NOUVEAU REGLEMENT MACHINE UE 2023/1230 : INTEGRER LA CYBERSECURITE DANS LA CONFORMITE INDUSTRIELLE

Le paysage réglementaire européen connaît une transformation majeure avec l'adoption du Règlement Machine UE 2023/1230, qui marque un tournant historique dans la conception et la commercialisation des équipements industriels. Pour la première fois, la cybersécurité devient une exigence explicite au même titre que la sécurité physique traditionnelle. Cette évolution répond aux menaces croissantes pesant sur les systèmes de production connectés et impose aux fabricants de repenser leurs processus de développement. Comprendre ce nouveau cadre réglementaire est désormais essentiel pour toute organisation industrielle souhaitant maintenir son accès au marché européen.

Qu'est-ce que le RM ?

Un nouveau cadre juridique pour les machines

Le Règlement Machine (RM) UE 2023/1230, publié au Journal officiel de l'Union européenne le 29 juin 2023, remplace la directive historique 2006/42/CE qui régissait jusqu'alors la sécurité des machines en Europe. Contrairement à une directive qui nécessite une transposition dans le droit national de chaque État membre, un règlement européen s'applique directement et uniformément dans l'ensemble des 27 pays de l'Union européenne dès son entrée en vigueur.

Ce changement de format juridique n'est pas anodin : il garantit une harmonisation totale des exigences sur l'ensemble du territoire européen, éliminant ainsi les divergences d'interprétation nationales qui pouvaient créer des complexités pour les fabricants exportant dans plusieurs pays membres.

L'intégration historique de la cybersécurité

La véritable révolution du Règlement Machine 2023/1230 réside dans l'intégration explicite d'exigences de cybersécurité. Alors que l'ancienne directive se concentrait exclusivement sur les risques physiques et mécaniques, le nouveau texte reconnaît que les machines modernes, de plus en plus connectées et pilotées par des systèmes numériques, sont exposées à des cybermenaces susceptibles de compromettre leur sécurité physique.

Cette évolution reflète la réalité industrielle contemporaine : selon le rapport annuel 2024 de l'ANSSI, les attaques ciblant les systèmes industriels ont augmenté de manière significative ces dernières années, et les équipements connectés constituent des points d'entrée privilégiés pour les cybercriminels.

Dates clés d'application

Le Règlement Machine est entré en vigueur le 19 juillet 2023, mais sa date d'application effective est fixée au **20 janvier 2027**. Cette période de transition de plus de trois ans permet aux fabricants d'adapter leurs processus de conception, leurs systèmes documentaires et leurs chaînes de production aux nouvelles exigences. Passé cette date, toute machine mise sur le marché européen devra impérativement respecter les dispositions du nouveau règlement.

Quels sont les objectifs du RM ?

Harmoniser la sécurité des machines dans l'UE

L'objectif premier du Règlement Machine est de garantir un niveau de sécurité élevé et uniforme pour tous les équipements commercialisés sur le territoire européen. En adoptant le format d'un règlement plutôt qu'une directive, l'Union européenne élimine les variations d'interprétation entre États membres et simplifie les démarches pour les fabricants qui n'ont plus à naviguer entre différentes transpositions nationales.

Cette harmonisation facilite également la libre circulation des machines au sein du marché unique européen, réduisant ainsi les barrières commerciales et les coûts de mise en conformité pour les industriels.

Adapter le cadre réglementaire aux technologies numériques

Le développement fulgurant de l'Industrie 4.0, caractérisé par l'interconnexion croissante des équipements, l'utilisation de l'intelligence artificielle et l'intégration de composants IoT (Internet des Objets), a rendu obsolète le cadre réglementaire de 2006. Le RM répond à cette transformation en introduisant des exigences spécifiques pour les machines intégrant des éléments numériques, notamment en matière de :

- Protection contre les accès non autorisés
- Sécurisation des interfaces de communication
- Mise à jour sécurisée des logiciels et firmwares
- Résilience face aux cyberattaques

Protéger les utilisateurs contre les risques cyber-physiques

L'innovation majeure du Règlement Machine réside dans la reconnaissance des **risques cyber-physiques** : des vulnérabilités numériques peuvent désormais compromettre la sécurité physique des opérateurs. Une machine compromise par une cyberattaque peut provoquer des accidents industriels graves, des blessures ou des décès.

