Le financement d’infrastructures intelligentes et numériques

9 novembre 2026

Auteurs

David Tournier

Associé, Avocat

Jessy Menard

Avocat

Comme nous le concluions dans notre précédent article de cette série[1], les données et les indicateurs de performance des infrastructures intelligentes doivent être fiables, vérifiables et encadrés contractuellement pour qu’un projet dans ce domaine puisse être financé. La couche technologique ajoute des risques propres qui, comme tous les autres risques[2], doivent être alloués de manière claire et efficace au sein des contrats d’infrastructure.

Cet article examine la question en trois temps. Premièrement, la cybersécurité, qui demeure un risque orphelin dans bien des contrats. Deuxièmement, l’intégration des systèmes et la durée de vie, plus courte, de la technologie. Troisièmement, la donnée et le jumeau numérique, qui peuvent servir de preuve au prêteur comme au donneur d’ouvrage.

La cybersécurité, risque orphelin des contrats

Les systèmes d’automatisation et de gestion des bâtiments (en anglais, *BAS* et *BMS*) en pilotent le chauffage, la ventilation et la climatisation, l’éclairage, le contrôle d’accès et parfois la protection incendie. Longtemps isolés, ils sont aujourd’hui reliés au réseau de l’entreprise, à l’infonuagique et aux outils d’accès à distance des fournisseurs.

Plusieurs de ces systèmes reposent encore sur des protocoles anciens, non chiffrés, et sur des identifiants par défaut. Selon une étude de Claroty portant sur plus de 467 000 appareils de gestion de bâtiments dans 529 organisations :

- 75 % de ces organisations utilisent des appareils présentant des vulnérabilités connues; et
- 69 % utilisent des appareils dont les vulnérabilités ont déjà servi à des attaques par rançongiciel[3].

Ce dernier chiffre rejoint le constat du Centre canadien pour la cybersécurité, pour qui l’exposition

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

aux cybermenaces augmente avec l'essor des objets connectés et les rançongiciels constituent la principale menace cybercriminelle visant les infrastructures essentielles du Canada[4].

Une attaque sur le système de gestion d'un bâtiment peut paralyser les opérations d'une infrastructure et causer des dommages bien réels, que ce soit :

des équipements endommagés;
des stocks perdus;
des données détruites ou divulguées;
des coûts de remise en état; et
dans les cas les plus graves, la mise en danger des occupants.

En plus de ces coûts, dans un PPP à paiements de disponibilité, cette indisponibilité entraîne par elle-même des déductions, donc une baisse des flux qui servent la dette. Le risque cyber devient ainsi un risque de revenus, que les prêteurs auraient de bonnes raisons de traiter comme n'importe quel risque d'exploitation, au même titre qu'un bris d'équipement.

Le plus grave, c'est que la cybersécurité est encore trop souvent oubliée dans la structure contractuelle. En conséquence, ni le concepteur, ni le constructeur, ni l'intégrateur, ni l'exploitant n'en prend réellement la charge, alors que tous peuvent être impactés en cas de bris.

Par ailleurs, ce risque n'attend pas la phase d'exploitation : une simple clé USB infectée utilisée lors de la programmation d'un équipement peut suffire à compromettre l'ensemble des installations et retarder la mise en service, alourdissant la facture.

Prévenir le risque dès la conception et la construction

Pour éviter d'en arriver là, la protection doit donc commencer avant même le chantier. La Smart Buildings Alliance recommande ainsi d'intégrer la cybersécurité dès la conception et de l'inscrire dans chaque cahier des charges, notamment :

en répertoriant les équipements connectés;
en segmentant les réseaux du bâtiment;
en sécurisant les accès à distance;
en encadrant la gestion des mots de passe, des identités et des droits d'accès; et
en prévoyant des exigences de tests, de certification et de protocole[5].

Sur le chantier, à l'image de l'agent de prévention qui veille au port des équipements de protection, un « agent cyber » pourrait être désigné pour contrôler les logiciels, les ordinateurs portables et les clés USB utilisés pour le projet.

Répartir les obligations et préserver les droits d'intervention

Contractuellement, une section sur la cybersécurité devrait être intégrée à l'appel d'offres et déclinée à chaque phase (conception, construction, mise en service, exploitation), avec un responsable désigné et des rencontres de coordination tenues tôt dans le projet.

