San Diego, March 10th 2017

<u>Author</u>: Albert Vazquez- California Smart City Institute

<u>Contributors:</u> Ignacio Yanez, Dr. Oscar Montero

To: National Telecommunications and Information Administration, U.S. Department of Commerce
Email iotrfc2017@ntia.doc.gov
[Docket No. 170105023–7023–01]
RIN 0660–XC033

<u>Topic:</u> Comments regarding IoT categorization about January 7th 2017 paper on "Fostering the Advancement of the Internet of Things"

The Department of Commerce paper rightly points the requirements to develop applications based in "security-by-design" and "privacy-by-design" principles (page 27 of the January 7th 2017 paper). However, we believe "power-efficiency-by-design" is key in the design process, especially in IoT application. We believe that should be highlighted in your paper.

Though there are several parameters that affect the energy-efficiency of connected devices (topology of the network, noise…) signal processing is the most relevant one. Signal processing relates to the frequency to which the components of the application, such as sensors and communication devices, need to operate. Some applications require being active constantly for real time monitoring. Others require the device to be active intermittently, either through an internal schedule or an external trigger. That frequency drives the energy consumption, which is critical when those sensors are battery operated. That is relevant because despite each device may have a low power level consumption (in the mA level), the impact of the aggregated number of billions of devices projected will not become negligible at some stage in the future. An analogy can be drawn from internet users randomly connecting and disconnecting to and from websites which in some cases may lead to overloads. An additional consideration relates to efficiency and frequency is whether the devices are connected to the AC grid or powered by batteries. In the latter case, additional costs associated to servicing the device may limit the attractiveness of IoT.

We believe categorizing applications based in privacy and safety is a good approach; however, we do not recommend that applications should be segmented by industry (that's what we understood on page 7)

We consider segmenting by industry creates the following difficulties

a) The industry classification is constantly evolving and segmentation by industry would require a constant review process. The practical consequence would be of having IoT standards that are not responding to the speed in which each Industry advances while leaving new emerging industries out of scope.
b) As expressed on page 46 of your paper, the need of adopting these new standards at International level is of great importance. Given every industry currently has its own regional or national standards a classification by industry may contribute to widen the existing gap in international standardization

We think that what ultimately makes every application different in terms of needs for IoT standards is not the industry it sits within but some specific characteristics related to IoT. We think the key ones of are the nature and volume of the data (safety and privacy) and the energy efficiency demands. The standard requirements per these variables may well be similar for industries of very different nature.

Therefore, the model we propose for categorizing applications is based on two criteria:

- Signal processing requirements (which is the main driver for the energy efficiency of the sensor)
- Security and Safety requirements

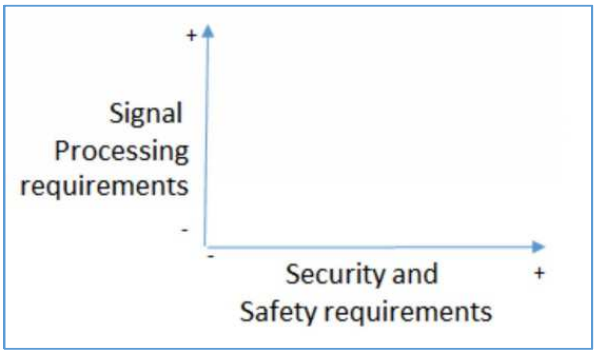

Figure 1

Signal Processing requirements would be differentiated between application that operate on real time versus the ones that are triggered, either by an internal schedule or an external input.

Security and Safety requirements are based in criticality assessment:

