IEC 62443-3-3:2013 Exigences de sécurité système pour l'automatisation industrielle

Sept exigences fondamentales, 51 exigences système

100 exigences. Cette norme peut être certifiée par un organisme accrédité. Version de 07/2026.

La norme IEC 62443-3-3 permet une certification, et ce qui est certifié est un système, ni une organisation ni une personne. Les voies possibles sont ISASecure SSA et le IECEE CB Scheme. Quiconque veut certifier l'organisation a besoin de la 62443-2-1 ou de la 2-4, quiconque vise le composant a besoin de la 62443-4-2. Cette liste contient les 51 exigences système et les 49 améliorations d'exigence. Celles qui s'appliquent dépendent du niveau de sécurité visé : 38 dès le SL 1, 60 dès le SL 2, 90 dès le SL 3, les 100 au SL 4. Aucune amélioration ne s'applique déjà au SL 1. Cette liste est une aide de travail pour l'auto-évaluation, pas une preuve.

Entreprise	Date	Établi par

5 FR 1 : Qui ou quoi demande l'accès, et est-ce vraiment ce que cela prétend être 24

SR 1.1 **Les utilisateurs humains sont identifiés et leur identité est vérifiée avant qu'ils obtiennent l'accès, en tout point où ils peuvent exploiter ou configurer le système d'automatisation. Cela inclut les pupitres opérateur sur la machine, les accès d'ingénierie et les services réseau.**

Comment le prouver: Inventaire de tous les points de connexion du système, c'est-à-dire IHM, salle de contrôle, accès de programmation de l'automate, commutateur, VPN et client de télémaintenance, chacun avec le mécanisme d'authentification utilisé à cet endroit. Ajouter un extrait de configuration ou une capture d'écran de l'écran de connexion pour chaque classe d'appareil. Une petite structure commence avec un tableau par appareil, colonnes : appareil, interface, authentification présente oui ou non, justification si non. Exigé dès le SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 1.1 RE 1 **Chaque utilisateur humain travaille sous un identifiant individuel attribué exclusivement à cette personne. Les comptes partagés et les comptes d'équipe sont désactivés, les exceptions restantes sont justifiées au cas par cas et étayées par des mesures supplémentaires.**

Comment le prouver: Export des comptes par système faisant correspondre l'identifiant à la personne, liste des exceptions avec justification et mesure compensatoire, par exemple une caméra ou un registre de présence au poste opérateur. Cette ligne est une amélioration d'exigence et n'est donc jamais obligatoire au SL 1, elle est exigée dès le SL 2.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 1.1 RE 2 **Quiconque se connecte depuis un réseau non fiable, par exemple depuis internet ou via une connexion de télémaintenance, prouve son identité à l'aide d'au moins deux facteurs indépendants.**

Comment le prouver: Configuration de l'accès distant avec le second facteur activé, un exemple d'enregistrement de connexion montrant les deux facteurs, et la liste d'émission des jetons ou des enregistrements d'application. Une petite structure utilise le second facteur de la passerelle VPN existante ou une application d'authentification, ce qui ne coûte rien au-delà du temps de configuration. Amélioration d'exigence, exigée dès le SL 3, pas au SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 1.1 RE 3 **La preuve par deux facteurs indépendants s'applique non seulement à l'accès depuis l'extérieur, mais à chaque connexion d'un utilisateur humain, y compris les connexions à l'intérieur du réseau classé comme fiable.**

Comment le prouver: Extrait de la politique du service d'authentification central montrant que le second facteur est appliqué sans aucune exemption réseau, plus des exemples d'enregistrements de connexion issus de la salle de contrôle et du pupitre opérateur. Amélioration d'exigence, exigée seulement dès le SL 4.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 1.2 **Non seulement les personnes, mais aussi les processus logiciels et les appareils s'authentifient auprès du système avant d'être autorisés à échanger des données ou à utiliser des services. Cela inclut les couplages entre automates, les liaisons de données vers des systèmes de niveau supérieur et les outils de diagnostic.**

Comment le prouver: Liste des connexions machine à machine avec source, destination, protocole et l'identifiant utilisé dans chaque cas, par exemple certificat, compte de service ou clé pré-partagée. Ajouter un extrait de configuration d'un couplage rendant l'authentification visible. Exigé dès le SL 2, pas exigé au SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.2 RE 1 **Chaque processus logiciel et chaque appareil présente son propre identifiant unique. Les comptes de service partagés ou une clé unique utilisée dans tout le système par de nombreux appareils ne sont pas autorisés.** Document

Comment le prouver: Correspondance entre appareil et identifiant ou numéro de série de certificat montrant qu'aucun identifiant n'apparaît deux fois. Amélioration d'exigence, exigée dès le SL 3 et donc absente du SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.3 **Les comptes sont gérés sur l'ensemble de leur cycle de vie : création, changement de privilèges, désactivation au départ et suppression sont régis par des règles et pris en charge par les systèmes concernés. Cela couvre les comptes utilisateur, les comptes de service et les comptes d'urgence.** Document

Comment le prouver: Registre des comptes avec type, propriétaire, finalité et statut, plus des justificatifs d'arrivée et de départ, par exemple une remise signée ou un ticket montrant la désactivation avec sa date. Une revue périodique des comptes est recommandée, et dans une petite structure un rapprochement annuel de la liste des comptes avec la liste du personnel suffit. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.3 RE 1 **La gestion des comptes est unifiée sur l'ensemble des composants du système, de sorte que la désactivation d'un compte à un endroit ne reste pas sans effet sur des appareils individuels.**

Comment le prouver: Preuve de l'intégration à l'annuaire central, par exemple service d'annuaire ou RADIUS, avec une liste des composants connectés et une liste explicite des appareils qui ne peuvent pas être connectés ensemble avec leur procédure alternative. Enregistrement de test d'une désactivation prenant effet sur tous les systèmes connectés. Amélioration d'exigence, exigée dès le SL 3.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.4 **Les identifiants sont émis selon des règles fixes, attribués sans ambiguïté à une personne, un appareil ou un rôle, retirés lorsqu'ils ne sont plus utilisés et jamais réattribués ultérieurement à un autre titulaire.**

Comment le prouver: Règle de nommage des identifiants, par exemple nom de famille plus initiale ou code de site plus numéro, plus l'historique des identifiants retirés montrant qu'ils ne sont pas réutilisés. Une petite structure tient une liste unique avec date d'émission et date de retrait. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.5 **Les moyens d'authentification tels que mots de passe, clés, certificats et jetons sont émis de manière ordonnée, changés en cas de suspicion de divulgation et révoqués en cas de besoin. Les comptes par défaut et les mots de passe d'usine livrés sont changés avant la mise en service.**

Comment le prouver: Liste d'émission des jetons et certificats avec destinataire et date, preuve des changements et révocations, plus une liste de contrôle de mise en service par appareil avec le point mot de passe d'usine changé, signée. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.5 RE 1 **Les identifiants d'authentification des processus logiciels ne sont pas stockés sous forme de fichier lisible sur le support de stockage, mais dans un stockage protégé par matériel qui empêche la lecture de la partie secrète.**