On retrouve ici le principe exposé dans notre troisième article : si la société de projet promet un standard de service au donneur d'ouvrage, elle doit pouvoir « acheter » ce même standard auprès de ses contractants, faute de quoi le risque reste coincé chez elle.

L'obligation de cybersécurité doit donc descendre en cascade dans le contrat de conception-construction, le contrat d'exploitation et les contrats de fourniture, avec des définitions communes (ce qu'est un incident, les délais de notification, les droits d'audit).

Quant aux droits d'intervention des prêteurs, ils ne valent pas grand-chose si personne ne peut reprendre la main sur les systèmes. Il faut donc prévoir la remise ou le dépôt des identifiants, des codes et de la documentation, au même titre que les plans de l'ouvrage.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

Cadre législatif applicable au Canada et au Québec

Le cadre normatif, lui, accuse un retard certain en la matière. Au fédéral, le projet de loi C-8 a reçu la sanction royale le 15 juin 2026 et édicte la *Loi sur la protection des cybersystèmes essentiels*[6].

Cette loi, qui n'est pas encore en vigueur, vise à assurer la continuité et la sécurité de systèmes critiques exploités par certains exploitants désignés dans des secteurs de compétence fédérale, comme :

> les télécommunications;
> les pipelines et lignes électriques interprovinciaux ou internationaux;
> l'énergie nucléaire;
> les transports de compétence fédérale; et
> les systèmes bancaires, de compensation et de règlement[7].

Les hôpitaux, les écoles et les édifices municipaux, qui composent l'essentiel de nos infrastructures publiques, demeurent donc hors de son champ.

Au Québec, la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* oblige certes les organismes publics à assurer la sécurité de leurs ressources informationnelles, mais il n'existe pas encore, pour la cybersécurité des bâtiments, d'équivalent du code du bâtiment ou des règles de santé et de sécurité du travail.

En attendant que le législateur édicte un code du bâtiment numérique, c'est donc au contrat de s'inventer régulateur.

Par ailleurs, les prêteurs examinent généralement l'assurabilité du risque, ses exclusions et ses franchises, et un risque ni assuré ni alloué peut appeler des réserves, un cautionnement des actionnaires ou une marge plus élevée. La Banque mondiale rappelle d'ailleurs que l'assurance est souvent laissée à la fin des négociations, alors qu'elle influe directement sur les risques assumés par le donneur d'ouvrage, la société de projet et les prêteurs[8].

Intégrer les systèmes, et les faire durer

Le rôle du maître de l'intégration des systèmes

Un bâtiment intelligent réunit des systèmes de plusieurs fournisseurs, chacun avec son mandat, son interface et sa logique propre. Or, une interface que personne ne gère est un risque que personne ne porte, et que le prêteur pourrait bien faire porter à la société de projet ou à ses actionnaires.

C'est tout l'intérêt du maître de l'intégration des systèmes (en anglais, *Master Systems Integrator* ou *MSI*). Celui-ci coordonne l'intégration des sous-systèmes en un ensemble cohérent, établit des formats de données communs et assume la responsabilité du cycle de vie du système de gestion, de la planification aux mises à niveau, en passant par les essais et l'entretien[9]. Il permet au constructeur de se décharger de ces interfaces technologiques et offre au prêteur un point unique de responsabilité.

Encore faut-il régler quelques questions contractuelles pour ne pas remplacer une interface mal gérée par un nouvel interstice entre le MSI et le constructeur. Il faut déterminer si le MSI est lié à la société de projet, au constructeur ou à l'exploitant, s'assurer que ses obligations reflètent celles du contrat de projet et que son mandat survit à la réception de l'ouvrage, vérifier que son assurance responsabilité professionnelle couvre le risque de cybersécurité de façon satisfaisante…

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

Financer le cycle de vie technologique et réduire la dépendance envers les fournisseurs

Par ailleurs, l'ouvrage physique est conçu pour durer des décennies, alors que les équipements et les logiciels qui le pilotent se renouvellent à l'échelle de quelques années.

Licences, correctifs, surveillance et remplacement des capteurs sont des dépenses d'exploitation dont doit tenir compte le modèle financier. Il faut budgétiser ce renouvellement, par exemple au moyen de réserves de cycle de vie propres au numérique ou d'une indexation des paiements.

