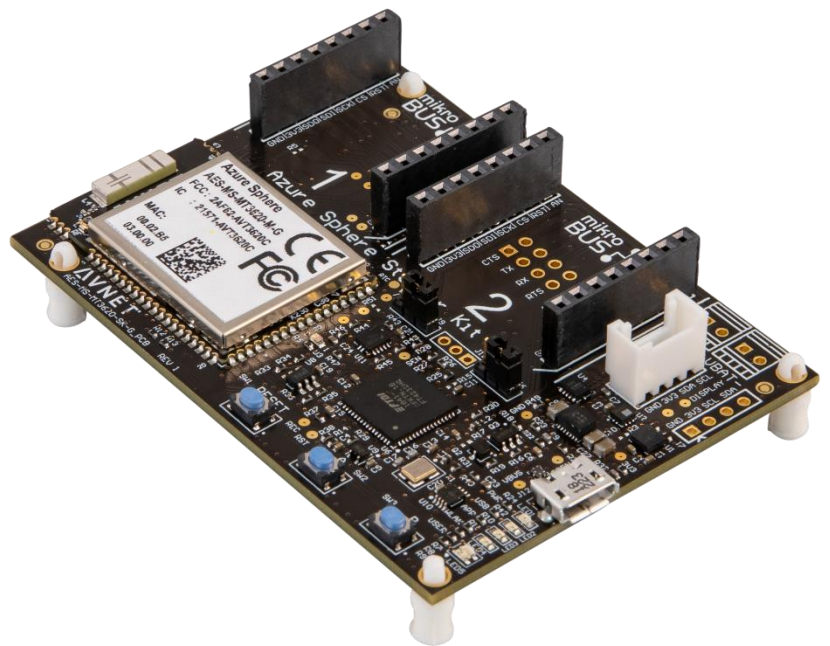


Avnet Technical Training Course

Azure Sphere: Digging Deeper Into Application Code Lab 3



Azure Sphere SDK:	19.05
Training Version:	v1
Date:	1 July 2019

© 2019 Avnet. All rights reserved. All trademarks and registered trademarks are the property of their respective owners. All specifications are subject to change without notice.

NOTICE OF DISCLAIMER: Avnet is providing this design, code, or information "as is." By providing the design, code, or information as one possible implementation of this feature, application, or standard, Avnet makes no representation that this implementation is free from any claims of infringement. You are responsible for obtaining any rights you may require for your implementation. Avnet expressly disclaims any warranty whatsoever with respect to the adequacy of the implementation, including but not limited to any warranties or representations that this implementation is free from claims of infringement and any implied warranties of merchantability or fitness for a particular purpose.

Introduction

This Lab will document the pieces of code that implements a few basic IoT concepts. We'll review how to read a GPIO pin, how to send IoT telemetry to Azure, and how to manage device twin messages. There are many different ways to code these concepts, this lab will document how the example project implements the features. After reviewing the source code, there is a section on the application manifest file that's required for every Azure Sphere project.

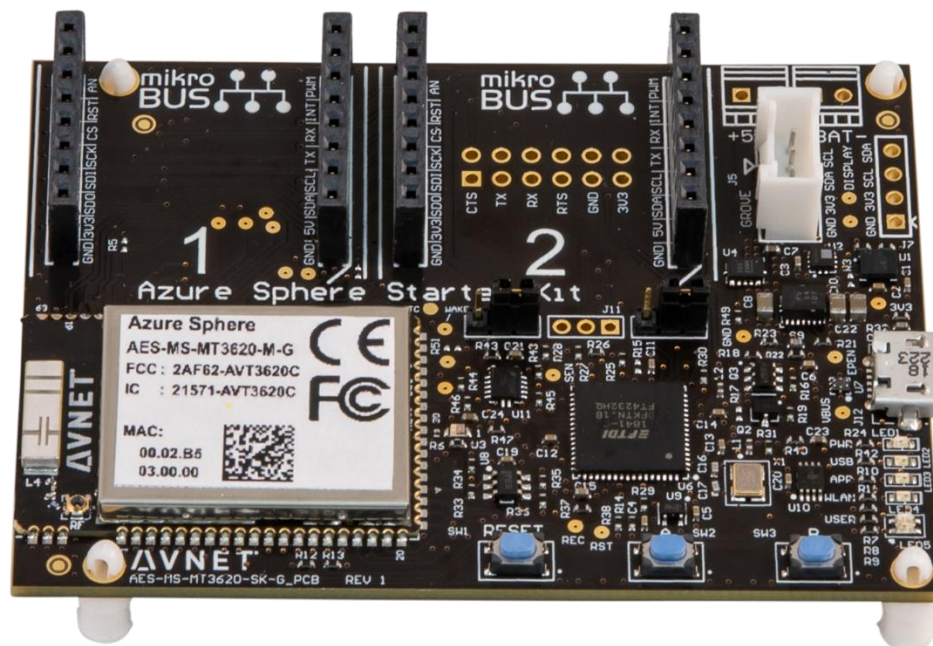
The telemetry and device twin code is currently not enabled by Lab-2 (the non-connected build configuration), but Lab-4 and Lab-5 will use these implementations and I'll assign a couple of code assignments related to the concepts described in this lab.