Comment le prouver: Preuve de type du composant de sécurité utilisé, par exemple TPM, élément sécurisé ou HSM, avec un extrait de configuration prouvant que la clé est stockée à l'intérieur du composant. Un justificatif d'achat ou une fiche technique suffit comme preuve de type. Amélioration d'exigence, exigée dès le SL 3, pas exigée au SL 1 ni au SL 2.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.6 **L'accès sans fil au système, par exemple WLAN, télécommandes radio ou diagnostic Bluetooth, n'est utilisable qu'après identification et authentification de l'utilisateur et de l'appareil, et est géré de manière délibérée.**

Comment le prouver: Inventaire de toutes les liaisons sans fil avec finalité, portée et méthode de chiffrement, extrait de configuration du point d'accès et liste des appareils terminaux approuvés. Une petite structure documente en plus quelles interfaces sans fil des appareils ont été délibérément désactivées. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.6 RE 1 **Chaque accès sans fil doit pouvoir être attribué à un utilisateur spécifique ou à un appareil spécifique, une clé réseau partagée par tous les participants n'est pas suffisante.**

Comment le prouver: Preuve d'une méthode avec identifiants individuels, par exemple authentification WLAN d'entreprise contre un annuaire ou certificats par appareil, plus un journal de connexion montrant l'identifiant individuel. Amélioration d'exigence, exigée dès le SL 2 et donc pas au SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.7 **Partout où des mots de passe sont utilisés, leur force minimale peut être configurée, par exemple longueur minimale et types de caractères requis, et les valeurs configurées s'appliquent à tous les comptes concernés.**

Comment le prouver: Extrait de configuration de la politique de mots de passe par système avec les valeurs réellement définies, par exemple longueur >= 10 caractères et au moins trois types de caractères, plus une liste des systèmes qui ne peuvent techniquement pas prendre en charge ce réglage avec leur mesure compensatoire. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.7 RE 1 **Pour les utilisateurs humains, des règles supplémentaires régissent la génération et la durée de vie des mots de passe : la réutilisation d'anciens mots de passe est empêchée et la validité est limitée dans le temps.**

Comment le prouver: Extrait de configuration montrant l'historique des mots de passe, par exemple réutilisation des cinq derniers mots de passe bloquée, et la validité maximale configurée. Amélioration d'exigence, exigée dès le SL 3.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.7 RE 2 **La limite de durée de vie du mot de passe s'applique non seulement aux personnes, mais à tous les comptes, y compris les comptes de service, de maintenance et d'appareil.**

Comment le prouver: Plan de rotation des comptes techniques avec la date du dernier et du prochain changement par compte, plus preuve des changements, par exemple un enregistrement de changement ou un ticket. Amélioration d'exigence, exigée seulement dès le SL 4.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.8 **Là où des certificats sont utilisés, ils proviennent d'une gestion ordonnée des certificats avec des règles définies pour la demande, l'émission, la période de validité, le renouvellement et la révocation.** Document

Comment le prouver: Politique de certificats ou brève règle écrite indiquant la responsabilité, les périodes de validité et la voie de révocation, plus un inventaire des certificats émis avec leurs dates d'expiration. Une petite structure tient un tableau avec certificat, appareil, date d'expiration et date de rappel, ce qui évite les arrêts de production silencieux causés par des certificats expirés. Exigé dès le SL 2.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.9 **Lorsque des paires de clés sont utilisées pour l'authentification, le système valide le certificat intégralement : chaîne de confiance, période de validité, statut de révocation et preuve que la contrepartie possède réellement la clé privée. Le lien entre certificat et compte est sans ambiguïté.**

Comment le prouver: Extrait de configuration avec vérification de révocation activée, par exemple CRL ou OCSP, enregistrement de test d'une connexion rejetée avec un certificat expiré ou révoqué, plus le tableau de correspondance entre certificat et compte. Exigé dès le SL 3, pas exigé au SL 1 ni au SL 2.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.9 RE 1 **Les clés privées résident exclusivement dans un stockage protégé par matériel dont elles ne peuvent pas être extraites, et elles sont également utilisées à l'intérieur de ce stockage.**

Comment le prouver: Fiche technique ou preuve de certification du composant de sécurité utilisé et un extrait de configuration montrant que la clé est générée à l'intérieur du composant, de sorte que la clé privée ne le quitte jamais. Amélioration d'exigence, exigée seulement dès le SL 4.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.10 **Pendant la connexion, le système ne révèle aucune information exploitable. Les mots de passe saisis sont masqués et les messages d'erreur ne révèlent pas si l'identifiant ou le mot de passe était incorrect.**

Comment le prouver: Capture d'écran de l'écran de connexion avec saisie masquée et capture d'écran du message d'erreur après une tentative échouée. Pour les appareils qui ne peuvent techniquement pas le faire, par exemple d'anciens pupitres opérateur, ajouter une brève note sur la mesure compensatoire, par exemple un accès physique restreint au site de l'installation. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.11 **Le nombre de tentatives de connexion échouées consécutives est limité et la réponse à cela est configurable, par exemple un verrouillage temporaire. La réponse choisie n'entrave pas l'exploitation liée à la sécurité de l'installation.**

Comment le prouver: Extrait de configuration avec le seuil, par exemple verrouillage après <= 5 tentatives échouées, et la durée de verrouillage, plus une brève évaluation expliquant pourquoi le verrouillage n'empêche pas l'exploitation d'urgence ni un arrêt sûr de l'installation. Sur les postes opérateur avec fonction de sécurité, un verrouillage temporisé est préférable à un blocage de compte permanent. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.12 **Un avis d'utilisation peut être affiché avant la connexion, renvoyant aux règles d'utilisation et de surveillance du système. Le texte et son affichage sont configurables par le propriétaire de l'actif.**

Comment le prouver: Capture d'écran du texte d'avis affiché et le libellé approuvé avec la date d'approbation. Les petites structures conviennent brièvement du libellé avec la représentation du personnel ou avec la direction, un paragraphe suffit. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.13 **L'accès depuis des réseaux non fiables, par exemple la télémaintenance par des fournisseurs, est restreint à des chemins définis, est surveillé et peut être interrompu à tout moment.**

Comment le prouver: Inventaire des chemins d'accès distant avec finalité, partie distante, personne de contact et le chemin utilisé, plus des journaux de connexion et une preuve de la capacité de déconnexion, par exemple un interrupteur à clé, une règle de pare-feu ou un routeur de télémaintenance pouvant être coupé. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 1.13 RE 1 **Chaque session individuelle depuis un réseau non fiable est explicitement approuvée par une personne responsable avant l'établissement de la connexion, une connexion ouverte en permanence n'est pas suffisante.**

Comment le prouver: Enregistrements d'approbation par session de télémaintenance avec heure, motif, personne approbatrice et durée, techniquement par exemple via un interrupteur à clé sur le routeur d'accès ou via un portail d'approbation. Dans une petite structure, un cahier de télémaintenance à l'armoire de commande, signé par le technicien de maintenance pour chaque session, suffit. Amélioration d'exigence, exigée dès le SL 2 et donc jamais au SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

6 FR 2 : Contrôle d'utilisation (privilèges, sessions, journaux d'audit) 24

SR 2.1 **Le système applique techniquement les privilèges qui ont été accordés : chaque personne connectée, chaque appareil et chaque processus logiciel reçoit exactement l'accès qui lui a été attribué, et toute tentative allant au-delà est rejetée.**

