Nations Unies ECE/CTCS/WP.6/2018/9

Conseil économique et social

Distr. générale
10 septembre 2018
Français
Original : anglais

Commission économique pour l'Europe

Comité directeur des capacités et des normes commerciales

Groupe de travail des politiques de coopération en matière de réglementation et de normalisation

Vingt-huitième session
Genève, 14-16 novembre 2018
Point 9 b) de l'ordre du jour provisoire
Coopération internationale en matière de réglementation : Projets sectoriels

Projet de proposition de cadre réglementaire commun sur la cybersécurité

Document présenté par le secrétariat

Résumé

Le présent document contient un projet de proposition de cadre réglementaire commun sur la cybersécurité ; il est soumis au Groupe de travail pour examen.

Ce premier examen visera à recueillir l'avis des représentants sur l'orientation prise par le cadre réglementaire commun proposé. Si leur avis est favorable, une proposition finale sera soumise à la réunion annuelle du Groupe de travail en 2019.

Décision proposée

« Le Groupe de travail exprime un avis favorable au sujet de l'approche globale du cadre réglementaire commun, telle qu'elle est exposée dans le présent projet de proposition.

Il demande que la proposition soit affinée ; que le Groupe d'experts des systèmes de réglementation et le secrétariat soient chargés d'en établir la version définitive ; et qu'un projet plus mûr lui soit soumis à sa réunion annuelle en 2019. Il prie également le secrétariat de continuer de rendre compte de l'état d'avancement de cette initiative. »

GE.18-14944 (F) 140918 021018
1814944

I. Introduction

1. À sa vingt-septième session annuelle, le Groupe de travail a approuvé la proposition relative à une nouvelle initiative sectorielle sur la cybersécurité (décision 21, ECE/CTCS/WP.6/2017/2)

2. Suite à cette décision, un partenariat a été établi avec le Groupe de travail 17 du Bureau d'évaluation de la conformité de la Commission électrotechnique internationale (CEI) et le Système d'évaluation de la conformité des matériels et composants électrotechniques (IECEE) de la CEI, qui soutiennent activement ce projet.

3. Des débats ont eu lieu et des projets de propositions relatives à un cadre réglementaire commun sur la cybersécurité ont été présentés à deux réunions du Groupe d'experts de la gestion du risque dans les systèmes de réglementation (mars 2018 et juillet 2018).

4. Le présent document expose un avant-projet de cadre réglementaire commun dans ce secteur.

II. Objectifs du cadre réglementaire commun

5. L'objectif de l'initiative sectorielle sur la cybersécurité est de promouvoir la convergence des réglementations techniques nationales déjà en place ou à mettre en place dans ce secteur vers un cadre commun reposant sur une approche fondée sur le risque et s'inspirant d'autres pratiques exemplaires internationales. Cela réduira les obstacles aux échanges dont pâtissent les composants, le matériel, le personnel qualifié et les services, favorisera la concurrence, élargira le choix du marché et diminuera les coûts. Il sera également possible d'accroître le niveau de protection des données pour les services bancaires, sanitaires et autres services essentiels, ainsi que le degré de fiabilité, de continuité, de sûreté et de sécurité des infrastructures critiques, comme celles nécessaires à l'approvisionnement en énergie électrique, et d'autres services essentiels qui constituent l'épine dorsale de toute économie nationale. Ainsi, l'initiative contribuera à assurer le bien-être général et la prospérité des citoyens.

6. Plus précisément, le cadre réglementaire commun permettra :

- De promouvoir une législation harmonisée à l'échelle mondiale ;
- De promouvoir une législation proportionnée aux risques qu'il est prévu de prendre en compte ;
- De garantir l'acceptation réciproque des procédures d'essai et d'évaluation et des résultats entre les laboratoires d'essai ;
- D'œuvrer à mettre en place des procédures cohérentes et comparables pour l'évaluation et l'application des mesures de cybersécurité.

III. Contexte

7. À l'ère du numérique, la cybersécurité est un élément essentiel de la compétitivité et de la sécurité économiques de la plupart des économies mondiales.

8. Garantir un niveau élevé de cyber-résilience dans le monde entier est d'une importance capitale pour assurer les services essentiels et gagner la confiance des consommateurs à l'ère numérique, et pour poursuivre le développement d'un monde plus sûr, innovant, compétitif, durable et prospère.

9. Les cybermenaces sont un phénomène mondial qui traverse les frontières nationales, régionales et internationales. La cybersécurité exige donc l'adoption d'une approche intégrée à tous les niveaux.

10. Pour être efficaces, les mesures de cybersécurité sur le plan commercial et aux niveaux national et international devraient être fondées sur les résultats d'un processus de gestion des risques systémiques, et toutes les parties prenantes concernées devraient être associées au processus.