Avnet Azure Sphere Starter Kit Overview

The Avnet Azure Sphere Starter Kit from Avnet Electronics Marketing provides engineers with a complete system for prototyping and evaluating systems based on the MT3620 Azure Sphere device.

The Avnet Azure Sphere MT3620 Starter Kit supports rapid prototyping of highly secure, end-to-end IoT implementations using Microsoft's Azure Sphere. The small form-factor carrier board includes a production-ready MT3620 Sphere module with Wi-Fi connectivity, along with multiple expansion interfaces for easy integration of off-the-shelf sensors, displays, motors, relays, and more.

The Starter Kit includes Avnet's MT3620 Module. Having the module on the Starter Kit means that you can do all your development work for your IoT project on the Starter Kit and then easily migrate your Azure Sphere Application to your custom hardware design using Avnet's MT3620 Module.



Avnet Azure Sphere Starter Kit

Lab 3: Objectives

The objectives of Lab-3 are to dig into the sample project source code and understand how some basic IoT features are implemented. At the end of the lab we'll discuss the app_manifest.json file and its contents.

- Understand how to configure and read a button press using a GPIO hardware signal
- Understand how to send IoT telemetry to Azure
- Understand how to process device twin messages from Azure
- Learn about the app_manifest.json file that's included in every Azure Sphere project

Lab-3 must be started after Lab-0 and Lab-1 have been completed.

Requirements

Hardware

- A PC running Windows 10 Anniversary Update or later (Version 1607 or greater)
- An unused USB port on the PC
- An Avnet Azure Sphere Starter Kit
- A micro USB cable to connect the Starter Kit to your PC

Software

- Visual Studio 2019 Enterprise, Professional, or Community version 16.04 or later; or Visual Studio 2017 version 15.9 or later **installed**
- Azure Sphere SDK 19.05 or the current SDK release **installed**

GPIO

Working with hardware interfaces is common with IoT projects. Whether it's driving an LED, or reading an I2C sensor the Azure Sphere OS and OS services have the APIs to help you work with your hardware devices. In this section we'll identify the code required to read the General Purpose I/O (GPIO) signal in our Azure Sphere project that's connected to User Button A. Working with GPIO interfaces is pretty simple, we need to do 5 things . . .

1. Add the GPIO reference to the app_manifest.json file
2. Declare a file descriptor that we'll associate to our GPIO signal
3. Open the GPIO as an input and assign a file descriptor to work with the hardware
4. Read the GPIO level using the file descriptor as a reference to the hardware
5. Close the file descriptor

Let's identify the source code for each of these items . . .

Add the GPIO reference to the app_manifest.json file

We need to explicitly grant the application permission to use the GPIO signal #12. We add the number 12 to the app_manifest.json file in the Capabilities → Gpio section. If we were to omit this step then the OS would not allow the application to open the GPIO when we attempt to open it as an input.

