Appendix A:
Questions & Answers

Contents

A.1.Questions & Answer:

During the execution of the project, several concerns from the VdM team about the design and implementation of Smart City are also acknowledged through an extensive list of questions presented in Section A.1. These questions are re-arranged/grouped for better connections between them, and addressed in Section A.2 with further details referred to the other corresponding sections/appendices.

A.1.1 List of Questions:

M01: What is the optimal number of cameras or devices per gateway?
M02: What is the optimal number of cameras or device per wifi transceiver?
M03: Optimal and scalable target architecture (with existing technology)
M04: IPv6 effects on deployment?
M05: Large-scaled Firmware management?
M06: Strategy - How multiple applications can share a single camera?
M07: Strategy - When to use radar over camera for crowd or person, bike or car counting?
M08: When to use Wifi instead of LTE (coverage, capacity)?
M09: Frequency usage and interference?
M10: Device Security - How to secure and authenticate cameras or radars?
M11: Device meta-data management? built-in or configurable?
M12: Strategy for device power management? (i.e. battery life cycle)
M13: Camera installation procedure? (hauteur, azimuth, etc.)?
M14: Radar installation procedure (hauteur, azimuth, line of sight etc.)?
M15: What are the best standards and protocols (ie. LoraWAN, IPv6, MQTT, CSU, etc.)?
M16: What are key environmental factors affecting device deployment?
M17: How do we manage device discovery and identification?
M18: How to do large scale management of devices/sensors?

M19: What are some next research topics to investigate to prepare for enterprise-grade deployment of sensor (IoT Edge)?
M20: How to manage security during transmission and storage? (encryption, etc.)?
M21: How to estimate or dimension the architecture for scaling out to 100,000 devices?

SUGGESTED POTENTIAL VIDEO ANALYTICS FUNCTIONS TO TEST:
V01. Vehicle counting and direction
V02. Bike counting and direction
V03. Pedestrian counting and direction
V04. Detection of double-parked or obstructing vehicles
V05. Detection of suspicious packages
V06. Theft detection (ex: car break-in, building break-in, bicycle theft)
V07. Altercation detection
V08. Measurement of pedestrian, bike and vehicle density
V09. Detection of broken aquaduc or man-hole
V10. Fire detection
V11. Injury detection (ex: heart attack)
V12. Accident detection
V13. Detection of street obstructions (ex: snow, downed electrical power line, downed telephone pole, dead animal)
V14. Detection of hazardous road conditions (ex: black ice, hydro-planing, etc.)
V15. Detection and profiling of pot-holes (depth, area, proximity to side walk)
V16. Detection of road fissures
V17. Detection of dangerous substance spillage or leakage (ex: oil)

A.1.2. Re-arranged Questions and Answers:

In the following, the questions are re-arranged/grouped for better connections between them and addressed. For easy reference, the questions are reproduced in italics and followed by the reply.

M02: *What is the optimal number of cameras or devices per WiFi transceiver?*
Answer to M02: It depends on several factors such as the fiber drop capability/availability, the operational mode of the AP WiFi transceiver (Point-to-Point or Point-to-Multipoint), the number of Station WiFi transceivers per AP, the level of interference as well as the configured frame-rate and resolution at the connected cameras. For example, according to our tests in the pilot deployment, the minimum average UDP throughput per transceiver pair using 802.11n is 32Mbps while the bandwidth of a camera at HD resolution (1280x720) is about 9Mbps. As a result, taking in consideration the WiFi transceiver capability only, it is estimated that a transceiver can support at most 3 cameras at HD resolution, leaving only 5Mbps margin. It is remarked that due to the difference and its variation, a throughput test must be regularly performed to provide an insight of the wireless link capacity. It is also recommended that a safe margin of about 30% of the wireless link capacity is reserved for peak traffic and potential increase in interference in the future. Also, if possible, a *dedicated* spectrum for deployment should be a good way to mitigate from the interference of public WiFi. More details on this issue related to the pilot system deployment can be found in Chapter 3.

M01: *What is the optimal number of cameras or devices per gateway?*
Answer to M01: Similar to M02, the answer to this question depends on many factors as stated in M02. In addition, the capacity of the VPN tunnel and the capacity of each connected transceiver have to be

taken into consideration (the current VPN tunnel bandwidth is 60Mbps). More details on this issue related to the pilot system deployment can be found in Chapter 3.

M09: *Frequency usage and interference?*
Answer to M09: As discussed in M02, interference with public 2.5GHz or 5GHz WiFi could severely affect the performance of the deployed network. If possible, a dedicated/licensed frequency spectrum (for example 3GHz) for deployment should be a good way to mitigate from the interference of public WiFi. However, it would imply additional reoccurring costs for frequency license. In our tests during the last two months, we have observed that the interference from other Wi-Fi systems, varies from day to day, and thus the capacity of a given link also varies. Chapter 3 includes the studies and observed results on the behavior and variation of interference from other systems and its effect on capacity/throughput of 6 WiFi links at different locations. Note that, so far, with all 6 deployed cameras configured with 1280x720 resolution 24fps CBR 6144kbps, the transmitted video seems to be recorded continuously without significant loss of quality; however, from time to time, we have observed video frames being lost. As video resolution increases to 4096x2160 24fps CBR 16384kbps, we have observed that the video stream becomes intermittent, and the loss of frames is significant on some of the cameras (performance not acceptable). However, this issues is likely to be related to the compatibility between cameras and VMS software (more tests with specific camera vendor supplied recording software to be verified).

M03: *Optimal and scalable target architecture (with existing technology)*
Answer to M03: The area of deployment should be divided into a number of hierarchical network sectors based on the maximum rate supported by the final links to the *big-database* location. For example, based on the 10Gbps optical-fiber pipe, there would be several 10Gbps pipes entering the database location, each for one sector. This architecture is applicable to both private data centers and cloud-based servers. Cloud-based solution although more expensive would provide easy scalability. Chapter 4 discusses the suggested scalable network and server architectures based on current industry deployed and recommended examples.

M21: *How to estimate or dimension the architecture for scaling out to 100,000 devices?*
Answer to M21: Chapter 3 provides an estimation on the number of cameras and wi-fi gateway radios based on rough assumptions for the down-town and complete Montreal island area and use this information to estimate the total network and datacenter throughput requirements/feasibility, and storage requirements. In terms of server architecture we use the examples of enterprise level camera VMS software such as Milestone, and investigate Cloud based solutions based on MS Azure examples.

M04: *IPv6 effects on deployment?*
Answer to M04: Among the deployed devices, it is noticed that some of them do not support IPv6 protocol, and this could be a potential issue, or main requirement for IoT deployment. For example, CISCO MX84 device in VPN tunnel mode does not support IPv6, and some of the low-cost Ethernet to RS232 serial adapters (needed to interface with sensors) also do not support IPv6. Most of the remaining Ethernet devices on our deployed pilot system, including all the cameras and the WiFi bridges, do support co-existent IPv6 and IPv4 operation. As of Sep. 2017, the management system was replicated to VdM network, which is directly connected to the pilot network through fiber, so IPv6 tests can be conducted between VdM network and the pilot system (as no VPN is required).

M05: *Large-scaled Firmware management?*
M18: *How to do large scale management of devices/sensors?*

Answer to M05 and M18: So far, we have already experimented with automatic firmware management/updates using vendor specific central management software, for example, "AirController" Wi-Fi radios management application from Ubiquity, and other similar applications for Hikvision, Axis and Panasonic Cameras. These separate vendor-specific applications could be installed on VdM private servers, but will need to be deployed per batch of certain limited number of IoT devices, and thus would not be easily a scalable solution. For automatic/mass number of device firmware management, scripted/automated configurations can be implemented to trigger the update procedure. During the time of the project, we didn't find any software that can check and manage firmware from different manufacturers. As a result, for a unified centralized device management, custom software must be developed making use of the devices' standard APIs or protocols.

