What are Smart Cities and a Smart Transportation Systems without a Cyber Secured Smart Grid Fortified Network?

For the last 60 years, transportation experts have been trying to improve fluidity and reduce congestion using some other way than investing in the building of new roads and other infrastructures. After several trials and errors, this gave rise, 20 years ago, to a new practice in surface transport called Intelligent Transportation Systems. This practice consists essentially in the digitization of the transport system through integrated IT and OT solutions that will require a robust network with quality of service. In other words, ITS will require electricity and telecommunication infrastructure. The four main pillars of our ground transportation system: roads, rail, air, sea – are directly impacted by the digitization of their operations, for security, safety, regulation of the traffic flow for transportation of goods and people. The implementation of technologies in the last mile, similar to the first generation of fiber to the home concept in 2000, allows public and private organizations to provide data that demonstrates the benefits and positive impacts on operating in their daily lives. The critical mission of such system is to better balance the offer and the demand in transportation. Between the IT giants, energy, telecommunication carrier, automation and engineering consulting; the administrative priorities of each public and para public clients, in 2017, can be very complex for one reason: How we communicate and secure our digital infrastructure?

If you can't explain it simply, you do not understand it well enough. Albert Einstein.

I could not help but return in 1901, the year of the first transatlantic communication between Europe and Canada. Let's put aside the patent claim between Marconi and Tesla. More than a hundred years later, the key important fact is that Marconi proved, with $50,000 dollars (More or less 1.3 Million in 2017 dollars) subsidy from the Canadian Government approved by no other than the Prime Minister Wilfrid Laurier, the importance of a dedicated telecommunication infrastructure. This was the first concept to build a strong global telecommunication network that got sold to the government of Canada several years later (Remember Teleglobe). When we go back at the turn of the 20th century, this was more than just wireless communication; it was the beginning of the connection of the world with electricity and phone lines through dense areas till 1960. Now, in 2017, we are at the beginning of the 21st century and the energy and telecommunications are facing the same challenges with technologies available today that are now subject to fierce competition at every level. The bipolarity shifting between protectionists and open markets create another layer of complexity to bring smart cities in the warp mode, but most of all, avoid another technology bubble.

Massive investments over the last fifteen years allowed us to include telecommunication in the daily operations of our society with unfortunately several buts. Protection of privacy, cyber security, costs of ownership, maintenance, returns on investment. Only well structure regulated sectors can support such initiatives for one simple reason: Security parameter agreements.

Can we claim that all of us agree on the importance of centralized operations center to protect big data, cloud services in an open data policy? Not quite. The arrival of technology plunged energy, transportation and industrial sector into a transition that is still going on. With new protocols combine with a mixed of international standards and acronyms, you can imagine how many pieces this puzzle requires to ensure interoperability between different software and manufacturers. Just one word to summarize: “communication” between the different technology engineers with very noble intentions to assists the various political actors to consider a SIL (Safety integrity level) approach. The implementation of several by-laws and regulations will change the vision of how we will see the world and has to be put in place to mitigate the risk of bringing down any form of integration and interoperability initiatives. At the core of Smart Cities Systems, Cyber Secured Smart Grid and Fortified Network is the backbone of investing in for three major reasons:

- Improving interinstitutional coordination
- Savings on duplicating operations
- Safe and secure services to the population

Safety and security in the context of any SMART or autonomous systems have to be a priority for all decision makers. Concern remains with the increase in the amount of data on existing systems and the potential for risk of none intendant, illegal or terrorist acts. The concept of “safety” can be very similar to that of “security”, depending on the context or field of application. The difference in meaning may be presented according to the following principles. Security mainly expresses a notion of protection against the commission of inappropriate acts (voluntary or involuntary) not in conformity with the established rules which could result in damage affecting the system and the population. For example, a security measure may result in a coherent set of defensive measures put in place and enforced for the purpose of obtaining and maintaining the order or security of users.

Safety in the context rather linked to the concept of proper functioning of systems or equipment so that they can perform their function correctly without causing any damage. The standards of design or maintenance of mission critical infrastructure requirements, inspection, evaluation, are all in the field of safety. Concerning high risk systems, systemic approach like SIL (Safety Integrity Level) is intended to avoid damage or accident and thus respect the physical integrity of the population by protecting the environment, which remains in the safety side. On the other hand, when a measure is related to protection against a malicious act, it is a matter of security. Detecting incidents more quickly, better coordinating relief efforts and informing users of the presence of obstacles, are all actions that result in an increased safety of the Smart World Network.