11. Les principes fondamentaux de la cybersécurité sont bien étayés dans de nombreuses normes internationales, mais ils ne sont pas bien connus, ni compris ou appliqués. On peut citer à titre d'exemple la série CEI 62443 et la série de normes internationales de l'Organisation internationale de normalisation (ISO)/CEI 27000.

12. Il existe une confusion entre les besoins des applications cyberphysiques, appelées systèmes de technologie opérationnelle, tels que les infrastructures critiques et les systèmes intelligents, et la nécessité de faire fonctionner ces systèmes dans le monde réel, et les besoins des systèmes purement informationnels, appelés systèmes informatiques, et la nécessité de protéger les données et de les faire circuler en toute sécurité dans le monde virtuel.

13. Il est évident que la cyberprotection d'un système technique impose l'adoption d'une approche systémique. Il va de soi qu'une approche fondée sur les risques est nécessaire pour les raisons suivantes :

- Dans tout système, certains éléments sont plus utiles ou plus vulnérables que d'autres et ont besoin d'une protection renforcée et plus coûteuse, alors que d'autres éléments peuvent bénéficier de mesures de protection moins coûteuses. Cette analyse devrait être fondée sur les risques ;
- Il faut trouver un juste milieu entre le niveau de protection et le coût de la protection.

14. Il est évident que, dans une approche systémique, des formes de protection plus ou moins contraignantes sont appropriées, ce qui signifie que des formes plus ou moins contraignantes de confirmation que les exigences de protection ont été respectées sont également appropriées.

15. Il est donc évident qu'une approche globale de la cybersécurité devrait être neutre en ce qui concerne l'évaluation de la conformité et tenir compte des différentes formes d'évaluation − évaluation de la conformité par la première partie, la deuxième partie et la troisième partie − selon les différents niveaux de risque déterminés pour les divers éléments du système à protéger.

16. Les cybermenaces pouvant être nationales, régionales ou internationales, les pratiques exemplaires internationales sont les plus appropriées. Les normes internationales de l'ISO et de la CEI sont de plus en plus souvent adoptées par les pays à l'échelle régionale et nationale, soit intégralement, sans aucune modification, soit en partie, avec des prescriptions supplémentaires énoncées dans des normes nationales.

17. Les pays utilisent les normes dans leurs réglementations de différentes manières, notamment :

- En rendant les normes obligatoires par le biais d'un texte législatif ;
- En faisant du respect des normes un moyen de prouver la conformité aux exigences essentielles énoncées dans la législation ; selon cette approche, le matériel, les qualifications du personnel, les services, les pratiques et les processus qui sont conformes aux dispositions des normes sont « réputés conformes » aux exigences précisées dans les règlements.

18. Lorsque l'analyse des risques conclut que l'évaluation de la conformité par une tierce partie est appropriée, il est conseillé d'utiliser les meilleures pratiques internationales et de recourir à des services de certification mondiale tels que ceux offerts par l'IECEE, lorsque ceux-ci sont disponibles et pertinents.

IV. Énoncé des objectifs de réglementation communs

19. Les objectifs de réglementation communs (ORC) examinés dans le présent document ont été élaborés conformément à la recommandation L du Groupe de travail des politiques de coopération en matière de réglementation et de normalisation (Groupe de travail 6) de la Commission économique pour l'Europe (ECE/TRADE/378 − Recommandations de la CEE sur les politiques de normalisation).

20. Les ORC ont un double objectif. D'une part, ils peuvent servir de modèle pour l'élaboration de textes législatifs dans les pays actuellement dépourvus de réglementation dans ce secteur. D'autre part, ils peuvent servir à aligner la réglementation nationale en vigueur sur une pratique exemplaire harmonisée à l'échelle internationale.

21. Les ORC sont élaborés compte tenu des normes internationales et des méthodes d'évaluation de la conformité élaborées par la CEI et l'ISO, ainsi que des pratiques exemplaires en matière d'évaluation de la conformité à ces normes, dans le cadre de l'IECEE.

22. Les ORC font appel à une méthode systématique pour déterminer un niveau approprié d'exigences et d'évaluation de la conformité en fonction du risque.

23. Les ORC portent sur les prescriptions relatives à la technologie des systèmes, y compris les composants, les produits et le matériel, ainsi qu'à la compétence et aux qualifications du personnel et aux méthodes de gestion, notamment la conception des composants, l'intégration et la réalisation des systèmes, l'exploitation, la maintenance, la mise à niveau, etc. (ORC − quatrième partie du présent document).