The app_manifest.json file is described on page 11 in this document. The Microsoft documentation on the app_manifest.json file can be reviewed [here](#).



```
1  {
2      "SchemaVersion": 1,
3      "Name": "AvnetStarterKit-Hackster.io-V1.0",
4      "ComponentId": "685f13af-25a5-40b2-8dd8-8cbc253ecbd8",
5      "EntryPoint": "/bin/app",
6      "CmdArgs": [ ],
7      "Capabilities": {
8          "AllowedConnections": [ ],
9          "AllowedTcpServerPorts": [ ],
10         "AllowedUdpServerPorts": [ ],
11         "Gpio": [ 0, 4, 5, 8, 9, 10, 12, 13, 34 ],
12         "Uart": [ ],
13         "I2cMaster": [ "ISU2" ],
14         "SpiMaster": [ ],
15         "WifiConfig": true,
16         "NetworkConfig": false,
17         "SystemTime": false,
18         "DeviceAuthentication": "00000000-0000-0000-0000-000000000000"
19     }
20 }
```

Declare a file descriptor

The system uses file descriptors to operate on hardware interfaces. We declare a file descriptor `buttonAGpioFd` to allow the code to operate on the GPIO interface. You'll notice that all calls to initialize and read the GPIO pin use the file descriptor.

```
main.c  [X]
AvnetStarterKitReferenceDesign

74
75 // File descriptors - initialized to invalid value
76 int epollFd = -1;
77 static int buttonPollTimerFd = -1;
78 static int buttonAGpioFd = -1;
79 static int buttonBGpioFd = -1;
80
```

Open the GPIO as an input

This line of code opens GPIO 12 (MT3620_RDB_BUTTON_A) as an input. That will allow us to read the GPIO level.

```
main.c  [X]
AvnetStarterKitReferenceDesign (Global Scope)

250 Log_Debug("Opening Starter Kit Button A as input.\n");
251 buttonAGpioFd = GPIO_OpenAsInput(MT3620_RDB_BUTTON_A);
252 if (buttonAGpioFd < 0) {
253     Log_Debug("ERROR: Could not open button A GPIO: %s (%d).\n", strerror(errno), errno);
254     return -1;
255 }
```

Read the GPIO level

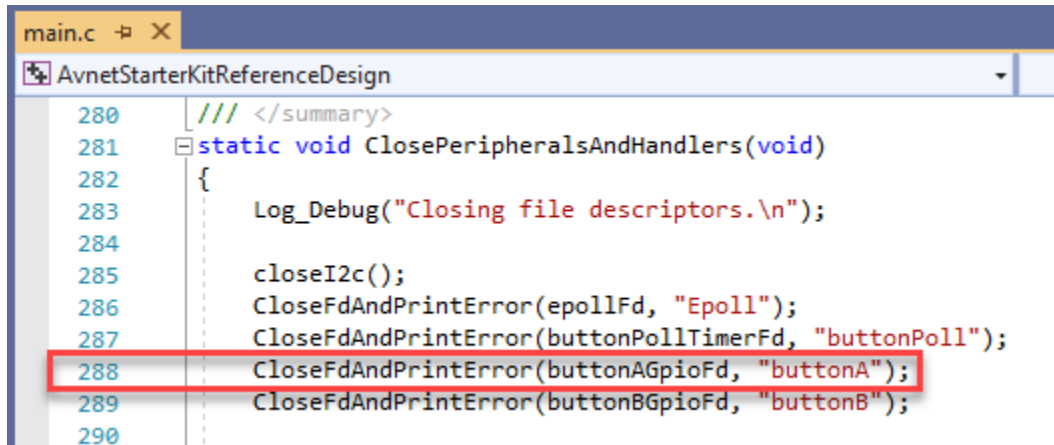
This is the code that actually reads the GPIO level.

```
main.c  [X]
AvnetStarterKitReferenceDesign (Global Scope)

131 // Check for button A press
132 GPIO_Value_Type newButtonAState;
133 int result = GPIO_GetValue(buttonAGpioFd, &newButtonAState);
134 if (result != 0) {
135     Log_Debug("ERROR: Could not read button GPIO: %s (%d).\n", strerror(errno), errno);
136     terminationRequired = true;
137     return;
138 }
139
```

Close the file descriptor

When the application exits, it calls the routine to clean up. We call the routine that will close the file descriptor.



```
main.c  X
AvnetStarterKitReferenceDesign
280  ///
```

That's all there is to reading a GPIO signal. I welcome you to review the source code to see the logic when the GPIO (newButtonAState) is read.