Comment le prouver: Un concept de privilèges faisant correspondre les comptes aux permissions, plus une capture d'écran ou un extrait de configuration par système de contrôle, IHM et poste d'ingénierie montrant les privilèges actifs. En plus, un enregistrement de test dans lequel un compte à faibles privilèges tente une action bloquée et est rejeté. Exigé dès le SL 1. Une petite structure se gère avec deux ou trois rôles, par exemple exploiter, entretenir, concevoir, et les documente sur une seule page.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.1 RE 1 **L'application des privilèges concerne non seulement les opérateurs humains, mais également les processus logiciels et les appareils qui accèdent au système par eux-mêmes.**

Comment le prouver: Une liste des comptes techniques et de service, par exemple clients OPC UA, connexions historian, services de sauvegarde, chacun avec son ensemble de privilèges attribué. Un extrait de la gestion des privilèges montrant que ces comptes ne fonctionnent pas avec des droits d'administrateur. Amélioration d'exigence, exigée dès le SL 2, pas au SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.1 RE 2 **Les privilèges ne sont pas accordés aux personnes individuellement mais via des rôles, et la correspondance entre rôle et actions autorisées est consignée de manière traçable.** Document

Comment le prouver: Une matrice de rôles et privilèges sous forme de tableau : les lignes sont les rôles, les colonnes les actions telles que changer une consigne, télécharger un programme, acquitter une alarme, créer un compte. Plus la liste de correspondance entre personne et rôle. Amélioration d'exigence, exigée dès le SL 2. Un tableur tenu à jour portant une date de modification constitue une preuve tout à fait suffisante.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.1 RE 3 **Pour des cas exceptionnels strictement définis, un superviseur autorisé peut lever une restriction de privilège pour une durée limitée, et chacune de ces dérogations est consignée dans la piste d'audit.**

Comment le prouver: Une description de la procédure d'approbation des exceptions indiquant qui peut l'accorder et pendant combien de temps elle reste valable, plus des enregistrements d'audit des dérogations déjà accordées, extraits du journal système. Amélioration d'exigence, exigée dès le SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.1 RE 4 **Les interventions particulièrement critiques nécessitent l'approbation de deux personnes autorisées indépendantes avant l'exécution de l'action.**

Comment le prouver: Une liste des actions soumises à double approbation, par exemple modifier des paramètres de sécurité ou télécharger un nouveau programme de contrôle, avec une preuve de configuration et des enregistrements d'audit nommant les deux approbateurs. Amélioration d'exigence, exigée seulement dès le SL 4.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.2 **L'utilisation de connexions sans fil dans le réseau d'automatisation est liée à une autorisation explicite, et seuls les participants approuvés peuvent échanger des données ou intervenir sans fil.**

Comment le prouver: Un inventaire de toutes les liaisons sans fil, par exemple points d'accès WLAN, appairages Bluetooth, routeurs cellulaires, chacun avec sa finalité et ses participants approuvés. Plus la configuration du contrôle d'accès au point d'accès. Exigé dès le SL 1. Quiconque n'exploite aucune liaison sans fil dans le réseau de process le déclare exactement par écrit et l'étaye par une vue de configuration montrant le sans fil désactivé.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.2 RE 1 **Les appareils sans fil non autorisés à proximité du réseau d'automatisation sont détectés et signalés.**

Comment le prouver: Un enregistrement de la surveillance sans fil ou d'un balayage sans fil périodique avec date, liste de résultats et une note sur chaque appareil inconnu. La voie de signalement à la fonction responsable est nommée. Amélioration d'exigence, exigée dès le SL 2, pas au SL 1. Une petite structure peut effectuer un balayage trimestriel avec un ordinateur portable et archiver le résultat comme enregistrement.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.3 **L'utilisation d'appareils portables et mobiles sur le système, par exemple ordinateurs portables de service, stockage USB ou tablettes, est régie par des règles et techniquement limitée aux appareils explicitement approuvés.**

Comment le prouver: L'ensemble des règles d'utilisation des appareils, une liste des appareils de service approuvés avec leurs identifiants, et une preuve de la restriction technique, par exemple ports USB désactivés ou limités à des appareils spécifiques sur l'IHM et le poste d'ingénierie. Exigé dès le SL 1. Une petite structure travaille avec deux clés de service étiquetées qui ne sont écrites que sur une seule station de transfert.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.3 RE 1 **Avant la connexion, l'état de sécurité d'un appareil portable ou mobile est vérifié, et les appareils qui ne répondent pas aux exigences se voient refuser l'accès.**

Comment le prouver: Les critères de vérification de l'état de l'appareil, par exemple protection antimalware actualisée et niveau de correctifs, plus des enregistrements de vérification par appareil de service et une preuve de l'application technique, par exemple via une station de transfert ou un contrôle d'accès réseau. Amélioration d'exigence, exigée dès le SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.4 **Pour le code mobile exécuté sur le système, par exemple des scripts dans les interfaces opérateur ou du contenu actif dans des rapports, il est défini quels types sont autorisés, et les types non autorisés sont empêchés de s'exécuter.** Document

Comment le prouver: Une définition de quel code mobile est autorisé sur quels systèmes, plus une preuve de configuration de la restriction, par exemple exécution de scripts désactivée dans le navigateur IHM, macros bloquées dans les fichiers d'évaluation. Exigé dès le SL 1. Une définition d'une page couvrant les trois ou quatre cas réellement existants suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.4 RE 1 **Avant l'exécution du code mobile, il est vérifié qu'il provient de la source attendue et n'a pas été altéré.**

Comment le prouver: Preuve de configuration de la vérification de signature ou du contrôle de somme de contrôle, plus un enregistrement de test dans lequel du code manipulé ou non signé est rejeté. Amélioration d'exigence, exigée dès le SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.5 **Une session est verrouillée après une période définie sans action de l'opérateur et n'est libérée à nouveau qu'après une nouvelle authentification, sans perdre l'affichage des informations de process pertinentes pour la sécurité.**

Comment le prouver: Un extrait de configuration avec le temps de verrouillage configuré par poste de travail, plus une justification pour les postes de travail dans des salles de contrôle en permanence occupées où le verrouillage est délibérément réglé différemment. Exigé dès le SL 1. Preuve visuelle : une capture d'écran de l'écran de verrouillage avec la ligne d'alarme encore visible.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.6 **Les sessions distantes sont terminées après une période définie sans activité ou à la demande de l'opérateur, de sorte qu'aucune connexion distante ouverte ne reste sans surveillance.**

Comment le prouver: La configuration d'accès distant avec sa limite de temps d'inactivité, des enregistrements d'audit des sessions distantes terminées, et une description de la manière dont l'opérateur peut immédiatement déconnecter une session de télémaintenance en cours, par exemple via un interrupteur à clé ou une libération par session. Exigé dès le SL 2, pas au SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.7 **Le nombre de sessions simultanées par compte ou par rôle est limité, et les tentatives de connexion au-delà de cette limite sont rejetées.**

Comment le prouver: Un extrait de configuration avec la limite supérieure définie par rôle, par exemple <= 1 session simultanée pour les comptes d'ingénierie, plus un enregistrement de test de la seconde tentative de connexion rejetée. Exigé dès le SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.8 **Les événements pertinents pour la sécurité sont enregistrés, et chaque entrée indique au moins l'heure, la source, le compte à l'origine, le type d'événement et le résultat.** Document

Comment le prouver: Une définition des types d'événements à enregistrer, par exemple connexion, connexion échouée, changement de privilège, changement de programme, changement de configuration, plus un extrait réel du journal d'audit montrant les champs nommés. Exigé dès le SL 1. Une petite structure rassemble les journaux du système de contrôle, de l'IHM et du pare-feu dans un dossier avec une période de rétention fixe.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.8 RE 1 **Les journaux d'audit des différents composants sont rassemblés en un point central et forment un journal unique à l'échelle du système, qui peut être évalué dans son ensemble.**