24. La cybersécurité peut être assurée par différents moyens légitimes. Le présent document décrit une méthode systématique à l'appui d'une approche systémique de la cybersécurité. Elle se distingue des autres méthodes par le fait qu'en plus de la modélisation du système technique, de l'analyse des risques et de l'analyse des lacunes en matière d'exigences, elle comprend une analyse des besoins en ce qui concerne l'évaluation de la conformité. C'est aussi, et ce doit être, une méthode souple car elle doit être applicable à une grande diversité de systèmes techniques.

25. En outre, le présent document adopte une approche fondée sur le cycle de vie qui exige que le système technique soit convenablement inspecté, entretenu, réparé et mis à niveau. Cette approche garantit l'efficacité et l'efficience de la cybersécurité au fil du temps à mesure que le système proprement dit évolue, de même que la nature de la menace.

26. Un cadre réglementaire national peut utiliser ce modèle pour certains secteurs et applications critiques ou exiger que les acteurs commerciaux intervenant dans le cadre de ces mêmes secteurs et applications, ou d'autres, l'utilisent pour faire dûment la preuve de la conformité. L'évaluation de la conformité par un tiers ne devrait être exigée qu'en cas de besoin, en fonction des résultats de l'analyse des risques.

27. La convergence vers une méthode commune fondée sur des normes internationales harmonisées et sur les meilleures pratiques internationales en matière d'évaluation de la conformité présente plusieurs avantages. Entre autres, lorsque l'évaluation de la conformité par une tierce partie est utilisée pour établir la conformité des composants et de la technologie ainsi que des compétences et des qualifications du personnel, la reconnaissance de cette conformité dans le commerce international et la circulation des personnes qualifiées s'en trouve facilitée.

28. Inversement, l'existence ou l'utilisation de prescriptions et de procédures disparates dans des secteurs qui fonctionnent comme des applications vraiment globales et intégrées peuvent, en soi, constituer un risque accru.

29. C'est pourquoi, lorsque l'évaluation de la conformité par une tierce partie est requise, un mécanisme de certification reconnu à l'échelle internationale, tel que l'IECEE, est d'une importance fondamentale pour réduire les coûts inutiles liés à la répétition des inspections, évaluations et essais et au chevauchement des compétences.

30. Un dernier élément essentiel du présent document concerne la surveillance des marchés. La surveillance des marchés est nécessaire pour s'assurer de la bonne réalisation des ORC par les professionnels et pour accroître la confiance dans l'efficacité des ORC. Des lignes directrices communes seront élaborées pour aider les autorités nationales à définir et à mettre en œuvre des mesures et des procédures pertinentes, notamment pour retirer du marché national des composants et produits non conformes.

V. Objectifs de réglementation communs

1. ORC − Partie 1 : Méthode pour assurer une cybersécurité appropriée − vue d'ensemble

31. Le cadre réglementaire commun décrit une méthode globale et systématique à l'appui d'une approche systémique de la cybersécurité. Cette méthode générique comporte cinq étapes qui sont ensuite répétées périodiquement. Ces cinq étapes sont les suivantes :

- Analyse et notation des risques ;
- Prescriptions − analyse des lacunes des normes (quatrième partie du présent document) ;
- Analyse de l'évaluation de la conformité en fonction de l'évaluation des risques (cinquième partie du présent document) ;
- Application − Preuve de conformité ;
- 3R − Revoir, Réviser, Renouveler.

2. ORC − Partie 2 : Méthode pour déterminer les prescriptions appropriées

32. Analyse des lacunes − le modèle de matrice générique (voir l'annexe A) est utilisé pour déterminer les points auxquels des prescriptions sont nécessaires pour un système. L'analyse de différents systèmes dans différentes situations conduira à des besoins différents en matière de prescriptions. Les prescriptions seront fondées sur des normes internationales comme celles de la CEI et de l'ISO (telles qu'elles figurent dans la quatrième partie et sont énumérées dans l'appendice du présent document) ou, en l'absence de telles normes, sur des normes régionales ou enfin sur des normes nationales. En l'absence de normes les prescriptions devraient être fondées sur les meilleures pratiques et procédures acceptées par le marché.

33. La recommandation R du Groupe de travail 6 de la CEE intitulée « Gestion du risque dans les systèmes de réglementation » devrait être utilisée par les organismes de réglementation pour assurer la cohérence et la proportionnalité entre les risques existants en matière de cybersécurité et les prescriptions réglementaires respectives.

3. ORC − Partie 3 : Méthode pour déterminer les prescriptions à appliquer à l'évaluation de la conformité

34. Analyse des risques − le modèle de matrice générique (voir l'annexe A) est utilisé pour déterminer les points auxquels des prescriptions sont nécessaires pour un système. La méthode permettant de déterminer quelles prescriptions sont appropriées est indiquée dans la deuxième partie du présent document. Le niveau d'évaluation de la conformité qui devrait être appliqué aux prescriptions sera déterminé au moyen d'une évaluation des risques qui donnera lieu à une notation des risques pour chaque point du modèle de matrice générique. L'analyse de différents systèmes dans différentes situations conduira à différentes notations des risques. Les points de valeur élevée se traduiront par des niveaux plus élevés d'évaluation de la conformité, tout comme les points de vulnérabilité élevée, tandis que les points de valeur et de vulnérabilité plus faibles donneront lieu à des niveaux inférieurs d'évaluation de la conformité.