En intégrant la cybersécurité aux exigences essentielles de sécurité et de santé (EESS), le RM impose aux fabricants de considérer les menaces numériques dès la phase de conception, selon une approche "security by design".

Qu'est-ce qui change avec le RM ?

Des exigences de cybersécurité explicites

L'annexe III du Règlement Machine introduit des exigences essentielles de sécurité et de santé spécifiquement dédiées à la cybersécurité des machines. Ces nouvelles dispositions imposent notamment :

- **L'évaluation des cyber risques** : Les fabricants doivent identifier les menaces numériques susceptibles d'affecter la sécurité de leurs machines
- **La protection contre les accès non autorisés** : Mise en place de mécanismes d'authentification et de contrôle d'accès robustes
- **La sécurisation des communications** : Chiffrement des données échangées et protection des interfaces réseau
- **La traçabilité des événements** : Journalisation des accès et des modifications pour détecter les incidents de sécurité

Une documentation technique enrichie

Le dossier technique accompagnant la déclaration de conformité doit désormais inclure une analyse détaillée des risques de cybersécurité et les mesures de protection mises en œuvre. Cette documentation doit démontrer comment les vulnérabilités potentielles ont été identifiées et atténuées tout au long du cycle de vie du produit.

La notice d'instructions fournie aux utilisateurs doit également contenir des informations sur les bonnes pratiques de cybersécurité : configuration sécurisée, procédures de mise à jour, contacts en cas d'incident de sécurité.

Un élargissement du champ d'application

Le Règlement Machine étend son périmètre à de nouvelles catégories de produits qui n'étaient pas explicitement couvertes par l'ancienne directive, notamment :

- Les systèmes d'intelligence artificielle intégrés dans les machines
- Certains équipements logiciels ayant un impact sur la sécurité

- Les machines partiellement achevées, avec des exigences renforcées

Une approche par le cycle de vie complet

Contrairement à l'ancienne directive centrée sur la phase de conception, le RM adopte une vision du cycle de vie complet de la machine. Les fabricants doivent prévoir la maintenance de la cybersécurité après la mise sur le marché, notamment :

- Des procédures de mise à jour sécurisée
- Un processus de gestion des vulnérabilités découvertes
- Une communication transparente avec les utilisateurs sur les incidents de sécurité

Qui est concerné par le RM ?

Les fabricants de machines

Les premiers concernés par le Règlement Machine sont naturellement les **fabricants**, qu'ils soient établis dans l'Union européenne ou dans un pays tiers. Tout industriel concevant et produisant des machines destinées au marché européen doit garantir la conformité de ses produits aux exigences du règlement avant leur première mise sur le marché.

Cette obligation s'applique indépendamment du lieu de fabrication : un producteur chinois, américain ou japonais exportant vers l'UE est soumis aux mêmes exigences qu'un fabricant européen.

Les importateurs et distributeurs

Les **importateurs** qui introduisent sur le marché européen des machines fabriquées hors UE assument une responsabilité importante : ils doivent vérifier que le fabricant a respecté ses obligations et que la machine porte le marquage CE approprié. En cas de non-conformité constatée, l'importateur peut être tenu responsable.

Les **distributeurs**, bien que moins directement impliqués, doivent s'assurer que les machines qu'ils commercialisent portent le marquage CE requis et sont accompagnées de la documentation appropriée dans la langue du pays de commercialisation.

Les intégrateurs et installateurs

Les entreprises qui assemblent plusieurs machines ou composants pour créer une installation industrielle complète peuvent se retrouver dans la position de fabricant si elles créent un nouvel ensemble dont les caractéristiques de sécurité diffèrent des éléments individuels.