Comment le prouver: Un schéma d'architecture de la collecte des journaux montrant toutes les sources connectées, plus une évaluation plaçant des événements d'au moins deux composants sur une même ligne temporelle. Amélioration d'exigence, exigée dès le SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.9 **Un stockage suffisant est prévu pour les journaux d'audit afin que les événements soient conservés pendant la période de rétention définie et ne soient pas écrasés involontairement.**

Comment le prouver: Un calcul ou une estimation du besoin de stockage à partir du volume quotidien de journaux multiplié par la période de rétention, plus la taille de stockage configurée et la règle d'archivage. Exigé dès le SL 1. En pratique, une copie quotidienne vers un emplacement de stockage séparé avec une période de rétention documentée suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.9 RE 1 **Lorsqu'un seuil défini de niveau de remplissage du stockage d'audit est atteint, un avertissement est émis à la fonction responsable avant que la capacité de stockage ne soit entièrement épuisée.**

Comment le prouver: Un extrait de configuration du seuil, par exemple un avertissement à partir de >= 80 pour cent d'utilisation, plus un exemple de la notification déclenchée et la liste des destinataires. Amélioration d'exigence, exigée dès le SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 2.10 **Si la journalisation d'audit échoue ou si le stockage d'audit est saturé, le système réagit d'une manière définie au préalable et la fonction responsable en est informée, sans mettre en danger l'exploitation sûre de l'installation.**

Comment le prouver: La réaction définie pour chaque cas de défaillance, par exemple écraser les entrées les plus anciennes et déclencher une notification plutôt que d'arrêter l'installation, avec une justification du point de vue du process. Preuve via une notification de test déclenchée et l'entrée d'audit correspondante. Exigé dès le SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 2.11 **Chaque enregistrement d'audit porte un horodatage provenant d'une source de temps nommée, de sorte que les événements de différents composants puissent être classés les uns par rapport aux autres.**

Comment le prouver: Une indication de la source de temps utilisée par composant et un extrait de journal avec un horodatage visible incluant le fuseau horaire. Exigé dès le SL 2, pas au SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 2.11 RE 1 **Les horloges de tous les composants participants sont synchronisées sur une source de temps commune de sorte que l'écart reste dans une limite définie.**

Comment le prouver: La configuration de synchronisation temporelle, par exemple serveur NTP et intervalle de synchronisation, plus un enregistrement de vérification avec l'écart mesuré par composant par rapport à la limite définie, par exemple <= 1 seconde. Amélioration d'exigence, exigée dès le SL 3.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 2.11 RE 2 **La source de temps elle-même est protégée contre la manipulation, et une référence temporelle invraisemblable ou altérée est détectée et signalée.**

Comment le prouver: Une description de la manière dont la source de temps est protégée, par exemple synchronisation temporelle authentifiée, restriction à une source interne, surveillance des sauts de temps, plus des notifications ou enregistrements d'audit d'un écart détecté. Amélioration d'exigence, exigée seulement dès le SL 4.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 2.12 **Pour des actions critiques définies, il peut être établi sans aucun doute a posteriori qui les a déclenchées, de sorte que la personne ayant agi ne puisse pas nier de manière crédible l'avoir fait.** Document

Comment le prouver: Une liste des actions auxquelles s'applique cette preuve, par exemple changement de recette, libération de lot, changement de valeurs limites, plus les enregistrements correspondants avec un identifiant de personne unique et une preuve que les comptes de groupe sont exclus pour ces actions. Exigé dès le SL 3.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 2.12 RE 1 **L'attribution incontestable de la personne ayant agi s'applique non seulement à des actions critiques sélectionnées, mais à tous les utilisateurs et à toutes les actions qu'ils déclenchent.**

Comment le prouver: Preuve que chaque compte est lié à une seule personne et qu'il ne subsiste aucune connexion partagée, plus un extrait de journal d'actions quelconques dans lequel un identifiant de personne unique apparaît de façon constante. Amélioration d'exigence, exigée seulement dès le SL 4.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

7 FR 3 : Intégrité du système, protection des données, des logiciels et des sessions contre toute modification non autorisée 19

SR 3.1 **Le système de contrôle détecte lorsque des informations ont été altérées en transit sur un canal de communication, et ce aussi bien pour les données de contrôle que pour les données de configuration et le trafic de gestion. La protection couvre également les connexions qui quittent le système ou qui traversent des segments réseau non fiables.**

Comment le prouver: Une vue d'ensemble réseau et protocoles indiquant quel canal utilise quel mécanisme d'intégrité (somme de contrôle, code d'authentification de message, télégrammes signés), un extrait de configuration des paramètres de sécurité du bus de terrain ou d'OPC UA, et un enregistrement de test montrant qu'un télégramme altéré a été rejeté de manière démontrable. Une petite structure consigne cela dans un tableau par connexion avec les colonnes source, destination, protocole et mécanisme d'intégrité, et démontre l'efficacité une fois avec une capture de trafic. Exigé à partir du SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.1 RE 1 **La protection de l'intégrité en transit s'appuie sur des mécanismes cryptographiques, de sorte qu'une manipulation délibérée par un attaquant utilisant ses propres moyens ne puisse pas passer inaperçue. Une simple somme de contrôle contre les erreurs de transmission n'est pas suffisante ici.**

Comment le prouver: Une liste des mécanismes cryptographiques et longueurs de clé utilisés par canal, une référence à la gestion de clés sous-jacente, et des extraits de configuration (par exemple suites de chiffrement TLS, SecurityPolicy OPC UA, profils IPsec). Les petites structures s'appuient sur les profils sécurisés par défaut de leurs automates et archivent une capture d'écran du réglage actif. Amélioration d'exigence, exigée à partir du SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.2 **Des mécanismes de protection contre les codes malveillants sont en place, empêchant l'exécution de code de programme indésirable sur les composants du système et signalant toute détection. Les mécanismes sont choisis de manière à ne pas perturber le fonctionnement prévu de l'installation, et ils sont maintenus à jour.**

Comment le prouver: Une vue d'ensemble par composant du mécanisme applicable (antivirus, liste blanche d'applications, système d'exploitation durci sans droits d'exécution), preuve que les signatures ou listes blanches sont mises à jour, et alertes du système de protection. Lorsque l'antivirus n'est pas réalisable, par exemple sur un automate, la mesure compensatoire est consignée avec sa justification. Les petites structures s'en sortent bien avec une liste blanche sur le PC opérateur et une règle écrite pour les supports USB. Exigé à partir du SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.2 RE 1 **La protection contre les codes malveillants s'applique en outre aux points d'entrée et de sortie de l'installation, là où les données entrent ou sortent, et pas uniquement sur les appareils terminaux eux-mêmes.**

Comment le prouver: Une liste de tous les points d'entrée et de sortie (accès de télémaintenance, passerelle de transfert de données, supports amovibles, transfert vers le réseau bureautique, voie de courrier électronique pour les versions de programme) avec le mécanisme d'analyse effectif à chacun, plus des enregistrements des transferts contrôlés. Les petites structures mettent en place un unique PC de transfert avec analyse antivirus comme passerelle et le fixent dans une instruction de travail. Amélioration d'exigence, exigée à partir du SL 2.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.2 RE 2 **Les mécanismes de protection contre les codes malveillants sont gérés depuis un point central, les mises à jour sont distribuées de manière centralisée, et les détections sont rassemblées en un seul endroit pour évaluation.**