À défaut, le sous-financement de l'exploitation peut devenir un risque d'indisponibilité, puis de défaut. La dépendance envers un fournisseur appelle enfin des obligations de documentation, d'interopérabilité et d'assistance à la transition, qui serviraient aussi la continuité du service si les prêteurs devaient intervenir.

La donnée, preuve de performance et source de revenus

Encadrer la propriété, l'accès et la vérification des données

Les paiements fondés sur le rendement, présentés dans notre deuxième article[10], comme les indicateurs environnementaux dont traitait notre quatrième[11], reposent sur des données. Il faut donc savoir qui les détient, qui y a accès, selon quelle méthode elles sont produites et qui peut les vérifier. Sinon, le mécanisme de paiement pourrait devenir contestable, ce qui constitue un risque de crédit pour un prêteur.

Deep Sky, dont nous parlions dans notre précédent article, offre une illustration éloquente de fiabilité des données. Le 29 juin 2026, l'entreprise montréalaise et le certificateur Isometric ont annoncé l'émission, à partir de l'installation Deep Sky Alpha en Alberta, des premiers crédits de retrait de carbone par captage direct dans l'air certifiés en Amérique du Nord, au bénéfice de Microsoft et de la Banque Royale du Canada. Le protocole applicable exige la comptabilisation de l'ensemble des émissions du projet et une surveillance à long terme du stockage[12]. Dans ce modèle, aucun crédit n'est émis sans mesure vérifiée, et aucun paiement n'est dû sans crédit. La donnée est donc ici littéralement la source du revenu.

Le même raisonnement s'applique à l'échelle d'un réseau. Le programme de biénergie d'Énergir, évoqué lui aussi dans notre précédent article, repose sur des bâtiments capables de passer d'une source d'énergie à une autre, notamment lors des pointes hivernales[13].

Une telle gestion de l'énergie comme système suppose des équipements qui communiquent des données fiables, des systèmes bien intégrés et des contrats qui précisent à qui appartiennent ces données.

Le développement des jumeaux numériques

L'innovation du jumeau numérique est une autre illustration de l'impact des données sur le financement de projets modernes. Au Québec, la feuille de route gouvernementale sur la modélisation des données des infrastructures (*Building Information Modeling (BIM)*) a vu le nombre de projets de ses huit donneurs d'ouvrage publics partenaires passer de 77 à 265 entre 2021 et 2025[14].

Au poste des Irlandais d'Hydro-Québec, achevé en septembre 2024, le recours au BIM a permis de limiter les coûts des modifications à 3,6 %, contre 15 à 18 % pour des projets traditionnels. La Ville

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

de Québec, qui a lancé 12 projets en BIM en une année, dont sept en génie civil et voirie, a pour sa part mis en place un environnement de données commun afin d'améliorer la gestion de ses actifs publics[15].

Pour le financement, moins de modifications signifie davantage de certitude sur le coût d'achèvement, au soutien de l'obtention d'un prix ferme. En exploitation, la maintenance prédictive renforce la disponibilité. En contexte de refinancement, un ouvrage bien documenté facilite la vérification diligente des investisseurs de long terme qui prennent le relais après la construction.

Le jumeau numérique est cependant aussi un actif à protéger, puisqu'il cartographie l'ouvrage dans le détail, et un objet de propriété à régler au contrat. On doit donc se poser les questions de la propriété du modèle et des données, des règles de confidentialité applicables, notamment si des capteurs d'occupation recueillent des renseignements personnels, et de la forme dans laquelle la documentation numérique sera remise au donneur d'ouvrage en fin de contrat.

La valeur de l'ouvrage à la remise et sa cessibilité en dépendent, puisqu'un modèle inutilisable ou retenu par un fournisseur réduit d'autant la valeur de l'actif.

Conclusion

Une infrastructure intelligente ne sera finançable que si quelqu'un, au contrat, répond de sa couche technologique. Il faut donc identifier les risques que la technologie introduit, les confier à ceux qui peuvent les gérer et prévoir la preuve qui permettra de vérifier que les obligations y associées ont été remplies. Une certaine littératie numérique des donneurs d'ouvrage et de leurs conseillers devrait d'ailleurs devenir une condition de bonne gouvernance.