- Mission Critical
- Vital (synonym of essential, necessary)
- Desirable

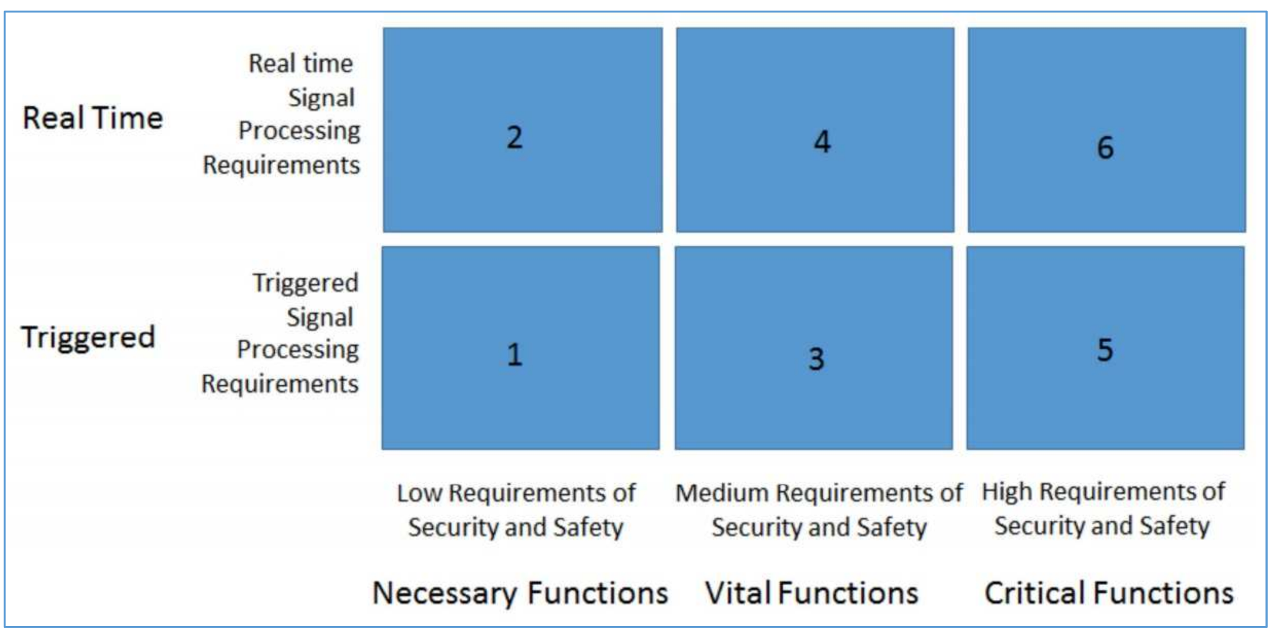

Figure 2

That model can help us identify six categories for IoT systems

Level 1: Real Time Critical systems.

Level 2: Triggered Time Vital Functions.

Level 3: Real Time Vital Functions.

Level 4: Triggered Vital Functions.

Level 5: Real Time Desirable Functions.

Level 6: Triggered Desirable Functions.

This classification would be applied at IoT component level. At IoT system level the rating would be the one for the component within the system with the lower level. To illustrate with an example: in a given IoT system with components rated at level 6, 5 and 1. The system categorization would be at 1 despite one of the components is 6. That model is inspired in safety standards, such as UL 508 standard for Industrial Control Equipment, where the "weakest" link is the one that categorizes the overall system.

It is our opinion that the six categories for every IoT device should be certified by an independent body. The designer or manufacturer would apply for one of the levels described before and a third party would certificate of compliance to those.

One could apply a similar approach to the one by OSHA (Occupational Safety and Health Administration) that approves a selected list of testing laboratories (Nationally Recognized Testing Laboratories - NRTL https://www.osha.gov/dts/otpca/nrtl/nrtllist.html). Those laboratories have the necessary qualifications to perform safety testing and certification of products in accordance with US consensus-based product safety test standards developed or issued by US standards organizations. NRTLs may not have yet the most advanced cyber-security skills to evaluate the security axis, but they already have the electrical and electronic skills to evaluate the energy efficiency aspects of the classification. If the market recognizes them as stakeholders in cyber-security certification, we suspect they would hire the specialists to match market expectations.

Another example of the same approach is to be found in the Implementation of Software Integrity Levels (SIL) in the Avionics Industry. These levels are defined by the standard DO-178B that is created by the RTCA (Radio Technical Commission for Aeronautics) which is a Federal Advisory Committee to the FAA. FAA then defines and qualifies the agents and procedures to approve any avionics software according to the SIL level declared by the manufacturer (DERs, Designated Engineer Representatives that proceed according to 8110.3form)

Conclusions

Considerations to include power-efficiency-by design as one of the drivers during the early stages of development of IoT applications were discussed. Signal processing stands out as one of the main factors contributing to power consumption.

With a classification based on two variables (signal processing requirements and security requirements), but independent of each industry, it is possible to define 6 levels of differentiation in terms of

Standardization needs. That makes the categorization at component level a much easier task and widens its scope with a relatively simple rule.

Applying different standards for each of the 6 levels would then make every application much easier to control in terms of IoT Standard requirements just by classifying the application per these defined levels.

This model also eliminates the complication of keeping new specific standards for every industry up to date and bridges the gap of international standardization as it is not constrained a priori by any specific industry standard. **We suggest the NTIA and the Department of commerce to follow this two-variable approach for all industries and abandon any attempts to regulate by industry approach (ie medical, automotive…)**

We suggest the following next step: To identify the relevant US organization that would require manufacturers of IoT equipment to certify their design per one of the 6 levels in the described matrix (figure 2). That would be in our opinion the role of a US Standards organizations. We believe an organization like ANSI (the American National Standards Institute), a private non-profit organization, should have such role and arrive at by consensus among representatives of other international standards organizations, government agencies, consumer groups, companies and others.

-----------------------0---------------------

About California Smart City Institute – www.california-smart.city – info@california-smart.city

California Smart City Institute, based in San Diego, is a think-tank dedicated to the studies of smart city initiatives within the state of California. Its main goal is to contribute to communities in reducing the gap between technology available for smarter city applications and the real adoption by the citizenship.

About Albert Vazquez

Mr Vazquez is Chair of the California Smart City Institute. He is an executive with +15 years' international experience in the fields of sensors, controls and actuators. His experience goes from component level to systems level in diverse industries. That allows him to see the big picture of opportunities and difficulties for IoT, specially applied to Smart City applications. He is an active actor in the entrepreneurship ecosystem of Southern California.

About Ignacio Yanez

Mr. Yanez is co-Chair of the California Smart City Institute. He is currently a senior advisor and mentor at a start-ups incubator in San Diego and has a wide international experience of 15 years+ in electronic components and electromechanical devices. His background and exposure to the innovative efforts in IoT allows him to connect the entrepreneurship community with the requirements of the Smart Cities.

About Oscar Montero

Dr. Montero is a technical leader with +10 years leading multidisciplinary teams generating high-tech, yet cost effective, solutions for components and systems in power conversion. Currently, engaged in design of medium voltage motors and drives for the oil & gas industry.