Comment le prouver: La configuration de la console de gestion centrale, un rapport sur l'état de mise à jour de tous les composants connectés, et une évaluation des détections signalées sur une période donnée. Amélioration d'exigence, exigée à partir du SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.3 **Les fonctions de sécurité du système sont vérifiées à intervalles planifiés et après des changements pour confirmer qu'elles fonctionnent réellement. Les tests sont programmés de manière à ne pas mettre en danger le fonctionnement de l'installation, et les résultats sont consignés.**

Document

Comment le prouver: Un plan de test indiquant l'objet du test, l'intervalle et la fenêtre de temps, ainsi que les enregistrements de test montrant date, testeur, comportement attendu et comportement observé. Des tests individuels utiles sont : une connexion avec un compte désactivé échoue, l'antivirus réagit à un fichier de test, l'accès de télémaintenance est inaccessible sans autorisation. Les petites structures associent les tests à l'arrêt de maintenance déjà planifié et travaillent avec une liste de contrôle fixe. Exigé à partir du SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.3 RE 1 **La vérification des fonctions de sécurité s'exécute avec des moyens automatisés, de sorte qu'elle soit reproductible sans effort manuel et fournisse un résultat cohérent.**

Comment le prouver: Les scripts ou outils de test avec leur calendrier, leurs fichiers de sortie, et une comparaison de plusieurs exécutions montrant que les écarts sont détectés. Amélioration d'exigence, exigée à partir du SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.3 RE 2 **La vérification des fonctions de sécurité est également possible pendant le fonctionnement normal, sans devoir arrêter l'installation ni la placer dans un état particulier.**

Comment le prouver: Une description de la procédure de test avec preuve qu'elle n'a pas d'effet négatif sur le process, par exemple une analyse de l'impact sur les temps de cycle et la charge réseau, plus des enregistrements de test issus de l'exploitation productive. Amélioration d'exigence, exigée à partir du SL 4.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.4 **Les modifications non autorisées du logiciel, du micrologiciel et des informations au repos sont détectées. Cela s'applique également aux programmes de contrôle, aux jeux de paramètres, aux recettes et aux fichiers de configuration.**

Comment le prouver: Un inventaire des versions à protéger avec les valeurs de contrôle ou signatures stockées, les résultats des comparaisons d'intégrité, et le rapprochement documenté avec la version tenue dans le contrôle de versions. Les petites structures stockent la version de programme validée avec sa somme de contrôle dans un emplacement protégé en écriture et comparent en cas de suspicion ou après maintenance. Exigé à partir du SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.4 RE 1 **Si une violation de l'intégrité du logiciel ou de l'information est détectée, le système le signale automatiquement à un point responsable, sans que personne n'ait à le rechercher activement.**

Comment le prouver: La configuration des voies de notification (alarme en salle de contrôle, courrier électronique, message au système de surveillance), une liste de destinataires avec dispositions de suppléance, et au moins une alarme de test avec un temps de réponse documenté. Amélioration d'exigence, exigée à partir du SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.5 **Les entrées que le système accepte à partir de données de process, d'interfaces ou d'interfaces utilisateur sont vérifiées quant à la syntaxe autorisée, la plage de valeurs autorisée et la longueur autorisée avant d'être traitées. Les entrées invalides n'entraînent pas de comportement incontrôlé.**

Comment le prouver: Une spécification des limites et formats par entrée, des extraits de la logique de validation dans l'automate ou l'application, et des cas de test avec des entrées délibérément invalides (une valeur trop grande, un type de donnée erroné, une chaîne de caractères trop longue) ainsi que le comportement documenté du système. Les petites structures consignent les limites de plausibilité par point de mesure dans un tableau et les vérifient lors de la mise en service. Exigé à partir du SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.6 **Pour le cas d'une défaillance, il est défini quel état les sorties vers l'installation adoptent, et le système adopte exactement cet état. L'état défini est aligné sur la sécurité fonctionnelle de l'installation.**

Comment le prouver: Une définition par sortie ou groupe de sorties (maintenir la valeur, valeur de substitution définie, état d'arrêt sûr) avec une justification issue de l'évaluation des risques, un extrait de configuration de l'automate, et une preuve issue d'un test de défaillance, par exemple une rupture de câble ou une perte de communication, montrant le comportement attendu. Exigé à partir du SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.7 **Le système gère les conditions d'erreur de manière à ce que l'exploitation reste maîtrisée et qu'aucune information susceptible d'aider un attaquant ne soit divulguée. Les messages d'erreur affichés aux opérateurs restent brefs, tandis que les détails techniques ne vont que dans les enregistrements internes.**

Comment le prouver: Une vue d'ensemble des classes d'erreur avec le comportement système prévu pour chacune, des exemples des messages affichés comparés aux entrées de journal internes correspondantes, et une preuve de test qu'aucun chemin de fichier, nom de compte, sortie de base de données ou détail de version n'apparaît sur l'interface opérateur. Exigé à partir du SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.8 **Les sessions actives sont protégées contre le détournement et contre l'injection de messages étrangers. Une session se termine après déconnexion ou après une période définie sans activité, et ne peut plus ensuite être réutilisée.**

Comment le prouver: La configuration de la gestion de session avec les limites configurées pour le temps d'inactivité et la durée maximale, une preuve du mécanisme protégeant contre la rejouabilité des messages, et un enregistrement de test dans lequel une session capturée ne fonctionne plus après déconnexion. Exigé à partir du SL 2.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.8 RE 1 **Les identifiants de session perdent leur validité lorsque la session se termine et ne sont plus acceptés par le système, même s'ils sont présentés à nouveau depuis l'extérieur.**

Comment le prouver: Un extrait de configuration de la gestion de session couvrant l'invalidation, plus un enregistrement de test dans lequel un identifiant précédemment valide est renvoyé après déconnexion et rejeté par le système. Amélioration d'exigence, exigée à partir du SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.8 RE 2 **Pour chaque nouvelle session, un identifiant dédié à usage unique est généré. Les identifiants ne sont pas réutilisés entre sessions, utilisateurs ou appareils.**

Comment le prouver: Une description de la procédure de génération et une preuve issue du journal ou d'une capture de trafic que plusieurs connexions consécutives reçoivent des identifiants différents. Amélioration d'exigence, exigée à partir du SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.8 RE 3 **Les identifiants de session sont générés avec des mécanismes aléatoires reconnus, de sorte qu'ils ne puissent être ni devinés ni dérivés d'identifiants précédents.**

Comment le prouver: Une indication du générateur de nombres aléatoires utilisé et de sa source d'entropie, une déclaration du fournisseur ou un rapport de test à ce sujet, et une évaluation statistique d'un échantillon d'identifiants générés. Amélioration d'exigence, exigée à partir du SL 4.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 3.9 **Les enregistrements liés à la sécurité et les outils utilisés pour les évaluer sont protégés contre l'accès, la modification et la suppression non autorisés. Le cercle des personnes autorisées à modifier ou supprimer des enregistrements est restreint et nommé.** Document