The easiest way I've found to look at an existing Azure Sphere project to understand how a hardware interface is implemented is to look at the file descriptor. If you can find all the code that uses some piece of hardware's file descriptor, you'll see all the necessary code for that interface.

Assignment: In Visual Studio trace the following file descriptors to see how each is used

- i2cFd
- epollFd;

Send IoT Telemetry to Azure

Sending telemetry is a basic function for any IoT project. Typically, IoT devices collect data, they may or may not pre-process the data, and then they send data in the form of telemetry to the cloud. Our project reads the on-board I2C sensors and sends that data to Azure. Sending telemetry data to Azure is pretty easy. There are 3 things that need to happen . . .

1. Establish and maintain a secure connection to an Azure IoT Hub or IoT Central application
2. Construct a JSON object that contains one or more {"key": value} pairs
3. Call the routine to send the data to our IoT Hub or IoT Central application

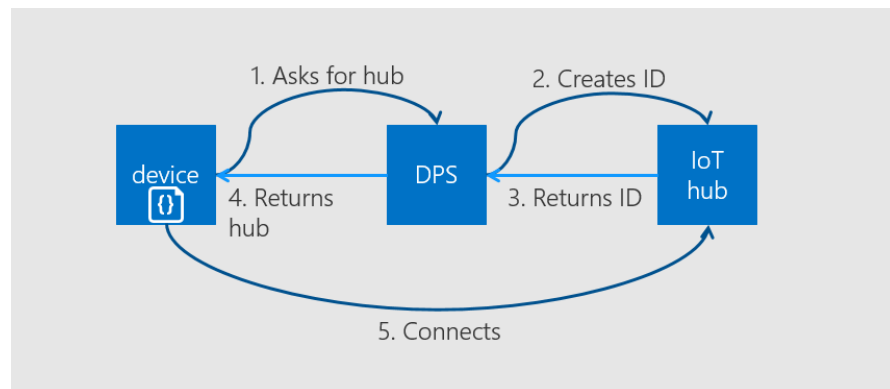
Establish a connection to Azure

I'm not really going to dive into this step as it could consume an entire course all by itself. I'll provide a brief description instead, here's the 50,000' overview.

The process to connect to an Azure IoT Hub or an IoT Central application is pretty much the same.

1. Provision the device

- a. The recommended method to provision IoT devices in Azure is to use an Azure service called a Device Provisioning Service (DPS). You can read all about DPS [here](#). Using DPS you can deploy a single software application build onto millions of devices. The first time each device connects to the internet, and then the global DPS server, they will all automatically be provisioned to one or more IoT Hubs and then connect to the IoT Hub that each device was provisioned to. This is a powerful IoT concept and is required to deploy IoT devices at scale. The diagram below shows the process.



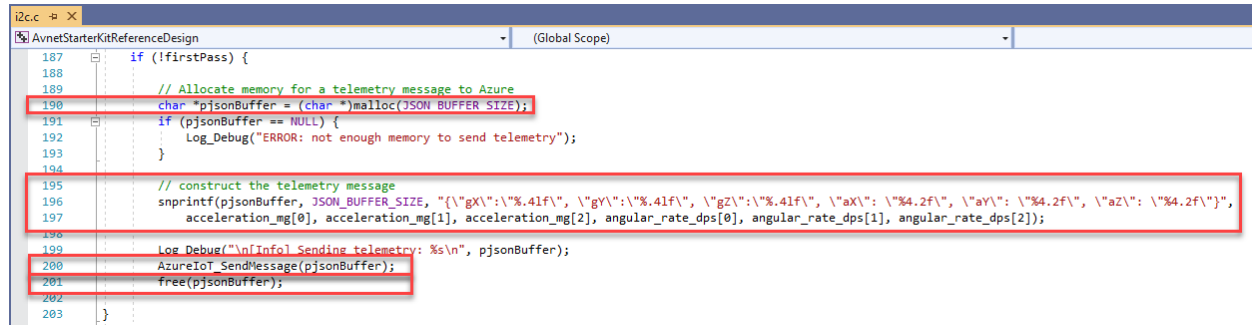
2. Establish and Maintain a secure connection

- a. There are Sphere OS services that establish and maintain a secure (TLS) connection to Azure. If you're really interested in the details search the example project for `iothubClientHandle`.

