IoT 7 Critical Musts

Abstract

Making an IoT device or platform decision involves many issues to consider. This paper discusses the seven (7) critical musts that need to be considered when deciding on your IoT solution or service offering.

Clint Smith, P.E.
csmith@nextgconnect.com

The internet of things (IoT) whether it is for industrial, military, commercial, enterprise or consumer devices is anything but a simple topic. The vastness of the types of IoT devices, their operating system, capabilities, method of communication, as well as initial and recurring cost makes selecting the proper device for the job at hand, the use case, challenging.

The IoT decision process involves many steps or decisions however the first thing that you need to do is determine your objective. This is more of a business decision than a technical one because the business decision should be driving the technical decision. Specifically defining what your use case or cases are that you need to address critical in the IoT selection process.

Selecting an IoT device or devices that meet your particular use case has numerous attributes that need to be addressed. In addition to defining the attributes needed for an IoT device there are likely to be some tradeoffs that will take place in the process. As with any decision the devil is always in the details and it is important to know how to cull the potential candidate list in order to arrive at the best decision possible given what is known at the time.

For IoT decision process you can either rely on a vendor or your consultant to provide recommendations or solutions. Keep in mind that there are numerous IoT devices and protocols which have not been commercially successful, however many of them have seen limited roll outs resulting in stranded devices from a product enhancement. However, I have found that it is always best to understand some of the options so the best decision can be made to meet your needs.

Therefore, what follows are the seven critical requirements you need to consider when pursing an IoT solution. The seven critical musts should be part of the IoT decision whether for a greenfield deployment, retrofit or enhancement. The 7 critical must list is generic and vendor neutral on purpose. The list is also not all inclusive however it is always easier to criticize/edit than it is to create.

IoT Decision 7 Critical Musts:

1. Objective/Purpose
2. Security (cyber/physical)
3. Data Acquisition/Functions
4. Standards and Compliance Regulations
5. Business (CapEx/OpEx/Revenue)
6. Interface /User Experience
7. Technology

Each item of the 7 Critical Musts can easily be expanded. The order is not as important as making sure they are all addressed. However, I would keep the objective/purpose as the first step since everything else is determined from that point onward.

1. Objective/Purpose.

Think of this as a high-level design/decision where you need to answer some questions pertaining to what problem you are solving.

a) What is the problem you are solving and how is it being addressed now.
b) Are you offering the IoT device as a paid service or for internal consumption.
c) What do you want to control or monitor.

d) How do you want to convert the physical signal into some digital form.
e) What do you want to do with the data, monitor/report/act.
f) Will this involve edge computing and or artificial intelligence.
g) What is the plan for the data collected from all the IoT devices.
h) Is there a need for a Northbound interface to communicate with 3rd party systems (local or cloud).
i) When do you need the device installed, ready.
j) Are there legacy systems, requirements, that you need to include.

Once you know what you want one of the follow-up decisions is do you want to design and build your own platform, write code, be a system integrator or just be a reseller.

2. Security (cyber/physical)

Security means many things to different people even within the same organization. However, including Security by Design (SbD) from the inception is more important than ever as the amount of IoT devices continue to grow increasing the security threat landscape and vectors.

a) Will the IoT device be placed in a trusted or non-trusted environment.
b) Does the device need to be physically protected.
c) Does the data being sent need to be encrypted.
d) How is the data collected stored and protected.
e) How is the device authorized/authenticated.
f) Will remote access to the device be required and if so how.
g) Will IoT device use an agent or agent-less security process.
h) Will the IoT device operate in a zero-trust environment.
i) How are software patches, configuration changes and updates be performed.
j) Will the IoT device utilize open source code.
k) Compliance and regulation requirements.
l) What is the resiliency/disaster recovery program/process you will use.
m) How do you verify that the IoT device is not a counterfeit.
n) How do you verify that the IoT device is in security compliance.
o) How are you ensuring that IoT devices are not compromised for MitM attacks.
p) Does the security governance program/process need to be modified due to the IoT device.

3. Data acquisition/storage and functions

Data acquisition (DAQ) is the process of measuring real-world conditions and then converting those measurements into a digital format at some fixed time interval. The data storage is referring to where the data provided by the IoT device as well as any post processing reside. The functions define what the IoT device, middleware or system is going to do with the data.

a) Will the IoT device perform any Edge Process.
b) Will data be passed upstream.
c) Who will be able to access and use the data.
d) Do you need to share or make available to data to legacy or 3rd party platforms.
e) Where will the analytics take place, cloud, local, hybrid.
f) How long do you need the data to be available, data life expectancy.
g) Are there any data storage/archive requirements and if so what.
h) What analytics will be performed on the data collected.

i) Life- how long do you need the platform function.

