Financing smart and digital infrastructure

November 9, 2026

Authors

David Tournier

Partner, Lawyer

Jessy Menard

Lawyer

As we concluded in our previous article in this series,[1] smart infrastructure projects require reliable, verifiable and contractually governed data and performance indicators to be bankable. The technology layer embedded in smart infrastructure introduces distinct risks that infrastructure contracts must allocate clearly and effectively, just like any other project risk.[2]

This article examines the issue in three parts. First, cybersecurity, a risk that often goes unallocated in contracts. Second, the risks tied to integrating systems while accounting for technology's shorter lifespan. Third, data and digital twin, which can serve as evidence for both the lender and the project owner.

Cybersecurity, the orphan risk of contracts

Building automation and management systems (*BAS* and *BMS*) control a building's heating, ventilation and air conditioning, lighting, access control and, in some cases, fire protection. Long kept isolated, they are now connected to internal networks, cloud-based platforms and vendor remote-access tools.

Many of them still rely on outdated, unencrypted protocols and default credentials. According to a Claroty study covering more than 467,000 building management devices across 529 organizations:

> 75% of these organizations use devices with known vulnerabilities; and
> 69% use devices with vulnerabilities already exploited in ransomware attacks.[3]

This latter figure echoes the Canadian Centre for Cyber Security's warning that cyber threat exposure grows along with the proliferation of connected devices and that ransomware poses the top cybercrime threat to Canada's critical infrastructure.[4]

An attack on a building management system can paralyze an infrastructure asset's operations and cause tangible harm, including:

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

damaged equipment;
lost inventory;
destroyed or compromised data;
remediation costs; and
in the most severe cases, physical danger to occupants.

In addition to these costs, in an availability-payment PPP, the downtime itself triggers payment deductions, reducing the cash flows available to service debt. Cyber risk therefore becomes a revenue risk that lenders have every reason to treat like any other operational risk, on par with equipment failure.

Most concerning is that cybersecurity is still too often overlooked in the contractual structure. As a result, none of the project stakeholders—designer, contractor, systems integrator or operator—takes genuine responsibility for it, even though a breach can affect them all.

Moreover, systems are exposed long before operations begin: a single infected USB drive used while programming equipment can compromise an entire facility and delay commissioning, driving up costs.

Preventing risk during design and construction

To prevent a breach from ever occurring, protection must begin before construction even starts. The Smart Buildings Alliance recommends building cybersecurity into the design phase and embedding it in every set of specifications, including:

inventorying connected devices;
segmenting building networks;
securing remote access;
enforcing strict identity, password and access controls; and
setting testing, certification and protocol requirements.[5]

Much like a safety officer who ensures workers wear protective gear on a jobsite, a “cyber officer” could be appointed to inspect the software, laptops and USB drives used on a project.

Allocating obligations and preserving step-in rights

From a contractual standpoint, a project’s request for proposals should include a dedicated cybersecurity section broken down across every project phase (design, construction, commissioning and operations), with a designated lead and coordination meetings held early on.

This reflects the principle set out in our third article: if a project company commits to a given service standard toward a public authority, it must be able to secure the same standard from its contractors, failing which the risk is left for the project company to bear.

Accordingly, cybersecurity obligations must flow down into design-build contracts, operating agreements and supply contracts, with uniform definitions (what constitutes an incident, reporting timelines and audit rights).

As for lenders’ step-in rights, they are worth little if no one can take control of the systems. Provision must therefore be made for the delivery or escrow of credentials, codes and documentation, much like blueprints of the work.

Legislative framework in Canada and Quebec

The regulatory framework governing building cybersecurity, however, is lagging behind. At the federal level, Bill C-8 received royal assent on June 15, 2026, and enacts the *Critical Cyber Systems Protection Act*.[6]

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

Not yet in force, the Act is designed to safeguard critical systems and prevent service disruptions among designated operators in federally regulated sectors, such as:

telecommunications;
interprovincial or international pipelines and power lines;
nuclear energy;
federally regulated transportation; and
banking, clearing and settlement systems.[7]

Hospitals, schools and municipal buildings—which make up the bulk of our public infrastructure—therefore remain outside its scope.

In Quebec, while the *Act respecting the governance and management of the information resources of public bodies and government enterprises* requires public bodies to safeguard their information resources, there is still no equivalent to the building code or occupational health and safety rules for building cybersecurity.

Until the legislature enacts a digital building code, contracts will have to fill the regulatory gap.

Furthermore, lenders generally scrutinize a risk's insurability, exclusions and deductibles; an uninsured and unallocated risk can trigger reserve requirements, shareholder guarantees or a higher lending margin. As the World Bank points out, insurance is often left until the end of negotiations, even though it directly affects the risks assumed by the project owner, the project company and the lenders.[8]

Integrating systems and making them last

The role of a master systems integrator

A smart building brings together systems from multiple vendors, each with its own scope of work, interface and internal logic. Left unmanaged, an interface becomes a risk that no one bears, and one that lenders may well shift onto a project company or its shareholders.

This is precisely where a master systems integrator (MSI) comes in. The MSI coordinates the integration of subsystems into a cohesive whole, establishes common data formats and assumes lifecycle responsibility for the management system, from planning and testing through to maintenance and upgrades.[9] By assuming responsibility for technological interfaces, the MSI gives lenders a single point of accountability.

Still, parties must iron out a number of contractual details to avoid replacing one poorly managed interface with a new gap between the MSI and the contractor. They must decide whether the MSI contracts with the project company, the contractor or the operator; ensure the MSI's obligations mirror those of the project agreement and survive acceptance of the work; and verify that the MSI's professional liability insurance adequately covers cybersecurity risks, among other things.

Funding the technology lifecycle and reducing vendor lock-in

Beyond system integration, stakeholders must contend with a basic disconnect in lifespans: a physical structure is built to last for decades, but the hardware and software running it turn over every few years.

Licences, patches, monitoring and sensor replacement are all operating expenses that a project's financial model must capture. Ongoing upgrades must be budgeted for, through dedicated digital

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

lifecycle reserves or payment indexation, for example.

Left unbudgeted, they can create availability risk and ultimately become default risk. Lastly, preventing vendor lock-in requires binding documentation, interoperability and transition-assistance obligations, all of which would also protect service continuity if lenders had to step in.

Data as proof of performance and a revenue driver

Governing data ownership, access and verification

Performance-based payments, introduced in our second article,[10] and the environmental indicators covered in our fourth[11] both rely on data. The parties must therefore establish who owns that data, who can access it, how it is generated and who can verify it. Without clear rules, payment mechanisms can be challenged, creating credit risk for lenders.

Deep Sky, discussed in our previous article, provides a compelling illustration of data reliability in practice. On June 29, 2026, Montréal-based Deep Sky and the carbon removal registry Isometric announced they had issued North America's first certified direct air capture carbon removal credits. Tied to carbon removed at the Deep Sky Alpha facility in Alberta, the credits were purchased by Microsoft and Royal Bank of Canada. Because Isometric's protocol requires accounting for all project emissions and long-term storage monitoring,[12] no credit is issued without verified measurement, and no payment is owed without a credit being issued. Here, data quite literally generates the revenue.

On a larger scale, data is just as critical. Énergir's dual-energy program, also discussed in our previous article, relies on buildings capable of switching from one energy source to another, particularly during winter peak periods.[13]

Managing energy as a system requires equipment that transmits reliable data, well-integrated platforms and contracts specifying who owns the data.

Digital twins

Digital twin innovation further illustrates how data shapes modern project financing. In Quebec, the government's Building Information Modeling (BIM) roadmap saw projects across its eight partner public project owners jump from 77 to 265 between 2021 and 2025.[14]

At Hydro-Québec's Des Irlandais substation, completed in September 2024, using BIM held change costs down to 3.6%, compared to 15% to 18% for traditional projects. The Ville de Québec, which launched 12 BIM projects in a single year—7 of them in civil engineering and roadwork—implemented a common data environment to improve public asset management.[15]

From a financing standpoint, fewer changes mean greater certainty around completion costs, helping secure a fixed price. During operations, predictive maintenance strengthens asset availability. When refinancing, a well-documented asset streamlines due diligence for long-term investors who step in after construction.

However, because a digital twin maps the infrastructure in full detail, it must also be protected as an asset, and its ownership must be settled by contract. Parties must therefore address who owns a digital twin and its underlying data, which privacy rules apply, especially if occupancy sensors collect personal information, and in what format digital documentation will be handed over to the public authority at contract end.

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

An asset's handover value and transferability depend on it, because an unusable digital twin, or one withheld by a vendor, diminishes the infrastructure's value.

Conclusion

Smart infrastructure will be bankable only if one of the parties to the contract takes responsibility for the asset's technology layer. Parties must therefore identify the risks technology introduces, allocate them to those best placed to manage them and establish the evidence needed to verify that related obligations are met. A degree of digital literacy among public authorities and their advisors should also become a condition of good governance.

In 1978, author Isaac Asimov wrote that "it is change, continuing change, inevitable change, that is the dominant factor in society today," and that "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."[16] Multi-decade infrastructure contracts demand the same foresight, as the technology they govern will turn over several times before contract expiry.

Bibliography

1. D. Tournier and J. Menard. 2026. Sustainable infrastructure financing: from promise to proof. Lavery. https://www.lavery.ca/en/publications/our-publications/6471-sustainable-infrastructure-financing-from-promise-to-proof.html
2. D. Tournier and J. Menard. 2026. Our infrastructure contracts: from the ideal project to the bankable project. Lavery. https://www.lavery.ca/en/publications/our-publications/6468-our-infrastructure-contracts-from-the-ideal-project-to-the-bankable-project.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. Canadian Centre for Cyber Security. 2024. National Cyber Threat Assessment 2025-2026. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026
5. Smart Buildings Alliance. n.d. *Bâtiment intelligent : quelle stratégie pour prévenir les risques en matière de cybersécurité ?* (white paper titled *La cybersécurisation des bâtiments tertiaires*). https://www.smartbuildingsalliance.org/strategie-cybersecurite-smart-building [French only]
6. Public Safety 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. World Bank. n.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? Schneider Electric Blog. https://blog.se.com/buildings/building-management/2023/08/24/what-is-a-master-systems-integrator/
10. D. Tournier and J. Menard. 2026. Funding our infrastructure: proven models and innovative approaches. Lavery. https://www.lavery.ca/en/publications/our-publications/6449-funding-our-infrastructure-proven-models-and-innovative-approaches.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. Dual-Energy Electricity and Natural Gas Program. https://energir.com/files/energir_common/import/Fichiers/Subvention_bienergie/Guide-Participation_bienergie_EN.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. I. Asimov. 1978. "My Own View," in R. Holdstock (ed.), *The Encyclopedia of Science Fiction*, London, Octopus Books; quoted in I. Asimov. 1981. *Asimov on Science Fiction*, New York, Doubleday.

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

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