4. ORC − Partie 4 : Conditions d'acceptation sur le marché

A. Prescriptions relatives aux composants, aux produits et au matériel

35. Les prescriptions relatives aux composants, aux produits et au matériel utilisés comme éléments du système seront fondées sur des normes internationales comme celles de la CEI et de l'ISO (telles qu'elles figurent dans la quatrième partie et sont énumérées dans l'appendice du présent document) ou, en l'absence de telles normes, sur des normes régionales ou enfin sur des normes nationales.

B. Prescriptions relatives aux compétences personnelles

36. Les prescriptions relatives aux compétences personnelles seront fondées sur des normes internationales comme celles de la CEI et de l'ISO (telles qu'elles figurent dans la quatrième partie et sont énumérées dans l'appendice du présent document) ou, en l'absence de telles normes, sur des normes régionales ou enfin sur des normes nationales. En l'absence de normes les prescriptions devraient être fondées sur les compétences acceptées par le marché.

C. Prescriptions relatives aux processus

37. Les prescriptions relatives aux processus seront fondées sur des normes internationales comme celles de la CEI et de l'ISO (telles qu'elles figurent dans la quatrième partie et sont énumérées dans l'appendice du présent document) ou, en l'absence de telles normes, sur des normes régionales ou enfin sur des normes nationales.

5. ORC − Partie 5 : Liste de référence des normes internationales permettant d'établir la présomption de conformité au présent règlement type

38. Les normes permettant d'établir la présomption de conformité aux prescriptions mentionnées dans la quatrième partie sont énumérées dans l'appendice (chap. A, B et C). Cette liste de normes doit être fréquemment mise à jour, en fonction de la publication des normes internationales CEI ou ISO/CEI se rapportant aux objectifs du présent règlement type.

39. Sous réserve d'un examen approprié effectué par les organes de gestion et de gouvernance de la CEE, le groupe des pays ayant appliqué le présent règlement type constituera un groupe de l'acceptation des normes, qui sera chargé d'approuver les normes internationales CEI ou ISO/CEI permettant d'établir la présomption de conformité audit règlement. Les membres de ce groupe s'efforcent d'accéder à l'ensemble des travaux de normalisation de la CEI (projets de texte, réunions) pour faire en sorte que, dès le début, les préoccupations des organes de réglementation soient prises en compte. Une fois que le Groupe de travail aura accepté une norme, celle-ci sera inscrite à l'appendice du présent règlement type. S'il existe une ancienne version de la norme, cette ancienne version sera retirée de la liste dans un délai de trois ans.

6. ORC − Partie 6 : Prescriptions pour l'évaluation de la conformité

A. Définition des procédures applicables en matière d'évaluation de la conformité

40. La conformité aux ORC sera vérifiée à l'aide d'un mécanisme approprié d'évaluation de la conformité eu égard aux prescriptions indiquées dans l'application spécifique, telles que déterminées par le processus décrit dans la première partie du présent document.

41. Lorsque l'évaluation de la conformité par une tierce partie est requise, la conformité au présent ORC sera évaluée à l'aide d'un système international de certification tel que l'IECEE pour l'acceptation directe sur le marché des produits, personnes, services et organismes certifiés IECEE. Sinon, dans les pays où la législation ne permet pas le recours à des certificats de l'IECEE, la certification nationale de la conformité devra être basée sur les essais, les inspections et les évaluations prévus dans le cadre de l'IECEE.

B. Reconnaissance des organes d'évaluation de la conformité

42. L'agrément des organes d'évaluation de la conformité et des laboratoires d'essai doit se fonder sur les normes internationales ISO/CEI applicables (voir l'appendice, chap. D.1). L'organe d'agrément doit être membre de la Conférence internationale sur l'agrément des laboratoires d'essais et du Forum international de l'accréditation. Au moins un membre de l'équipe d'évaluateurs doit posséder des compétences correspondant aux prescriptions pertinentes en matière de cybersécurité (voir par exemple la liste des évaluateurs agréés de l'IECEE).

43. Les certificats doivent être conformes aux prescriptions relatives au type de système correspondant, telles qu'indiquées dans la norme ISO/CEI applicable (voir l'appendice, chap. D. 2).

44. Le système d'évaluation de la conformité IECEE permet d'établir la présomption de conformité aux prescriptions énoncées dans la sixième partie.