Comment le prouver: Un concept d'autorisation pour les données de journal avec attribution nominative, la configuration du transfert vers un système de journalisation séparé, des périodes de rétention, et une preuve de test qu'un opérateur ordinaire ne peut pas supprimer d'entrées. Les petites structures transfèrent les journaux vers un appareil séparé auquel les exploitants de l'installation n'ont pas d'accès en écriture. Exigé à partir du SL 2.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 3.9 RE 1 **Les enregistrements liés à la sécurité sont en outre stockés sur un support excluant toute réécriture ultérieure, de sorte qu'une entrée déjà écrite ne puisse plus être modifiée, même avec des droits administratifs.** Document

Comment le prouver: Une description du stockage utilisé (support à écriture unique, archive résistante à la falsification, chaîne de signatures étendue en continu), une preuve d'une tentative infructueuse de modifier une entrée, et la règle de conservation et de récupération des supports. Amélioration d'exigence, exigée à partir du SL 3.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8 FR 4 : Confidentialité des données 6

SR 4.1 **Le système d'automatisation protège les informations confidentielles contre la divulgation non autorisée, aussi bien en transit qu'au repos. Il est défini quelles données comptent comme confidentielles, par exemple recettes, jeux de paramètres, identifiants d'authentification, fichiers de configuration ou données de diagnostic à caractère personnel.** Document

Comment le prouver: Une liste des types de données à protéger, indiquant où elles sont conservées et comment elles sont transmises, plus la mesure de protection spécifique pour chaque entrée, par exemple une connexion chiffrée, un support de stockage chiffré ou un partage restreint. Une petite structure se contente d'un tableau d'une page : type de donnée, où elle se trouve, qui peut la voir, ce qui la protège. Exigé à partir du SL 1.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 4.1 RE 1 **Pour les informations qui circulent sur des réseaux non fiables ou sont stockées hors de l'environnement protégé, la confidentialité est imposée par des moyens techniques et non simplement promise par une règle organisationnelle.**

Comment le prouver: Un extrait de configuration du chiffrement de transport ou de stockage utilisé, par exemple le profil VPN pour la télémaintenance, les paramètres TLS de l'interface du système de contrôle, ou le chiffrement des supports de sauvegarde. Une capture d'écran datée du réglage actif suffit comme preuve. Exigé à partir du SL 2, pas à partir du SL 1, car il s'agit d'une amélioration d'exigence.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 4.1 RE 2 **La confidentialité est également imposée aux limites entre zones, de sorte que l'information ne devienne pas visible en clair lorsqu'elle passe d'une zone à une autre.**

Comment le prouver: Un plan de zones et conduits marquant les franchissements chiffrés, avec la configuration du composant de frontière tel qu'une passerelle, un pare-feu ou une diode de données. Une capture de trafic ou un enregistrement de test montrant qu'aucune donnée en clair n'apparaît à la frontière. Exigé à partir du SL 4.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

SR 4.2 **Il est défini comment l'information confidentielle est supprimée de manière fiable lorsque des appareils sont mis hors service, changent de propriétaire, partent en réparation ou sont réutilisés, de sorte qu'aucune donnée résiduelle lisible ne subsiste.** Document

Comment le prouver: Une procédure de mise hors service écrite avec la méthode d'assainissement par type d'appareil, plus des enregistrements d'effacement indiquant l'identification de l'appareil, la date et la personne l'ayant réalisé. Une petite structure consigne cela comme une ligne par appareil dans une liste partagée et archive à côté les certificats des prestataires externes d'élimination. Exigé à partir du SL 2.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 4.2 RE 1 **Les zones de stockage partagées sont purgées avant d'être réattribuées à un autre utilisateur ou processus, de sorte que le contenu appartenant à l'utilisateur précédent ne puisse pas être lu.**

Comment le prouver: Une déclaration du fournisseur ou un enregistrement de configuration couvrant la purge des zones de mémoire et de tampon réutilisées, complété par un enregistrement de test issu de la réception ou de la maintenance. Lorsqu'un composant ne peut pas le faire, la mesure compensatoire documentée sert de preuve, par exemple ne pas partager l'appareil entre différents rôles. Exigé à partir du SL 3, pas à partir du SL 1, car il s'agit d'une amélioration d'exigence.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 4.3 **Partout où la cryptographie est utilisée, les algorithmes, longueurs de clé et gestion des clés suivent les bonnes pratiques reconnues, et il est défini comment les clés sont générées, distribuées, stockées, tournées et révoquées.** Document

Comment le prouver: Une vue d'ensemble des mécanismes utilisés par système, indiquant algorithme, longueur de clé et période de validité, plus les règles de gestion des clés et des enregistrements des rotations de clés et renouvellements de certificats. Les recommandations publiques servent de référence, par exemple les guides techniques du BSI allemand. Une petite structure tient une liste de certificats avec dates d'expiration et un rappel >= 30 jours avant échéance. Exigé à partir du SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9 FR 5 : Flux de données restreint, zones et conduits 11

SR 5.1 **Le système de contrôle peut être partitionné en zones séparées, et le trafic entre ces zones ne passe que par des conduits définis. Le partitionnement suit une logique explicable, par exemple selon le besoin de protection, la propriété ou la fonction des sections d'installation concernées.** Document

Comment le prouver: Schéma réseau montrant les zones et les conduits entre elles, une liste de zones avec la logique de chaque frontière, et la configuration des composants de séparation tels que définitions VLAN ou interfaces de pare-feu. Une petite structure se contente d'un schéma d'une page montrant bureau, réseau machine et accès distant comme trois cases avec les liaisons entre elles, plus une capture d'écran de la configuration VLAN du commutateur.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.1 RE 1 **La séparation des zones est mise en œuvre physiquement, c'est-à-dire via des composants réseau dédiés et un câblage dédié, et ne repose pas uniquement sur une configuration logique à l'intérieur d'appareils partagés. Article 9.1 de cette liste, exigé à partir du SL 2. Les améliorations d'exigence de cette norme ne sont jamais obligatoires dès le SL 1.**

Comment le prouver: Inventaire des composants réseau indiquant quel commutateur ou routeur dessert quelle zone, photos ou plan d'armoire des distributions séparées, étiquetage des câbles. Les petites structures en apportent la preuve avec deux commutateurs séparés, clairement étiquetés, au lieu d'un appareil unique partagé et une photo de l'armoire de commande dans la documentation de l'installation.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.1 RE 2 **Le réseau d'automatisation peut fonctionner indépendamment des réseaux extérieurs à l'automatisation. Si l'informatique de bureau ou une liaison externe tombe en panne, le contrôle et la surveillance de l'installation continuent de fonctionner. Exigé à partir du SL 3.**

Comment le prouver: Liste des dépendances des services utilisés à l'intérieur du réseau d'automatisation tels que serveur de temps, résolution de noms, service d'annuaire ou serveur de licences, indiquant où chacun est hébergé, avec un enregistrement de test d'un essai de déconnexion dans lequel la liaison avec l'informatique de bureau a été coupée. Une petite structure note le résultat d'un tel essai dans le journal de maintenance : liaison montante coupée, l'installation a continué de fonctionner, seuls les rapports du bureau manquaient.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.1 RE 3 **Les zones abritant des fonctions particulièrement critiques, par exemple des fonctions de sécurité ou de protection, sont séparées des autres zones à la fois logiquement et physiquement. Exigé à partir du SL 4.**

