

Intrusion Into the World of Cybersecurity

Canadians' exposure to cyber threats continues to increase due to the growing number of Internet-connected devices, digital innovations and automated processes. Today's highly connected building automation systems can also provide a point of entry to the corporate network and be subject to cyber attacks.

Cybersecurity in Evolution

Remote services are hosted on secure servers. As a result, the services and the server must instill confidence in the user. In this context, we often talk about the use of authentication certificates. But what are they and how do they work?

Authentication certificates are used to identify a specific server so that a secure session can be established during data exchanges and they guarantee the existence of the organization to which they belong.

SSL Certificate

Initially, the SSL (Secure Sockets Layer) certificate was designed to secure sensitive data between two systems (for example, between a server and a client, such as a shopping site and a browser, or between a server and another server, such as an application with personally identifiable information) primarily in the context of online payments. Subsequently, it has become the standard for, among other things, protecting access to user accounts, sending dematerialized documents or tax returns. Even social networks have adopted the SSL protocol.

The main objectives of SSL are:

- 🔒 Server authentication
- 🔒 Confidentiality of the data exchanged (with a cryptographic key)
- 🔒 Integrity of the data exchanged

Installed on a server, SSL allows secure connections on the browser. These are indicated by the presence of the HTTPS protocol in the URL of the server, and by the display of a security padlock in the address bar (left or right, depending on the browser).

SSL thus makes it possible to differentiate a secure and legitimate site from a poorly protected or even malicious site, as in the case of phishing.

TLS Certificate

When Netscape Communications was terminated, the Internet Engineering Task Force (IETF), which was responsible for most Internet standards, continued to develop and improve SSL, renaming it Transport Layer Security (TLS). Like SSL, TLS provides data security and encryption, the authentication code for messages.

Unlike SSL, TLS:

- 🔒 Consists of two layers: TSL recording protocol, which provides a secure connection, and TSL Handshake protocol, which allows the server and computer to identify each other and then together choose an encryption algorithm and secret keys before sending data or messages to each other
- 🔒 Is immune to cyber attacks
- 🔒 Is enabled by default in all browsers
- 🔒 Supports newer, stronger and more secure encryption algorithm suites
- 🔒 Supports the message authentication code algorithm suites (HMAC-SHA256 / 384 and AEAD)

Consequently, TLS fulfils the desired security objectives: it ensures the mutual authentication of actors, confidentiality, spatial and temporal integrity of transactions. TLS can be said to represent a secure protocol in its construction and mechanisms. That is why, as part of its commitment to the security of personal information, Regulvar now uses TLS, as well as the BACnet/SC protocol, an improved and more secure version of BACnet/IP. Indeed, TLS is an essential function for secure communication, and certificate management is now one of the requirements that must be met in order to set up a BACnet/SC network.

Regulvar is adapting

Twenty years ago, companies were not aware that people could take advantage of the information they had by using gaps in the network. But who doesn't remember the recent data leak at Desjardins?

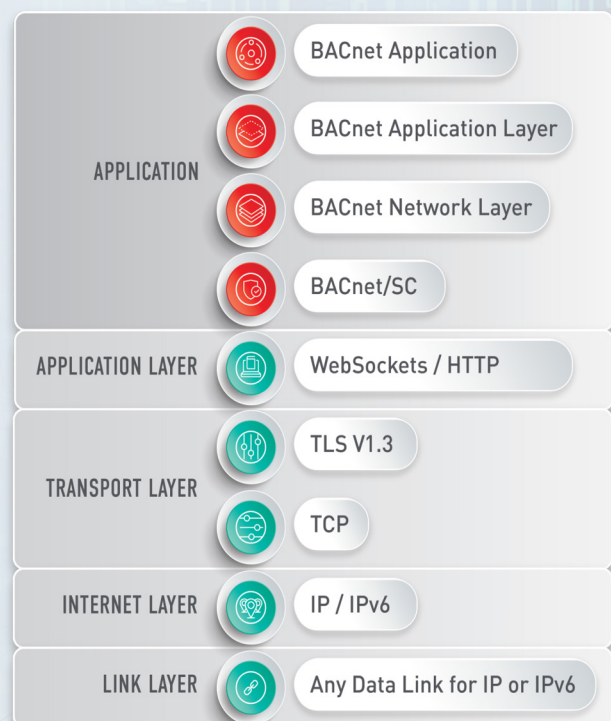
Regulvar has been installing IP control systems, such as BACnet/IP, for nearly 20 years. This protocol has allowed the HVAC industry to evolve considerably. However, since it is open, it can constitute a breach in networks. That is why it is important to have appropriate protection systems in place and properly managed by the IT department when using it. Moreover, it is based on standards that are no longer widely adopted by the IT community, especially with regard to security.