7. ORC − Partie 7 : Comité directeur de la cybersécurité de la CEE

45. Sous réserve d'un examen approprié effectué par les organes de gestion et de gouvernance de la CEE, il est prévu de constituer un Comité directeur de la cybersécurité de la CEE qui sera placé sous l'égide du Groupe de travail 6 de la CEE et dont la tâche consistera à suivre la réalisation des ORC dans les pays qui ont fondé leur législation nationale sur le règlement type de la CEE et à actualiser ce règlement au regard de l'expérience acquise.

46. Le Comité directeur adopte des statuts et d'autres règles et procédures de fonctionnement (modalités de vote, par exemple).

47. Le Comité directeur fait rapport aux membres du groupe de l'acceptation des normes de la CEE.

48. Les membres du Comité directeur de la cybersécurité ayant un droit de vote sont les représentants des pays ayant appliqué le règlement type. Peuvent également participer aux réunions des observateurs représentant le Conseil de gestion de la normalisation de la CEI, le Bureau d'évaluation de la conformité de la CEI, le Comité technique 65 de la CEI, le Comité technique mixte ISO/CEI 1/SC27, l'IECEE, le Système de la CEI pour la certification des équipements utilisés à proximité d'explosifs et le Groupe consultatif de la surveillance des marchés de la CEE.

8. ORC − Partie 8 − Surveillance des marchés

49. Sous réserve d'un examen approprié effectué par les organes de gestion et de gouvernance de la CEE et pour surveiller la conformité aux prescriptions du présent règlement type sur le marché, il sera créé un réseau d'experts de la surveillance des marchés spécialisés dans la cybersécurité (voir l'appendice, chap. F.1).

50. La planification des mécanismes de surveillance du marché devrait se fonder, entre autres, sur la recommandation « S » du Groupe de travail 6 de la CEE relative à l'utilisation d'outils prévisionnels de gestion du risque pour la surveillance ciblée des marchés.

51. En cas de non-conformité critique, un système international d'alerte devrait être mis en place pour informer tous les États membres de la CEE des risques récemment détectés.

Appendice

Liste des normes et lignes directrices acceptées, tenue à jour par la CEE, la CEI et l'ISO

A.1 Notions fondamentales et méthodes

1. Ce point doit être approfondi.

A.2 Critères de conception des composants des systèmes

2. Ce point doit être approfondi.

A.3 Production de l'équipement

3. Ce point doit être approfondi.

B.1 Prescriptions en matière de compétences

4. Ce point doit être approfondi.

D.1 Normes d'évaluation de la conformité

5. ISO/CEI 17065, ISO/CEI 17021, ISO/CEI 17024, ISO/CEI 17025.

D.2 Éléments fondamentaux de la certification des produits

6. ISO/CEI 17067.

F.1 Lignes directrices pour la surveillance du marché

7. Des lignes directrices pour la surveillance du marché sont en cours d'élaboration dans le cadre de cette initiative sectorielle, en coopération avec le Groupe consultatif de la surveillance des marchés.

Annexe A

Explication du modèle de matrice générique

1. Le modèle de matrice générique est un outil utilisé pour modéliser un système technique, puis pour comparer ce modèle avec des objets de l'évaluation de la conformité (ou les éléments dont la conformité peut effectivement être évaluée au regard des prescriptions). Le modèle de matrice générique est généralement représenté sous la forme d'une matrice comme suit : le système est modélisé verticalement sur le côté gauche et les objets de l'évaluation de la conformité sont énumérés en haut.

2. Dans une représentation graphique du modèle de matrice générique, des lignes horizontales sont tracées à partir des éléments du modèle système à travers la page sous les objets de l'évaluation de la conformité. De même, des lignes sont tracées verticalement vers le bas à partir des objets de l'évaluation de la conformité. Les points d'intersection des axes verticaux et horizontaux sont les points où l'évaluation de la conformité peut être effectuée au regard des prescriptions, si ces prescriptions sont disponibles.

3. Le modèle de matrice générique peut être utilisé pour déterminer ce qui est important pour un système technique donné lorsqu'on le considère sous un angle particulier. Cela permettra de déterminer les éléments et sous-éléments les plus importants qui devraient être visibles sous cet angle et qui devraient donc être apparents dans le modèle système. Lorsque l'on examine la question de la cybersécurité sous cet angle, le système peut être modélisé avec des éléments tels que la technologie ou les composants, les interconnexions, les interventions, les zones de sécurité, les tests d'intrusion, etc.

4. Les prescriptions pourraient être multiples, selon ce que l'on cherche à obtenir. En général, elles prennent la forme de pratiques exemplaires, de qualifications, de spécifications, de normes, d'un résultat minimal ou maximal de tests normalisés, etc. Pour satisfaire aux prescriptions, il peut également être nécessaire de disposer d'un certain type ou niveau de matériel, de savoir-faire, de qualifications, de compétences, d'expérience, etc.