M6: *Strategy - How multiple applications can share a single camera*?
Answer to M6: Video analytics could be designed to detect a given known location view and run a given application process only on those range of video streams detected as valid. For example, a camera could have a number of pre-set viewing angles and periodically scan and record each viewing angle for a specified amount of time, one view could be at intersection to count the number of passing cars, other view could be at the park to estimate the number of present people, the car video analytics software would ignore the frames which are showing park view and only use only the correctly detected intersection frames to count the cars (for example). The video applications could run in parallel on different servers and read the same video file from common database. We do not intend to try this in this phase of the project. However, as discussed in Chapter 4, virtualization can be a good solution for sharing the use of hardware between applications. A virtualization structure abstracts the physical resources so that different applications can utilize the same infrastructure at the same time. It is acknowledged that this is more of a research issue and commercialized solution may not be available yet.

M7: *Strategy - When to use radar over camera for crowd or person, bike or car counting?*
Answer to M7: Radar is a single-purpose sensor and can only be used for the sole purpose of counting for example in a fixed context, which means different types of radar should be used in one place if different applications are needed. Cameras on the other hand can be used as a universal type of sensor. However, the problem with cameras is that their accuracy depends heavily on the capability of image processing techniques that are implemented. For some applications, the image processing may also require heavy processing power which is not feasible for real-time application. It is worth mentioning that the accuracy of image processing algorithms can varies depending on various factors such as the weather, lighting, day/night and camera resolution, framerate. However, it is widely believe that the accuracy of image processing techniques will likely improve in the future. Due to the software implementation, video analytic functions can be upgraded and one video feed can be used to support many applications.
Another important factor is privacy, video feeds can be used to extract the identities of the people in the scene which may cause some privacy implications.
According to our tests in Appendix H, it is observed that the accuracy of camera based traffic statistics could be affected by environmental factors, heavy fog, snow, rain, poor street lighting, or direct sun camera view overexposure. On the other hand, traffic radar is a cheaper and more reliable solution. If even higher resolution and accuracy is needed, the solid-state LiDAR sensors from LeddarTech could be used, however, the cost of these devices could be comparable to or higher than high resolution cameras. Note that, specialized infrared traffic cameras, for example from Flir, could also provide weather independent reliable readings, and not intrude privacy. We did not try IR Flir camera due to high price for low number of cameras.

M8: *When to use Wifi instead of LTE (coverage, capacity)?*

Answer to M8: In general, WiFi is a more economical way of data transportation, it also offers better throughput in comparison to LTE. However, LTE has a significant advantage of ubiquitous coverage city wide. The usage of each technology depends on the budget, coverage and data speed/volume that need to be transport. For high bandwidth devices such as camera, it is suggested to use specialised Wi-Fi with TDMA protocol, such as currently deployed Ubiquity M5 and AC5 Nanobeam radios (not a typical commercial Wi-Fi with CSMA protocol) for communications. For mobile sensors with medium and low data rate that are constantly on the move, it is suggested to use LTE (for wide coverage), but for limited number of devices due to relatively high operating cost. NOTE, for very low data rate per sensor applications, LoRaWAN system would be recommended. More details about the coverage, capacity and limitations are provided in Chapters 3.

M10: *Device Security - How to secure and authenticate cameras or radars?*
Answer to M10: Some of the recommendations for security can be found in Chapter 5. For camera streaming, username and password can be configured to protect access to the video feeds. To protect the configurations, HTTPS can be enabled and used along with username/password protection.
For devices such as Axis cameras, Owner Authentication Key (OAK), which can be obtained alongside with the serial number in the packaging of devices, can be used for authentication with supported software. For non-IP devices, no authentication or encryption techniques are available and authentication, encryption can only be realized through the capabilities of the adapters. Further details on other potential authentication techniques for other type of devices are included in Chapter 5.

M20: *How to manage security during transmission and storage? (encryption, etc.)?*
Answer to M20: Some of the recommendations and security standards are described in Chapter 5. Data security composed of three basic requirements: confidentiality, integrity and availability. To protect the exchanged packets from revealing information, strong encryption methods such as AES, 3DES is required. In order to protect the transferred data from alerting and manipulating, proper mechanisms can be used to verify the authenticity of the data such as digital signature, Message Authentication Code (MAC), key based hashing can be used. Besides, the use of random numbers (nonce) can also be utilized to prevent attacks such as replay attacks.
Data storage security features are also discussed in Chapter 5. For on premise setups, it is observed that storage encryption can be achieved at either the storage device level (NAS encryption) or at the software level. However, only enterprise software (for example XProtect Corporation or CosmosDB Enterprise Advanced) integrated the encryption features for data at rest. For cloud-based solution, encryption for data at rest and database are typically supported by the cloud service providers.

M11: *Device meta-data management? built-in or configurable*?
Answer to M11: Need more clarification for the question.

M12: *Strategy for device power management? (i.e., battery life cycle)*
Answer to M12: For stationary devices in the pilot deployment, as they are installed on streetlights, they can be power directly from the AC power source. For mobile devices such as the level sensor, the battery life depends on the wakeup time and communication rate of the sensors. Table ***1*** shows the estimated battery life of the level sensor with different wake up and status report rate from the level sensor datasheets. The longer the communication rate, the longer the battery life; however, depending on the application, the battery life and the utilization of the application should be traded off. For example, the sensors on the salt truck can be re-programmed to be dynamically adjust the update time, i.e. faster update rate while moving and slower update rate when stands still. Supposed that the service time of the

salt truck is 12hrs/day, during which the update rate is 1min/update, the battery life can be estimated (according to ***Table 1***) to be at least 9 months (long enough to service through one winter).

Table 1: Battery life estimation of level sensor.

	Wake up and report status rate						
	24 hrs	**12 hrs**	**8 hrs**	**6 hrs**	**4 hrs**	**1 hr**	**1 min**
Battery life	3.63 yrs	3.60 yrs	3.58 yrs	3.56 yrs	3.52 yrs	3.17 yrs	4.36 mths

M17: *How do we manage device discovery and identification?*
Answer to M17: During the project, Milestone VMS was tested for device discovery and identification. Although Milestone VMS claims to be compatible with cameras with ONVIF standards, it is observed that some cameras were not detected correctly, for instance, the Panasonic camera was detected without PTZ capability. The discovery of wireless radios is also feasible through the use of Ubiquiti Air Control software. For other devices, no support for device discovery and identification is currently available and development of customized software should be done to provide this feature.

M13: *Camera installation procedure? (hauteur, azimuth, etc.)?*
Answer to M13: The camera installation procedure will be presented in Appendix D.

M14: *Radar installation procedure (hauteur, azimuth, line of sight etc.)?*
Answer to M14: The radar installation procedure will be presented in Appendix D.

M15: *What are the best standards and protocols (ie. LoraWAN, IPv6, MQTT, CSU, etc.)?*
Answer to M15:
Communication standards:

- *For high bandwidth devices (such as cameras)*
  - *Stationary installation:* the best way for data transfer is using wired connection such as fiber network for stability and supplementing by WiFi bridges to extend the reach from the fiber drops. For WiFi bridges, it is best to use dedicated spectrum instead of shared bandwidth and it is noted that TDMA protocol provide a better achievable throughput than the traditional CDMA protocol.
  - *Mobile installation:* due to the high volume data requirement, it is best to store the data into some storage and offload the data latter, using wired Gigabit Ethernet or High speed WiFi AC connection.
- *For medium bandwidth devices (such as radars, RFIDs, etc.)*
  - *Stationary installation:* the data can be uploaded through WiFi networks or even Zigbee communications.
  - *Mobile installation:* since the data volume is not huge, LTE network can be used for data upload. However, due to the cost, the number of devices must be traded off.
- *For low bandwidth devices (such as parking sensors, garbage sensors, etc.):* LoRaWAN could be a good choice due to its wide coverage. However, the base station might need to be deployed and operated by VdM itself, since, at the present time, there are not LoRaWAN base station operators/service providers in Montreal area.