Construct a JSON object, and send the telemetry

Below you'll see the code to create the JSON telemetry message. There are basically four things to do . . .

1. Allocate a buffer in memory to store the JSON object (see line 190)
2. Construct the JSON object in the new memory buffer (see line 196-197)
3. Send the JSON object to Azure (see line 200)
4. Free the memory (see line 201)

A screenshot of a C code editor window titled 'i2c.c'. The code is part of a function 'if (!firstPass) {'. Lines 187-194 show an initial check for 'pjsonBuffer'. Line 190 allocates memory for 'pjsonBuffer' using 'malloc(JSON_BUFFER_SIZE)'. Lines 196-197 use 'snprintf' to construct a JSON string in 'pjsonBuffer' with sensor data. Line 199 logs the message. Line 200 sends the message to Azure IoT using 'AzureIoT_SendMessage(pjsonBuffer)'. Line 201 frees the memory with 'free(pjsonBuffer)'. Lines 202-203 close the function. Red boxes highlight the allocation, construction, sending, and freeing steps.

```
187 if (!firstPass) {
188
189     // Allocate memory for a telemetry message to Azure
190     char *pjsonBuffer = (char *)malloc(JSON_BUFFER_SIZE);
191     if (pjsonBuffer == NULL) {
192         Log_Debug("ERROR: not enough memory to send telemetry");
193     }
194
195     // construct the telemetry message
196     snprintf(pjsonBuffer, JSON_BUFFER_SIZE, "{\"gX\": \"%4.1f\", \"gY\": \"%4.1f\", \"gZ\": \"%4.1f\", \"aX\": \"%4.2f\", \"aY\": \"%4.2f\", \"aZ\": \"%4.2f\"}\",
197            acceleration_mg[0], acceleration_mg[1], acceleration_mg[2], angular_rate_dps[0], angular_rate_dps[1], angular_rate_dps[2]);
198
199     Log_Debug("\n\nInfo! Sending telemetry: %s\n", pjsonBuffer);
200     AzureIoT_SendMessage(pjsonBuffer);
201     free(pjsonBuffer);
202 }
203 }
```

One thing that I think is really cool about telemetry is that you can send any {"key": value} pair, or any valid JSON object, you want to Azure. You don't have to tell Azure anything about your data. As long as the data is valid JSON the IoT Hub will accept the data and store it for you to use. Of course if you want to access that data, some other Azure thing will need to know about your data so it can ingest it and do something meaningful with it, but the IoT Hub does not care as long as it's valid JSON.

Process Device Twin Messages from Azure

Device twins are another powerful IoT concept. You can read the Azure documentation on device twins [here](#).

"*Device twins* are JSON documents that store device state information including metadata, configurations, and conditions. Azure IoT Hub maintains a device twin for each device that you connect to IoT Hub."

Using device twins you can make changes in the cloud to a device twin's desired property and the IoT device will receive a message containing the new desired property. Your application then uses the information in the desired property to do something in your application. For example, toggle a GPIO signal to control an LED, change a property that defines how your application behaves, or anything that your creative mind can think up.

The Lab-3 lecture walks the student through the Device Twin Implementation in our example code. For the Lab, I'll show a different Device Twin implementation that is more straightforward than the table driven example project's implementation. The code below was taken from the Microsoft Azure Sphere GitHub Sample called AzureIoT. You can find the project [here](#).

To work with Device Twins we need four different things . . .

1. Define the JSON {"key": value} pair that we want to implement for our solution
2. Setup a callback routine that will be instantiated when the Azure IoT Hub sends a Device Twin update

3. Implement the callback routine, then add code to look for and do something with our specific {"key": value} pair data
4. Send a Device Twin reported properties message back to Azure with the new reported value of our property.