BACnet/SC

Delta Controls has adapted to the situation by implementing a cybersecurity program with the necessary policies, processes and testing, compliant with OWASP, ISO and NIST standards, to deliver secure products. Its goal? To ensure that building networks remain protected through information technology integration best practices, ongoing product evaluation and timely security updates.

As a result, Delta Controls and Regulvar now use [BACnet Secure Connect \(SC\)](#), a secure BACnet protocol for TCP/IP networks that complies with the IEEE 802.1X standard, as well as TLS tools.

Based on SSL and TLS, BACnet/SC is an open and closed protocol that has its own network security mechanisms for authenticating a controller or software and authorizing it to use a network. In addition, for added security, BACnet/SC devices can be deployed in Virtual Local Area Networks (VLANs) or Virtual Private Networks (VPNs). Moreover, BACnet/SC is adapted to conventional IT security methods, procedures and protocols, making it very user-friendly and more secure.



Representation of the different BACnet layers in the OSI model

In addition, BACnet/SC is compatible with all BACnet systems and devices that are already installed. Nothing needs to be removed, no functionality is lost. The programming and customer-server language have not changed. Users do not need to learn anything new. Those who already have a BACnet system and wish to switch to BACnet/SC communication simply use a BACnet router, as this is a different data link. The same concept applies if the user wants to switch from BACnet MS/TP to BACnet/IP. The BACnet message remains the same, only the envelope changes.

Main differences between BACnet/IP & BACnet/SC

	BACnet/IP	BACnet/SC
Transport protocol	UDP	TCP
Encrypted communication	No	Yes (using TLS protocol)
Device authentication	No	Yes (using TLS protocol)
IP addresses	Usually static	Static or dynamic
DNS	Not used	Used by some manufacturer
NAT tolerant	Using special devices	yes
Building connection type	BACnet/IP BBMDs	BACnet/SC hub
IT port opening	Required	non required

Advantages of BACnet/SC

- 🔒 User-friendly: adapted to IT field
- 🔒 Use of standard security technologies (TLS protocol) of TCP/IP networks
- 🔒 Message encryption
- 🔒 Authentication of building, system, network, manager, etc. controllers with certificates
- 🔒 Compatibility with BACnet systems and devices
- 🔒 Support for IPv4 and IPv6 networks

The digital revolution has brought many benefits, but also additional risks. Today, various approaches are used to secure the BACnet infrastructure; however, these solutions can be difficult to implement and are a burden on IT organizations. BACnet/SC greatly facilitates the creation of a secure and standardized BACnet infrastructure that is fully compatible with existing BACnet deployments.

Cybersecurity is not just an information technology issue: it is a company issue that requires an interdisciplinary approach and a broad commitment to governance to ensure that all parts of the company are well aligned to support effective cybersecurity practices.

Régulvar has always focused its efforts on offering innovative, adapted and easy-to-implement solutions, and its cybersecurity program is no different.



A major project

Réseau
express
métropolitain



Who hasn't heard about the REM project? This vast project, launched more than a year ago, is currently the largest public transit project in Quebec. What is the objective of the REM? To serve the Greater Montreal region over 67 km (Rive-Sud, Montreal-Pierre Elliott Trudeau International Airport Sainte-Anne-de-Bellevue, Deux-Montagnes) through a network of 26 stations.

Regulvar is pleased to announce that it has been mandated to participate in this prestigious project. Regulvar will design and install the REM BACnet/SC building automation system in the 26 stations, two maintenance centres and the administrative building. In total, it will install nearly 2,700 controllers (eBMGR, eBM404, eBM440, eBM800, O3-DIN-SRC, O3-DIN-CPU, O3-DIN-8xP) on a highly secure industrial network. Regulvar's work began on February 25.

What will be the challenges?

Discover more in another newsletter once the works are completed. Stay tuned!

Written by
Caroline Gras, C. Tr.,
Regulvar inc.

Graphic Design
Stéphanie Harel
Regulvar inc.

Source
Marc Dugré, Eng., GSC
President, Regulvar inc.

Upcoming
Training

	In Laval (French)	In Gatineau (English)
BACnet OBJECT HANDLING	September 14 - 15	Upon request
ADVANCED OBJECTS AND CONTROLLERS	September 16 - 17	Upon request
GCL PROGRAMMING	September 22 - 23 - 24	Upon request
CREATING GRAPHICAL INTERFACES with Illustrator	September 29 & 30	Upon request
CREATING GRAPHICAL INTERFACES with entelivIZ	Upon request	Upon request
INTRODUCTION TO WIRELESS CONTROL	Upon request	Upon request

For more information,
visit our Website

www.regulvar.com

or contact the **training department**
at 450-629-0435, ext. 1777
formation@regulvar.com