Studies have shown significant reduction in accidents with centralized control systems now can provide accurate information in case of an accident, fact-based incident formulation for the stakeholders and accident reconstruction to support the litigation. All displacements, events and intervals can be access without zero packets lost. The data and the accident analysis begin even in real time with appropriate activated scenario. Various reports and graphs can clearly demonstrate the double impact of an incident or accident. The use of GPS combines with network time protocols in communications to locate from centralized control when there is: panic alert, off-limit access, unauthorized port connections, entry of vehicles or individuals into a forbidden zone, no contact and movement according to a time. Access to these smart systems may be restricted to certain categories or groups, and with the circuit-cut put access key, thereby validating the individual and anti-theft, anti-terrorism can be increased. The addition of a power and telecommunication redundancy makes it possible to operate with 99.999%, so even if the power or telecommunication is interrupted, the active events linking the subsystems will be configured on the system and an alert will be sent to the centralized control or to a mobile unit.

Institutional issues, rather than those of a technological nature, are important aspects to consider when implementing technologies in mission critical operations. The reasons for implementing these systems varied and have an impact on most aspects of the IT/OT infrastructure. Identification of institutional pains is a key step in the planning of migration and deployment of any smart system. For the past decade, the implementation of an intelligent system has been a privileged approach to consulting and considering the specific needs of stakeholders in order to maximize the chances of success.

Can smart transportation systems be a solution for congestion that is a critical problem for all major metropolitan areas? The OECD (Organization for Economic Corporation and Development) estimates the financial impact of congestion on the GTAA (Greater Toronto Airport Authority) at approximately $3.3 billion, annually; will the use of any autonomous independent standalone proprietary wireless device really allow us to reduce congestion? Not if you do not think that your smart city concept is mission critical. Even the best technique of measuring distance through instrumentation DMI (Distance Measuring Instruments) or a new VMT (Vehicle Miles Travelled) concept will not resolve the situation. Only modulation of travel according to the available transportation alternative will alleviate the problems of congestion. London with its tax on congestion increased by 3 km/hours moving in the city, despite this considerable gain, a massive infrastructure refurbishing programmed questioned eliminated that gain. The great strength of technologies is to share and secure the data in real time and propose an alternative to avoid congestion caused by three elements that we cannot control: Climate conditions, human behavior and political changes.

Technically, a common vision must make it possible to offer something greater than a smart city, a quality of life. The challenges lie in coordinating the actions of multiple participants. On any scale, the concerted development of a vision between stakeholders and institutional cooperation are key elements in the process of realizing any technology projects. So it is from centralized management centers that priority can be given in emergency situations caused by severe climatic conditions or just to better plan the projects that are affecting the population. The coordination in the event of incidents or accidents involving dangerous products or materials can be implemented according to pre-established intervention plans and can be carried out from a center to center communication protocol.

In the event of an emergency, the "Critical mission," having at its disposal such a secured center, is thus endowed with a very important element, since it contains means of communication that can be linked to the center of operations on the site and the coordination center. This system has to describe the functionalities of a surveillance center and their sub systems communication links and equipment's for control of the smart systems network. Several devices are identified in these systems ranging from fixed automation and control system to system that adapt to conditions or priority requests in this now echo technology system called IIoT. (Industrial Internet of Things).

Smart concepts have to be set up under the best possible conditions. Other aspects than purely technical aspects have to be taken into account. Technological issues, standards and communications protocol, are the most important aspects to consider when implementing a mission critical system. The political reasons of the various stakeholders are varied and will have an impact on all aspects. The financing arms of technology infrastructure and regulations in Canada are sufficiently different from the global market so that we can feel the repercussions. The power to invest is legislated by the provinces, cities and the municipal level in some case linked with the federal. The notion of digital networks deployed in for a better use of the existing right of ways have to be considered as a critical mission for our nationwide asset technology infrastructure monitoring. The vision for a smart city concept releases barely enough money to put in place a robust system architecture that could allow decision makers to have most important tool in their hand. Finally, the shortage of succession causes also a problem to the democratization of this Smart Concept. There is general agreement on the importance of education and training with some differences of opinion on a renewed practice of this new practice called Smart Cities.