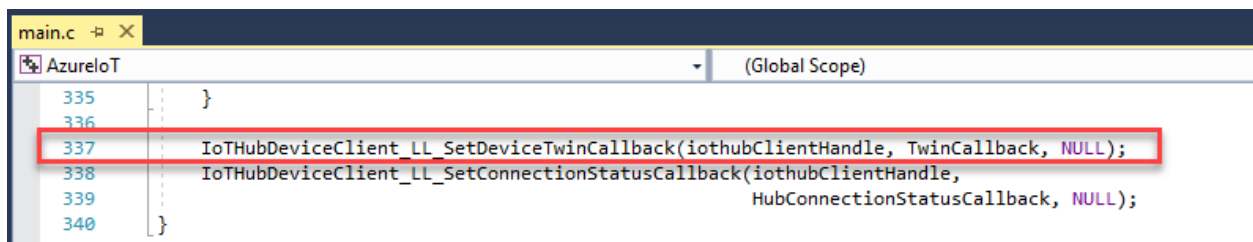
Define the JSON {"key": value}

The first thing we need to do is define our {"key": value} pair. For the AzureIoT example they implement a Device Twin called `statusLED`, the JSON is shown below, it's a Boolean entry.

```
{"statusLED": (true | false)}
```

Setup a Device Twin callback routine

Before we can receive a Device Twin update, we need to tell the Azure OS services how to inform the application when a new Device Twin message is received. In `main.c` on line #337 the application informs the OS services that the routine `TwinCallback`, will be used to process incoming Device Twin messages.



```
main.c -P X
AzureIoT (Global Scope)
335 }
336
337 IoTHubDeviceClient_LL_SetDeviceTwinCallback(iothubClientHandle, TwinCallback, NULL);
338 IoTHubDeviceClient_LL_SetConnectionStatusCallback(iothubClientHandle,
339 HubConnectionStatusCallback, NULL);
340 }
```

Implement the callback routine

The callback implementation is shown below. There are basically four sections identified in the graphic.

(1) Allocate memory to construct a null terminated desired properties JSON object

This section of code (lines 351 – 356) simply allocates memory that will be used to store the desired properties JSON object.

(2) Pull the desired properties out of the incoming payload

The code (lines 358 – 374) builds out a null terminated desired properties JSON object in the allocated buffer and then sets up a pointer to the `desiredProperties` JSON object.

(3) Process the `statusLED` device twin

Lines 376 – 383 handle the device twin property. Coming into this code we have a null terminated JSON object called `desiredProperties`.

- Line 377 we pull out the `statusLED` object, if it exists.
- Line 378 we check to see we found the `statusLED` object
- Line 379 pulls the value piece of our {"key": value} pair and stores it into our variable `statusLedOn`
- Line 380 – 381, changes the GPIO signal for the LED based on the new value
- Line 382 calls the routine to report our reported property to Azure

(4) Cleanup

The last section of code lines 386 – 388, cleans up the `rootProperties` pointer and frees the buffer created at the top of the routine.

```
main.c  X
AzureIoT  (Global Scope)

347  ///
```