Les secteurs industriels particulièrement impactés

Certains secteurs sont particulièrement concernés par les nouvelles exigences de cybersécurité du RM :

- **Industrie manufacturière** : lignes de production automatisées, robots collaboratifs
- **Agroalimentaire** : machines de conditionnement, systèmes de traçabilité connectés
- **Logistique** : systèmes de convoyage automatisés, AGV (véhicules à guidage automatique)
- **Construction** : engins de chantier connectés, équipements de levage intelligents
- **Énergie** : machines et équipements de production intégrant des systèmes de contrôle-commande

Quelles sont les obligations principales pour les organisations industrielles ?

Réaliser une analyse de risques cyber-physiques

La première obligation imposée par le RM consiste à mener une **évaluation complète des risques** intégrant les dimensions physiques et numériques. Cette analyse doit identifier :

- Les actifs critiques de la machine (automates, capteurs, interfaces réseau)
- Les menaces potentielles (accès non autorisé, malware, déni de service)

- Les vulnérabilités exploitables (authentification faible, protocoles non sécurisés)
- L'impact potentiel sur la sécurité des personnes

Cette démarche s'inscrit dans la continuité des approches normatives comme l'IEC 62443 pour la cybersécurité des systèmes industriels.

Concevoir selon le principe "security by design"

Le Règlement Machine impose d'intégrer la cybersécurité **dès la phase de conception**, et non comme une couche ajoutée a posteriori. Cela implique :

- Architecture réseau segmentée limitant la surface d'attaque
- Durcissement des systèmes d'exploitation et suppression des services inutiles
- Implémentation de mécanismes d'authentification forte
- Chiffrement des communications et des données sensibles
- Mécanismes de mise à jour sécurisée (signature cryptographique des firmwares)

Constituer un dossier technique de conformité

Chaque machine doit être accompagnée d'un **dossier technique** démontrant sa conformité aux exigences essentielles du règlement. Ce dossier doit contenir :

- L'analyse de risques complète (mécanique et cyber)
- Les spécifications techniques et plans de conception
- Les normes harmonisées appliquées (par exemple, la future norme européenne EN ISO 19087 sur la cybersécurité des machines)
- Les résultats des tests et essais de conformité
- La déclaration UE de conformité signée

Assurer une communication transparente

Les fabricants doivent fournir aux utilisateurs une **documentation claire et complète** comprenant :

- Instructions d'installation et de configuration sécurisée
- Bonnes pratiques d'utilisation en matière de cybersécurité
- Procédures de mise à jour des logiciels et firmwares
- Coordonnées du point de contact pour signaler une vulnérabilité
- Informations sur la durée de support en cybersécurité prévue

Mettre en place un processus de gestion des vulnérabilités

Le cycle de vie ne s'arrête pas à la mise sur le marché. Les fabricants doivent établir un **processus de surveillance et de réponse** aux vulnérabilités découvertes après commercialisation, incluant :

- Veille sur les vulnérabilités affectant les composants utilisés
- Mécanisme de signalement pour les chercheurs en sécurité
- Processus d'évaluation et de correction des failles identifiées
- Communication rapide vers les clients en cas de vulnérabilité critique

Quelles sont les sanctions prévues par le RM ?

Un cadre de sanctions harmonisé

Le Règlement Machine prévoit un **régime de sanctions** que les États membres doivent mettre en œuvre dans leur législation nationale. Bien que les modalités précises puissent varier d'un pays à l'autre, le règlement impose que les sanctions soient "effectives, proportionnées et dissuasives".

Sanctions administratives et financières

Les autorités nationales de surveillance du marché peuvent infliger des **amendes significatives** aux fabricants, importateurs ou distributeurs ne respectant pas leurs obligations. Bien que le texte ne spécifie pas de montants précis (contrairement au RGPD ou à NIS 2), les États membres sont tenus d'établir des pénalités suffisamment importantes pour décourager les infractions.

