STANDARDS RESEARCH

Information and Communication Technology Infrastructure (ICTi) in Buildings

Exploring Today's Reality for Tomorrow's Needs

November 2020

Author

Andrew Pride, P.Eng., Andrew Pride Consulting, Burlington, Ontario

CSA Group Project Leader

Parag Phalak, B.Eng., MBA

Disclaimer

Table of Contents

Executive Summary

The information and communication technology (ICT) industry is rapidly evolving as significantly more "smart" devices are being connected in buildings. This will put a strain on the ICT infrastructure (ICTi). Many stakeholders are looking for a predictable, secure, and safe operation from their ICTi. This report identifies the gaps between today's market realities and tomorrow's needs, and provides recommendations to help resolve them.

Ultimately the ICTi is about data's movement through the building and data that enters and leaves the building at the building's edge. Historically, data flowed through wires and often used proprietary systems. Today, there are several wired and wireless protocols handling much of the data flow within the building. New and faster wireless solutions, such as fifth generation (5G) cellular and upcoming light fidelity (LiFi) systems, will add another dimension to the ICTi requirements. Standards documents are being continuously updated, and some jurisdictions are creating new specifications for the ICTi. It is challenging for standards to keep pace with ever-evolving technology. This is compounded by the Internet of Things (IoT) expanding connected devices exponentially. Power over Ethernet (PoE) lighting, for instance, could add thousands of new data points in today's average building. The situation has created a new field called operational technology (OT). OT is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, assets, processes, and events in building-related systems. The overarching power of OT may assist in controlling and prioritizing data flow; however, OT alone cannot resolve the market demand for new connected technology. Further, the commingled data streams may contain private and confidential information that will need protection from cybersecurity threats and accidental transmissions.

Stakeholders are looking for predictability, reliability, flexibility, and protection (e.g., safety) in systems that are comprehensive, resilient, and future proof. The buildings industry can depend on codes for building construction, fire systems, plumbing systems, electrical systems, and energy use; however, there are no such regulations or codes available for the ICTi. There is a large roster of standards, available from several standards development organizations, that can be referenced to assist with designing an ICTi. Understanding and selecting the correct one can be challenging. This has resulted in the recent creation of programs and guidelines, such as the Telecommunications Industry Association's (TIA) smart building ecosystem and the Building Industry Consulting Services International's (BICSI) 007 standard. These assist in creating an understanding of ICT and ICTi systems, while not reaching as far as being design tools. On the cybersecurity front, the National Institute of Standards and Technology (NIST) has developed a cybersecurity framework for a critical infrastructure in the United States. The NIST framework could be a starting point for a Canadian model. Often gaps are initially filled by voluntary programs, which is happening in the ICTi commercial sector. A program called WiredScore has entered the market offering a LEED-like rating system for ICTi.

The building industry has identified the following as its primary drivers: to improve the speed of ICT execution; foster innovation; create easy to use systems supporting plug-and-play devices; and facilitate predictable, safe, system-to-system communications that can grow. There are common needs for all building types and likely some unique and specific needs for various occupancies. For example, health care facilities will have some similar needs to multi-unit residential or factory buildings; however, they will have significantly greater need for privacy, resiliency, and security.

There are several notable gaps between today's infrastructure needs and the available tools to support the industry. Building owners, managers, and occupants are looking for consistency and predictably from their ICTi, which do not currently exist. They are looking for service quality levels to be identifiable and enforced, which can be challenging when connected devices are growing at an unpredictable rate and are being promoted by unsubstantiated claims. Commissioning challenges were also identified as a gap as there are few rules to follow and potentially millions of connection points, and so was the increased requirement for data privacy and cybersecurity. New OT systems will help; however, there aren't enough human resources or educational programs to build the needed OT capacity.

To address the gaps and align with ICT values, this report recommends 12 actions that can be pursued. The recommendations are grouped into three categories: standards documents; capacity and awareness; and research.

For standards documents, the recommendation is to develop an ICTi code for buildings that can be enforced and provide rigour to ICTi designs without losing the needed flexibility for future growth. The code, or other new standards documents, should build on the available array of published documents and should not be duplicative. With enforceable documents available, such as an ICTi code, voluntary programs could use those documents as a baseline from which higher performance could be rewarded. ICTi commissioning documents should also be developed to potentially augment commissioning standards used for other building systems, such as heating, ventilation, and air-conditioning (HVAC) and lighting. Lastly, cybersecurity documents should be created to enable an understanding of the level of security rigour in the building's ICTi. This could be developed from the extensive NIST framework.

For capacity and awareness, the recommendations include clearly defined ICT terminology, training material, awareness collateral, and demonstration programs. These recommendations are intended to increase ICT awareness and build a stronger marketplace that supports ICTi needs. With effective communication tools, building managers will be in a better position to engage contractors and consultants, while managing occupants' expectations.

From a research perspective, there are a few areas that could be explored to assist in longer-term ICTi planning. First, as noted earlier, there may be unique needs for different occupancy types. Engaging those industries may provide valuable insights for future needs and could support the expansion of the prior recommendations. The second area of future research is the opportunity for artificial intelligence (AI) to be used in ICT commissioning. This may be beneficial to building managers, particularly where connected devices exceed the pragmatic use of human resources. And finally, as building owners are looking for enforceable ICTi performance, there is an opportunity to explore enforcement techniques to see how they could be used in the ICT sector.

Overall, the ICT market is growing at a pace that is exceeding the abilities of today's ICTi systems. Stakeholders are looking to enable this growth and want support to ensure consistency and predictability in their buildings. This report offers many recommendations that may lead to better and higher quality ICT in buildings.

"More buildings are marketed as "intelligent" by adding connected, smart devices that are networked throughout the ICT infrastructure (ICTi)."

1.0 Introduction

The information and communication technology (ICT) industry is rapidly expanding. More buildings are marketed as "intelligent" by adding connected, smart devices that are networked throughout the ICT infrastructure (ICTi). The uptake and rapid expansion of connected devices has provided numerous benefits to end users together with new challenges for the ICTi and for the data that are flowing through it. Codes, standards, guidelines, specifications, and other documents address aspects of ICT and connected devices; however, there are few, if any, documents that tie together all aspects of ICTi. Furthermore, there are limited insights from stakeholders as to their needs in Canada.

What is ICT?

Diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players and storage devices) and telephony (fixed or mobile, satellite, visio/video-conferencing, etc.). [17]

This research report outlines the current state of ICT in buildings as compared to stakeholder expectations of ICTi in buildings. From there, gaps are identified, and recommendations provided.

2.0 Methodology

The research comprised a review of current materials related to ICT systems in buildings. There are several white papers, case studies, and articles under the moniker of "Intelligent Buildings" or "Smart Buildings" that speculate on the expansive nature of connected devices and infrastructure. Several of these documents were reviewed to create the context for today's ICTi landscape. Standards referenced throughout this report are expressed in their short form; the tables in Appendix A provide the full standard designation.

To validate and build on the observations from the review of materials, several key stakeholders were interviewed. The insights provided led to the creation of a stakeholder workshop that helped validate the current status of ICTi standardizations as well as articulate the industry's needs. In total, 17 stakeholders, including senior executives, provided input from the following stakeholder categories:

- Building owners and managers
- Contractors and consultants
- Product and technology suppliers
- Integrators
- Utilities

A gap analysis compared the currently available standards documents to stakeholders' expectations. Recommendations were then compiled to address the gaps.

3.0 ICTi for Buildings

The infrastructure required for ICT systems in buildings is evolving at a rapid pace. More building owners are beginning to explore innovative ICT options, such as Power over Ethernet (PoE), connected lighting devices, and advanced heating, ventilation, and air conditioning (HVAC) controls. Technology suppliers are providing these smart and connected devices with consideration that they will have two-way communication over the building's ICTi, along with other connected devices such as mainstream building systems like security, fire, and elevators. There are several innovative uses and valued rationales for deploying ICT solutions. As illustrated by the Government of Canada in Figure 1, energy savings is one of many benefits for building owners, along with operating cost reductions and improved comfort and convenience. This section explores the systems and protocols that support ICTi.