1

2

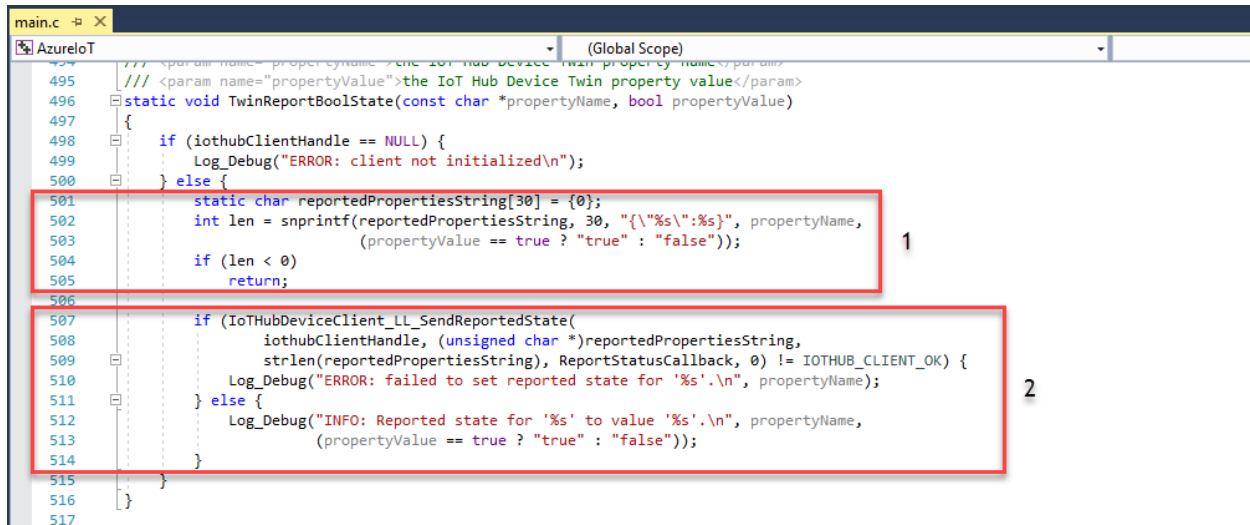
3

4

Send a Device Twin reported properties message back to Azure

The last thing we need to do is to send Azure a message with our new `{"key": value}` reported property. This implementation created a routine called `TwinReportBoolState()` that does this work for any boolean key: value pair.

- Lines 501 – 505 create the JSON `{"key": value}` pair string and use the passed in `propertyName` (key) and the bool `propertyValue` (value). The code uses the `snprintf()` routine to construct the object.
- Lines 507 – 514 send the object to Azure and checks to make sure the message was accepted by the `IoHubDeviceClient_LL_SendReportedState()` routine.



```
main.c - X
AzureIoT
(Global Scope)
495  /// <param name="propertyName">the IoT Hub Device Twin property name</param>
496  /// <param name="propertyValue">the IoT Hub Device Twin property value</param>
497  static void TwinReportBoolState(const char *propertyName, bool propertyValue)
498  {
499      if (iothubClientHandle == NULL) {
500          Log_Debug("ERROR: client not initialized\n");
501      } else {
502          static char reportedPropertiesString[30] = {0};
503          int len = snprintf(reportedPropertiesString, 30, "{\"%s\":%s}", propertyName,
504                          (propertyValue == true ? "true" : "false"));
505          if (len < 0)
506              return;
507          if (IoHubDeviceClient_LL_SendReportedState(
508              iothubClientHandle, (unsigned char *)reportedPropertiesString,
509              strlen(reportedPropertiesString), ReportStatusCallback, 0) != IOTHUB_CLIENT_OK) {
510              Log_Debug("ERROR: failed to set reported state for '%s'.\n", propertyName);
511          } else {
512              Log_Debug("INFO: Reported state for '%s' to value '%s'.\n", propertyName,
513                      (propertyValue == true ? "true" : "false"));
514          }
515      }
516  }
517
```

This section reviewed the device twin implementation from the AzureIoT example project on Microsoft's GitHub Azure Sphere project. This implementation is different from the example application we've been working with. I wanted to share both methods for variety.

app_manifest.json

The Microsoft documentation on this Azure Sphere feature is very well written, and I don't think I can add anything to this very important discussion. The documentation is [here](#), it's a short document that should be reviewed by every Azure Sphere developer. **The text below is taken from the Microsoft documentation.**

"Every Azure Sphere application must have an `app_manifest.json` file. The application manifest describes the resources, also called application capabilities, which an application requires when it executes.

Applications must opt-in to use capabilities by listing each required resource in the Capabilities section of the application manifest; no capabilities are enabled by default. If an application requests a capability that is not listed, the request fails. If the application manifest file contains errors, sideloading the application fails.

Each application's manifest must be stored as `app_manifest.json` in the root directory of the application folder on your PC. The Azure Sphere templates automatically create a default application manifest when you create an application based on a template. You must edit the default manifest to list the capabilities that your application requires. When the application is sideloaded or deployed to the device, the Azure Sphere runtime reads the application manifest to ascertain which capabilities the application is allowed to use. Attempts to access resources that are not listed in the manifest will result in API errors such as `EPERM` (permission denied)."

Wrap Up

In this Lab we learned a little more about the code in the example project

- How to configure and read a button press using a GPIO signal
- How to send IoT telemetry to Azure
- How to process device twin messages from Azure
- Learned about the `app_manifest.json` file

Revision History

Date	Version	Revision
1 July 19	01	Preliminary release
9 July 19	02	Minor updates based on document reviews