Data, Device management:
For data and device management, the support of IP, especially IPv6 is critical to provide a unified all-IP network. For cameras, the support for ONVIF standards is essential for unified management. For other devices, SMNPv3 (although many of the current devices still only support, less secure, SMNP v1 or v2), SSH and HTTPS support is needed for the ease of device management.

M16: *What are key environmental factors affecting device deployment?*

Answer to M6: For outdoor installation, key environmental factors include water proof, operational temperature, and low maintenance. In general, devices with certifications such as IP66 and IP67 are best practices for outdoor installation.

M19: *What are some next research topics to investigate to prepare for enterprise-grade deployment of sensor (IoT Edge)?*
Answer to M19: There are several research topics to be studied for enterprise-grade deployment of sensor. These research topics are discussed in the section on "*Challenges*" in Chapters 2, 4, 5, and 6. A brief summary of the research topics is as follows.

- *Scalability*: network throughput, data storage, standards for compatible operation of different kinds of sensors from different manufacturers, mass device management platform, mass device re-configurations, collaboration data sharing.
- *Virtualization*: efficient resource management and provisioning for services, cooperation between IoT devices to support for future services, optimization methods to support different types of services.
- *Security and privacy*: physical security, efficient encryption, authentication methods for low power devices, secure re-configuration, support for public keys and digital certificates, multi-factor authentication, artificial intelligence based Security. Masking of private information when sharing, data ownership control.
- *Data analytics*: unified data quality and formatting, centralized and distributed data analytics, real-time analytics, machine learning and deep learning techniques for big data mining.

ABOUT VIDEO ANALYTICS FUNCTIONS:
V01. Vehicle counting and direction
V03. Pedestrian counting and direction
V04. Detection of double-parked or obstructing vehicles
Answer: These applications have been investigated and described in Chapter 6, Section 6.2.1 with further implementation details provided in Appendix H. Commercial products investigated in Appendix L.
V08. Measurement of pedestrian, bike and vehicle density
Answer: The application for crowd counting/estimation has been investigated, and described in Chapter 6, Section 6.2.2 with further implementation details provided in Appendix I.

V05. Detection of suspicious packages
Answer: Some preliminary experiments with the available camera software such as that was integrated with HikVision cameras were done but the obtained results were not very good, and probably limited to very simple scenarios. More accurate algorithms are needed to be developed/researched. In order to have a good idea about practical/realistic capabilities of the commercial product specialized in video analytics for security purposes, we have asked iOmniscient to use our staged suspicious packages events, recorded with our QdS deployed cameras, to detect these events using their ¨iQ-140¨ Non Motion Detection Software - for abandoned objects detection. For more preliminary information see Appendix K.
V10. Fire detection
Answer: We have done some preliminary available open source applications for fire detection, however, the results were very poor, for example, these simple analytic application were detecting an orange object in the video clip as a fire. More accurate algorithms are needed to be developed/researched. In order to have a good idea about practical/realistic capabilities of the commercial product specialized in video analytics for security purposes, we have asked

iOmniscient to use our simple fire and smoke video clip, recorded with our QdS deployed cameras, to detect these events using their ¨ iQ-Smoke¨ Smoke and Fire (Advanced) Software Detection. For more preliminary information see Appendix K.

V02. *Bike counting and direction*
V06. *Theft detection (ex: car break-in, building break-in, bicycle theft)*
V07. *Altercation detection*
V09. *Detection of broken aquaduc or man-hole*
V11. *Injury detection (ex: heart attack)*
V12. *Accident detection*
V13. *Detection of street obstructions (ex: snow, downed electrical power line, downed telephone pole, dead animal)*
V14. *Detection of hazardous road conditions (ex: black ice, hydro-planing, etc.)*
V15. *Detection and profiling of pot-holes (depth, area, proximity to side walk)*
V16. *Detection of road fissures*
V17. *Detection of dangerous substance spillage or leakage (ex: oil)*

Answer: These applications are not investigated in this phase. They are more involved and can be interesting for further detailed studies in the next phase.

A.2 Replies to VdM Comments on the draft Technical Report

This section provides replies to the VdM comments on the draft TR.

For easy reference, the VdM comments are reproduced and, in some cases, grouped if they are related, followed by point-by-point replies.

Appendix E: Database Integration

Comment 1 (page 2): *This image does not appear or render ???*

Reply: We find that among the 3 documents that you sent back, Appendix E and F have this problem but the main report does not. We opened the file originally sent to you, and did not have any problem. We think that this can be just a formatting mismatch, e.g., a version mismatch problem. The document processing program that we used is Microsoft Word 2013. It is noted that there are known formatting mismatch when importing a Word document to Google docs application.

Comment 2 (page 14): *Though we agree this is just a prototype, a survey of existing industry-based literature would reveal that there are over 300 IoT-plateform vendors at this time. Hence, there are many existing useful IoT platform and storage reference architectures that could have been used as a source of inspiration to guide this prototype implementation.*

Reply: It seems that our presentation is not sufficiently clear to you.

In the MSCPS project, our focus is to consider a *generic* framework for a Smart City for a wide range of applications with various sensor/actuator types and devices from *multiple* vendors. For this, *ideally* a *generic* platform (either non-cloud or cloud-based) that can accommodate various sensor/actuator types and devices from *multiple* vendors is *needed*. Furthermore, it is *desired* to select and use such a generic platform *commercially available* rather than to develop it by ourselves.

With the above-mentioned objective in mind, in this work, we intend to find such a *commercially available, generic* platform, and investigate its potentials. We agree with you that there are several industry-based IoT platforms, for example, MS Azure IoT Hub, Cisco-Jasper, Ericsson IoT Accelerator, etc. Within our constrained time and accessibility, we have considered some of them, and found that, unfortunately, those *currently* available platforms are not quite *generic*. They seem to be *application*-specific, *device*-specific, or *technology*-specific, for example, only supporting some hardware models from some specific vendors, or only supporting video, or only supporting communications over cellular network, etc. This could be explained by the fact that the development of a *generic* platform can be complex and time-consuming, and to come out timely in the market, developers may select to focus first more *specific* to certain *high-priority*, or *demanded* applications. It seems that the IoT platform provider like Ericsson, Cisco-Jasper, in addition to the platform itself, also sells "System Integration" services, which perhaps would take care of this custom interface development to make mass-deployment and device registration as easy and smooth as possible, so called "zero touch".

As a result, configuring such a *currently* available platform to support multivendor/multi-type IoT sensors will need significant effort of either the sub-contractor(s), or the Ville de Montreal IoT team. Each of the IoT sensor types will have a different *interface*, different *set* of *data/control/monitoring commands* to be accounted for; a kind of application interface would have to be developed for each sensor type, and API functions from multi-vendors would have to be integrated.

One question from VdM was to investigate use of open or free platforms, an economic solution could be to use vendor-dependent management applications, which are usually free and included with the IoT device hardware, for example, Hikvision camera central operational/firmware upgrade management and video recording control, or Ubiquity AirView operational/firmware upgrade management control. However, in a stand-alone deployment on VdM IoT servers, this might not be a good path to follow, for its poor scalability, inflexibility.

In summary, while we are on the same page and agree that it is better to consider a commercially available platform (rather than developing it by either the sub-contractor, or the Ville de Montreal IoT team), we just highlight some potential concerns as discussed above since the *desired generic* platform is *not yet* available.