Comment le prouver: Marquage des zones critiques dans le schéma de zones avec la justification du classement, preuve de composants réseau dédiés et de câblage dédié pour ces zones, configuration des conduits avec preuve qu'aucun chemin partagé n'existe.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.2 **Aux frontières de zone, le trafic est contrôlé, surveillé et soit autorisé soit refusé selon des règles définies. Il n'existe aucun chemin entre deux zones qui contourne ce point de contrôle.**

Comment le prouver: Ensemble de règles exporté du pare-feu ou du dispositif de frontière, journaux des connexions refusées et autorisées, preuve qu'il n'existe aucun chemin latéral, par exemple via une vérification de cartes réseau supplémentaires, de modems ou de routeurs cellulaires dans les ordinateurs d'installation. Une petite structure en apporte la preuve avec l'export de règles de son pare-feu unique et une brève note de vérification confirmant qu'aucun routeur non planifié ne se trouve dans une armoire de commande.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.2 RE 1 **L'ensemble de règles à la frontière de zone fonctionne selon le principe que tout est refusé sauf ce qui a été explicitement autorisé. Chaque règle d'autorisation est justifiée individuellement et liée à une finalité. Exigé à partir du SL 2.**

Comment le prouver: Ensemble de règles avec une règle finale visible qui rejette le reste, et une liste d'autorisations indiquant source, destination, service, finalité et personne responsable pour chaque règle. Les petites structures tiennent cette liste comme un tableau à cinq colonnes à côté de l'export du pare-feu et la révisent une fois par an pour repérer les règles dont plus personne n'a besoin.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.2 RE 2 **Le réseau d'automatisation peut être délibérément coupé de toutes les connexions externes et maintenu en fonctionnement en mode îlot. L'action peut être déclenchée sans devoir arrêter l'installation. Exigé à partir du SL 3.**

Comment le prouver: Description de la procédure d'isolement indiquant qui peut la déclencher et comment, preuve de la mise en œuvre technique telle qu'un ensemble de règles d'urgence ou un interrupteur d'isolement étiqueté, plus l'enregistrement d'un exercice dans lequel l'isolement a réellement été mis en pratique. Une petite structure réalise l'exercice une fois par an pendant la maintenance et note date, durée et tout élément inhabituel.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.2 RE 3 **Si l'appareil à la frontière de zone tombe en panne ou perd ses règles, il refuse le trafic au lieu de le laisser passer. Une panne ne doit pas laisser derrière elle une connexion ouverte. Exigé à partir du SL 4.**

Comment le prouver: Déclaration du fournisseur ou preuve de configuration sur le comportement du composant en cas de panne et au redémarrage, enregistrement de test d'une panne délibérément provoquée avec le résultat observé, alignement avec l'évaluation des risques de l'installation, car une frontière qui refuse le trafic peut elle-même avoir des conséquences selon le process.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.3 **Les services généraux de communication de personne à personne tels que courrier électronique, messagerie ou appels vidéo peuvent être empêchés sur les appareils d'automatisation et à l'intérieur des réseaux d'automatisation. L'étendue du blocage est définie et justifiée.**

Comment le prouver: Définition des services non autorisés dans le réseau d'automatisation, plus la mise en œuvre technique : ports et destinations bloqués dans l'ensemble de règles, applications supprimées ou bloquées sur les postes opérateur, preuve issue de l'inventaire logiciel des appareils. Une petite structure résout cela avec un blocage d'applications sur le poste IHM et une règle refusant le trafic de courrier et web sortant depuis le réseau machine.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.3 RE 1 **Ces services de communication de personne à personne sont empêchés sur l'ensemble du réseau d'automatisation, et non simplement restreints en partie ou limités à des appareils individuels. Exigé à partir du SL 2.**

Comment le prouver: Preuve que le blocage s'applique à chaque appareil de la zone, par exemple via une revue du logiciel installé sur chaque ordinateur de la zone et un test de connexion depuis un ordinateur d'installation quelconque. Les petites structures en apportent la preuve avec une liste d'appareils dans laquelle chaque ligne est cochée avec la date de vérification, et une capture d'écran de la tentative de connexion échouée.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 5.4 **Les données et fonctions applicatives sont compartimentées de sorte que les processus ayant des besoins de protection ou des privilèges différents ne puissent pas accéder aux mêmes zones. La séparation est intégrée à l'architecture du système et n'est pas laissée au hasard de l'installation.**

Comment le prouver: Vue d'ensemble des applications indiquant quelles données et quels services elles utilisent et quels comptes se trouvent derrière elles, configuration d'instances, bases de données, répertoires ou machines virtuelles séparés, et une liste de privilèges par zone. Une petite structure résout cela avec des comptes utilisateur séparés et des dossiers de données séparés pour l'ingénierie et l'exploitation, plus une note sur quelle application accède à quel dossier.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

10 FR 6 : Réponse rapide aux événements 3

SR 6.1 **Les journaux d'audit collectés dans le système peuvent être lus et évalués par les personnes et rôles autorisés à cet effet sans perturber le fonctionnement en cours de l'installation, et l'accès à ces journaux est lui-même restreint aux utilisateurs autorisés.**

Comment le prouver: Une matrice de rôles et permissions montrant qui peut consulter les données de journal, plus une capture d'écran ou un export d'une vue de journal réellement récupérée, portant un horodatage. Ajouter une brève note sur la voie utilisée pour la récupération, par exemple l'interface opérateur de l'automate, un serveur de journaux ou un export de fichier. Les petites structures se contentent d'une vue d'ensemble d'une page par installation : où se trouve le journal, qui a un accès en lecture, comment il est récupéré. Une récupération de test une fois par an, consignée dans le journal de maintenance, montre que la voie fonctionne. S'applique à partir du SL 1 pour tous les niveaux de sécurité.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 6.1 RE 1 **Les journaux d'audit peuvent être récupérés via une interface automatique afin que les outils d'analyse puissent les traiter davantage sans nouvelle saisie manuelle, et les données sont fournies dans un format documenté et d'usage courant.**

Comment le prouver: Une description de l'interface utilisée avec le format, par exemple syslog, OPC UA Alarms and Conditions, une requête REST ou un export CSV, plus un enregistrement d'exemple et la configuration du système récepteur. La preuve peut être un extrait de la configuration du SIEM ou du collecteur de journaux avec la preuve des enregistrements entrants. Sans SIEM, un collecteur de journaux sur un serveur simple qui récupère les journaux la nuit via un script et les stocke suffit ; le script lui-même plus un listing de répertoire des fichiers collectés constitue la preuve. En tant qu'amélioration, cela n'est exigé qu'à partir du SL 3, pas à partir du SL 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 6.2 **L'activité pertinente pour la sécurité dans le système est surveillée en continu, la surveillance détecte les tentatives d'attaque et les usages abusifs et les signale rapidement à un point de contact nommé, et les outils, voies de signalement et responsabilités utilisés à cet effet sont définis.**

Comment le prouver: Une vue d'ensemble des outils de surveillance par zone, par exemple un capteur réseau, des alertes antivirus, des alarmes de pare-feu ou un contrôle d'intégrité, indiquant qui reçoit l'alerte et dans quel délai une réponse est attendue. Des configurations d'alarme, une liste des alertes déclenchées ces derniers mois et les notes de traitement correspondantes servent de preuve. Les petites structures n'ont pas besoin d'une salle de contrôle permanente : une boîte mail partagée ou une file de tickets rassemblant les alertes des systèmes existants, plus une règle fixe qu'une personne nommée la consulte chaque jour ouvré, suffit et se prouve par l'historique de la boîte mail. Exigé à partir du SL 2.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