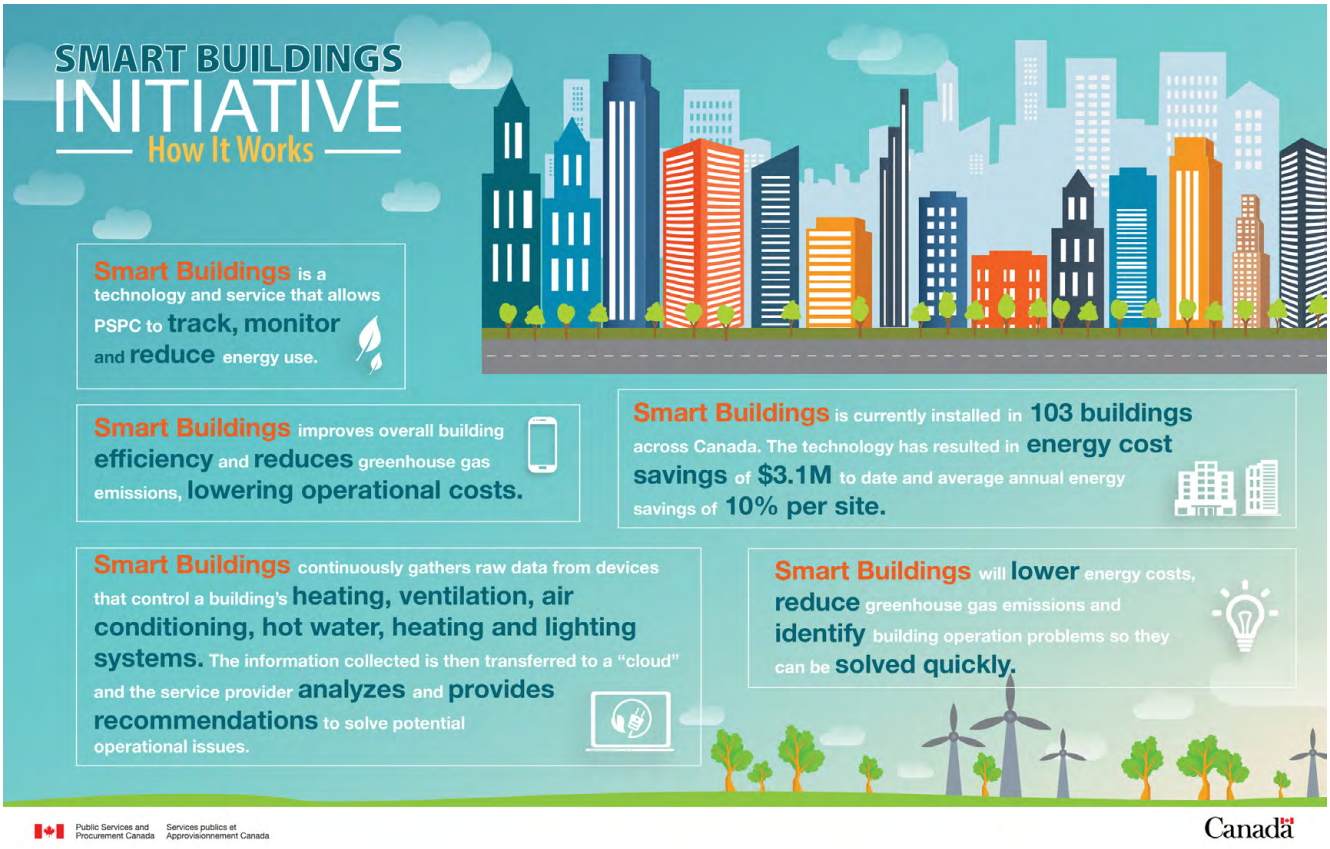
3.1 Systems and Architecture

Ultimately, ICTi in buildings is about data movement. There are multiple mediums and paths for the data to flow; this could be through various forms of physical connections (copper or optical cabling), wireless (Wi-Fi, cellular, fifth generation [5G], etc.), or hybrid combinations. Intelligent buildings' ICTi have numerous interconnected nodes. The effective flow of data relies on established protocols for transmission, meeting the ICTi power needs, and how data flow in and out of the building.

3.1.1 Protocols

There are several communication protocols used for building systems' ICTi. Protocols are used to ensure accurate transfer of data from system to system and they are selected depending on the product solutions connected to the ICTi. Historically, the protocols were

Figure 1: *Smart Buildings Value Proposition. Source: Public Services and Procurement Canada. Source: Public Services and Procurement Canada [16]*



based on wired systems; however, the expansion of wireless technologies and solutions have, over the past decade, created the need for wireless protocols.

There are three protocols used primarily for wired building automation systems: BACnet, LonWorks, and Modbus. General background information on these is presented in Table 1. BACnet is the most commonly used protocol for building automation systems, and many original equipment manufacturers (OEMs) have a built-in BACnet interface to ease direct connection to compatible building automation systems. Some OEMs originally selected LonWorks, as it provided web-based access to the OEMs' equipment; however, many consider LonWorks as outdated, as web-based tools are now much easier to develop and integrate through the ICT systems. One of the oldest wired automation protocols, Modbus, is still popular in factories and where systems are not expected to expand exponentially. Being one of the first free-to-use open protocols, it was, and still is, popular for custom programmable logic controls (PLC) found in industrial facilities.

While there is some limited ability to interconnect devices using different protocols, generally a building owner must choose one protocol to network the building automation systems. This can create an exclusive relationship between the building automation vendor and the owner due to limitations in connecting other manufactures' devices and the potential added costs for protocol integrators.

Wireless system and device connections are gaining market traction through various protocols such as Wi-Fi, Bluetooth, Zigbee, low-power wide area networks (LPWAN), and cellular networks. Each wireless technology has its individual uses. Wi-Fi and Bluetooth are commonly found in smart homes and are generally known protocols. Zigbee is used in the residential market and its interfaces can be built into devices to connect into larger building networks that can accept its short-range transmission. LPWAN appearance has increased with the Internet of Things (IoT) movement as it can handle millions of low-power devices in a wide area. It consumes less power than cellular transmitters thereby offering improved battery life. The wireless protocols discussed here are presented in Table 2.

New wireless systems are also being developed, such as light fidelity (LiFi). This potentially next-generation wireless networking technology uses light-emitting diode (LED) lights to transmit data at extremely high speeds. This could mean that buildings, which are increasingly converting to LED lamps, could have data flowing through to all illuminated areas of the building. According to LiFi.co, the biggest selling point of LiFi technology is that it can transmit data at far greater speeds than Wi-Fi. Further, LiFi.co states that during lab tests, researchers were able to reach bidirectional transfer speeds of 224 gigabits per second. Of course, it would be difficult to reach those speeds in a real-world setting. But reaching even one percent of that means

Table 1: *Three Common Wired Protocols*

	Wired Protocols		
	LonWorks	**BACnet**	**Modbus**
Original version	1999	1987	1979
Originally developed by	Echelon Corporation (Motorola)	ASHRAE	Modicon (Schneider)
Communication standard	ANSI/EIA 709.1	ASHRAE 135-2016	IEC-61158-1 (Fieldbus)
Key market	Control networks, most devices are building related (HVAC and lighting)	Building automation, HVAC, fire, access control, security, lighting	Industrial controls and factory automation

"Data movement is not exclusive to the inner workings of the building. Often, data need to flow out of and into buildings from external sources and clouds."

speeds of 2.24 gigabits per second – a significant improvement over Wi-Fi, which nets transfer speeds of about 20 megabits per second [1]. The limitation to LiFi is that it transmits in the visible light spectrum, meaning interference will be prevalent in daylighted areas and where spaces have multiple partitions.

3.1.2 The Building's Connections to the World

Data movement is not exclusive to the inner workings of the building. Often, data need to flow out of and into buildings from external sources and clouds. This presents additional risks and challenges for ICT users. Traditionally, data flow to the outside world was through hard-wired connection at the building's point-of-presence (POP) demarcation point. Today, wireless communications are rapidly evolving with cellular networks, and soon, 5G wireless networks accessing devices will make data available anywhere, at anytime.

3.1.3 Power Requirements

The standard wired-based infrastructure by its nature does not require any power, as wiring is a passive element of the network. The active components — routers, network controllers, etc. — do need reliable sources of electricity to keep the data flowing on the network. Critical systems require a backup supply to keep them operational through power outages. As systems expand into the deployment of IoT systems such as PoE, power consumption and reliability will become a major factor for designing the ICTi.

Table 2: *Wireless Protocols*

Protocols	Based on Standard	Operated By	Transmission Range
Wi-Fi	IEEE 802.11	Wi-Fi Alliance	20-40 m
Zigbee	IEEE 802.15.4	Zigbee Alliance	10-100 m
Bluetooth	IEEE 802.15.1	Bluetooth SIG	50-150 m
LPWAN (LoRa, NB-IOT)	Under development (current task under IEEE 802.15.4w)	IEEE	2-5 km (LoRa) Up to 10 km (NB-IOT)
Cellular (GSM/GPRS/ 2G/3G 4G/5G protocols)	Multiple		35-100 km

3.2 ICTi Relevance in Today's Built Environment

As more ICT devices integrate and communicate over the ICTi, opportunities for energy efficiency, operational cost reductions, increased comfort, and productivity for occupants and building owners will materialize. However, there are also increased risks. If the ICTi becomes overburdened, it may slow down to the point of reducing device response time. Further, the slow speeds could frustrate end users accustomed to higher levels of service quality. While customer service risk is important to owners, the security risk is of increasing concern, particularly for privacy and cybersecurity threats. As stated by Intelligent Buildings, LLC, the increasing number of cybersecurity breaches in building control systems around the world has raised the awareness of building owners and managers [2].

Operational technology (OT)

Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of physical devices, assets, processes, and events in building-related systems.

Information Technology (IT) is well understood by the industry as referring to the computer systems, software, and networks that process, move, and store data. However, the interaction and interdependence of devices connected to a series of networks, via the ICTi, is creating a new and expanded field of operational technology (OT). OT oversees how the ICTi operates and regulates interactions between buildings systems. Gartner, a leading research and advisory company, defines OT as "hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events" [3]. In a non-industrial environment, the definition of OT can be modified to include physical devices rather than industrial equipment, in addition to assets, processes, and events in building-related systems. A building system OT example, one of many permutations and combinations, would be a system that monitors security system activity to turn on a lighting zone within the building, while signalling the HVAC system to resume the zone's temperature controls, and perhaps simultaneously turn on the Wi-Fi–connected coffee pot for the user. While the latter point is more advanced than most buildings, the possibilities can be limitless with the appropriate ICT infrastructure.