Following the comment, we have briefly incorporated the above discussions in the Introduction of Appendix E

Comment 3 (page 15): *This is the most viable approach for collecting sensor data. We must decouple the edge (sensors) from the application layer for robustness, scalability, etc. A database such as MongoDB should be used more for back-end storage and processing*.

Reply: We acknowledge the comment that *this is the most viable approach for collecting sensor data*. At the end of the project, we already implemented a MQTT broker based on Node-Red for real-time data query.

Following the comment, the following text is added into the conclusion of the Appendix:

"In this project, for testing purpose, a MQTT broker based on Node-Red was implemented for real-time data query and the MQTT topics are as the following:"

Appendix F: Monitoring and Control of the IoT Network

Comment (page 15): *I fail to see the relevance and effort of trying to implement an IoT platform layer for control and monitoring, when a simple commercial market survey will yield over 300 providers. Building such a component from scratch would be a total waste of time.*

Reply: It seems that our presentation is not sufficiently clear to you.

In the MSCPS project, our focus is to consider a *generic* framework for a Smart City for a wide range of applications with various sensor/actuator types and devices from *multiple* vendors. For this, *ideally* a *generic* platform (either non-cloud or cloud-based) that can accommodate various sensor/actuator types and devices from *multiple* vendors is *needed*. Furthermore, it is *desired* to select and use such a generic platform *commercially available* rather than to develop it by ourselves.

With the above-mentioned objective in mind, in this work, we intend to find such a *commercially available, generic* platform, and investigate its potentials. We agree with you that there are several industry-based IoT platforms, for example, MS Azure IoT Hub, Cisco-Jasper, Ericsson IoT Accelerator, etc. Within our constrained time and accessibility, we have considered some of them, and found that, unfortunately, those *currently* available platforms are not quite *generic*. They seem to be *application*-specific, *device*-specific, or *technology*-specific, for example, only supporting some hardware models from some specific vendors, or only supporting video, or only supporting communications over cellular network, etc. This could be explained by the fact that the development of a *generic* platform can be complex and time-consuming, and to come out timely in the market, developers may select to focus first more *specific* to certain *high-priority*, or *demanded* applications. It seems that the IoT platform provider like Ericsson, Cisco-Jasper, in addition to the platform itself, also sells “System Integration” services, which perhaps would take care of this custom interface development to make mass-deployment and device registration as easy and smooth as possible, so called “zero touch”.

As a result, configuring such a *currently* available platform to support multivendor/multi-type IoT sensors will need significant effort of either the sub-contractor(s), or the Ville de Montreal IoT team. Each of the IoT sensor types will have a different *interface*, different *set* of *data/control/monitoring commands* to be accounted for; a kind of application interface would have to be developed for each sensor type, and API functions from multi-vendors would have to be integrated.

For example, as shown in Section 2.2 of Appendix F, even the management software that comes from the vendors does not support well their devices and lacks of many important functionalities. Given that many types of devices from many manufacturers coexisting in the same network, full control implementation of these heterogeneous devices could be very complex, even using commercially available “sensor vendor-independent” IoT platforms. For example, as discussed in page 11 of Appendix F, even for the cameras that support ONVIF protocol, their parsers can be drastically different from each other.

In addition, service/device provider “locked in” should be avoided in a Smart City setup, a highly customized platform is desired.

In summary, while we are on the same page and agree that it is better to consider a commercially available platform (rather than developing it by either the sub-contractor, or the Ville de Montreal IoT team), we just highlight some potential concerns as discussed above since the *desired generic* platform is *not yet* available.

Appendix H: Data Analytic Application – Parking place occupancy and vehicle/pedestrian counting

Comments: *"It would be better to have an automated detection mechanism for parking spaces with street markings rather than having to enter the coordinates manually. Very useful if the camera is not fixed."*

"By using street markings to identify the number of places available, one could also consider an algo that detects parked cars (easier than detecting empty spaces) to infer the number of places available."

"More old school technique, i.e., one tries to use a method "one size fits all" rather than auxiliary data to better parameterize the models (or develop several models) for specific times and conditions.

In addition, existing state-of-the-art tools for extracting image / video information such as Yolo or Faster R-CNN could have been considered instead of mathematical morphology tools. contour detection, etc.

These tools might have made it possible to exploit the video aspect of the data instead of the static images."

"Here again, CNN-based softwares such as Yolo could have been tested before doing development based on edge detection approaches."

"Here too we have a "one size fits all" approach rather than using auxiliary information to change the parameters or the treatment in general depending on the time of day or the weather conditions."

"The generation of the background can be complex but there is a lot of time to generate it, the solutions do not need to be applicable at time t = 0."

Reply: We agree with you that there are rooms for improving the performance of the application including applying different types of algorithms. However, the objective of Appendix H is not to compare the performance of different approaches to come up with the best solution but rather to illustrate the *capabilities* of the *deployed devices* in supporting data-analytic applications. For this, we selected *well-established* algorithms primarily to show/investigate the feasibility of such data-analytic applications on the *deployed devices*.

Following the comments, the following text is added to the abstract of the appendix:

"Two programs have been developed based on well-established algorithms using open-source library as a reference to illustrate the feasibility of integrating analytic applications over the deployed cameras: a parking detection program and a traffic count program."

Appendix I: Data Analytic Application – Crowd Counting

Comments: *"These references are far too much for ML (1998-1999). It is better to do a review of more recent literature (post 2010). Because the state-of-the-art in image / video information extraction is ML, especially convolutional neuron networks (CNN). There is a lot of literature on crowd estimation with these techniques."*

" I have doubts about it. Some examples of labeled crowd datasets (dense and non-dense):

- see page 16 of https://arxiv.org/pdf/1502.01812.pdf for a list of video datasets

- UCF CC 50: http://crcv.ucf.edu/data/crowd_counting.php

- Shanghaitech Part A and Part B"

"The choice to combine CNN and SVM here is consistent. But I find it surprising to apply this approach at the head size classification level instead of the crowd density classification. The tagged head dataset contains only 100 examples, while the crowd datasets are larger.

If this approach (classifying the size of the heads) is chosen, the size of the dataset must be increased because it is too small (low precision of the SVM - 45%)."

"In these situations (non-dense crowd), could not one resort to machine learning relying on datasets more easily available. More potential seems to me than to resort to conventional detection (Viola-Jones, 2001!). I bet even an already trained model and public domain would make a better job!"

"I think there is an error, the cited reference does not seem to concern the cascade upper body detection."

"In total, the method was tested on 6 images. It is a set of validation far too small to draw valid conclusions. It would be necessary to calculate the error of the method they propose on the datasets quoted above to have a clear idea of their value (comparison with state-of-the-art errors)."

Reply: We agree with you that there are a lot of rooms for improving the performance of the application including: (i) using different types of algorithms, (ii) investigating more trained models and (iii) doing more extensive testing. However, the objective of Appendix I is not to compare the performance of different approaches to come up with the best solution but rather to illustrate the *capabilities* of the *deployed devices* in supporting data-analytic applications.

Following the comments, the following text is added to the abstract of Appendix I:

"This appendix considers the role of automatic estimation of crowd size in very crowded scenarios. A variation of well-established techniques is proposed, which is able to estimate crowd size in a distorted video where objects close to the camera appear to be larger. The technique is based on a machine learning method which can automatically decide the size of people's heads in different parts of the image."