Les sanctions peuvent être graduées selon la gravité du manquement :

- Non-conformité documentaire (absence de dossier technique)
- Défaut de marquage CE ou marquage frauduleux
- Non-respect des exigences essentielles de sécurité
- Mise en danger délibérée des utilisateurs

Mesures correctives et retrait du marché

Au-delà des amendes, les autorités peuvent ordonner des **mesures correctives** contraignantes :

- Suspension de la commercialisation jusqu'à mise en conformité
- Rappel et retrait des machines déjà commercialisées
- Publication des infractions constatées (effet réputationnel majeur)
- Interdiction temporaire ou permanente de commercialiser dans l'UE

Responsabilité civile et pénale

En cas d'accident causé par une machine non conforme, le fabricant s'expose à des **poursuites civiles** pour dommages et intérêts, ainsi qu'à des poursuites pénales si une négligence grave ou une mise en danger délibérée est établie.

La jurisprudence européenne en matière de responsabilité du fait des produits défectueux peut conduire à des condamnations très lourdes, particulièrement lorsque des vies humaines sont en jeu.

Comment se préparer à l'application du RM ?

Réaliser un diagnostic de maturité

La première étape consiste à **évaluer l'écart** entre vos pratiques actuelles et les exigences du Règlement Machine. Ce diagnostic doit couvrir :

- Processus de conception et d'analyse de risques actuels
- Niveau de prise en compte de la cybersécurité dans le développement produit
- Documentation technique existante et ses lacunes
- Compétences disponibles en interne en matière de cybersécurité OT/IoT
- Processus de gestion du cycle de vie et de maintenance

Former les équipes aux nouvelles exigences

La conformité au RM nécessite des **compétences spécifiques** à l'intersection de la sécurité machine traditionnelle et de la cybersécurité industrielle. Il est essentiel de former :

- Les ingénieurs de conception aux principes du "security by design"
- Les responsables qualité aux nouvelles exigences documentaires
- Les équipes support aux processus de gestion des vulnérabilités
- La direction aux enjeux stratégiques et risques juridiques

Adopter les référentiels normatifs pertinents

Bien qu'aucune norme ne soit obligatoire, l'application de **normes harmonisées** facilite grandement la

démonstration de conformité. Les référentiels clés incluent :

- **ISA/IEC 62443** (série) : cybersécurité des systèmes d'automatisation et de contrôle industriel
- **ISO/IEC 27001** : système de management de la sécurité de l'information
- Futures normes européennes spécifiques au RM (en cours d'élaboration)

L'utilisation de ces normes crée une présomption de conformité aux exigences correspondantes du règlement.

Restructurer les processus de développement

L'intégration de la cybersécurité dès la conception nécessite souvent de **revoir l'organisation** du développement produit :

- Intégrer des revues de sécurité aux jalons projet
- Établir des critères de cybersécurité dans le choix des composants
- Mettre en place des tests de sécurité avant mise sur le marché
- Créer un processus de validation de la documentation de conformité

Établir une gouvernance de la conformité

Au niveau organisationnel, la préparation au RM implique de définir clairement les **responsabilités** :

- Désigner un responsable conformité RM
- Créer un comité de pilotage réunissant R&D, qualité, juridique et cybersécurité
- Établir des procédures de veille réglementaire
- Définir un processus de décision pour les arbitrages conformité/coûts

Checklist opérationnelle OT/IoT (10 actions clés)

Pour vous aider à structurer votre démarche de conformité, voici une checklist opérationnelle des actions prioritaires à entreprendre :

1. Cartographier les machines dans le périmètre du RM

Identifiez précisément quelles machines de votre portefeuille sont concernées par le règlement, en tenant compte des machines complètes, partiellement achevées et des modifications substantielles.

2. Réaliser une analyse de risques cyber-physiques

Menez une évaluation structurée des menaces numériques pesant sur chaque type de machine et de leur impact potentiel sur la sécurité des personnes, en utilisant une méthodologie reconnue (EBIOS Risk Manager, ISO 31000).

3. Durcir les configurations par défaut

Éliminez les comptes et mots de passe par défaut, désactivez les services inutiles, et configurez vos équipements selon les principes du moindre privilège.

4. Segmenter les architectures réseau

Isolez les systèmes critiques de sécurité des réseaux généraux, implémentez des zones de confiance et contrôlez les flux entre zones par des pare-feux industriels.