As the trend towards valued intelligent buildings accelerates, managing data will become more complex and could increase risks for building owners as previously outlined.

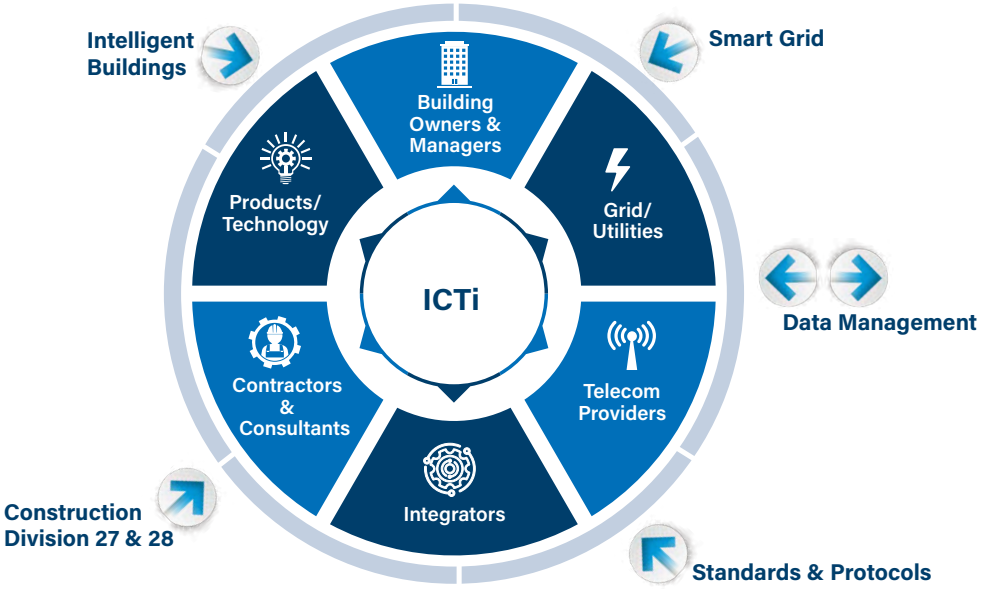
3.3 ICT Stakeholders

Various players and the tools surrounding the ICT space are illustrated in Figure 2. Each stakeholder has subject matter expertise with a distinct perspective on the ICT systems and the ICTi needs. Stakeholder perspectives are often influenced by regulations, marketing terms, and industry best practices. For example, utilities see the ICTi from the perspective of how a smart grid will interact with the building system; whereas a contractor or consultant may see their dealings in ICTi from the perspective of the national construction documents and specifications. This subsection will provide further context on these stakeholder interactions and perspectives.

Building Owners and Managers have a responsibility to deliver a reasonable level of infrastructure to meet the expectations of the occupants. Some building owners and managers have internal business units dedicated to smart buildings and digital innovation.

Contractors and Consultants enable the ICTi infrastructure. Consultants need to be able to provide a specification that is clear and understood by the installing contractors. Contractors need to understand the specifications and translate them into efficient installation techniques. Both need to identify challenges associated with the growth of digital products on the wired and wireless systems and provide options to balance the cost with the functionality needed today and into the future. Traditionally, for other building systems, contractors and consultants rely on the Canadian National Master Specification guidance documents developed by the National Research Council of Canada (NRC) [4]. However, with a rapidly changing industry like ICTi, it is challenging to keep the document up to date.

Figure 2: *ICTi Stakeholders*



Product and Technology suppliers and manufacturers often innovate to keep relevant in the industry. The smart and intelligent connected devices are targets for many technology companies. Further, with the globalization of products and technologies, there are constantly new players entering the market, with low-cost or novel unproven technologies. This presents opportunities for innovative building owners; however, it presents a challenge for the industry to keep uncertified or untested products out of buildings.

Integrators are becoming an essential stakeholder in the ICT market. Integrators pull all the pieces together to ensure functionality and interoperability between systems. They can be specialized firms or can be included in another stakeholder group, such as building managers, contractors, product suppliers, or consultants.

Telecommunication Providers (telcos) are stakeholders to the ICT market as they typically provide the connection point from the building to the outside world. This can be through a central POP space or via wireless transmission in and out of the building. As telecommunication providers are located outside of buildings, they were not one of the key industry participants interviewed for this research. However, the business models for telcos may expand over time to beyond the POP, through maintenance and ownership of the ICTi.

Grid Utilities, like telcos, are looking for new business models around distributed energy resources (DERs) found in direct current (DC) microgrids[1] which are tied into the ICTi. In addition, the electric utilities also have a key role in keeping the ICTi powered reliably.

4.0 ICT in Buildings – Today's Landscape

ICTi for buildings has evolved organically with few codes, standards, specifications, and guidelines. Other building-related systems have well-established sets of laws, codes, and policies to ensure they meet a minimum compliance level, be it safety, energy, health, environment, or other objectives. There are also standards and specifications that can be referenced in the codes, or on a standalone basis, to ensure building components are, within their operating silo, operating within a specific tolerance.

[1] *DC microgrids are networks of DC systems that interconnect building-level distributed energy resources to other DC systems.*

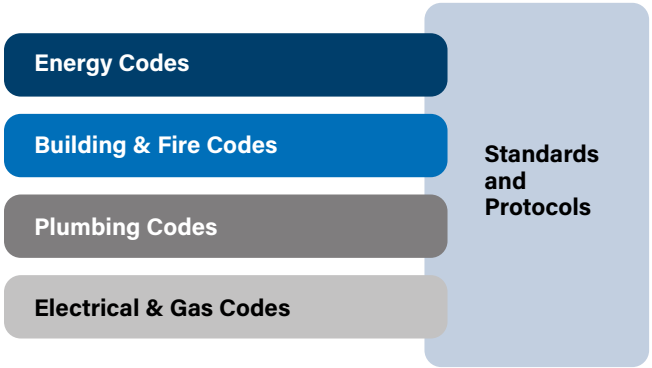
As ICT is becoming more relevant, the industry is beginning to develop using traditional building compliance methodologies. This section explores the codes, laws, and policies, as well as standards and specifications available for building-related systems. It also provides a few examples of upcoming guidelines and a rating system that may assist in the future development of standardized ICTi design, installation, and operations.

4.1 Codes, Laws, and Policies

There are several governing policies and documents for buildings in Canada. From a federal perspective, the government creates policies and model codes. These codes are models since the Constitution Act in Canada puts building regulations into the jurisdictional authority of the provinces, territories, and some local governments. Therefore, the models may be adopted as written, or the provinces and territories may develop and enforce their own set of building codes.

Currently, there are several model national codes published by Codes Canada [5], including the National Building Code, National Fire Code, National Plumbing Code, and National Energy Code for Buildings (see Figure 3). Most provinces and territories have adopted or adapted these codes. However, there is no language in the codes to provide guidance or rules for the ICT sector.

Figure 3: *Codes and Standards*



CSA Group publishes the Canadian Electric Code, with the recent edition including more support for the safe implementation of new technologies and renewable energy solutions [6]. The coverage of ICTi remains limited; although the 2018 version does address PoE cables and electric vehicle charging systems.

In the ICT space, the privacy of data and personal information flowing through the ICTi is of increasing importance. Federally, the Privacy Act sets out privacy rights for interactions with the federal government and how the government collects, uses, and discloses personal information [7]. There are additional privacy regulations at the provincial and territorial level. These rules may govern the freedom of information, protection of private data, and health records.

The Personal Information Protection and Electronic Documents Act (PIPEDA) [8] covers how businesses handle personal information. The provinces of British Columbia, Alberta, and Québec have their own versions of PIPEDA, which are substantially similar to the federal law [9].

Further, in the building space, there are no codes in Canada to help protect the ICTi from cybersecurity threats. Overall, there are layers of regulations and acts that vary between provinces and territories. This can make it challenging for ICT industry participants that operate across Canada.

4.2 Standards

In the building space, codes typically set the high-level requirements while standards and protocols help all industry stakeholders with specific rule sets for components and systems. The general purpose of standards is to create a uniform set of requirements. Standards can address objectives, such as safety, operational performance, or interoperability, and provide the end user with the ability to use different materials, components, or equipment, with an expectation of compliance to an applicable standard.

Wiring standards and wireless protocols are well established and mature, as evidenced by the partial list provided in Appendix A. Standards development organizations and industry associations have been able

"The Canadian Electrical Code's latest edition includes a new subsection for PoE cabling [6], and the Institute of Electrical and Electronic Engineers (IEEE) 802.3af series provides standards for power delivery over the Ethernet."

to define the rules for how a wire is to perform and what is expected when one connects to a wireless system.

ICTi wiring can be copper or glass optical. It comes in various forms, from simple unshielded twisted pair (UTP) and coaxial, to faster single-mode and multimode fibre optic cabling. Depending on the use and the surrounding environment, the specifier can choose the appropriate, speed, size, and shielding needed. They can reference various documents from standards development organizations, such as those referenced in Appendix A, to help ensure that the installers provide and owners receive products tested to relevant performance criteria.