Main Technical Report: Montreal Smart City Pilot System (MSCPS)

Comment 1 (page 12): *“The Integration of IoT to the Cloud is not required in this POC. We have to determine the standards, the design approaches and the architecture principles of the first two layers: Data Acquisition and Transport/Communication Layer for 3 domains: Intelligent Traffic, Urban Asset Management and Public Security.*
The storage in this POC will be used for the testing purpose of the Transport Layer. The storage service is part of the Platform layer and will be the subject of the next research”

Reply: As the data management platform plays a central role in a Smart City setup, the setup of at least a simplified data management platform is mandatory to test the feasibility of data collection, device capabilities and device control for the pilot project. In this process, the traditional local setup was investigated. However, most of the literatures today are pointing to the direction of cloud setup for the many reasons that we discussed at the beginning of Chapter 4 in the main report. While we fully agree that a full-fledged management platform must be one of the important topics for the next research, the feasibility and constraints of integrating a data management platform, both on premise and cloud-based, should be investigated in this step to have a clear view for the next researches.

Comment 2 (page 13): *“Architectures to solve the issues? What is the objective of the MSCPS?”*

Reply: The purpose of chapter 2 is to serve as a reference/background on Smart City for the whole project. Before diving deep into the deployment, installation and analysis, we need to take a step back to look at what is the current status of Smart Cities around the world, what are the important trends and what the lessons are to learn. Then, a structural architecture of a Smart City has to be built as the umbrella for the project. As explained above, Chapter 2 may not involve any physical installation but it lays an important foundation/reference and is critical to the overall report/project.

Comment 3 (page 13): *“The Security Architecture has to be considered within the Architecture of the Smart City. In the context of Smart cities, the Data may come from a variety of source not only from the IoT infrastructure of the City and undergo several transformation and will be shared with multiple participants. The security must then be based on the notion of trust-based data, the concept of data perception trust and reasoning with trust related policies. The Infrastructure Security will contribute to the determination the trust level for the data. We are not there yet.”*

Reply: We acknowledge the importance of Security in the context of Smart City. As the result, we dedicate the whole Chapter 5 to discuss this issue. As Chapter 2 serves as the foundation for the whole project, diving too deep into security here (Chapter 2) would miss the overall picture and hence is not recommended.

Comment 4 (page 13): *“It's not required in the POC. The architecture has to be determined first before to decide if we can deploy this architecture/infrastructure on the premise, or on the Cloud.”*

Reply: As discussed in the reply to Comment 1 above, while a full-fledged data management platform must be one of the important topics for the next study, a simplified version is critical in exploring the feasibility and constraints of integrating different types of devices to the Smart City infrastructure.

Comment 5 (page 14): *“Smart Object: ordinary object equipped with a sensor/actuator linked to an analytic applications.*

Smart sensor: sensor with a extended processing power allowing the deployment of some security functions."

Reply: We agree that the definition of smart object in the report is somewhat ambiguous.

Following this comment, the following text is added to the main report:

"smart objects – ordinary objects that become "smart" by integrating with advanced technologies to enable identification, communication, awareness and interaction capabilities"

Comment 6 (page 14): "Agreed"

Reply: Thank you.

Comment 7 (page 15): *"Smart City = Unified network + Meaningful Data Sharing"*

Reply: Thanks for the comment, actually, there are many definition of the term "Smart City". This footnote[1] provides an interesting discussion of this term. We guess what is meant by the comment is to have a *common* network that connects everything together to provide data sharing, which is exactly the ultimate objective to the IoT. Due to this reason, in this project, we propose to apply IoT as a technology to resolve the issues in Smart City applications.

Comment 8 (page 17): *"Why ? do we have a ESB like for the Architecture ? Data Brokers?"*

Reply: The service-oriented architecture (SoA) paradigm is a widely adopted approach when constructing an architecture for IoT in general and specifically Smart City[2]. In this part, we adopt this widely accepted model approach to build a system architecture for the Smart City project. The EBS and Data Brokers are detailed components beyond the scope of this project.

Comment 9 (page 17): *"The management Layer and the Security Layer must be transversal to the Data Acquisition , communication, platform, application layer."*

Reply: Thanks for your comment that indicates our presentation was not sufficiently clear to you. While we agree with you that that *system management* and *security* features should be present at *planes, transversal* to the other layers, the "management layer" in *Figure 2.5: Smart City IoT multi-layered system architecture* is for *data* management that deals with transformation, accumulation, and abstraction, (and *not* for *system* management). Since Chapter 2 focuses on the *data handling* aspects, and describes the generic IoT system architecture to support end-to-end data handling, security is not covered in Chapter 2 and not shown in Figure 2.5. Instead, as security aspect is important in a Smart City environment, we dedicate the whole Chapter 5 to discuss this matter. It is noted that even in the latest publications on security aspects of IoT[3], the system architecture is still constructed in a layered manner. Security can be visualized as a *plane* across the layers such as in the Cisco White paper for "The Internet of Things Reference Model", illustrated in Figure 1.

[1] A. Cocchia, "Smart and Digital City: A Systematic Literature Review", *Smart City*, Springer Press, pp. 13-43, 2014

[2] S. Li, L. D. Xu, "The internet of things: a survey", *Springer Information Systems Frontiers*, Vol. 17 (2), pp. 243-259, 2015.

[3] A. M. Nia, N. K. Jha, "A Comprehensive study of security of Internet of Things*", IEEE Transaction on Emerging Topics in Computing*, Vol. PP (99), 2016

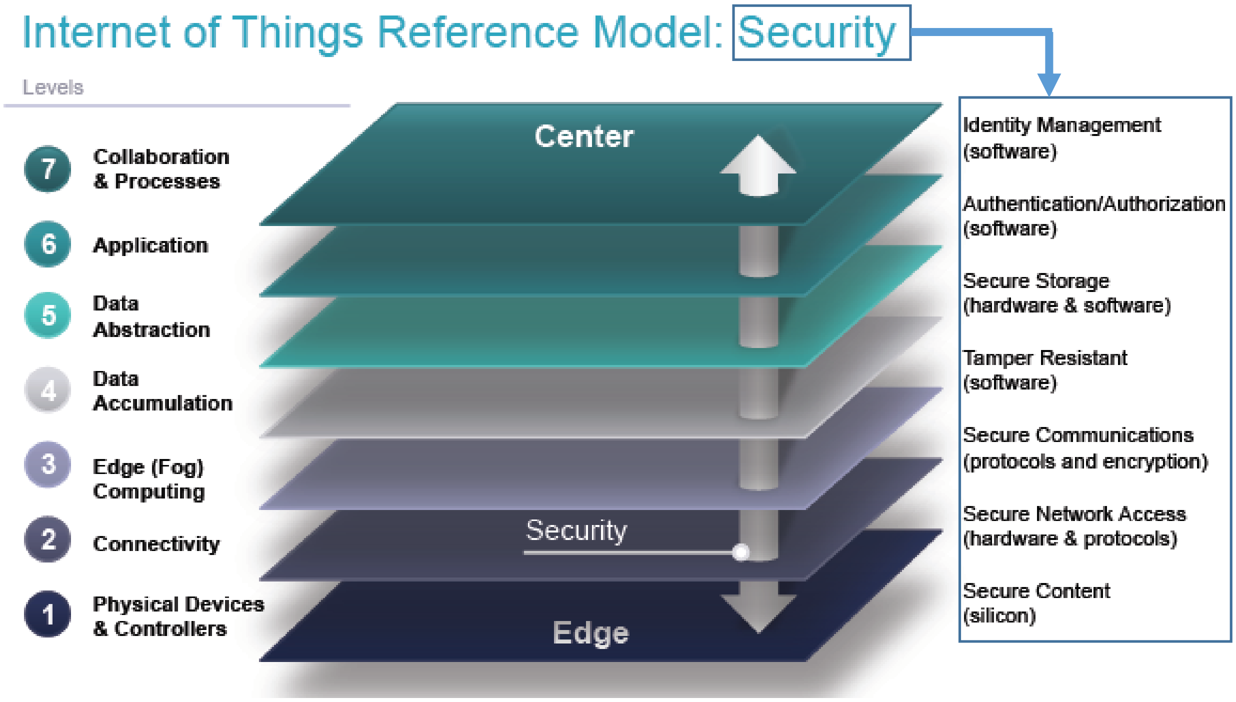

Internet of Things Reference Model: Security
Levels
7 Collaboration & Processes
6 Application
5 Data Abstraction
4 Data Accumulation
3 Edge (Fog) Computing
2 Connectivity
1 Physical Devices & Controllers
Center
Security
Edge
Identity Management (software)
Authentication/Authorization (software)
Secure Storage (hardware & software)
Tamper Resistant (software)
Secure Communications (protocols and encryption)
Secure Network Access (hardware & protocols)
Secure Content (silicon)