5. L'acte consistant à effectuer une évaluation pour voir si les prescriptions ont été respectées correspond à l'acte consistant à évaluer la conformité aux prescriptions. Le terme officiel est l'évaluation de la conformité. Il y a essentiellement trois objets possibles de l'évaluation de la conformité. Il s'agit des produits, des personnes (compétences) et des processus.

6. Ce sont là les trois principaux objets de l'évaluation de la conformité. De nombreux autres objets ont été proposés, tels que les services, les données, les installations, les projets, les organes ou organisations et les systèmes. Mais en réalité, chacun d'entre eux correspond simplement à l'un des trois principaux objets ou à une combinaison des trois. Par exemple, les services ne sont essentiellement que des processus, exécutés par des personnes (possédant les compétences requises), peut-être à l'aide de produits ou de matériel appropriés. Il n'y a rien d'autre. Ainsi, les services sont déjà visés par les trois principaux objets de l'évaluation de la conformité et n'ont pas besoin de s'inscrire dans une catégorie qui leur soit propre.

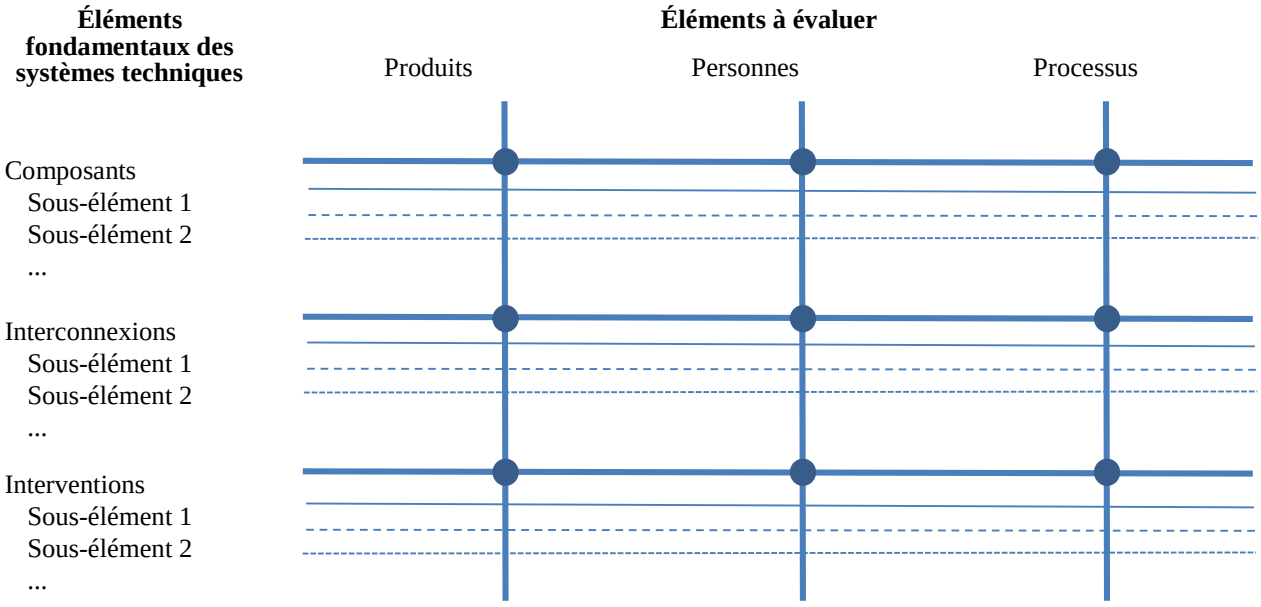
7. Cela étant dit, s'il est utile pour un secteur que soient indiqués d'autres objets en sus des trois principaux objets, alors l'objet/les objets supplémentaire(s) doit/doivent être inclus dans le modèle de matrice générique considéré.

8. C'est aux points d'intersection des éléments du modèle-système et des objets de l'évaluation de la conformité que les prescriptions peuvent être appliquées. Une analyse des lacunes permettra de déterminer quelles sont les prescriptions et si elles existent.