5. Mettre en place une authentification forte

Remplacez les authentifications faibles (mots de passe simples) par des mécanismes robustes : authentification multi-facteurs, certificats, ou solutions de gestion d'identité industrielle.

6. Chiffrer les communications sensibles

Protégez les données en transit par des protocoles sécurisés (TLS, VPN) et chiffrez les données au repos

contenant des informations sensibles (paramètres de sécurité, logs).

7. Établir un processus de mise à jour sécurisée

Définissez comment les firmwares et logiciels seront mis à jour de manière sécurisée (signature cryptographique, canal authentifié) et communiquez ces procédures aux utilisateurs.

8. Constituer le dossier technique de conformité

Compilez l'ensemble de la documentation requise : analyse de risques, justifications techniques, résultats de tests, déclaration de conformité et notice d'instructions enrichie.

9. Créer un PSIRT ou un processus de gestion des vulnérabilités

Mettez en place une structure (Product Security Incident Response Team) ou un processus formel pour surveiller, évaluer et corriger les vulnérabilités découvertes après commercialisation.

10. Former et sensibiliser l'ensemble de la chaîne

Organisez des sessions de formation pour tous les acteurs impliqués, de la conception à la maintenance, et créez une culture de la cybersécurité dans l'organisation.

Comment AKENATECH vous accompagne ?

Face à la complexité du Règlement Machine et à l'intersection entre exigences de sécurité machine traditionnelle et cybersécurité industrielle, **nous proposons un accompagnement complet et sur-mesure** aux fabricants et intégrateurs de machines.

Diagnostic et feuille de route de conformité

Nous commençons par **auditer votre situation actuelle** : analyse de votre portefeuille de machines, évaluation de vos processus de conception, revue de votre documentation existante. Sur cette base, nous élaborons une feuille de route réaliste et priorisée pour atteindre la conformité.

Analyses de risques cyber-physiques

Nos experts mènent des **évaluations approfondies des risques** selon les méthodologies reconnues (ISA/IEC 62443-3-2, EBIOS RM) et adaptées au contexte industriel. Nous identifions les menaces spécifiques à vos machines, évaluons leur criticité et définissons les mesures de protection proportionnées.

Conception sécurisée et durcissement

Nous intervenons directement dans vos **projets de développement** pour intégrer la cybersécurité dès la phase de conception : définition d'architectures sécurisées, sélection de composants robustes, spécification de mécanismes de protection, et durcissement des configurations.

Constitution des dossiers techniques

Nous vous assistons dans la **constitution de la documentation de conformité** : rédaction de l'analyse de risques formelle, compilation du dossier technique, rédaction de la déclaration UE de conformité et enrichissement des notices d'instructions avec les éléments de cybersécurité requis.

Mise en place de PSIRT semi-externalisé

Pour les fabricants ne disposant pas des ressources internes nécessaires, nous proposons un **service de PSIRT semi-externalisé** : veille sur les vulnérabilités, gestion des signalements, évaluation des risques, coordination des correctifs et communication avec les clients.

Formation des équipes

Nous organisons des **sessions de formation sur-mesure** adaptées aux différents profils : sensibilisation des directions, formation technique des ingénieurs de conception, formation opérationnelle des équipes support et maintenance.

Accompagnement au marquage CE cyber

Au-delà du RM, nous accompagnons également nos clients sur le **Cyber Resilience Act** qui introduira prochainement des exigences complémentaires de cybersécurité pour les produits numériques. Notre expertise transversale nous permet d'optimiser vos efforts de conformité sur ces deux réglementations convergentes.

Notre approche combine expertise technique en cybersécurité OT/IoT, connaissance approfondie des référentiels (IEC 62443, ISO 27001) et compréhension des contraintes opérationnelles des industriels. Nous intervenons de la stratégie à l'implémentation opérationnelle, en privilégiant toujours des solutions pragmatiques et proportionnées.

FAQ

Quand le Règlement Machine devient-il obligatoire ?