Figure 1: Pervasive security throughout the IoT Reference Model (Cisco)

Comment 10 (page 21): *"This reference architecture is not following recent literature. Please see http://iotforum.org/wp-content/uploads/2014/09/D1.5-20130715-VERYFINAL.pdf for IoT-A consortium and Gartner proposed reference architecture."*

Reply: Many thanks for pointing out the interesting reference. We have known this IoT-A among the various proposed IoT architectures in the past several years, e.g., oneM2M (www.onem2m.org), IoTWF (IoT World Forum), Purdue Model, IIoT (by Industrial Internet Consortium), IoT-A, ITU-T IoT reference model. We are not interested in a reference architecture *which tries to break down the functionalities according to OSI or TCP/IP reference model*. Instead, we are interested in presenting the Smart City *system* structure model, i.e., how the Smart City system is realized and its components and how they are all connected together.

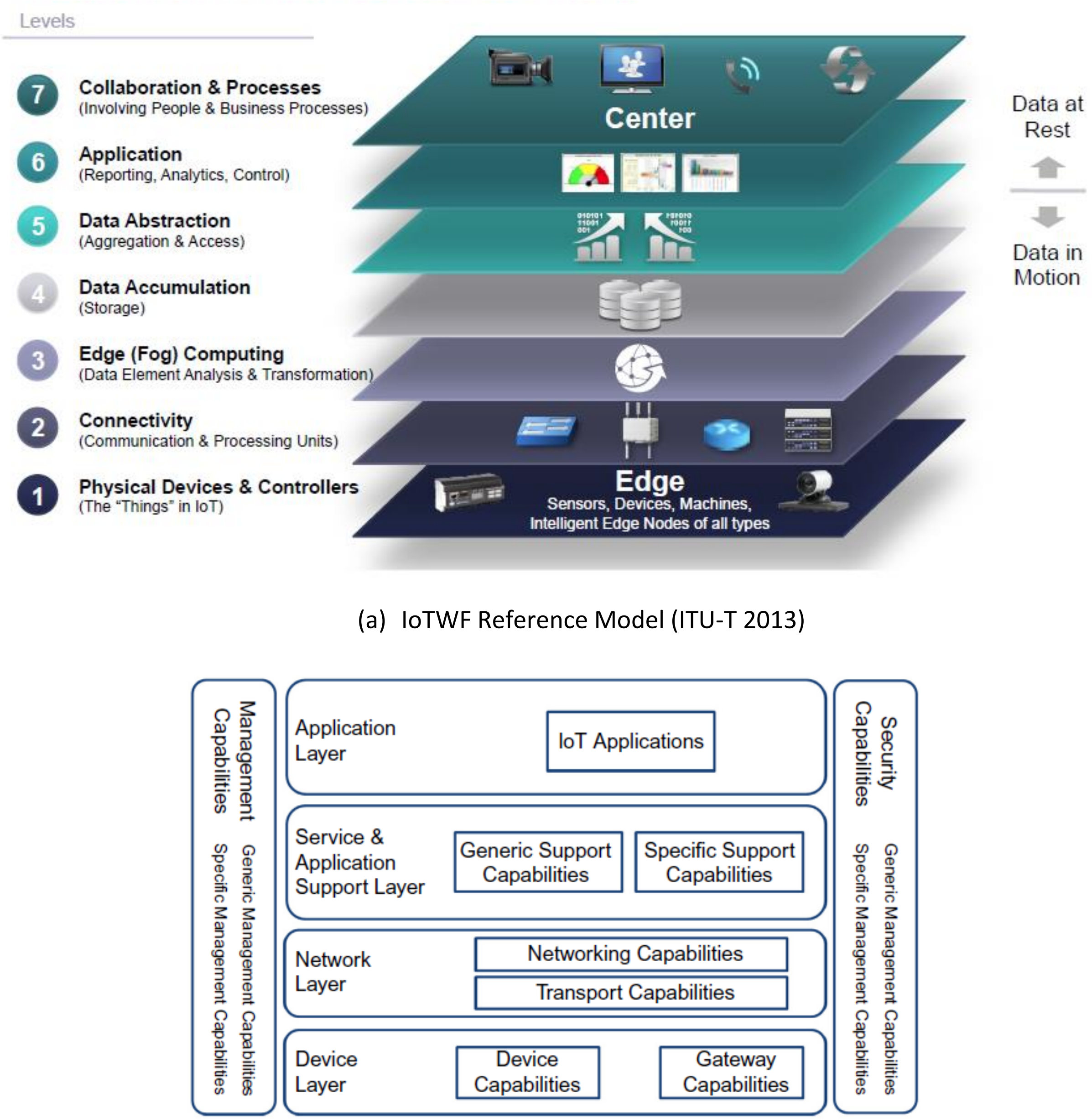
In fact, our proposed Smart City *system* architecture is quite closed to the well-known IoTWF[4] and ITU-T IoT reference models. As illustrated in Figure 2(a), the IoTWF architecture composes of 7 layers. While we share the similar view with this layered structure, we find the 7-layer architecture is unnecessarily complex to understand and may not show well the correlations between the architecture model and the real IoT components. As a result, we proposed the 4-layer architecture, which is closely corresponding to the IoTWF 7-layer architecture. Our *Data Acquisition & Control* and *Communications*[5] layers map directly to the Cisco *Physical Devices & Controllers* and *Connectivity* layers, respectively. The IoTWF next upper 3 layers: Edge Computing, Data Accumulation, and Data Abstraction are simplified into the *Management* [6]

[4] Cisco White Paper - "The Internet of Things Reference Model", Cisco Press, 2014.

[5] We found the term "Communications" less general than "Connectivity" and hence changed it to "Connectivity" in the revised version

[6] We found the term "Management" less specific than "Data Management" and hence changed it to "Data Management" in the revised version

layer in our proposed architecture. The two IoTWF highest layers: *Application* and *Collaboration & Processes* correspond to the *Application* layer in our architecture.


Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge (Fog) Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types
Data at Rest
Data in Motion
Management Capabilities
Generic Management Capabilities
Specific Management Capabilities
Application Layer
IoT Applications
Service & Application Support Layer
Generic Support Capabilities
Specific Support Capabilities
Network Layer
Networking Capabilities
Transport Capabilities
Device Layer
Device Capabilities
Gateway Capabilities
Security Capabilities
Generic Management Capabilities
Specific Management Capabilities

(a) IoTWF Reference Model (ITU-T 2013)

(b) ITU-T IoT Reference Model (ITU-T 2013)

Figure 2: IoTWF and ITU-T IoT multi-layer architectures.

Following this comment, for better/clearer presentation, we changed the sub-title of Fig.2.5 to *Smart City IoT multi-layered system architecture* in the revised Chapter 2.

We have incorporated in brief the above discussions in the introductory paragraph of Section 2.2 of Chapter 2 of the revised report.