11 FR 7 : Disponibilité des ressources 13

SR 7.1 **En cas de surcharge ou d'attaques par saturation délibérées, le système reste dans un état de fonctionnement défini, les fonctions de contrôle essentielles continuent de fonctionner, et la défaillance d'un service individuel n'entraîne pas toute l'installation avec elle.**

Comment le prouver: Configuration des mécanismes de protection (limitation de débit, limites de connexion, contrôle des tempêtes de diffusion sur les commutateurs), déclarations du fournisseur sur le comportement en charge, plus un enregistrement d'un test de charge ou d'un événement de surcharge réel avec observation de la fonction de contrôle. Exigé dès le SL 1. Une petite structure couvre cela avec des captures d'écran des paramètres du commutateur et du pare-feu et une brève note sur quelle fonction a continué de fonctionner pendant un test de la cellule la plus importante.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.1 RE 1 **La charge de communication que les composants individuels peuvent injecter dans le réseau est plafonnée, de sorte qu'un composant défectueux ou compromis ne puisse pas saturer le segment réseau.**

Comment le prouver: Limites de bande passante et de multicast par port sur les composants réseau, preuve du plafond pour chaque connexion, plus une mesure de la charge de base réelle par appareil. Exigé dès le SL 2, pas dès le SL 1. Sans commutateurs administrables, cette ligne ne peut pas être prouvée, et c'est alors le point ouvert.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.1 RE 2 **Une situation de surcharge à l'intérieur du système considéré ne se propage pas aux systèmes ou réseaux adjacents ; l'impact vers l'extérieur est techniquement contenu.**

Comment le prouver: Règles de segmentation et de filtrage aux frontières, preuve que le trafic sortant est plafonné, plus un enregistrement de test montrant qu'une charge générée dans le réseau de cellule n'a pas dégradé le réseau bureautique ni un réseau voisin. Exigé dès le SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.2 **L'utilisation du temps de traitement, de la mémoire, de l'espace de stockage et de la bande passante réseau est bornée de sorte qu'un processus ou service unique ne puisse pas consommer les ressources nécessaires au contrôle.**

Comment le prouver: Configuration des limites de ressources (quotas, priorités de processus, limites de mémoire), évaluation de la surveillance d'utilisation sur une période représentative, plus les seuils à partir desquels un avertissement est déclenché. Exigé dès le SL 1. Les petites structures utilisent les moyens intégrés du système d'exploitation et une surveillance simple avec une alerte d'espace disque et de CPU par courrier électronique.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.3 **Des sauvegardes existent pour les configurations système, les données applicatives et les versions de programme ; elles peuvent être produites sans interrompre le fonctionnement en cours et sont protégées contre l'accès et la modification non autorisés.** Document

Comment le prouver: Concept de sauvegarde couvrant portée, fréquence et période de rétention, journaux de sauvegarde des exécutions les plus récentes, plus preuve de la protection d'accès des supports de sauvegarde (stockage séparé, chiffrement, permissions dédiées). Exigé dès le SL 1. Une petite structure sauvegarde les projets automate et les versions IHM sur un support chiffré déconnecté physiquement après la sauvegarde, et consigne date et version dans une liste simple.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.3 RE 1 **L'utilisabilité des sauvegardes a été vérifiée ; il est prouvé qu'un état fonctionnel peut réellement être restauré à partir d'elles.**

Comment le prouver: Enregistrement d'un essai de restauration avec date, version de sauvegarde testée, système cible et résultat, au moins pour les composants critiques. Exigé dès le SL 2, pas dès le SL 1. Les petites structures vérifient un programme automate et une image IHM sur un appareil de secours une fois par an à titre d'échantillon et consignent le résultat en deux phrases.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.3 RE 2 **La sauvegarde s'exécute automatiquement selon un calendrier défini ; une exécution échouée est détectée et signalée.**

Comment le prouver: Calendrier de la tâche de sauvegarde, journaux d'exécution sans lacune, plus preuve de la notification d'échec pour une exécution qui n'a pas réussi (alarme, ticket, courrier). Exigé dès le SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.4 **Après une perturbation, une défaillance ou une attaque, le système peut être ramené à un état connu et sûr ; la récupération a été répétée et les responsabilités sont nommées.** Document

Comment le prouver: Plan de redémarrage pour chaque composant critique avec séquence, supports nécessaires, contacts et temps cible, ainsi que l'enregistrement du dernier exercice de récupération. Exigé dès le SL 1. Une petite structure se contente d'une fiche de redémarrage d'une page par ligne, conservée dans l'armoire de commande et vérifiée à chaque remplacement de pièce de rechange.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.5 **Si l'alimentation électrique normale tombe en panne, le système passe dans un état défini : soit l'alimentation est maintenue par une source de secours, soit un arrêt ordonné a lieu sans perte de l'état sûr.**

Comment le prouver: Preuve de dimensionnement et de maintenance de l'alimentation sans interruption ou du générateur de secours, enregistrement de test du dernier test de batterie ou de charge, plus une description du comportement lors de la commutation et du rétablissement du secteur. Exigé dès le SL 1. Les petites structures testent l'onduleur en charge une fois par an et consignent la date de test, le temps d'autonomie et l'âge de la batterie.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.6 **Les paramètres réseau et de sécurité du système sont fixés à un état cible approuvé, les écarts par rapport à cet état cible sont détectables, et l'état actuel peut être consulté à tout moment.** Document

Comment le prouver: Configuration cible approuvée par classe d'appareil (spécification de durcissement), états de configuration actuels des appareils, plus le résultat d'une comparaison entre état cible et état réel avec une liste d'écarts et le motif de chacun. Exigé dès le SL 1. Une petite structure stocke les exports de configuration sous contrôle de versions et compare avant et après chaque changement.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.6 RE 1 **L'état actuel des paramètres de sécurité peut être fourni sous une forme lisible par machine afin qu'il puisse être vérifié automatiquement par rapport à l'état cible.**

Comment le prouver: Sortie d'exemple dans un format lisible par machine (export de configuration, fichier structuré, requête d'interface) et le script ou l'outil qui effectue la comparaison par rapport à l'état cible, ainsi que le rapport de résultat d'une exécution. Exigé dès le SL 3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.7 **Le système est restreint aux fonctions nécessaires à l'exploitation ; les services, ports, protocoles et interfaces qui ne sont pas nécessaires sont désactivés ou supprimés.**

Comment le prouver: Liste des services actifs et ports ouverts par composant avec une justification du besoin, preuve que les autres sont désactivés (configuration, résultat de balayage de ports), plus une règle pour les interfaces USB et de maintenance. Exigé dès le SL 1. Les petites structures réalisent un simple balayage de ports par segment et justifient chaque élément ouvert en une ligne.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

SR 7.8 **Un inventaire actuel de tous les composants du système avec fabricant, type, version de micrologiciel ou de logiciel et adresse réseau est disponible et est tenu à jour lorsque des changements surviennent.** Document

Comment le prouver: Inventaire des composants avec sa date de révision et son propriétaire, preuve de tenue à jour via l'historique des changements, plus une comparaison avec une découverte réseau pour trouver les appareils non enregistrés. Exigé dès le SL 2, pas dès le SL 1. Une petite structure tient l'inventaire comme un tableau et le met à jour comme règle fixe à chaque remplacement d'appareil et à chaque mise à jour de firmware.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification