FOCUS
— Investigations & Consulting —

Libre blanc

GÉRER LES RISQUES HYBRIDES

Convergence entre cybersécurité et sécurité physique dans les organisations modernes

Comprendre les interdépendances
Décloisonner les fonctions de sécurité
Renforcer la résilience



Avant-propos

Des frontières de plus en plus difficiles à tracer

La transformation numérique a profondément modifié le fonctionnement des organisations. Systèmes d'information, technologies opérationnelles, bâtiments intelligents, contrôle d'accès, vidéosurveillance, objets connectés et infrastructures techniques sont aujourd'hui de plus en plus interconnectés.

Cette évolution apporte des gains considérables en matière d'efficacité, de supervision et d'automatisation. Elle crée également de nouvelles dépendances.

Une cyberattaque ne produit plus nécessairement des effets uniquement numériques. Elle peut perturber des opérations, empêcher l'accès à des installations, affecter des équipements ou compromettre la continuité d'une activité.

À l'inverse, une intrusion physique peut permettre d'accéder à un poste informatique, à un équipement réseau, à un système technique ou à une information facilitant ensuite une compromission numérique.

La distinction traditionnelle entre cybersécurité et sécurité physique devient ainsi moins évidente lorsque les actifs, les technologies et les processus qu'elles protègent sont eux-mêmes interdépendants.

Ces interactions font émerger des risques hybrides : des risques dont l'origine, la propagation ou les conséquences traversent plusieurs domaines de sécurité.

Pourtant, dans de nombreuses organisations, ces domaines continuent d'être gérés par des fonctions différentes, disposant de leurs propres responsabilités, outils, processus et cultures professionnelles.

L'enjeu n'est pas de remettre en cause cette spécialisation. Il est de déterminer si ces différentes fonctions sont suffisamment coordonnées lorsque le risque franchit leurs frontières respectives.

C'est l'objet de ce livre blanc.

Table des matières

1. Pourquoi parler aujourd'hui de risques hybrides ? 1

2. Comprendre les risques hybrides 2

3. Le problème des silos 3

4. Quatre enjeux majeurs 5

5. Six dimensions pour comprendre la convergence 7

01 — Gouvernance & leadership 7
02 — Organisation & collaboration 8
03 — Gestion des risques hybrides 8
04 — Technologies & intégration 9
05 — Détection & réponse 9
06 — Culture, compétences & amélioration continue 9

6. Évaluer son niveau de maturité 10

7. Du diagnostic à l'amélioration 11

8. Dix bonnes pratiques 12

9. Votre organisation est-elle préparée aux risques hybrides ? 13

10. Ce que la convergence ne doit pas devenir 14

11. Une sécurité dynamique 15

Conclusion 15

Le diagnostic de maturité FOCUS 16

À propos de cette publication 16

À propos de FOCUS 17

Références principales 17

1. Pourquoi parler aujourd'hui de risques hybrides ?

Des organisations devenues cyber-physiques

La sécurité physique et la cybersécurité se sont historiquement développées autour de problématiques différentes.

La sécurité physique protège principalement les personnes, les biens, les installations et les infrastructures. La cybersécurité s'est développée autour de la protection des systèmes d'information, des réseaux et des données.

Cette distinction reste pertinente. Les compétences nécessaires ne sont pas identiques et la convergence ne signifie pas que ces métiers doivent être fusionnés.

Ce qui a changé est **l'environnement dans lequel ils interviennent**.

Les bâtiments intègrent désormais des systèmes numériques. Les dispositifs de contrôle d'accès sont connectés. Les caméras fonctionnent sur des réseaux IP. Les installations techniques sont supervisées à distance. Les environnements industriels associent systèmes informatiques et technologies opérationnelles. Les collaborateurs accèdent à des ressources numériques depuis de multiples lieux et équipements.

Le monde physique dépend donc davantage du numérique, tandis que le numérique continue de dépendre d'éléments très physiques : bâtiments, alimentations électriques, équipements, réseaux, personnes et accès.

Une organisation moderne constitue ainsi un **système d'interdépendances**.

Une faiblesse dans un domaine peut produire des effets dans un autre.

C'est précisément dans ces interfaces que se situent les risques hybrides.

Le risque ne respecte pas l'organigramme

Une organisation peut disposer d'une excellente équipe cybersécurité et d'un dispositif de sécurité physique performant tout en conservant certaines vulnérabilités à leur interface.

Pourquoi ?

Parce qu'un attaquant, un incident ou une défaillance ne respecte pas nécessairement la répartition interne des responsabilités.

Un événement peut commencer dans le monde physique et se poursuivre dans le numérique. Il peut également suivre le chemin inverse ou combiner simultanément plusieurs modes d'action.

La question devient alors moins :

« Chaque fonction de sécurité fait-elle correctement son travail ? »

que :

« Que se passe-t-il lorsque le risque traverse plusieurs fonctions ? »

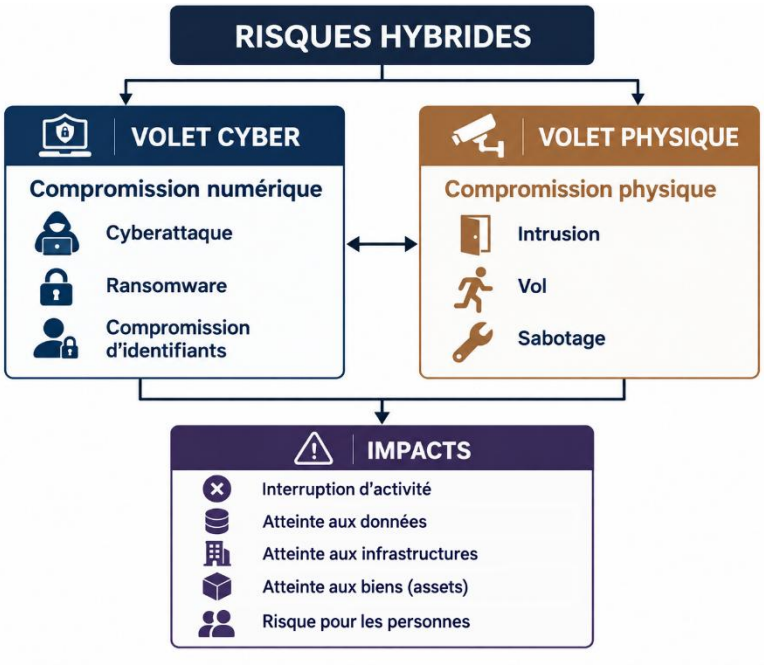
Cette évolution justifie une approche davantage transversale de la sécurité.

2. Comprendre les risques hybrides

Une interaction entre dimensions numériques et physiques

Dans le cadre de ce livre blanc, un **risque hybride** désigne un risque résultant de l'interaction entre les dimensions numériques et physiques d'une organisation, susceptible de produire des conséquences croisées sur les personnes, les biens, les processus, les systèmes ou les infrastructures.

Trois grandes dynamiques permettent de comprendre cette logique.



Du cyber vers le physique

Une compromission numérique peut perturber ou modifier le fonctionnement d'un système et produire des conséquences dans le monde physique.

Il peut s'agir, par exemple, d'une attaque affectant un système industriel, une installation technique, un dispositif de contrôle ou la disponibilité d'un service indispensable aux opérations.

L'incident commence dans l'environnement numérique mais ses conséquences dépassent celui-ci.

Du physique vers le cyber

Le chemin inverse existe également.

L'accès physique à un bâtiment, une zone technique, un poste de travail ou un équipement peut permettre d'atteindre des ressources numériques normalement protégées par plusieurs couches de sécurité logique.

Une intrusion physique peut également permettre d'observer des informations, de récupérer un équipement, d'exploiter un accès laissé actif ou de connecter un dispositif à une infrastructure.

La sûreté des accès devient alors une composante de la protection du système d'information.

Les actions combinées

Certains scénarios reposent enfin sur la combinaison de plusieurs dimensions : actions numériques, intrusion physique, ingénierie sociale, exploitation d'informations publiques ou manipulation humaine.

La force du scénario ne provient alors pas nécessairement de la sophistication d'une seule attaque, mais de **l'enchaînement de plusieurs vulnérabilités appartenant à des domaines différents**.

3. Le problème des silos

Des expertises fortes peuvent rester insuffisamment coordonnées

La spécialisation constitue une nécessité. Une organisation complexe a besoin de compétences cyber, IT, OT, sûreté, continuité, gestion de crise, gestion des risques, conformité et métiers.

Le problème apparaît lorsque cette spécialisation devient un **cloisonnement**.

Des chaînes hiérarchiques différentes, des budgets distincts, des outils propres à chaque fonction ou l'absence de processus communs peuvent limiter la circulation de l'information.

Une équipe peut alors disposer d'une information importante pour une autre sans nécessairement en identifier la pertinence.

Un événement considéré comme mineur dans un domaine peut également devenir un indicateur important lorsqu'il est rapproché d'un autre.

Notre approche souligne l'importance d'une gouvernance transverse, de mécanismes de coordination et d'une circulation efficace de l'information, **sans préconiser nécessairement la fusion des fonctions cyber et physiques**.

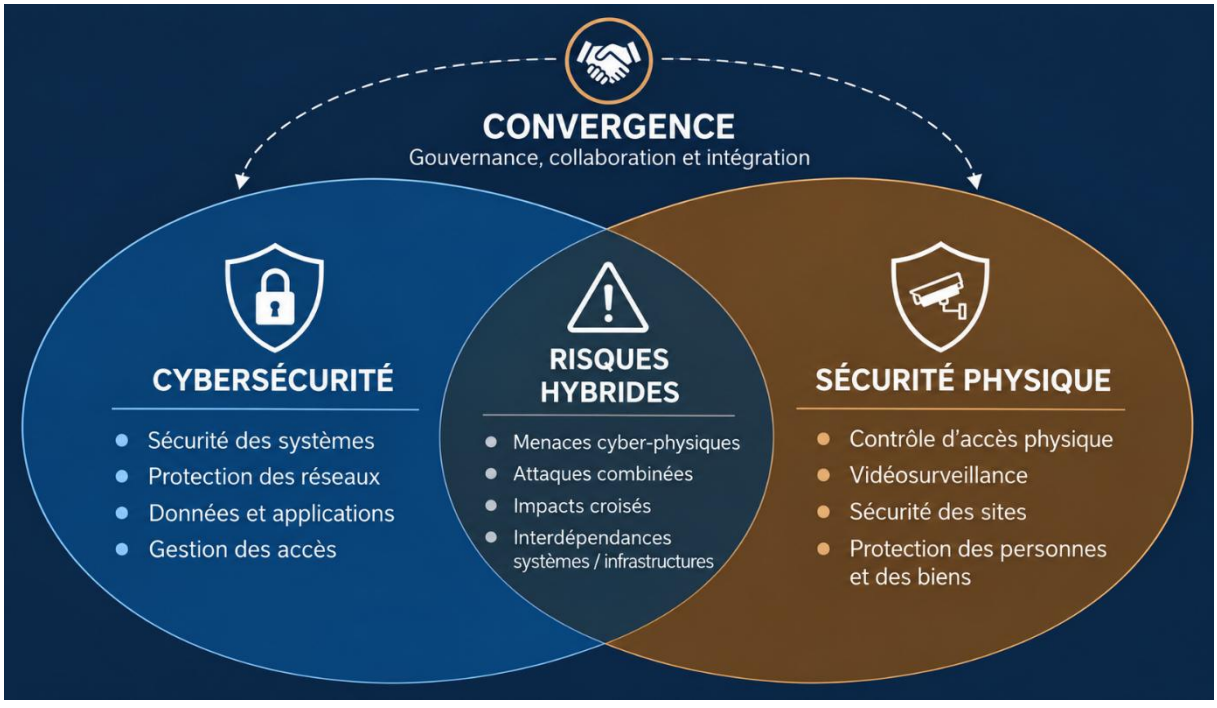
Convergence ne signifie pas fusion

C'est un point essentiel.

La convergence cyber-physique ne consiste pas à transformer les spécialistes de la sécurité physique en experts cyber, ni les spécialistes cyber en responsables de sûreté.

Elle ne nécessite pas non plus de placer systématiquement toutes les fonctions de sécurité sous une même direction.

La convergence consiste plutôt à créer les conditions permettant aux différentes expertises de **comprendre leurs interdépendances et de travailler ensemble lorsque cela est nécessaire**.



Elle peut notamment porter sur :

la gouvernance · les responsabilités · le partage d'information · l'évaluation des risques · les procédures · les technologies · la détection · la réponse aux incidents · la gestion de crise · la formation et la culture de sécurité.

Le niveau de convergence pertinent dépend donc de chaque organisation.

> **La convergence n'est pas une fin en soi. Elle constitue un moyen d'améliorer la capacité de l'organisation à comprendre, prévenir, détecter et gérer des risques qui traversent plusieurs domaines de sécurité.**

4. Quatre enjeux majeurs

Les travaux ayant conduit au développement de l'approche FOCUS font ressortir quatre grandes catégories d'enjeux : **organisationnels, techniques, humains et réglementaires**. Ces enjeux sont interdépendants : une faiblesse dans l'un d'eux peut produire des effets dans les autres.









01 — Enjeux organisationnels

La première difficulté réside souvent dans la gouvernance.

Qui possède une vision globale des risques hybrides ? Qui décide lorsqu'un événement concerne plusieurs domaines ? Existe-t-il des mécanismes permanents permettant aux différentes fonctions de partager leurs informations ?

Une organisation peut disposer d'excellentes capacités spécialisées tout en manquant d'une **vision commune de la situation**.

La convergence commence donc par la clarification des responsabilités et des interfaces.

02 — Enjeux techniques

L'interconnexion des technologies constitue une deuxième difficulté.

Les systèmes de contrôle d'accès, de vidéosurveillance, de gestion technique du bâtiment, les réseaux IT, les technologies opérationnelles et les équipements connectés peuvent partager des infrastructures, des identités ou des données.

La sécurité d'un système ne peut donc plus toujours être appréciée indépendamment de son environnement.

L'enjeu n'est pas nécessairement de connecter davantage les outils de sécurité, mais de **comprendre leurs dépendances et de maîtriser leurs interfaces**.

03 — Enjeux humains

La convergence repose également sur les personnes.

Les cultures professionnelles diffèrent. Les terminologies, les méthodes d'analyse, les priorités et même la perception du risque peuvent varier fortement entre équipes.

Créer une compréhension commune ne signifie pas uniformiser les compétences. Il s'agit plutôt de permettre à chacun de comprendre suffisamment les enjeux des autres fonctions pour **identifier une information pertinente, savoir à qui la transmettre et agir de manière coordonnée**.

04 — Enjeux réglementaires

Enfin, les organisations évoluent dans un environnement réglementaire et normatif de plus en plus exigeant.

Protection des données, cybersécurité, continuité d'activité, résilience des infrastructures et gouvernance des risques interagissent progressivement.

Les principaux référentiels étudiés dans les travaux à l'origine de ce livre blanc — notamment ISO/IEC 27001, ISO 31000, ISO 22301, NIST CSF 2.0 ainsi que les cadres suisses de cybersécurité et de résilience — convergent vers l'importance de la gouvernance, de la gestion des risques et de l'amélioration continue, même s'ils n'abordent pas tous directement la convergence cyber-physique.

La conformité reste cependant un socle et non une garantie absolue de sécurité.

> **Les quatre enjeux sont interdépendants. La convergence ne consiste pas à les traiter séparément, mais à comprendre leurs interactions.**

5. Six dimensions pour comprendre la convergence

Un modèle développé par FOCUS

Pour traduire ces enjeux en une démarche structurée, FOCUS a développé un **modèle de diagnostic de maturité de la convergence cyber-physique**.

Il ne cherche pas à certifier une organisation ni à vérifier sa conformité à une norme.

Son objectif est différent : **apprécier le niveau de maturité de la convergence, identifier les écarts entre différentes dimensions et orienter une trajectoire d'amélioration adaptée à son contexte.**

Le modèle complet repose sur six dimensions interdépendantes.

DIMENSION	RÔLE DANS LA CONVERGENCE
01 Gouvernance & leadership	Fournit l'impulsion stratégique, définit les responsabilités et crée les conditions d'une coordination efficace.
02 Organisation & collaboration	Favorise la coordination entre les fonctions, la circulation de l'information et le décloisonnement des pratiques.
03 Gestion des risques hybrides	Permet d'identifier, d'évaluer et de traiter les risques liés aux interdépendances entre les domaines physiques et numériques.
04 Technologies & intégration	Apporte les capacités techniques nécessaires à la convergence tout en garantissant la sécurité et la résilience des systèmes interconnectés.
05 Détection & réponse	Facilite la détection précoce des événements, une analyse commune de la situation et une réponse coordonnée.
06 Culture, compétences & amélioration continue	Développe une compréhension commune, renforce les compétences et soutient une amélioration continue adaptée aux enjeux de l'organisation.

01 — Gouvernance & leadership

Donner une direction commune

La convergence commence au niveau de la gouvernance.

Une organisation doit être capable de déterminer comment les risques hybrides sont intégrés dans ses décisions et comment les responsabilités sont réparties entre les différentes fonctions.

La direction joue ici un rôle essentiel.

Elle ne doit pas nécessairement intervenir dans les détails techniques, mais elle doit permettre une vision commune, clarifier les responsabilités et arbitrer les priorités.

Questions essentielles :

La convergence dispose-t-elle d'un pilotage identifiable ?
Les responsabilités sont-elles claires ?
Les risques hybrides remontent-ils au niveau décisionnel approprié ?
Les différentes fonctions partagent-elles des objectifs compatibles ?

Une convergence exclusivement portée par les équipes opérationnelles risque de rester ponctuelle. Pour devenir durable, elle doit être soutenue par la gouvernance.

02 — Organisation & collaboration

Dépasser les silos sans supprimer les expertises

Une gouvernance commune ne suffit pas si les équipes ne disposent pas de mécanismes leur permettant de collaborer au quotidien.

Cette dimension s'intéresse aux processus transverses, aux échanges d'information, aux interfaces entre équipes et aux mécanismes de coordination.

L'objectif n'est pas de multiplier les réunions.

Il est de s'assurer que **la bonne information parvient à la bonne fonction au bon moment**.

Cela peut passer par des échanges réguliers, des procédures communes, des points de contact identifiés ou des mécanismes d'escalade partagés.

La maturité se mesure moins au nombre de structures mises en place qu'à leur capacité réelle à fonctionner lorsque la situation l'exige.

03 — Gestion des risques hybrides

Voir les scénarios dans leur ensemble

Une cartographie séparée des risques cyber et des risques physiques peut laisser apparaître des angles morts.

Cette troisième dimension cherche donc à déterminer si l'organisation identifie les actifs critiques, leurs dépendances et les scénarios susceptibles de produire des effets croisés.

Un risque hybride doit être analysé comme une **chaîne d'événements**, et non uniquement comme un incident isolé.

Par exemple :

intrusion physique non autorisé → accès à un équipement → compromission numérique → perturbation opérationnelle.

Ou, dans l'autre sens :

compromission numérique → perte de supervision → perturbation d'un processus physique → impact sur l'activité.

L'objectif est d'identifier les chemins possibles de propagation du risque.

04 — Technologies & intégration

Comprendre les interdépendances technologiques

Les technologies soutiennent aujourd'hui aussi bien les opérations que les dispositifs de protection.

Cette dimension examine notamment les interactions entre systèmes connectés, technologies opérationnelles, contrôle des accès, identités et moyens de supervision.

Une intégration plus poussée n'est pas systématiquement synonyme de meilleure sécurité.

Une technologie supplémentaire peut également créer une nouvelle dépendance.

La question pertinente devient donc :

Nos technologies de sécurité sont-elles seulement performantes individuellement ou leur fonctionnement collectif est-il également compris et maîtrisé ?

Une organisation mature doit notamment connaître les principales dépendances entre ses systèmes critiques et savoir comment un incident dans l'un d'eux peut affecter les autres.

05 — Détection & réponse

Construire une représentation commune de l'incident

Détecter un événement ne suffit pas.

Encore faut-il comprendre ce qu'il signifie.

Un événement physique peut constituer le premier indicateur d'une attaque numérique. Un événement cyber peut annoncer ou accompagner une action physique.

Lorsque les informations restent séparées, les équipes risquent de ne percevoir qu'une partie du scénario.

Cette dimension examine donc la capacité de l'organisation à **détecter, partager, corréler et traiter les événements susceptibles de concerner plusieurs fonctions**.

Elle englobe également la réponse aux incidents et les mécanismes d'escalade.

Face à un incident hybride, la qualité de la coordination peut devenir aussi importante que la qualité des outils de détection.

06 — Culture, compétences & amélioration continue

Faire de la convergence une pratique durable

Les technologies et les procédures ne fonctionnent que si les personnes les comprennent et les utilisent.

La dernière dimension porte donc sur la culture de sécurité, la sensibilisation, les compétences transversales, l'implication du management et l'amélioration continue.

Les équipes n'ont pas besoin de maîtriser toutes les disciplines.

Elles doivent cependant comprendre suffisamment les domaines voisins pour reconnaître une situation inhabituelle et mobiliser rapidement les bonnes compétences.

La convergence devient réellement mature lorsqu'elle cesse d'être un projet ponctuel pour devenir **une manière habituelle de penser la sécurité**.

6. Évaluer son niveau de maturité

Mesurer la progression plutôt que rechercher une conformité

Le modèle FOCUS repose sur une logique de maturité.

Cette approche permet d'apprécier la progression d'une organisation depuis une situation essentiellement cloisonnée jusqu'à une coordination davantage intégrée et inscrite dans une démarche d'amélioration continue.

Le diagnostic comporte **plusieurs questions structurées autour des six dimensions**, associées à une échelle de maturité à cinq niveaux. Les résultats permettent notamment de visualiser les écarts entre dimensions et d'orienter les priorités.



Un point reste toutefois fondamental :

> **Le niveau global n'est pas le seul élément important. L'équilibre entre les différentes dimensions compte également.**

Une organisation peut, par exemple, disposer de technologies avancées mais d'une gouvernance insuffisamment structurée. Une autre peut avoir développé une excellente collaboration entre équipes tout en intégrant encore peu les risques hybrides dans ses processus.

La convergence doit donc être appréciée **dans son ensemble et dans le contexte propre à l'organisation**.

7. Du diagnostic à l'amélioration

Principaux éléments de restitution



Une démarche en quatre étapes

Un diagnostic n'a de valeur que s'il conduit à des décisions utiles. Il permet de traduire l'évaluation de la maturité en une lecture structurée des forces, des écarts et des priorités d'amélioration.

La démarche proposée repose donc sur quatre étapes.

Évaluer

Apprécier la situation existante, les pratiques en place et les interactions entre fonctions.

Identifier les écarts

Mettre en évidence les domaines dans lesquels la coordination est insuffisante, informelle ou dépend trop fortement des individus.

Prioriser

Hiérarchiser les améliorations en fonction du contexte, des enjeux, des dépendances et du niveau de maturité.

Orienter une feuille de route

Traduire les priorités en pistes d'amélioration réalistes et progressives.

La technologie n'est pas toujours la première réponse

Lorsqu'un nouveau risque apparaît, la réaction naturelle consiste parfois à rechercher une nouvelle solution technique.

Or les travaux à l'origine de ce livre blanc montrent que la gestion des risques hybrides dépend également — et souvent fortement — de **la gouvernance, de la coordination, des processus et des compétences**.

Avant d'investir dans un nouvel outil, plusieurs questions peuvent être posées :

Les responsabilités sont-elles claires ?
Les équipes communiquent-elles ?
Les scénarios hybrides sont-ils identifiés ?
Les informations disponibles sont-elles correctement partagées ?
Les procédures de réponse sont-elles coordonnées ?

Il est parfois possible d'améliorer significativement la résilience en faisant mieux fonctionner ensemble des capacités déjà existantes.

8. Dix bonnes pratiques

Des actions concrètes pour progresser

01 — Identifier les interdépendances critiques

Ne pas cartographier uniquement les actifs. Identifier également les relations entre systèmes, personnes, infrastructures, fournisseurs et processus.

02 — Clarifier les responsabilités

Déterminer qui pilote et qui intervient lorsqu'un événement concerne plusieurs domaines de sécurité.

03 — Organiser le partage d'information

Définir quelles informations doivent être échangées, entre quelles fonctions et dans quelles circonstances.

04 — Construire des scénarios hybrides

Intégrer aux exercices et réflexions des événements traversant les frontières traditionnelles : cyber vers physique, physique vers cyber ou actions combinées.

05 — Associer les métiers

La sécurité ne concerne pas uniquement les spécialistes. Les métiers connaissent les dépendances opérationnelles et les conséquences réelles d'une interruption.

06 — Intégrer IT, OT et sûreté lorsque cela est pertinent

Dans les environnements concernés, les interactions entre ces domaines doivent être connues et prises en compte dans les décisions.

07 — Coordonner la détection et la réponse

S'assurer qu'un événement détecté dans un domaine puisse être rapidement transmis et interprété par les autres fonctions concernées.

08 — Tester la coordination

Les procédures théoriques ne suffisent pas. Exercices, simulations et tests permettent de vérifier leur fonctionnement réel.

09 — Développer une culture commune

Former les spécialistes aux interfaces avec les autres disciplines plutôt que chercher à transformer chacun en expert de tous les domaines.

10 — Inscrire la convergence dans l'amélioration continue

Les technologies, menaces et organisations évoluent. Le niveau de convergence pertinent aujourd'hui ne sera pas nécessairement suffisant demain.

9. Votre organisation est-elle préparée aux risques hybrides ?

Six questions pour commencer

Une organisation peut disposer de dispositifs performants en cybersécurité et en sécurité physique sans être pleinement préparée à des événements impliquant simultanément ces deux dimensions.

Sans constituer un diagnostic, les questions suivantes permettent d'engager une première réflexion.

1 — Gouvernance

En cas d'incident impliquant simultanément les environnements physiques et numériques, **les responsabilités, le pilotage et les mécanismes de décision sont-ils clairement définis ?**

☐ Oui ☐ Partiellement ☐ Non ☐ Je ne sais pas

2 — Collaboration

Les fonctions cybersécurité, sécurité physique et, lorsque cela est pertinent, IT, OT, continuité ou métiers **échangent-elles régulièrement sur leurs menaces, vulnérabilités et incidents respectifs ?**

☐ Oui ☐ Partiellement ☐ Non ☐ Je ne sais pas

3 — Risques hybrides

Vos évaluations prennent-elles explicitement en compte des scénarios dans lesquels **une compromission physique produit une conséquence numérique — ou inversement ?**

☐ Oui ☐ Partiellement ☐ Non ☐ Je ne sais pas

4 — Technologies

Les interdépendances entre **contrôle d'accès, vidéosurveillance, systèmes connectés, réseaux, systèmes d'information et environnements opérationnels** sont-elles identifiées et comprises par les fonctions concernées ?

☐ Oui ☐ Partiellement ☐ Non ☐ Je ne sais pas

5 — Détection & réponse

Vos procédures permettent-elles de **détecter, qualifier, partager et traiter conjointement** un événement qui traverse la frontière entre cyber et physique ?

☐ Oui ☐ Partiellement ☐ Non ☐ Je ne sais pas

6 — Culture & compétences

Les collaborateurs concernés disposent-ils d'une compréhension suffisante des interactions cyber-physiques pour **identifier un signal faible susceptible de concerner une autre fonction de sécurité ?**

☐ Oui ☐ Partiellement ☐ Non ☐ Je ne sais pas

Comment interpréter vos réponses ?

Ces questions ne constituent volontairement **ni un score, ni un audit, ni une évaluation formelle de maturité**.

Une réponse « non », « partiellement » ou « je ne sais pas » ne signifie pas nécessairement que votre organisation est insuffisamment protégée.

En revanche, plusieurs réponses de ce type peuvent révéler des **zones de convergence à examiner** : responsabilités fragmentées, échanges insuffisamment structurés, interdépendances méconnues, scénarios hybrides peu considérés ou procédures de réponse encore cloisonnées.

La question n'est alors pas nécessairement d'ajouter de nouvelles mesures de sécurité.

Elle consiste d'abord à déterminer si **les mesures, les informations, les compétences et les fonctions déjà en place sont suffisamment coordonnées**.

10. Ce que la convergence ne doit pas devenir

Éviter quatre écueils

La convergence présente également des risques lorsqu'elle est mal comprise.

01 — Vouloir tout centraliser

Une gouvernance coordonnée ne nécessite pas nécessairement une organisation centralisée.

Les expertises spécialisées doivent conserver leur profondeur et leur capacité opérationnelle.

02 — Créer une intégration technologique sans besoin réel

Connecter davantage de systèmes peut améliorer la visibilité mais aussi augmenter la complexité et créer de nouvelles dépendances.

L'intégration doit répondre à un besoin clairement identifié.

03 — Réduire la convergence à un projet informatique

Les enjeux sont autant organisationnels et humains que techniques.

Un projet exclusivement technologique ne résoudra pas un problème de gouvernance ou de coopération.

04 — Chercher un niveau maximal de convergence

Il n'existe pas nécessairement un niveau idéal identique pour toutes les organisations.

Une PME, un établissement de santé, une entreprise industrielle ou une grande organisation n'ont ni les mêmes dépendances ni les mêmes besoins.

L'objectif est donc une convergence **proportionnée et adaptée**, pas une intégration maximale.

11. Une sécurité dynamique

La résilience comme processus

Les menaces évoluent. Les organisations également.

De nouveaux systèmes sont déployés, les infrastructures changent, les fournisseurs évoluent, de nouvelles dépendances apparaissent et les modes opératoires adverses s'adaptent.

La sécurité ne peut donc être considérée comme un état définitivement atteint.

> Une organisation résiliente doit pouvoir :
>
> **anticiper · détecter · comprendre · coordonner · répondre · apprendre · s'adapter.**

La convergence cyber-physique s'inscrit dans cette logique.

Elle ne remplace ni la cybersécurité, ni la sécurité physique, ni la gestion des risques, ni la continuité d'activité.

Elle cherche à **relier ces capacités lorsque leurs interactions deviennent déterminantes**.

Conclusion

Mieux coordonner plutôt que simplement protéger davantage

La transformation numérique a progressivement effacé une partie des frontières entre environnements physiques et numériques, créant de nouvelles opportunités mais aussi de nouvelles dépendances.

Une attaque, une erreur ou une défaillance peut désormais se propager d'un domaine à l'autre et affecter simultanément les informations, les opérations, les infrastructures et les personnes.

Face à cette réalité, l'accumulation de mesures de protection spécialisées ne suffit pas toujours. La capacité d'une organisation à gérer les risques hybrides dépend également de sa faculté à **comprendre ses interdépendances, coordonner ses fonctions de sécurité, partager l'information et développer une représentation commune des risques**.

La convergence ne signifie pas fusionner les métiers, mais créer les conditions permettant à leurs expertises respectives de fonctionner ensemble lorsque le risque l'exige.

Cette approche doit rester proportionnée au contexte, aux enjeux et au niveau de maturité de chaque organisation. La convergence doit ainsi être envisagée moins comme une destination que comme **une démarche progressive d'amélioration de la résilience**.

> **Vous avez peut-être déjà investi dans la cybersécurité et la sécurité physique. La question est désormais de savoir si toutes ces composantes fonctionnent réellement ensemble.**

Le diagnostic de maturité FOCUS

Du questionnement à une évaluation structurée

Les six questions proposées dans ce livre blanc constituent un premier outil de sensibilisation. Elles ne permettent pas d'établir le niveau de maturité d'une organisation.

FOCUS a développé un **modèle de diagnostic de maturité de la convergence cyber-physique** structuré autour de six dimensions :

Gouvernance & leadership
Organisation & collaboration
Gestion des risques hybrides
Technologies & intégration
Détection & réponse
Culture, compétences & amélioration continue

Le diagnostic vise à **identifier les principaux écarts de convergence, à apprécier le niveau de maturité et à orienter les priorités d'amélioration**.

Il ne se substitue ni à un audit technique de cybersécurité ni à une analyse détaillée des risques. Il apporte une **lecture transversale de la coordination entre les différentes fonctions de sécurité**.

ÉVALUER VOTRE NIVEAU DE CONVERGENCE CYBER-PHYSIQUE

FOCUS

Investigations · Sûreté · Conseil

À propos de cette publication

Origine de la démarche

Les travaux présentés dans ce livre blanc s'inscrivent dans le prolongement d'un **travail académique consacré à la gestion des risques hybrides et à la convergence entre cybersécurité et sécurité physique**, réalisé dans le cadre du **Certificate of Advanced Studies HES-SO en Sécurité et sûreté (CAS SEC) de la HEIG-VD**.

Cette recherche a notamment conduit au développement d'un **modèle de diagnostic de maturité de la convergence cyber-physique**.

Le modèle et les réflexions qui en découlent ont ensuite été adaptés et développés par FOCUS dans une perspective de **recherche appliquée et d'utilisation professionnelle**. Le travail académique dont cette démarche est issue reposait notamment sur une revue de littérature scientifique et professionnelle, l'étude de référentiels reconnus et des échanges avec des experts du domaine.

Le présent livre blanc constitue une publication FOCUS. Il vise à vulgariser la problématique, partager des bonnes pratiques et contribuer à la réflexion des organisations confrontées à des environnements physiques et numériques de plus en plus interdépendants.

À propos de FOCUS

Investigations · Sûreté · Conseil

FOCUS accompagne les entreprises et institutions dans l'analyse de situations sensibles, l'évaluation de leurs dispositifs de sûreté et la maîtrise de leurs risques.

Ses activités s'articulent autour de trois domaines complémentaires :

Investigations — établir les faits et comprendre les situations.

Audits & tests — identifier les vulnérabilités et évaluer les protections.

Conseil — accompagner les organisations dans leurs enjeux de sûreté et contribuer à une meilleure maîtrise des risques.

FOCUS développe également ses propres **méthodes, outils d'évaluation et approches opérationnelles**, enrichis par la pratique, la recherche appliquée et une démarche d'amélioration continue.

Les travaux consacrés aux risques hybrides et à la convergence cyber-physique s'inscrivent dans cette dynamique.

Références principales

ISO/IEC 27001:2022 — Organisation internationale de normalisation (ISO) et Commission électrotechnique internationale (IEC). *Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences*, 2022.

ISO 31000:2018 — Organisation internationale de normalisation (ISO). *Management du risque — Lignes directrices*, 2018.

ISO 22301:2019 — Organisation internationale de normalisation (ISO). *Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences*, 2019.

NIST CSF 2.0 — National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, 2024.

Norme minimale pour les TIC (2023) — Office fédéral pour l'approvisionnement économique du pays (OFAE). *Norme minimale pour améliorer la résilience informatique*, 2023.

MCSR (2025) — Office fédéral de la cybersécurité (OFCS). *Méthode de cybersécurité et de résilience — Une approche structurée pour renforcer la cybersécurité et la résilience*, 2025.

Cybersecurity and Physical Security Convergence — Cybersecurity and Infrastructure Security Agency (CISA). *Cybersecurity and Physical Security Convergence Action Guide*, 2021.

Directive (UE) 2022/2555 (NIS2) — Parlement européen et Conseil de l'Union européenne. *Directive du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union*, 2022.

Directive (UE) 2022/2557 (CER) — Parlement européen et Conseil de l'Union européenne. *Directive du 14 décembre 2022 sur la résilience des entités critiques*, 2022.