Comment 11 (page 23): *"This should ideally be renamed the platform layer. See Gartner IoT Ref model https://www.gartner.com/binaries//content/assets/events/keywords/catalyst/catus8/2017_planning_guide_for_the__iot.pdf"*

Reply: We acknowledge the comment and think that this is an interesting point of view. However, in our opinion, the word "*platform*" is general and ambiguous, for example, one could write "an embedded platform", "a development platform". In addition, the word "platform" could be misunderstood as the Smart City system as a whole. As a result, we suggest to keep the word "Data Management Layer" as it is less ambiguous.

Comment 12 (page 23): *"We don't have the description of the Security Layer..."*

Reply: As already mentioned in the reply for Comment 9, we think that security is not a layer but is instead an important feature that must be considered. Reckoning the importance of security, we devote an entire chapter 5 for Security discussions.

Comment 13 (page 25): *"This is not a issues..."; "This is a deployment model issue. This issue has been addressed by the industry with a micro-service based design paradigm.", "This is a deployment model issue. This issue has been addressed by the industry with a micro-service based design paradigm."*

Reply: Many thanks for your interesting perspective. In our opinion, virtualization is an important issue that should be addressed and the existing solutions are not yet there. We acknowledge that there are several solutions for virtualization at the software level such as the virtual machines and the Software Defined Network but when it comes to the hardware level, the current technology is not there yet. For instance, how can different users can control the same camera at the same time? How to change the traffic lights from several applications? In other words, how can devices in a Smart City be utilized in the most efficient way when there is the involvement of several users, parties, applications at the same time.

Following the comment, the following texts are added to the main report.

"As such, virtualization becomes an important issue in the context of a Smart City, for example, how can different users/applications control the same device at the same time?"

Comment 14 (page 25): *"Very complex topics. Has to be elaborated..Specific risks of the IoT and Smart City infrastructure?"*

Reply: We acknowledge that Security is an important issue in Smart Cities and security implementations have to be considered at all layers in the architecture. However, extensive discussion about Security in this part is not appropriate as Chapter 2 aims at providing the overall picture of Smart City structure. A more extensive discussion on Security is provided in Chapter 5.

Following the comment, the following texts are added to the main report.

"A more extensive discussion of Security will be provided in Chapter 5."

Comment 15 (page 26): *"Missing Objective pour each deployment. What we try to accomplish ?"*

Reply: Many thanks for the comments.

Following the comment, the following texts are added to the main report:

“Following Montreal’s Strategic Plan for the Smart and Digital City, in this pilot project, various types of sensors and commercial or free softwares are tested to determine the best standards to follow, to determine the best integration architecture and sensor management in terms of transport and data processing, and to validate the business gains of the smart transportation concept.”

Comment 16 (page 30): *“How this network structure are mapped to the architecture proposed (4 layers) . This diagram is more physical than logical presentation of the architecture”*

Reply: Many thanks for the comment. To avoid the confusion, the title of the sub-section is changed to “Network connectivity diagram”. Also, the texts related to this figure are changed to “network connectivity diagram”.

Following the comment, the following texts are added to the main report:

“The network diagram in Figure 3.1 follows closely the architecture in Chapter 2 with the different kinds of sensors and WiFi connection at the Data Acquisition & Control Layer, the fiber, VPN and LTE acts as the Connectivity Layer, the upper two layers are realized in software in servers so they are not physically separated.”

Comment 17 (page 30): *“Why we have so many communication protocol ? justification of the use for each protocol ? Standards , principals ?”*

Reply: Many thanks for the comment. Following the comment, the following text is added to the main report:

“Due to the fixed locations of the fiber drops, several wireless communication technologies were used depending on the use cases. WiFi was used to extend the network coverage and connect to high volume traffic such as cameras. For those devices which does not have IP connection (radars, RFID), adapters are used to bridge the communication mediums such as RS232 to Ethernet bridges, and Zigbee adapters, then to the WiFi network. In addition, data from sensors which are attached to mobile vehicles are collected in real-time via LTE networks (if data volume is low) or stored locally in an onboard storage (if data volume is high)”

Comment 18 (page 31): *“To much details. What the architecture principals of this approach ? How theses principals could be applied to the blue print of the Smart city architecture ? What we try to prove ? User cases ?”*

Reply: In this section, a step-by-step description to the whole system is presented. Due to the many types of devices, a certain level of details is necessary to provide the overall picture. However, we will try to give a more abstract view of the entire system.

Following the comment, the following text is added to the main report:

“To enable data collection and device control to the IoT network, a NAT gateway is used. The public IP representation of the whole IoT network is 132.206.68.25. A management server is in charge of this task, translating the destination addresses of incoming messages to the appropriate device’s address and forward the packets to the node. This server is also the source of NPT time synchronization across all of the devices.”

Comment 19 (page 33): *"Define Good View .. (for what analytic application), what the ratio between the high of the camera position and the area cover by the camera ? What the minimum quality of the images in order hey can be used by a different analytic applications (people counting, security applications..)"*

Reply: The good view will depend on the applications to be presented in Chapter 6. Following the comment, the following text is added:

"The position of camera installation must provide a good view of the target area, prevent vandalism, and reduce obstructions to the wireless bridge connection. The camera view will depend on the application and will be discussed in Chapter 6."

Comment 20 (page 34): *"Again User cases? Justification of the use of two types of WiFi .. why not one ? our objectif is to determine the rational approach for the massive deployment of sensors.."*

Reply: In the pilot deployment, two types of WiFi radios were used to determine the best solution for connectivity in terms of performance and cost.

Following the comment, the following text is added to the main report:

"Within the deployment project, two types of WiFi radios were used to determine the best solution for connectivity in terms of performance and cost: IEEE 802.11ac and IEEE 802.11n."

Comment 21 (Page 35): *"we don't need the explanation of NAT. It's not relevant for this POC..."*

Reply: Sorry for the misunderstanding, the purpose of this part is rather to describe the NAT configuration that was used and not for giving any theoretical NAT definition.

Following the comment, the sub-section title is changed into "Network Address Translation Configuration" to avoid the misunderstanding.

Comment 22 (Page 38): *"A Good justification of the approach. And the conclusion?"*

Reply: Many thanks for the comment. Following the comment, the following text is added to the main report:

"For ease of integration, the cameras should support ONVIF standards. However, from the experiments in this project, we have noticed that the claim of ONVIF-compliance may not warrant a complete interoperability; for example, some features of ONVIF-compliant camera may not be recognized by the ONVIF-compliant VMS software: more specifically, we experienced that the PTZ feature of the ONVIF-compliant Panasonic camera cannot be recognized, when using an ONVIF driver instead of its Panasonic specific driver. We suggest that for a larger scale installation, sample test must be done to verify the full compatibility between the different cameras and the VMS software functions before a mass purchase/deployment. Customer support and supporting management tools may vary from one vendor to another vendor, and this may contribute in making a huge difference in prices between brands as summarized in Section 10 of Appendix D. For example, in our experience, Panasonic support was not as good as the other two brands; Hikvision central management tool lacks a unified firmware upgrade feature; with the same feature set and quality of the video, the only reason for Axis high price could be good application supports, including central management tools with easy central mass firmware update feature."

Comment 23 (Page 44): *“Very good, we have a principal architecture here”*

Reply: Many thanks for sharing the same view.

Comment 24 (page 45): *“the lack of IPv4 is not identified in the chapter 2 as issues. IPV6 is not tested.”*

Reply: The issues presented in Chapter 2 aims at providing a foundation to the system and more details specific will be presented along way with the text. Regarding the IPv6 testing, automatic local-link addressing, same subnet network connection between PC and some camera and Wi-Fi radio bridge devices over IPv6, were successfully tested.[7]. It is noted that most of the devices in the project can support both IPv4 and IPv6 running in parallel.