9. Il faut d'abord comprendre le système et savoir où se trouve la valeur et où se trouvent les vulnérabilités puis procéder à une évaluation des risques à chacun des points d'intersection pour déterminer quel type d'évaluation de la conformité est nécessaire par rapport aux exigences de chaque point. Les points d'intersection de grande valeur ou de grande vulnérabilité nécessiteront une évaluation de la conformité plus rigoureuse, tandis

que les points de faible valeur ou de faible vulnérabilité nécessiteront une évaluation de la conformité moins stricte. L'ensemble des options en matière d'évaluation de la conformité devrait être disponible pour un usage approprié. Il s'agit de l'évaluation de la conformité par une première partie telle que la déclaration de conformité du fabricant ou du fournisseur ; de l'évaluation de la conformité par une deuxième partie, comme les auto-évaluations et les audits internes effectués par l'utilisateur ou le propriétaire du système ; et de l'évaluation de la conformité par une tierce partie, comme les essais de type 1 (ISO/CEI 17067) ou les essais de type 5, la certification complète de la conformité, etc. La plupart des réglementations devraient être neutres du point de vue de l'évaluation de la conformité et ne préciser que ce qui est approprié en fonction des résultats de l'analyse des risques.

10. Les points d'intersection verticaux et horizontaux du modèle de matrice générique sont les points d'intersection où se fait l'évaluation de la conformité, et l'approche systémique est la matrice globale des exigences et des activités d'évaluation de la conformité.



Modèle générique de l'approche systémique de l'évaluation de la conformité (forme la plus simple)

Qu'est-ce qu'un système technique ?

11. Un système technique n'est pas un système naturel comme un système biologique, par exemple le système circulatoire sanguin, ou un système environnemental, par exemple le système météorologique, ou encore un système céleste, par exemple le système solaire, etc. Un système technique est un système artificiel.

12. Quels sont les points communs entre les systèmes ferroviaires, l'informatique en nuage, les réseaux intelligents, les systèmes de contrôle industriels, une centrale nucléaire et un système de distribution d'électricité, une raffinerie de pétrole, un système de distribution de gaz, un système d'information sanitaire, des maisons intelligentes, etc. ?

13. Ce sont tous des systèmes techniques.

14. Maintenant, si l'on considère qu'un système technique est :

- Un groupe d'éléments interactifs, étroitement liés ou interdépendants formant un tout cohérent ;
- Et que ces éléments peuvent être d'ordre procédural, physique et/ou virtuel ;
- Et que ces éléments peuvent être des composants qui doivent être conçus et fabriqués ou créés ;

- Et que le système proprement dit sera conçu et fabriqué (ou intégré dans des systèmes) et que les éléments du système peuvent être confinés dans un emplacement physique limité ou largement répartis ;
- Et que ces éléments doivent être périodiquement révisés, entretenus et/ou mis à jour/modernisés ;
- Et que certains de ces éléments transmettent des informations entre eux et en reçoivent ;
- Et que le système est d'une certaine manière connecté au monde au-delà du système lui-même, soit physiquement, soit virtuellement (par exemple par Internet) ;
- Et que l'ensemble du système proprement dit fait périodiquement ou constamment l'objet de modifications et d'améliorations du fait d'interventions qui peuvent être virtuelles, automatisées ou humaines ;

alors, tous les systèmes techniques sont de nature assez générique.

15. Bien que les systèmes techniques soient de nature assez générique, ils sont aussi assez complexes et déroutants. Par conséquent, pour simplifier, tous les systèmes techniques peuvent être considérés comme étant constitués de trois éléments fondamentaux, à savoir : composants, interconnexions et interventions.

16. Ces trois éléments, tels qu'énumérés, interviennent l'un après l'autre de façon quelque peu chronologique dans le cycle de vie d'un système. Par exemple, les composants sont conçus et fabriqués, puis les intégrateurs de systèmes conçoivent le système, choisissent les composants et enfin réalisent le système. Celui-ci est ensuite exploité par le biais d'interventions. Chaque élément se succède. Mais il faut aussi souvent revenir en arrière. À mesure qu'un système vieillit et évolue, de nouveaux composants et des composants de remplacement sont nécessaires, ce qui implique souvent le recours à de nouvelles conceptions et technologies pour rétablir les fonctionnalités des composants. Le système lui-même peut évoluer avec des besoins nouveaux ou différents nécessitant l'intégration de nouveaux types de composants, de concepts et de technologies, ce qui permet de revenir à la fonction d'interconnexion. Et à mesure que les pratiques opérationnelles évoluent et s'améliorent, des types d'interventions nouveaux et différents deviennent nécessaires.

17. Composants : Chaque système technique comporte des composants qui peuvent être non seulement physiques, mais également virtuels (logiciels de contrôle, données, etc.). Chaque composant a une fonction et une raison de faire partie du système. Les composants doivent être conçus en fonction de leur utilisation, puis réalisés (fabrication, développement, etc.). Ils doivent parfois être réparés, mis à niveau ou remplacés. Il arrive aussi qu'il puisse y avoir un long délai (intervalle) entre la réalisation d'un composant et son intégration dans un système (durée de conservation). Ce délai doit être géré de manière à garantir l'intégrité du composant et du système.