PoE is beginning to grow in the ICT market, with lighting systems being added to the list of PoE devices that traditionally include cameras, phones, and other low-power electronics. The addition of lighting raised new concerns of how much current can safely flow through wires certified to meet the various standards. The Canadian Electrical Code's latest edition includes a new subsection for PoE cabling [6], and the Institute of Electrical and Electronic Engineers (IEEE) 802.3af series provides standards for power delivery over the Ethernet. This is a good start to protecting ICT wiring in the bourgeoning PoE industry.

For wireless systems, there are also several protocols depending on the need and often on the product suppliers being used. Standard IEEE 802, and the equivalent CAN/CSA-ISO/IEC/IEEE 8802, is the commonly referred to series of standards for wireless systems. A list of relevant standards is presented in Appendix A. Standard series IEEE 802.11 is one of the more commonly known standards for wireless local area networks (WLANs), medium access control (MAC), and physical layer (PHY) functions. Introduced in 1997, the series is continually updated and expanded as new technologies become available.

4.3 Specifications

Construction work typically follows a national set of specifications. NRC's Canadian National Master Construction Specification [4] are generally used by the industry and cover all facets of construction work. There is no specific section dedicated to ICT; however, Division 25 on Integrated Automation, Division 27 on Communications, and Division 28 on Electronic Safety and Security offer some input into how the ICTi can be built. The specifications related to data are covered at a high level requiring coordination of data work with the LAN providers.

The Province of Nova Scotia adapted the NRC's Canadian National Master Specification in a document called Design Requirements Manual 2010 Edition (DC350) [10]. The province elected to enhance Division 27 on Communication by adding a companion document for cabling [11]. This provided a clearer expectation for the ICT cabling work undertaken for the province.

4.4 Guidelines

Guidelines, by their nature, are not rules or requirements; they are intended to be documents to facilitate better understanding or use of systems. Two of the more prominent intelligent buildings documents were developed by the TIA and by Bicsi. The TIA document is called the TIA Smart Building Integrated Ecosystem; and the Bicsi's document is the ANSI/BICSI 007-2017. NIST has created a cybersecurity framework for US critical infrastructure. WiredScore [18] is a rating system that builds on other successful voluntary programs in the commercial sector. These are described in this section.

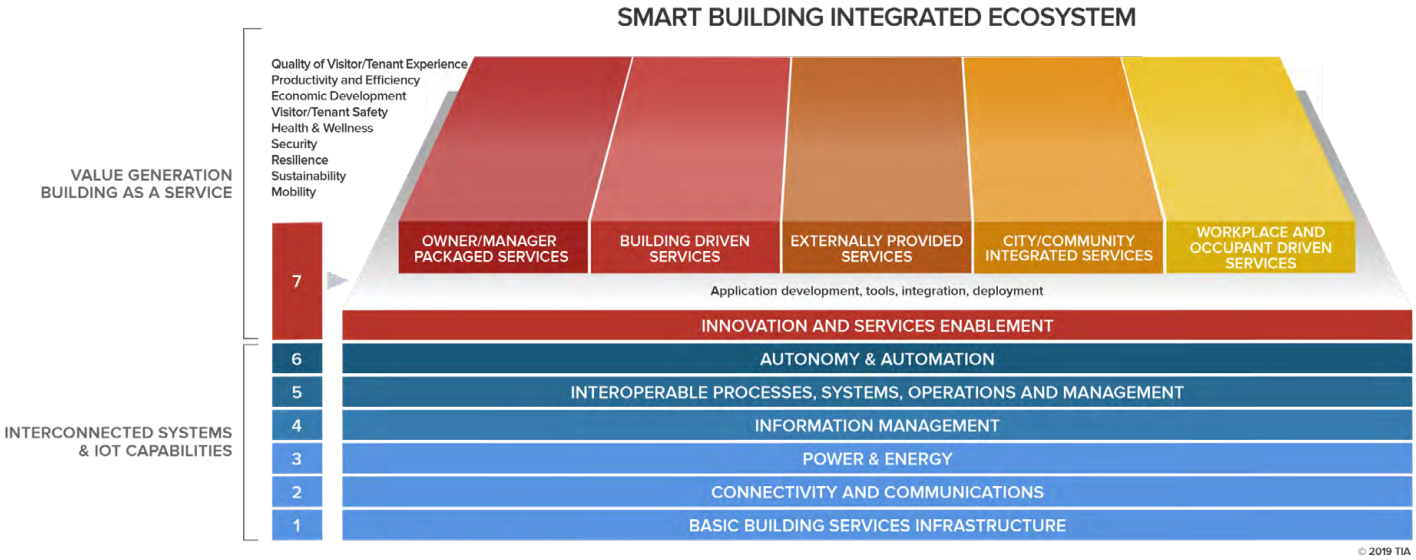
4.4.1 TIA Smart Building Integrated Ecosystem Guideline

In 2017, TIA launched a program to create clarity around connectivity, interoperability, communications, and capacity for smart buildings. It brought together leaders from the intelligent building sector to assist with defining smart building terms and develop the framework. As illustrated in Figure 4, TIA has created a seven-layer framework commencing with basic infrastructure and layering up the value chain to innovation and service enablement. The framework is presented in a logical format and can be segmented by the type of service offered by the smart building industry. The program is expected to develop over time and could eventually lead to a smart building certification program. ICTi is an enabling element that crosses several of the ecosystem layers.

4.4.2 Bicsi Intelligent Building Guidelines

The Bicsi 007 document, first published in August 2017, is referred to as a standard that provides design and implementation best practices for intelligent buildings. Bicsi is attempting to bring together the various important elements of intelligent buildings under a single document. It covers a broad area that includes reference standards, infrastructure options, design considerations, some building-related systems, integration, and commissioning. The Bicsi standard

Figure 4: *TIA Smart Building Integrated Ecosystem. Reproduced with permission from TIA Smart Buildings Program [15].*



helps owners, consultants, and contractors engage in conversations about their intelligent building. It is not intended to be the only reference, nor is does it provide a formula for creating an intelligent building, as it provides options and a variety of best practices.

4.4.3 NIST Cybersecurity Framework

Cybersecurity is becoming increasingly important in the ICT space. NIST has created a framework (see Figure 5) to assist in understanding and managing cybersecurity risks. It was created for companies that are part of the US critical infrastructure and can also be used by other organizations looking to manage cyber risks. The framework follows a risk cycle flowing from identification to protection, detection, response, then to recovery. It includes best practices, standards, and guidelines.

The NIST framework is divided into three main areas: core, implementation, tiers, and profiles. The core outlines cybersecurity activities and outcomes that are typical for most buildings and critical infrastructure. It provides a useful communication tool that allows the user to populate categories, subcategories, and the associated information reference (guidelines, codes, best practices, etc.) for each of the five risk steps. The framework continues to evolve and provides a model for organizations to identify and respond to risks. Importantly, it provides a means for communicating the risk and assesses the level of risk mitigation undertaken by the user. Tiers and profiles allow the framework user to build a strategy for further improving their cybersecurity.

The framework may provide a way for Canadian organizations to assess and evolve their cybersecurity.

4.4.4 WiredScore Rating System

Commercial building owners and managers often look to rating systems for third-party verification of their buildings' performance. The growth of the LEED rating system has transformed the high performance "green"

Figure 5: *NIST Cybersecurity Framework Core. Reproduced from National Institute of Standards and Technology [12]*

building sector. WiredScore is looking to use the LEED approach on commercial buildings' ICTi, and is promoted as an international digital connectivity rating scheme for real estate [13]. WiredScore was initially launched in 2013 in partnership with Mayor Michael Bloomberg and the City of New York.

Wired Certification is a commercial real estate rating system that empowers landlords to understand, improve, and promote their buildings' digital infrastructure. [29]

WiredScore believes that having a rated building will provide a benefit to tenants and provide a better understanding of the building's digital infrastructure. WiredScore establishes a point-based system for various aspects of the ICTi, which when added together will provide a score that then translates to a progressive rating of certified silver, gold, or platinum. The system also has several pre-requisites for certification and some mandatory requirements for any building certifying to the highest level of platinum. Areas covered by the rating system include outside plant and point of entry planning; telecommunication room planning and design; riser planning; electrical resiliency; mobility planning; and readiness and access.

Since its launch, over 2,000 buildings have certified under the WiredScore system. As noted, the system started in the United States and the United Kingdom followed a couple of years later. In Canada, commercial building owners and managers are beginning to take interest in the rating system. Several buildings have certified in the Greater Toronto Area, Greater Vancouver Area, Calgary, and Edmonton.

The industry movement towards developing high-level guidelines and participating in an ICTi rating system is reinforcing the need for additional tools to support the sector. Finding the right balance between rigour and flexibility requires input from all stakeholders, which will be explored in the next section.

5.0 ICT in Buildings – Stakeholders' Principles and Drivers

Experts from industry stakeholders – building owners and managers, contractors and consultants, product and technology suppliers, integrators, telecommunication providers, and electricity utilities – provided input on the importance of ICTi. The experts, represented by senior members of their organizations, participated in one-on-one interviews and a cross-stakeholder workshop. They described the expected value set, through principles and drivers, attributed to advanced ICT systems.