L'auteur Isaac Asimov écrivait en 1978 que c'est « le changement, le changement continu, le changement inévitable » qui domine la société d'aujourd'hui, et qu'« aucune décision sensée ne peut plus être prise sans tenir compte non seulement du monde tel qu'il est, mais du monde tel qu'il sera »[16]. C'est la perspective requise d'un contrat d'infrastructure conclu pour plusieurs décennies, alors que la technologie qu'il encadre aura changé plusieurs fois avant son échéance.

Bibliographie

1. D. Tournier et J. Menard. 2026. Financement d'infrastructures durables : de la promesse à la preuve. Lavery. https://www.lavery.ca/fr/publications/nos-publications/6471-financement-dinfrastructures-durables-de-la-promesse-a-la-preuve.html
2. D. Tournier et J. Menard. 2026. Les contrats de nos infras : du projet idéal au projet finançable. Lavery. https://www.lavery.ca/fr/publications/nos-publications/6468-les-contrats-de-nos-infras-du-projet-ideal-au-projet-financable.html
3. Claroty Team82. 2025. State of CPS Security 2025: Building Management System Exposures. https://web-assets.claroty.com/resource-downloads/t82-commercial-report-2025.pdf
4. Centre canadien pour la cybersécurité. 2024. Évaluation des cybermenaces nationales 2025-2026. https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026
5. Smart Buildings Alliance. s.d. Bâtiment intelligent : quelle stratégie pour prévenir les risques en matière de cybersécurité ? (livre blanc La cybersécurisation des bâtiments tertiaires). https://www.smartbuildingsalliance.org/strategie-cybersecurite-smart-building
6. Sécurité publique Canada. 2026. Government of Canada Strengthens Cyber Security and Critical Infrastructure with Royal Assent of Bill C-8. https://www.canada.ca/en/public-safety-canada/news/2026/06/government-of-canada-strengthens-cyber-security-and-critical-infrastructure-with-royal-assent-of-bill-c8.html
7. Osler. 2026. Canada's Bill C-8: what businesses need to know about the new cybersecurity framework. https://www.osler.com/en/insights/updates/canadas-bill-c-8-what-businesses-need-to-know-about-the-new-cybersecurity-framework/
8. Banque mondiale. s.d. Insurance Checklist (PPP Resource Center). https://ppp.worldbank.org/ppp-overview/practical-tools/checklists-and-risk-matrices/insurance-checklist
9. B. Boyd. 2023. Why should you engage a Master Systems Integrator to help develop your smart building?

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

Schneider Electric Blog. https://blog.se.com/buildings/building-management/2023/08/24/what-is-a-master-systems-integrator/
10. D. Tournier et J. Menard. 2026. Financer nos infrastructures : modèles éprouvés et approches innovantes. Lavery. https://www.lavery.ca/fr/publications/nos-publications/6449-financer-nos-infrastructures-modeles-eprouves-et-approches-innovantes.html
11. *Supra*, note 1.
12. Deep Sky. 2026. Deep Sky Delivers North America's First Certified Direct Air Capture Carbon Removal Credits. https://www.deepskyclimate.com/blog/deep-sky-delivers-north-americas-first-certified-direct-air-capture-carbon-removal-credits ; ESG Today. 2026. Deep Sky Delivers First Certified DAC Carbon Credits to Microsoft, RBC. https://www.esgtoday.com/deep-sky-delivers-first-certified-dac-carbon-credits-to-microsoft-rbc/
13. Énergir. 2026. Programme de biénergie électricité – gaz naturel. https://energir.com/files/energir_common/import/Fichiers/Subvention_bienergie/Guide-Participation_bienergie_FR.pdf
14. ReNew Canada. 2025. Quebec updates government roadmap for infrastructure data modeling. https://www.renewcanada.net/quebec-updates-government-roadmap-for-infrastructure-data-modeling/
15. *Supra*, note 14.
16. Notre traduction. Citation originale : « It is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be. » I. Asimov. 1978. « My Own View », dans R. Holdstock (dir.), The Encyclopedia of Science Fiction, Londres, Octopus Books; repris dans I. Asimov. 1981. Asimov on Science Fiction, New York, Doubleday.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.