشفافية في توضيح قدرات وحدود الروبوت.
- صياغة ميثاق "أخلاقيات الأتمتة السيادية" لضمان توافق سلوك الآلة مع القيم الوطنية.

اليوم الثاني:

الهندسة التقنية والسيادة السيبرانية للأتمتة

الأمان الرقمي والربط البيني للأنظمة السيبرانية-المادية

- هندسة المستشعرات (Lidar, Ultrasonic) وكيفية حوكمة بياناتها لضمان السيادة المعلوماتية.
- الأمان الرقمي كركيزة للأتمتة: حماية "أدمغة الروبوتات" من هجمات الاستيلاء أو التزييف الرقمي.
- إدارة الهوية الرقمية للأجهزة (Device Identity) وأثرها على موثوقية الأوامر والنزاهة الإجرائية.
- تمرين تقني: تصميم بروتوكول "تصفير الاختراق" لأنظمة التحكم الصناعية (ICS) بنزاهة.

أخلاقيات التفاعل مع أنظمة "الاستجابة الذكية للطوارئ"

- حدود استخدام الذكاء الاصطناعي في "التنبؤ بالأعطال" دون انتهاك السرية السيادية للبيانات.
- حوكمة مخرجات أنظمة "إدارة الحركة": الضمان الأخلاقي لعدم التحيز في الأولوية البشرية.
- مفهوم "الأمانة في البرمجة": تجنب الاعتماد الكلي على الآلة دون وجود "حكمة قيادية" بشرية.
- ورشة عمل: وضع ضوابط أخلاقية لاستخدام البيانات الضخمة في "تطوير كفاءة الروبوتات."

اليوم الثالث:

الحياد والعدالة في بيئة العمل المؤتمتة

النزاهة الرقمية ومكافحة الانحياز في "توزيع المهام بين البشر والآلة"

- أخلاقيات "العدالة المهنية": ضمان نزاهة توزيع المهام الشاقة على الآلات بنزاهة وشفافية.
- الرقابة الأخلاقية على أنظمة "الرقابة الآلية": كيف نضمن الشفافية والنزاهة في تقييم أداء البشر؟
- تطبيق قاعدة "الإرادة البشرية القيادية": التدخل لتجاوز "قرار آلي" قد يضر بالروح المعنوية للفريق.
- حساب معامل الثقة في أنظمة الأتمتة لتقليل احتمالات الخطأ الناتج عن "الهلوسة الرقمية" للبيانات.

حوكمة المسؤولية عن مخرجات "القرارات الآلية"

- المسؤولية المهنية للقائد عند حدوث "عطل برمج" أدى لحادث أو توقف في سلاسل الإمداد.
- إدارة العلاقة مع مزودي تقنيات "Robotics": ضمان السيادة والشفافية في الخوارزميات.
- بناء أنظمة "التحقق المزدوج" لضمان عدم غياب الحكمة البشرية في العمليات السيادية الحساسة.
- تمرين محاكاة: إدارة أزمة تواصل ناتجة عن "خطأ تقني" في روبوت تشاركي وكيفية علاجه بنزاهة.

اليوم الرابع:

المسؤولية المهنية وإدارة السمعة في عصر الروبوتات

القيادة الاتصالية وحماية السمعة في البيئات الذكية

- أخلاقيات إدارة السمعة عبر "التحول الروبوتي": الموازنة بين الابتكار والوقار والسيادة الحكومية.
- الرقابة على "البصمة الرقمية للآلات" وأثرها على حيادية ومصداقية القرار السيادي والقانوني.
- بناء نظام "الإفصاح الاستباقي للجاهزية التقنية": ضمان الشفافية لتصفير فرص انتشار الشائعات.
- التدقيق الأخلاقي على سلاسل "التوريد التقني" لضمان خلوها من الممارسات غير العادلة.

أخلاقيات الاستجابة للاختراقات والانتهاكات في أنظمة الأتمتة

- المسؤولية الأخلاقية في التبليغ عن الثغرات التقنية التي قد تؤدي لتعطيل "منظومات الأتمتة."
- فن التواصل الأخلاقي أثناء تعطل الروبوتات: حماية الثقة عبر بيانات صادقة ونزيهة دون تضليل.
- إدارة "التعافي المؤسسي": إجراءات إعادة بناء الصورة بعد رصد انحراف في أداء الآلات الرقمي.
- بناء خطة "الحصانة الرقمية للأتمتة": تحصين المنظومة ضد الهجمات أو الإهمال الممنهج.

اليوم الخامس:

مختبر الابتكار المهني وصناعة نموذج "السلامة الذكية" الريادي

التطبيق العملي وتصفير البيروقراطية في أنظمة الأتمتة والتميز المؤسسي

- تطوير خارطة الطريق التنفيذية لدمج معايير السلامة الروبوتية في العمليات اليومية بمرونة ورشاقة تضمن استمرارية الأعمال والتميز والنمو المستدام في عام 2026.
- تصميم بروتوكولات الحوكمة الذكية الخاصة بـ التفاعل بين الإنسان والآلة لتصفير المسارات البيروقراطية وضمان النزاهة والشفافية والوضوح في بيئات العمل الهجينة والريادة العالمية.
- منهجية صياغة ملفات التميز للمنافسة في الجوائز الوطنية مع التركيز على الابتكار في إدارة "مخاطر الأتمتة" والرشاقة في التبني التقني والنمو المؤسسي الشامل والوضوح.
- تمرين مختبر المحاكاة لإدارة المعضلات التقنية والأخلاقية (مثل توقف الأنظمة السيبرانية-المادية) وصياغة الحلول الاستباقية الناجحة والتميز في الأداء الحكومي والسيادة الرقمية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية "حصانة الأتمتة" تضمن نزاهة التعامل مع الأنظمة الذكية بنسبة 100.%
- القدرة على هندسة بيئات عمل "مؤتمتة وسيادية" بمرونة وتوافق مع متطلبات الريادة والتميز.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة التشاركية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي.
- بناء سجل ممارسات فضلى في إدارة "العلاقة مع الآلة" يدعم اتخاذ القرار القيادي الآمن والمستدام.
- تحقيق جاهزية كاملة للمؤسسة والمسؤول للمنافسة في فئات التميز والريادة في الابتكار والاتصال.

الفئة المستهدفة:

- القيادات ومدراء إدارات السلامة والصحة المهنية، التحول الرقمي، والهندسة الميدانية.
- مسؤولو العمليات، مهندسو الأتمتة، وخبراء الاستراتيجية في المنشآت الحكومية والسيادية.
- مستشارو الأمن السيبراني، مدراء السمعة المؤسسية، وفرق التميز والحوكمة الرقمية.
- رؤساء فرق مشاريع تصفير البيروقراطية وتطوير منظومات الأداء الحكومي الذكي.
- الكوادر الطموحة الساعية لامتلاك جدارات "قائد السلامة في عصر الروبوتات والذكاء الاصطناعي."

أساليب التدريب:

يتم استخدام بعض من الأساليب التالية أو الكل حسب المتطلبات لكل تخصص :

- دراسة الحالة المعقدة (Complex Case Studies)
- المحاكاة والألعاب الاستراتيجية (Simulation and War Gaming)
- ورش العمل القائمة على التفكير التصميمي (Design Thinking Workshops)
- حلقات النقاش مع خبير من القطاعين العام أوالخاص.(Expert Panels)
- المختبرات التقنية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)