4. Standards and Compliance Regulations

Within your industry are there specific compliance regulations you need to adhere related to IoT devices. Also do you need to utilize a specific IoT device protocol or system protocol based on your business model, use case, or regulatory reason.

a) Are there regulatory requirements for data storage.
b) Are you required to utilize only open source code.
c) Are you required to utilize only COTS devices.
d) Can you utilize proprietary/closed systems.
e) What industry standards do you need or want to follow.

5. Business (CapEx/OpEx/Revenue)

For the business what are your Capital expense (CapEx) that you need to adhere to on a per device or system level. Are there Operating expenses (OpEx) issues you need to factor into the decision like subscription services per device. Regarding revenue this depends on your business model and whether you are deploying the IoT platform for internal uses or as a service. If the IoT platform is being sold as a service, then it needs to operate at a profit and not as a loss leader since losing money in volume is never fun.

a) Will this be a hosted system?
b) Will the IoT device be purchased from an OEM/Vendor or be custom built.
c) What is the desired CapEx cost per device, wholesale and retail.
d) How do you plan on upselling services and capabilities to existing customers?
e) What is the data mining, analysis plan.
f) What is the OEM/Vendor – size, longevity, prior relationship.
g) What support is available for IoT device from the OEM/Vendor or is it just github and blogs.
h) Operating cost- what are the recurring costs for the IoT device.
i) Device ecosystem – what other vendors use or provide services/support for this.
j) IoT device/platform- is it possible to switch vendors without losing functionality.
k) What is the installation cost associated with each IoT device.
l) What is the truck roll cost and how is this minimized.
m) What features/functions are potentially needed in 1,2 & 5yrs.

6. Interface /User Experience

This area addresses how you and or the customer interact with the device and or data.

a) What is the device management plan to ensure that the IoT device is functioning properly.
b) How do you interact with the IoT device for maintenance/inventory/status/upgrades. (graphic or CLI).
c) What is your dashboard to determine the status of the IoT device's operational condition.
d) What visualization tools will be used to help with the management of the IoT devices.
e) Do you have any pre-defined reports that can be used.
f) How will additional rules/policies be implemented.

7. Technology

The technology portion is usually where the discussion of IoT devices and platforms begins. However, it is just one of the items that needs to be considered. The technology decision used for the IoT device and or platform should be determined by the other IoT critical musts.

a) What physical and logical interfaces are needed.
b) Are sensors integrated into the IoT device or are they connected via wire or wireless.
c) Is the IoT device a sensor or a SOC.
d) What is the operating system (OS) for the IoT device and whether it is open or closed (proprietary).
e) What is the operating environment the IoT device will be placed within.
f) What network topology will be used, local only, LAN, PAN, WAN.
g) Will the IoT device need to perform edge computing and will it need to extend to a fog or mist topology?
h) Wireless Topology used – star, mesh, ad-hoc, hybrid.
i) What is the source of the power for the IoT device, AC, DC, POE, battery, solar, energy harvesting.
j) How will power management be handled.
k) How often does the IoT device send data.
l) What is the bandwidth (bps) required for the IoT device.
m) Is the data sent real time, low latency, or can be it sent non-real time.
n) Will the IoT device support single or multiple application support.
o) Is modularity required of the IoT device for later enhancements, i.e. mezzanine board.
p) Scalable – how does this device scale, plan for success (100 to 100k endpoints).
q) How will software updates take place, over the air (OTA), physical, IP.
r) What data will be stored on the IoT device.
s) IoT device communication protocol type (open or closed- proprietary).

I trust that you found this article useful.

Clint Smith, P.E.
Next G Connect
CTO
csmith@nextgconnect.com

Who we are:

NGC is a consulting team of highly skilled and experienced professionals. Our background is in wireless communications for both the commercial and public safety sectors. The team has led deployment and operations spanning decades in the wireless technology. We have designed software and hardware for both network infrastructure and edge devices from concept to POC/FOA. Our current areas of focus include 4G/5G, IoT and security.

The team has collectively been granted over 160 patents in the wireless communication space during their careers. We have also written multiple books used extensively in the industry on wireless technology and published by McGraw-Hill.

Feel free to utilize this information in any presentation or article with the simple request you reference its origin.

If you see something that should be added, changed or simply want to talk about your potential needs please contact us at info@nextgconnect.com or call us at 1.845.987.1787.