Le RM s'appliquera obligatoirement à partir du 20 janvier 2027. Toute machine mise sur le marché européen après cette date devra respecter les nouvelles exigences, y compris celles relatives à la cybersécurité.

Mes machines actuellement en service doivent-elles être mises à jour ?

Non, le règlement s'applique uniquement aux machines neuves mises sur le marché après la date d'application. Les machines déjà en service ne sont pas soumises à une obligation de rétroconformité, sauf en cas de modification substantielle qui équivaudrait à une nouvelle mise sur le marché.

Le marquage CE suffit-il à garantir la conformité

Le marquage CE atteste que le fabricant déclare sa machine conforme aux exigences applicables, mais il ne constitue pas une certification par un organisme tiers. Le fabricant reste responsable de la conformité effective de sa machine et doit pouvoir la démontrer via son dossier technique en cas de contrôle.

Quelles normes dois-je appliquer pour être conforme au RM ?

Aucune norme n'est juridiquement obligatoire. Cependant, l'application de normes harmonisées (comme la série IEC 62443 pour la cybersécurité) crée une présomption de conformité et facilite grandement la démonstration. Les normes spécifiques au RM sont en cours d'élaboration par le CEN/CENELEC.

Comment traiter les composants logiciels tiers dans mes machines ?

Vous devez évaluer les risques de cybersécurité liés aux composants logiciels que vous intégrez, y compris ceux développés par des tiers. Cela implique de sélectionner des fournisseurs fiables, de maintenir un inventaire des composants (SBOM), et d'établir un processus pour gérer les vulnérabilités découvertes dans ces composants.

Dois-je créer un PSIRT pour être conforme ?

Le règlement n'impose pas explicitement la création d'un PSIRT (Product Security Incident Response Team), mais il exige un processus de gestion des vulnérabilités post-commercialisation. Un PSIRT est la solution la plus structurée pour répondre à cette obligation, mais des approches plus légères peuvent convenir selon la taille de votre organisation.

Comment s'articulent le RM et le Cyber Resilience Act ?

Ces deux réglementations sont complémentaires. Le RM couvre les machines dans leur globalité avec des exigences de sécurité physique et cyber. Le CRA se concentre sur les produits numériques (matériels et logiciels) avec des exigences de cybersécurité tout au long du cycle de vie. Certains équipements devront respecter les deux textes.

Quelle est la durée de conservation du dossier technique ?

Le dossier technique doit être conservé pendant 10 ans à compter de la mise sur le marché de la machine, ou pendant la durée de vie prévue de la machine si celle-ci est supérieure à 10 ans. Il doit pouvoir être

présenté aux autorités de surveillance en cas de contrôle.

Conclusion

Le Règlement Machine UE 2023/1230 marque une évolution majeure du cadre réglementaire européen, reconnaissant enfin que la cybersécurité n'est plus une option mais une composante essentielle de la sécurité des équipements industriels. En intégrant explicitement les exigences de protection contre les cybermenaces, le RM impose aux fabricants de machines une transformation profonde de leurs pratiques de conception, de documentation et de suivi du cycle de vie.

Au-delà de la simple obligation de conformité, le RM représente une opportunité de renforcer réellement la résilience de vos produits face à un paysage de menaces en constante évolution. Les fabricants qui sauront transformer cette contrainte réglementaire en avantage concurrentiel – en faisant de la cybersécurité un argument de différenciation – seront les mieux positionnés sur un marché européen de plus en plus exigeant.

Chez AKENATECH, nous sommes convaincus que la conformité au Règlement Machine ne doit pas être vécue comme un fardeau administratif, mais comme un levier de création de valeur. Notre mission est de vous accompagner dans cette transformation avec pragmatisme et efficacité, en conjuguant excellence technique et compréhension de vos réalités opérationnelles.

Le compte à rebours a commencé. Le moment d'agir, c'est maintenant.

Mots clés : Règlement Machine, RM 2023/1230, cybersécurité industrielle, marquage CE, conformité machines, IEC 62443, sécurité OT, Industrie 4.0, analyse de risques cyber-physiques, PSIRT