18. Interconnexions : Il s'agit de l'intégration des systèmes. C'est la manière dont les composants interagissent, communiquent et travaillent ensemble. Il peut s'agir d'interconnexions physiques comme des pièces passant par un système de fabrication, des trains sur rails, des câbles de transmission transportant de l'électricité ou des câbles pour signal de commande. Il peut s'agir de flux d'informations par fil ou sans fil. Les voies ferrées, les fils de transmission et les câbles de signaux seraient tous des composants, mais leur fonction, à savoir transport des trains, de l'électricité et des signaux est l'interconnexion.

19. L'intégration des systèmes doit être conçue et, parfois, les interconnexions doivent être remises en état, mises à niveau ou remplacées. Dans certains cas, les interconnexions peuvent changer radicalement et constamment, comme Internet et le réseau intelligent (avec de nouvelles capacités de production et de nouvelles charges entrant et sortant selon un développement organique incontrôlé et ce, en permanence).

20. Interventions : Elles peuvent être humaines, virtuelles ou automatiques. Les interventions sont essentiellement liées à l'exploitation du système tout au long de son cycle de vie, et peuvent comprendre des pratiques exemplaires, des processus et des

procédures. Elles peuvent également concerner des services fournis en interne ou externalisés, tels que les services de fournisseurs. Certaines interventions peuvent être automatisées, comme en témoignent la mise à niveau automatique des logiciels de protection antivirus et de protection contre le piratage dans les systèmes informatiques, ou le contrôle automatique de la transmission et du certificat virtuel des données entrantes. Souvent, les interventions sont banales, mais il s'agit de pratiques humaines exemplaires qui ont leur importance, comme changer régulièrement les mots de passe, signaler la perte des cartes magnétiques d'accès ou des badges et les invalider, etc.

21. Ce concept englobant trois éléments fondamentaux correspond à une approche très globale d'un système. Pour chacun de ces trois éléments, il y aura toujours des sous-éléments qui fourniront plus de détails sur le système. Nombre des sous-éléments seront les mêmes d'un système à l'autre, mais leur importance peut varier sensiblement selon le système. Et certains systèmes auront des sous-éléments qui leur sont propres. Selon le niveau de précision requis, on peut définir un grand nombre de sous-éléments dont certains peuvent même comprendre des sous-catégories.

Annexe B

Exemples du modèle de matrice générique utilisé dans différents secteurs d'application

Modèle de matrice générique (automatisation industrielle) sous forme de tableau

SYSTÈME		Informations générales	Objets de l'évaluation de la conformité		
Activités	Acteurs		Produits	Personnes	Processus
Composants					
Élaboration des composants du système	Producteurs des composants Propriétaires des actifs	Évaluation des lacunes Concepts et modèles terminologiques Glossaire général des termes et abréviations Mesures de conformité de la sécurité des systèmes IACS - Utilisations liées à la sécurité et au cycle de vie Critères communs pour l'évaluation de la sécurité des technologies de l'information Vue d'ensemble et vocabulaire 62443-0-3 62443-1-1 62443-1-2 62443-1-3 62443-1-4 ISO/CEI 15408 ISO/CEI 27000	CEI 62443-4-2 Exigences techniques de sécurité pour les composants IACS		CEI 62443-4-1 Exigences en matière de mise au point des produits
Fabrication des composants du système	Producteurs des composants Propriétaires des actifs		Normes de produits spécifiques assorties d'exigences techniques (fonctionnelles et de performance) (sécurité des périphériques d'extrémité dès la conception)		
Interconnexions					
Conception de l'intégration du système	Concepteurs du système Propriétaires des actifs				CEI 62443-2-4 Exigences pour les fournisseurs de solutions IACS
Intégration du système Mise en œuvre/réalisation	Créateurs du système Propriétaires des actifs				??
Interventions					
Système de gestion de la sécurité 1. Prescriptions	Propriétaire des actifs Prestataire de services				CEI 62443-2-1 Exigences relatives au système de gestion de la sécurité IACS
2. Mise en œuvre/réalisation					CEI 62443-2-2 Système de gestion de la sécurité IACS − mise en œuvre
3. IACS − Gestion des risques					CEI 62443-3-3 Exigences en matière de sécurité des systèmes et niveaux d'assurance de la sécurité
Dispositif de sécurité	Propriétaire des actifs Prestataire de services				CEI 62443-3-2 Niveaux d'assurance de la sécurité pour les zones et les contrôles
Opération de sécurité	Propriétaire des actifs Prestataire de services				?? ??
Solutions en matière de sécurité	Propriétaire des actifs Prestataire de services				CEI 62443-3-1 Technologies de sécurité IACS
1. Application de la gestion des correctifs	Propriétaire des actifs Prestataire de services				CEI 62443-2-3 Gestion des correctifs dans l'environnement IACS