Following the comment, the following text is added to the main report:

“Regarding the IPv6 testing, partial connection (of same subnet) between a PC and SmartCity devices (cameras, Wi-Fi radios) over IPv6 were successfully tested, using device automatically generated unique local-link addresses. However, a full-scale testing of the deployed devices and conversion to IPv6 have not been done yet due to the time limitation (beyond the scope of this project). It is noted that most of the devices in the project can support both IPv4 and IPv6 running in parallel. In the next steps, we suggest Stateless Auto-Configuration (AKA "Router Advertisement" IPv6 devices configuration) to be set up and tested for all Smart-City deployed devices. Stateless Auto-Configuration could be the easiest way to configure an IP address on all interfaces, allowing full automatic configuration. This configuration mode (in addition to manual or DHCPv6 mode) was created to allow all devices on the same data link to automatically configure themselves, reducing administrative overhead for the network administrators. In order for this mode to work, routers on the network will need to be manually configured with IPv6, this will need more investigation and proper access rights on the network routers.”

Comment 25 (page 47): *“Good”*

Reply: Many thanks.

Comment 26 (page 57): *“architecture principals and design approaches? What the link between the high level architecture proposed and the POC, what do we accomplish? the network infrastructure outlined in this POC don't give a unified or a rational approach for the design and the deployment of Smart city infratructure. The throughput test is excellent but we cannot apply this approach for the whole city.”*

Reply: Many thanks for the comment. For the full-scale deployment, the whole city should be divided into a number of hierarchical network sectors based on the connectivity availability and maximum bandwidth support. The data from the IoT network will be then routed to datacenters for storage and processing. The architecture proposed in this pilot project follows this approach and can be generalized to a bigger network. However, the hierarchical planning of network sectors is not addressed in this project as in depth data regarding fiber drop availability and application provisioning should be provided. This is an interesting and important subject for further investigations in the next steps. In Chapter 3, we provide simulation results for bandwidth requirement, access point and camera density in two scenarios (low density and high density) based on the actual map of Montreal.

[7] A full-scale testing and conversion to IPv6 is beyond the scope of this project due to time limitation.

Following the comment, the following text is added to the main report:

"For the full-scale deployment, the whole city should be divided into a number of hierarchical network sectors based on the connectivity availability and maximum bandwidth support. The data from the IoT network will be then routed to datacenters for storage and processing. The network architecture proposed in this pilot project follows this approach, match closely to the architecture in Chapter 2 and can be generalized to a larger network. However, the hierarchical planning of network sectors is not addressed in this project as in depth data regarding fiber drop availability and application provisioning should be provided. This is an interesting and important subject for further investigations in the next steps."

Comment 27 (page 57): *"This statement is unclear ? Which limitations ?"*

Reply: Many thanks for the comment, following the comment, the following text is added to the main report:

"Within the project, devices with state-of-the-art, commercially available technologies are purchased and deployed whenever the budget allows to help the determination of functionality, capability limitations in realizing a Smart City."

Comment 28 (page 58): *"Out of scope, but the control structure is pertinent"*

Reply: After the deployment of physical devices, data management platform arises as an important issue to be addressed before any further data-analysis, functionalities and developments can be added. This is essentially the glue that hold the whole system together and has to be seriously designed. Investigating this issue allows us to have a more in-depth understanding about the data and traffic characteristics from the deployed devices which lays a foundation for any expansion of the system in the future.

Following the comment, the following text is added to the main report:

"In a Smart City, data and device management is a key factor for the development of the whole system. It holds everything in the Smart City together as an integrated system, allowing data collection, device monitoring and control."

Comment 28 (page 90): *"Again, the same general comment applies here for this chapter. A solid commercial market survey of available device connection platforms (DCP) and Iot Platforms would be required here. There are over 300 Iot platform providers on the market. No need to customize this layer and its capabilities."*

Reply: We agree with the comment that there are several available IoT platforms. As previously mentioned in Sections 4.2 and 4.3, there can be many types of sensors from many manufacturers coexist in the same network. Even data formatting from different types of sensors of the same manufacturer could be drastically different or the software that comes from the vendors does not support well their devices and lacks of many important functionalities. Moreover, as service/device provider "locked in" is one of the factor that should be avoided, a highly customized and flexible platform must be selected and configured accordingly for the IoT sensor devices to be developed.

Following the comment, the following text is added into the introduction of chapter 4 in the main report:

"*Although many IoT platforms were already commercially developed, careful selection of the flexible and customizable multi-sensor-type and multi-data-communication-type IoT platform must be performed, and* *it should be noted that configuration of the already commercially available IoT platform for multi-type sensors will not be trivial, a system integration service may need to be sub-contracted besides the IoT platform purchase. As service/device provider "locked in" is one of the factor that should be avoided, a flexible, adaptable and customizable centralized data management structure is one of the most important components in a Smart City setup."*

Comment 29 (page 106): *"1. This algorithm would be more efficient if vehicle parking place markers were leveraged, instead of having to incur a laborious cost of apriori labelling or identifying parking space coordinates manually. Subsequently, counting occupied parking places would be much easier to manage (than trying to identify vacant parking spots).*

2. We do not agree with this general approach of using contour detection for object and motion detection. The state of the art of object recognition is now efficiently leveraging Convoluted Neural Network (CNN) techniques instead. A case in point example is the YOLO application and its ability to perform real-time object detection based on CNN. PLEASE REVIEW EXISTING RECENT SCIENTIFIC LITERATURE IN THIS DOMAIN.

3. The model could also be made more robust, by leveraging background information at different periods of the day or season (ex: morning, winter, spring, etc.).

4. Using a Faster or R-CNN approach would also allow a more efficient handling of the data since it can work stream-based, instead of frame-by-frame.

5. Bluntly put, contour detection algorithms are old-school."

" Same comment applies here that a more modern approach using R-CNN algorithms, instead of a contour-based approach would be more efficient here."

"1. The scientific literature references here are quite dated (Viola-Jones, 2001) ??? Again, here we would recommend more a modern approach using Convolutional Neural Networks (CNN)

2. We would not recommend trying to classify the size of heads, but rather trying classify entire crowd densities. Many labelled open data sets already exist. PROPER LITERATURE REVIEW HERE WOULD BE REQUIRED. See

https://arxiv.org/pdf/1502.01812.pdf pour une liste de dataset vidéo

- UCF CC 50: http://crcv.ucf.edu/data/crowd_counting.php

- Shanghaitech Part A and Part B

3. Again, we noticed that scientific references are outdated here (1998-1999)

4. We have provided some interesting recent articles in Appendix I (as a comment). For example: https://arxiv.org/pdf/1502.01812.pdf"

Reply: We acknowledge and thank you for your valuable comments. We agree with you that there are a lot of rooms for improving the performance of the application including using different types of algorithms, more extensive testing and customization.

However, the aim of this chapter is to illustrate the *capabilities* of the *deployed devices* in supporting analytic applications. The data-analytic functions including intensive performance evaluation/comparison of different approaches in order to come with the best solution are important and large subjects to be addressed in the next steps.

Given the scope and time limitation of the project and the wide range of available researches and algorithms, an extensive survey/research in this area is far beyond the scope of this current project. Instead, in Appendix I, data-analytic applications based on *well-established* algorithms were developed primarily to show the feasibility of such data-analytic applications on existing deployed devices.

Following the comments, the following text is added to the introduction of the chapter:

"Data analytics by itself is a large field and solutions in this area are normally either condition-, context-, or application-specific to achieve an acceptable performance. A generic "one solution fit all" is not yet possible. The aim of this chapter is not to explore the whole area with extensive testing for specific performance evaluation/comparison but rather to present some promising potentials of data analytics based on well-established algorithms and the possibility of provide some data analytic applications on top of the deployed hardware."