5.1 Principles

Thematically, stakeholders prioritized the following principles for ICTi:

- Predictable
- Reliable
- Flexible
- Comprehensive
- Resilient
- Future Proof
- Protected

The ICT industry is migrating out of proprietary solutions, favouring a more consistent and flexible system architecture. Almost all experts concurred that ICT devices are expanding exponentially and that the only appropriate direction is for those devices to simply connect to the systems as plug-and-play.

Predictable

Predictability means that the system expectations need to be clear and operate in a consistent fashion. Building owners and managers felt that predictability is important to managing their facilities' base building systems while providing services for the occupants. One stakeholder interviewed mentioned that there is mass confusion when it comes to smart buildings. As it is a marketing term, the interpretation of smart, or intelligent, is left to the imagination. ICT systems need to clearly identify the extent to which connected devices are to be supported and at what performance level.

Reliable

Following in line with predictability, end users need to know that the ICTi is always available for use. Critical systems are being connected and valuable data are being shared, leaving little room for "glitches" and "blips" in communications. Having a reliable system can avoid many unnecessary customer service calls.

Flexible

In a constantly evolving and growing need for data exchanges, ICTi needs to provide flexibility. Historically, building systems vendors had proprietary networks. While over time these networks have tried to adapt using gateways and integrators following industry protocols like BACnet and LonWorks (see Section 3.1.1), advanced buildings require more flexibility in products, vendor selection, and integration. Many owners believe it will be difficult for some vendors to give up their position as the exclusive vendor, due to the legacy proprietary systems.

> *It may be challenging for industry to give up the proprietary nature of their systems (locking in customers).*
>
> *—BUILDING OWNER AND MANAGER*

Comprehensive

ICTi needs to enable data movement to and from a comprehensive network of devices and controllers. Today's advanced buildings should have data instantly and securely, and data should be accessible from anywhere in the building. This will ultimately lead to improved user experience and drive extra value for the occupant, which translates to value for the building owner. As the building's ICT system incorporates more comprehensive systems, the need for OT to manage the ICTi data flow becomes essential. This will take the IT human resources outside of its traditional comfort zone, and perhaps lead to the new generation of OT resources to service buildings' ICTi.

Resilient

Owners and users are demanding higher resiliency levels for business continuity purposes. The ICTi is a significant factor for business resiliency as many organizations begin to keep data on the cloud and in secure locations. Owners and users also expect the building systems to keep operating despite externalities, such as power outages. Having a robust and resilient ICTi increases the value of the building.

Future Proof

A challenging value is that ICTi needs to be future proof, which means ready for new technologies and systems that perhaps have not yet been invented. This also supports the notions of flexibility and the non-proprietary nature of how devices and systems connect and share data across the ICTi. The example provided by one expert was how the ICTi will be able to shift from "glass and wire" based solutions to the new 5G wireless networks that transmit wirelessly through the building.

Protected

All stakeholders want to ensure that the ICTi operates in an enabling and safe environment. This principle covers physical environments (safety) as well as virtual or data environments (privacy and cybersecurity).

5.2 Drivers

There are several drivers that describe stakeholders' perspectives on how the ICTi will perform. As further described in this section, drivers include speed of execution; ease of use; system interoperability; future growth; and fostering innovation.

5.2.1 Speed of Execution

An ICT system needs to be constructed and commissioned expediently. Today, there are stories of some promised smart buildings that take over two years to enable promised data flow [14]. This anecdote was provided by a utility stakeholder that was creating a smart grid innovation demonstration facility. The stakeholder

installed the ICTi and relied primarily on legacy Modbus controllers, expecting systems to easily adapt to plug-and–play devices. However, the infrastructure did not materialize as advertised and there was no code or clear performance specifications to enable an effective ICTi. This user felt that if there had been a clear ICT code, the speed of execution would have been significantly accelerated.

Execution speed will also depend on how quickly the system is commissioned. As the number of connected devices may increase exponentially, faster commissioning processes – perhaps some form of artificial intelligence (AI) – will be required to ensure all data points are operating as expected.

5.2.2 Ease of Use

Similarly, a robust and clearly defined ICTi will enable devices to be added using any protocols without significant delays. Therefore, a high-performing ICTi will accommodate any product or solution. Further, ICTi will need to handle traditional IT systems and intelligent building system devices. Ease of use is a significant driver for all building owners and occupants.

5.2.3 Interoperability

As OT is increasing its presence in the ICT space, there is a need for ICT to facilitate integration where system-to-system communications can exist. Enabling interoperability allows end users and system operators to quickly and efficiently modify their ICT systems on the ICTi.

5.2.4 Future Growth

Of all the drivers discussed with stakeholders, the ability to seamlessly expand and grow the networked devices was a top priority. This relates to the other drivers, and when layered in with future growth of devices and associated data flow, the ICTi performance should not be affected. This then leads to a significant challenge considering the sheer growth of end points (i.e., connected components and devices). It is conceivable that a relatively small building could have thousands of networked devices.

5.2.5 Fostering Innovation

Adding to the challenges is the expectation that new, sometimes yet to be invented, devices should be able to integrate with the building's ICTi. Having an ICTi that fosters innovation and permits future technology to easily integrate is a strong preference for many stakeholders, although most informed stakeholders realize this is more of an aspirational driver.

5.3 Building Typologies and Their Specific ICTi Needs

ICTi needs can differ based on occupancy type. While all buildings and occupancies share similar basic ICTi needs, such as connectivity, plug-and-play flexibility, and clarity around performance and functionality, the extent to which each value is provided depends on the occupancy type and the tenant-owner relationship. Various occupancies can be found in commercial buildings, multi-residential buildings, factories, and public use buildings as discussed below. A comprehensive list of occupancies is provided in Appendix B.

Commercial buildings often incorporate intelligent building systems that provide a baseline for ICTi expectations. While single-use tenant occupancies can have differing requirements to multi-tenant buildings, there is a common need for flexibility, expandability, resilience, and cybersecurity on all aspects of the ICTi. Commercial building owners and managers can reference multiple standards and guidelines, (see Appendix A for a partial list) for wiring, wireless communications, as well as communication protocols; however, there is no single document that allows building owners to understand the performance or risks involved with the integrated systems. Standards and guidelines for OT systems, whose presence is ever increasing, are yet to be fully established. Some commercial property managers have defaulted to the use of rating systems, such as WiredScore, described in Section 4.3, to fill in the gap for missing standards and for commonly understood specifications.

Multi-unit residential buildings (MURBs), in most cases, require a reduced level of ICTi due to the nature of the relationship in which a condominium builder

"There is a need for a specialized focus on healthcare and other privacy-sensitive occupancy types, to ensure ICTi can be robust, flexible, and secure."

transfers the assets to a condominium board to own and administer. These situations often lead to lower costs and a reduced need for layers of security and redundancy. Typically, builders do not focus on future proofing. There are exceptions to this reduced standard particularly where the MURBs are purpose-built rentals. In these situations, the buildings tend to migrate towards a commercial-scale ICT system as the long-term asset value becomes a priority to the building owner.

Factory applications have some of the more advanced open-protocol networks, as there is a long history of programmable logic controls (PLC) automating process functions. More resilient twisted-pair communications protocols, such as Modbus, have been employed in industry environments for decades. There will be advancements in factory communication protocols; however, most experts believe that the factory floor is currently well served by the current systems and internal resources.

ICT in healthcare occupancies are evolving at a rapid pace. There are multiple points of data access on the ICTi that could include user interfaces (phones, smart devices, workstations, etc.), clinical processes (electronic medical records, nurse call stations, scheduling, etc.), support services (pharmacies, lab automation, etc.), facilities' systems (heating, lighting, security, energy metering, etc.), and audio-visual and television infrastructure. As such, the cybersecurity, privacy, and integration requirements are more stringent than other occupancy types as the data flow is more likely to contain sensitive information. There is a need for a specialized focus on healthcare and other privacy-sensitive occupancy types, to ensure ICTi can be robust, flexible, and secure.

Similarly, there are government and military applications that will require advanced guidelines and protocols. Some facilities are using physical "air gap" devices and systems to separate the ICTi from any outside intrusion. Connection to the outside world, if permitted at all, is sequenced through the air gap device in controlled and monitored bursts. Opening these facilities to wireless technologies and personal devices is a challenge for the ICT network design and operation.

Overall ICTi performance expectations can vary depending on the occupancy requirements. However, as discussed in this section, there is a common set of expectations based on stakeholder principles and drivers that need to be considered for ICTi development, today and in the future.

6.0 Gaps and Recommendations

ICT in all building types, particularly in intelligent buildings, is evolving, and expanding at a rapid pace. The once relatively simple provision of IT systems is more complex, and the data requirements are increasing exponentially. Today's market is demanding safe reliable data to be transmitted in near real-time from all systems. This has opened the door to OT managing data flow through the ICTi, using algorithms and AI to manage

speed and throughput. Technology such as connected lighting systems are also increasing demand on the ICT systems. Overall, there needs to be consistency, transparency, and predictability, in addition to the traditional specifications that provide safety, security, and reliability. With considerable quantities of data flowing from business and privacy-sensitive systems, there is also an increased need for cybersecurity.

> *Historically, data used to flow from point A to point B. Today, data are moving from point A to multiple points simultaneously.*
>
> *—CONSULTANT STAKEHOLDER*

6.1 Gaps Between Reference Documents and Stakeholder Needs and Expectations

6.1.1 Consistency for Owners and End Users

There is a discrepancy between products marketed as smart, buildings claiming to be intelligent, and user/owner expectations of those devices and building systems. Today, there are no rules for a building to be labelled as "intelligent". There is a need for something to level the playing field and create clear and consistent performance indicators for owners and end-users. Solutions like WiredScore are gaining popularity in the commercial office sector as it provides a rating system in the same fashion as other tools like LEED. However, the rating system is an unenforceable guideline, similar to LEED, and does not apply to all occupancy and building types. TIA's Smart Buildings Program [15], launched in 2017, attempts to create common definitions and define smart ecosystem layers to help communicate expectations from base building to high-value smart building outcomes.

6.1.2 Data Management Privacy and Security

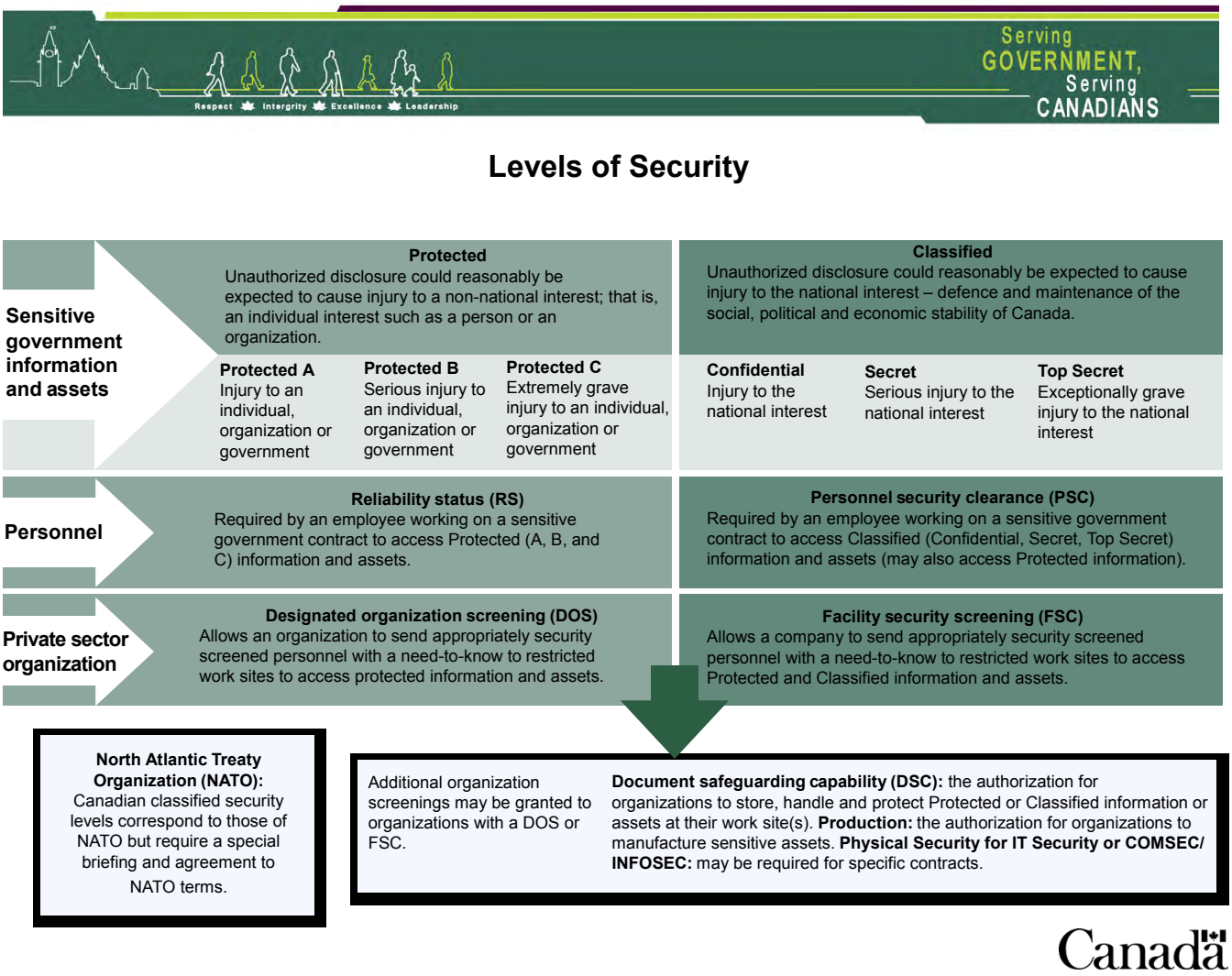
With potentially unlimited data flowing through multiple devices and nodes, there are few, if any, data governance specifications. Legacy systems often offer integration to other systems to enable some data sharing, which can be helpful; however, they do not meet today's OT needs. Legacy proprietary systems and dedicated communication pathways offer a degree of data security, or at least perceived controllability, however this can be a costly approach which doesn't support the future-proof value, nor the plug-and-play approach desired by owners and end users. There is a market desire for clearer data governance and structure in buildings, particularly with facility-related assets.

Each province has its own privacy legislation, with common aspects, most of which deal with securing personal data. In today's environment of open architecture and fast-moving data, building owners are seeking assurances that private data will not be accidentally transmitted through the building's ICTi. This is heightened in public buildings with government, education, and healthcare occupancies, considering the quantity of sensitive personal information collected and transmitted. Current ICT standards are lacking in privacy requirements.

Even with appropriate data governance and securing private data for intentional uses, building owners are increasingly concerned about unintentional breaches and access to the ICTi. These and other threats are cybersecurity risks that owners want to understand and mitigate. There is some activity in this space; however, building owners and managers are looking for more information and common themes to understand, then manage, the risks. The United States has developed a cybersecurity framework through NIST [12], as described in Section 4.4.

There are also groups forming, such as the LinkedIn group Real Estate Cyber Consortium (RECC), that are trying to develop more consistent approaches and provide information. It is a starting point, to enable proper and common mitigation strategies. Many owners would like to see a Canadian performance rating or progressive scale that could be used to identify security levels. This would be analogous to a government document classification system, as illustrated in Figure 6 – Protected A, Protected B, Protected C, etc., which includes varying degree of security.

Figure 6: *Government of Canada Document Security Levels. Source: Government of Canada [19]*



6.1.3 Operational Performance

Building occupants are looking for a predictable and consistent flow of data from the ICTi. Building owners and managers want to accurately promote and communicate the service quality provided by their building's infrastructure. Today, there is no adequate framework to confirm performance levels. Having a clear and concise service quality specification will enable more effective conversations with contractors and occupants and assist when the occupant or manager wants to add more devices and systems to the network. For example, if a tenant wishes to convert their lighting system to a network of PoE fixtures, will the ICTi be able to support the data flow required while keeping a promised level of service for other ICT devices?

6.1.4 Commissioning and Recommissioning

Currently, buildings are being commissioned to varying degrees. Commissioning services documents for HVAC and other buildings systems are available from the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) and the Illuminating Engineering Society of North America (IESNA); however, there are no relevant ICTi commissioning standards.

There are some cabling commissioning guidelines and journal articles that assist. Most guidance is geared towards data centres where more sophisticated wiring is deployed. Data centres may be a good starting point for developing commissioning guidelines for buildings, as the complexity of ICTi in buildings may begin to look like mini-data centres.

6.1.5 Operational Technology (OT) Capacity Building

The IT sector is mature, with human resources and education available to service building sector needs. The growth in OT requirements creates a need for a different skill set. There is limited human resource capacity available to oversee and operate OT systems and there are limited educational programs available to train new or transform existing personnel.

6.2 Recommendations

There are gaps between today's ICTi reality and the needs of the industry. This report has outlined some of the available documents as well as the values and drivers for all stakeholders. There are several recommendations, presented in Table 3, that could help meet industry needs. The recommendations are organized by: areas needing further standardization; capacity and awareness; and future research considerations. Of note, each recommendation should balance the rigour required for clear outcomes with the flexibility needed for an evolving industry.

6.2.1 Standards Documents

The industry is seeking a single-point area to clearly understand and communicate ICTi requirements. Today, there are numerous sources of information scattered amongst various standards development organizations and voluntary program managers. A single credible source for specifications and operational guidelines will provide needed consistency, reliability, and clarity for all stakeholders.

RECOMMENDATION 1: Develop an ICTi Code for Buildings

Many building owners would like documents to be enforceable, while remaining flexible enough to tailor to their specific needs. As such, the recommendation is to develop a code document. The code terminology is used to describe a governing document that can be enforced and establishes rules and requirements when specifying ICT infrastructure in buildings. A code would be more enforceable than a guideline. Guidelines can often be misinterpreted, which compromises the values of consistency and reliability. The code development needs to be comprehensive so that all aspects of ICTi are addressed, including service performance data and data governance. The code could be established in layers or tiers, with each tier representing a higher level of rigour and sophistication.

The primary purpose of the code should be to address the infrastructure and OT requirements rather than IT and device-level requirements, which may be less relevant. Maintaining the code at a non-device, higher level will enable flexibility for the addition of devices today and in the future.

RECOMMENDATION 2: Align ICTi Code to Current Standards

In terms of the consistency value, an ICTi code should reference existing standards where possible. Recreating standards that have been already developed would waste time and potentially propagate market confusion. The list of standards in Appendix A demonstrates that there is a robust standards market in the ICT domain. The code should strategically bring together those documents into a common document, while also addressing the ICTi as a system. The code could also refer to commissioning standards when they are developed, further expanding on the comprehensive nature of an ICTi code.

RECOMMENDATION 3: Voluntary Programs Build on Codes and Standards

With a comprehensive code available, voluntary programs can be developed that use the code as a starting point. This would be similar to the LEED green building rating system that uses the National Energy Code for Buildings as its reference baseline for performance improvements. Programs like WiredScore could then reference the ICTi code, and its potential tiers, as a baseline for achieving rating points. Future voluntary programs could be developed focusing on data governance or cybersecurity levels.

Table 3: *Recommendations Summary*

		GAPS					
	RECOMMENDATIONS	**Consistency for Owners and End Users**	**Data Management Privacy and Security**	**Operation Performance**	**Commissioning**	**OT Capacity**	**PRINCIPLES**
STANDARDS DOCUMENTS	Develop an ICTi Code for Buildings	✓	✓	?	?		
	Align ICTi Code to Current Standards	✓	✓		?		
	Voluntary Programs Build on Codes and Standards			✓	✓		
	Develop Commissioning Documents	✓	✓	✓	✓	✓	
	Develop Cybersecurity Performance Levels	✓	✓	✓			
CAPACITY & AWARENESS	Develop ICT Terminology Standard	✓		✓			
	Develop Training Material					✓	
	Develop Awareness Collateral	✓				?	
	Demonstration Projects	✓				?	
RESEARCH	Market Scan – Needs Assessment in Various Building Typologies		✓	?	?	✓	
	Research AI Solutions for Ongoing Commissioning	✓	✓	✓	✓	✓	
	Research ICTi Enforcement Options	✓	✓	✓	✓	?	

✓ Solution ***will*** help address the gap

? Solution ***may*** address the gap

PREDICTABLE ***RELIABLE*** ***FLEXIBLE*** ***COMPREHENSIVE*** ***RESILIENT*** ***FUTURE PROOF*** ***PROTECTED***

RECOMMENDATION 4: Develop Commissioning Documents

Commissioning ICTi and the associated intelligent building systems will become more challenging as the volume of connected devices grows. While HVAC and lighting systems have detailed commissioning standards and data centres have guidelines, the ICT sector does not have these. It would be helpful to develop standards and guidelines to complement other commissioning documents used in the buildings sector. The documents would guide system expectations tracked from end-device through the networks. It could also be used to identify system vulnerabilities and weaknesses from a bandwidth and cybersecurity perspective. It would also be beneficial to have the commissioning document address wired, wireless, and hybrid system configurations.

RECOMMENDATION 5: Develop Cybersecurity Performance Levels

Building from the NIST cybersecurity framework [12], cybersecurity performance levels and specifications should be developed. Levels could be prepared in a similar fashion to the Canadian government's levels of security for document classifications [16] or other easy-to-use scales. The performance levels could then be incorporated into specifications and other management documents to assess risk levels and strategies for improvement.

6.2.2 Capacity and Awareness

Documentation in the form of guidelines and codes is helpful when specifying new systems or upgrades. To be well understood and accepted by a broader audience, there needs to be an accompanying awareness effort and education process, commencing with developing common language, and building upon the value proposition for ICTi systems. All of which needs to filter into training programs for ICT professionals.

RECOMMENDATION 6: Develop ICT Terminology Standard

Marketing terms often create confusion for users by creating expectations without necessarily having the facts to support the term. For example, the green building industry started with the term "sustainable buildings". There were many interpretations of what sustainable meant; however, consistency was not seen until a voluntary rating system started to define specific elements and terms used for sustainable. Similarly, the ICT sector needs a terminology standard to help it understand what is expected from a smart device, or intelligent building. The standard can assist with clarifying other terms such as "operation technology" or "OT". In addition to terminology, the standard could also establish language cybersecurity, service quality terminology, and other more subjective concepts. The Smart Building initiative by TIA could be a starting point in developing, or as a reference in, an ICT terminology standard.

RECOMMENDATION 7: Develop Training Material

When technology evolves at a rapid pace, it is often difficult to keep trades, consultants, and owners current. ICT is growing exponentially as is its infrastructure. Education and training programs need to be developed to ensure all stakeholders are aware of the evolution, understand how to implement new systems, and better understand the standards and protocols available. OT system comprehension will allow building systems to operate productivity; however, a basic understanding of how they function is needed.

For ICT systems, open-protocol systems are moving large amounts of data on a shared infrastructure, moving away from legacy proprietary and dedicated systems. This creates a need to understand risk and to manage security on more complex networks – wired and wireless.

RECOMMENDATION 8: Develop Awareness Collateral

As with training and education, there is a need to develop clear messages and value propositions for the ICT infrastructure. The best intelligent buildings will not function well without a proper ICTi. Awareness collateral could be developed to provide a better understanding of what ICTi entails. Building on the other recommendations, owners, users, and other industry participants will want to understand ICT terminology; clarify pinch points for service quality and how to

maintain the ICTi for connected device load; qualify the safety and security risks that may be encountered; and communicate where and how system flexibility is provided.

RECOMMENDATION 9: Demonstration Projects

Having case studies and examples of intelligent buildings operating on high functioning ICTi systems will be helpful for the industry to understand the potential and the barriers associated with ICT's evolution. There are many examples of excellent infrastructures, as well as those that did not turn out as planned. Further, it would be valuable to demonstrate how ICTi helps smart grids and direct current (DC) microgrids, which are emerging systems. Having these case studies available to the industry will help clarify how ICTi works with direct exposure to the system, while building capacity and awareness at the same time.

6.2.3 Research Considerations

RECOMMENDATION 10: Market Scan – Needs Assessment in Various Building Typologies

This research report has focused on ICTi themes common to most building types. There are specific and unique ICTi needs based on occupancy types. As mentioned previously, healthcare and some government occupancies will have augmented privacy requirements. Factories will have highly functional legacy systems that are customized for them. Governments will have additional requirements. Understanding the ICTi needs of each of the occupancies will assist in the next evolution of standards, guidelines, and codes.

RECOMMENDATION 11: Research AI Solutions for Ongoing Commissioning

Discussed briefly in this report was the notion of using AI as an ongoing commissioning tool. Understanding the potential of OT incorporating AI would enable the industry to better understand the potential growth of the existing infrastructure by intelligently boosting capacity, as well as understanding how to increase system flexibility. A research project to explore current ICTi commissioning practices and review how AI could transform the industry would be informative.

RECOMMENDATION 12: Research ICTi Enforcement Options

Building owners and end users are looking for certainty that the ICTi, and their intelligent building systems, function as promised. There are many enforcement techniques at various levels of rigour. Research questions could include:

- Are voluntary programs enough?
- Does building code level of rigour remove flexibility?
- Can building owners or installers self-certify?

Additional research to explore appropriate enforcement approaches for ICTi would be a benefit to all recommendations.

7.0 Conclusions

ICT infrastructure (ICTi) expectations are increasing at a rate proportionate to the rapid expansion of intelligent buildings and the envisioned exponential growth of connected devices within them. Building owners and managers are looking for consistency and predictability from the building's ICTi, while new and innovative technology is being layered into the architecture. Traditional proprietary wire-based systems are no longer desired as devices are expected to connect seamlessly into commingled networks. The Internet of Things (IoT) is further exasperating the situation with systems such as Power over Ethernet (PoE) bringing millions of connection points, both wired and wireless to any building, large or small. Further, traditional IT resources are insufficient to manage the complex ICTi, creating a new field of operational technology (OT) that controls and administers the flow of data. There is an increasing need to build capacity and awareness in ICTi and OT.

Organizations such as TIA and Bicsi have started to create working groups to develop guidelines for smart and intelligent buildings, which will help with the dialogue between owners, operators, users, consultants, and contractors. These guidelines are an important first step in meeting stakeholder needs for consistency, reliability, safety, and flexibility in an ICTi that will be

comprehensive, resilient, and futureproof. However, they do not provide certainty that the installed systems will meet the quality and service expectations for today's needs let alone the building's future needs. Voluntary programs, such as WiredScore, that uses a LEED-like rating system, is gaining traction in the commercial marketplace to enable certifications for managers to validate the claims of being an intelligent building.

As intelligent buildings become the norm, the potential risks associated with unintended access to private and confidential data is becoming a priority for building owners. The framework developed by NIST for the US government may help with managing the overall process. This leads to the need for enhanced specifications or codes to create rigour around the safety, security, and performance of ICTi in Canadian buildings.

References

[1] LiFi, "LiFi: Wireless Data from Every Light Bulb." Accessed: Mar. 30, 2020. [Online]. Available: https://lifi.co/

[2] Intelligent Buildings, LLC, "Cybersecurity for Building Operation Technology (OT) vs. Informational Technology (IT) Whitepaper," Intelligent Buildings, LLC, Charlotte, NC, USA, Nov. 2019.

[3] Gartner, "Gartner Glossary," Gartner.com. Accessed: Mar. 3, 2020. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

[4] National Research Council of Canada, "Canadian National Master Construction Specification (NMS)," Apr. 2, 2019. [Online]. Available: https://nrc.canada.ca/en/certifications-evaluations-standards/canadian-national-master-construction-specification

[5] National Research Canada, "Codes Canada Publications." Accessed: Mar. 30, 2020. [Online]. Available: https://nrc.canada.ca/en/certifications-evaluations-standards/codes-canada/codes-canada-publications

[6] CSA Group, "Overview – New Canadian Electrical Code Now Available," CSA Group, Jan. 8, 2018. [Online]. Available: https://www.csagroup.org/news/new-canadian-electrical-code-now-available/

[7] Office of the Privacy Commissioner of Canada, "The Privacy Act in Brief," Government of Canada, Aug. 2019. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/

[8] Privacy Commissioner of Canada, "The Personal Information Protection and Electronic Documents Act (PIPEDA)," Office of the Privacy Commissioner of Canada, Sept. 4, 2019. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[9] Privacy Commissioner of Canada, "Summary of Privacy Laws in Canada," Office of the Privacy Commissioner of Canada, Jan. 31, 2018. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

[10] Province of Nova Scotia, "Design Requirements Manual 2010 Edition," Sept. 21, 2010. [Online]. Available: https://novascotia.ca/tran/works/dc350/Part1.pdf

[11] Province of Nova Scotia, "Detailed Design Requirements – Electrical Appendix – NS Government Structured Cabling Guidelines – Information Transport Systems," Apr. 4, 2019. [Online]. Available: https://novascotia.ca/tran/works/NS-Structured-Cabling-Guidelines.pdf

[12] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity. (U.S. Department of Commerce, Washington, D.C.), Version 1.1. April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[13] WiredScore, LinkedIn. Accessed: Mar. 30, 2020. [Online]. Available: www.linkedin.com/company/wiredscore

[14] Author, interview with Utility Stakeholder, Aug. 2019.

[15] Telecommunication Industry Association, "Smart Buildings," 2017. [Online]. Available: https://tiaonline.org/what-we-do/technology/programs/smart-buildings/

[16] Public Services and Procurement Canada (PSPC), "Smart Building Initiative," Canada.ca, Feb. 12, 2020. [Online]. Available: https://www.tpsgc-pwgsc.gc.ca/biens-property/intelligents-smart/index-eng.html

[17] UNESCO, "Glossary." Accessed: Sept. 9, 2020. [Online]. Available: http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict

[18] WiredScore, "Wired Certification Guidelines for Commercial Developments and Redevelopments." Accessed: Mar. 30, 2020. [Online]. Available: https://wiredscore.com/en/

[19] Public Works and Government Services Canada, "Levels of Security." Accessed: Mar. 27, 2020. [Online]. Available: https://www.tpsgc-pwgsc.gc.ca/esc-src/documents/Levels%20of%20security.pdf

Appendix A: List of Standards Documents

Table 4: *CSA Codes and Standards*

Publication	Title
CAN/CSA C22.1-18	Canadian Electrical Code
CAN/CSA-C22.2 No. 226-92	Protectors in Telecommunications Networks.
CAN/CSA-ISO/IEC/IEEE 8802-1 and derivatives	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 1: Overview of Local Area Network Standards
CAN/CSA-ISO/IEC/IEEE 8802-2:1998	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control
CAN/CSA-ISO/IEC/IEEE 8802-3 All parts plus amendments	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet
CAN/CSA-ISO/IEC/IEEE 8802-5:1998	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 5: Token ring access method and physical layer specifications
ISO/IEC/IEEE 8802-11:2018	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications
CSA ISO/IEC/IEEE 8802-11:19	Information technology – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications – Amendment 1: Fast initial link setup (Adopted amendment 1:2019 to ISO/IEC/IEEE 8802-11:2018)
CAN/CSA-ISO/IEC 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary
CAN/CSA-ISO/IEC 27001	Information technology – Security techniques – Information security management systems – Requirements
CAN/CSA-ISO/IEC 27002	Information technology – Security techniques – Code of practice for information security controls
CAN/CSA-ISO/IEC 27003	Information technology – Security techniques – Information security management systems – Guidance
CAN/CSA-ISO/IEC 27004	Information technology – Security techniques – Information security management - Monitoring, measurement, analysis, and evaluation
CAN/CSA-ISO/IEC 27005	Information technology – Security techniques – Information security risk management
CAN/CSA-ISO/IEC 27009	Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements

Publication	Title
CAN/CSA-ISO/IEC 27032	Information technology – Security techniques – Guidelines for cybersecurity
CAN/CSA-ISO/IEC 27033-1	Information technology – Security techniques – Network security – Part 1: Overview and concepts
CAN/CSA-ISO/IEC 27033-2	Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security
CAN/CSA-ISO/IEC 27033-3	Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues
CAN/CSA-ISO/IEC 27033-4	Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways
CAN/CSA-ISO/IEC 27033-5	Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
CAN/CSA-ISO/IEC 27033-6	Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access
CAN/CSA-IEC 62443-2-1	Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners
CAN/CSA-IEC 62443-2-4	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers
CAN/CSA-IEC 62443-3-3	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
CAN/CSA C22.1-18	Canadian Electrical Code

Table 5: *Wiring Standards*

Publication	Title
TIA-526-7	Measurement of Optical Power Loss of Installed Singlemode Fibre Cable Plant
TIA-526-14-A	Optical Power Loss Measurements of Installed Multimode Fibre Cable Plant
ANSI/TIA/EIA-568-C.0	Generic Telecommunications Cabling for Customer Premises
ANSI/TIA/EIA-568-C.1	Commercial Building Telecommunications Cabling Standard
ANSI/TIA/EIA-568-C.2	Balanced Twisted-Pair Telecommunication Cabling and Components Standard
ANSI/TIA/EIA-568-C.3	Optical Fiber Cabling Components Standard
ANSI/TIA/EIA-568-C.4	Broadband Coaxial Cabling and Components Standard
ANSI/TIA-569-B	Commercial Building Standard for Telecommunications Pathways and Spaces.
ANSI/TIA-569-C	Optical Fibre Colour Coding
ANSI/TIA/EIA-606-A	Administration Standard for Commercial Telecommunications Infrastructure
ANSI-J-STD-607-C	Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications
ANSI/TIA-758-A	Customer-Owned Outside Plant Telecommunications Infrastructure Standard

Table 6: *Best Practice and Installation Documents*

Publication	Title
ANSI/BICSI 002-2014	Data Center Design and Implementation Best Practices
ANSI/BICSI 003-2014	Building Information Modeling (BIM) Practices for Information Technology Systems
ANSI/BICSI 004-2018	Information Communication Technology Systems Design and Implementation Best Practices for Healthcare Institutions and Facilities
ANSI/BICSI 005-2016	Electronic Safety and Security (ESS) System Design and Implementation Best Practices
ANSI/BICSI 006-2015	Distributed Antenna System (DAS) Design and Implementation Best Practices
ANSI/BICSI 007-2017	Information Communication Technology Design and Implementation Practices for Intelligent Buildings and Premises
ANSI/BICSI 008-2018	Wireless Local Area Network (WLAN) Systems Design and Implementation Best Practices
ANSI/BICSI N2-17	Practices for the Installation of Telecommunications and ICT Cabling Intended to Support Remote Power Applications
ANSI/NECA/BICSI 568-2006	Standard for Installing Commercial Building Telecommunications Cabling
ANSI/NECA/BICSI 607-2011	Standard for Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings
BICSI-TDMM	Telecommunications Distribution Methods Manual
BICSI -ITSIMM	Information Transport Systems Installation Methods Manual
BICSI G1-17	ICT Outside Plant Construction and Installation: General Practices

Table 7: *Other Documents Referenced in Report*

Publication	Title
ANSI/EIA/CEA-709.1	Control Networking Protocol
ANSI/ASHRAE Standard 135-2016	BACnet™ A Data Communication Protocol for Building Automation and Control Networks
IEC 61158-1	Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series
IEEE 802.11	ISO/IEC/IEEE – International Standard – Information technology –Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications
IEEE 802.15.4	IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)
IEEE 802.15.1	IEEE Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN – Specific Requirements – Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)
IEEE 802.3af	802.3af-2003 - IEEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications – Data Terminal Equipment (DTE) Power Via Media Dependent Interface (MDI)
DC350	Province of Nova Scotia Department of Transportation and Infrastructure and Renewal – DTIR Document DC350 Design Requirements Manual 2010 Edition

Appendix B: Sample Occupancy Types

1) Office

a) Single tenant (e.g., owner occupied)
b) Multi-tenant
c) Data center

2) Multi-unit residential

a) Dormitory
b) Rental
c) Condo/strata
d) Hotel/motel

3) Institutional

a) Convention center
b) Hospital
c) Health care clinic
d) Penitentiary
e) School/university
f) Long-term care facility

4) Retail

a) General retail (e.g., Big Box)
b) Fitness facilities
c) Motion picture theatre

5) Warehouse

a) Workshop
b) Storage garage
c) Other warehouse

6) Public Single Use

a) Fire station
b) Police station
c) Courthouse
d) Sports arena
e) Museum
f) Library
g) Performing arts theatre
h) Post office
i) Religious building
j) Town hall
k) Transportation facility

7) Industrial

a) Automotive facility
b) Manufacturing facility
c) Greenhouses
d) Other industrial

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™