



Inovonics Wander Management Development Guide

Preface

- Trademarks and Copyrights

< to be completed >

- Contact info

< to be completed >

- Document conventions

< to be completed >

- Revision History

B. Oshinski	1/1/20	V0.1	Initial Pass
B. Oshinski	4/3/20	V0.2	Added content and updated terminology
B. Oshinski	4/30/20	V0.3	Minor verbiage updates
B. Oshinski	8/18/20	V0.4	Added WireShark filter and ip_address

Purpose

This document is intended to provide high level guidance for the integration to the Inovonics Wander Management system.

References

- Inovonics Wander Management – Installation including Fire system integration, Supervision, Maglock (i.e., relay), Door sensor.
- WM8311 MQTT Reference (AsyncAPI 2.0.0)
- WM8311 REST Reference (OpenAPI 3.0.0)

Introduction

The Inovonics Wander Management system is designed for assisted living facilities with the objective being to reduce the risk of resident elopement. When a monitored resident is in proximity to a managed door, the door will lock for a prescribed period of time, and an event message will be sent to the Host E-Call System to alert the appropriate staff.

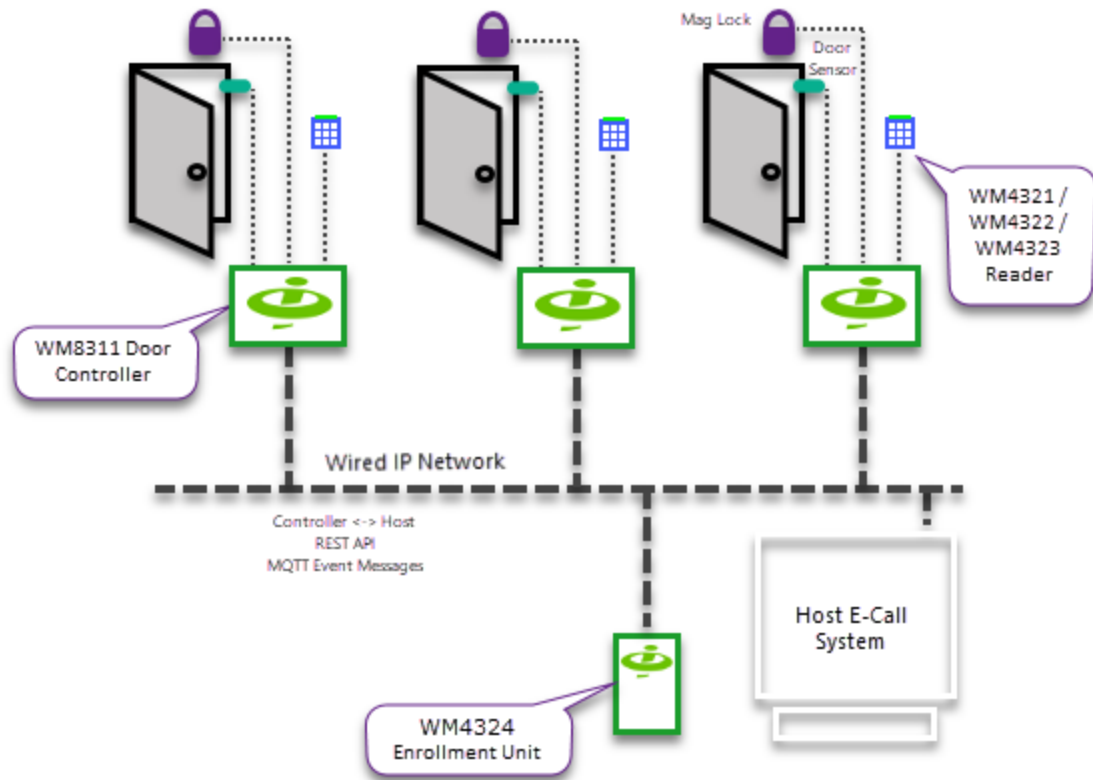


Figure 1 - High Level View of System Elements

Each door that is to be managed will require an Inovonics WM8311 Door Controller and associated RFID/Bluetooth reader (WM4321, WM4322, or WM4323). Monitored residents will wear a WM1320 Wander Tag on their wrist that will be detected by the reader. Staff can escort residents through managed doors by using their staff access card, if available or by using a PIN. A magnetic door lock (aka maglock) and door sensor, sourced independent of Inovonics, will also be necessary to momentarily lock the door and detect the state of the door. All the WM8311 door controllers are connected to a Host E-Call System via Ethernet / IP network.

E-Call system integrators are responsible for modifying the Host E-Call System to accept input from the Inovonics Wander Management solution and create the appropriate registration, event capture, reporting and notification mechanisms. The Host E-Call System will need to send commands to each WM8311 using the REST-based Inovonics Wander API. The Host E-Call System will also need to monitor events that occur at the door, by subscribing to MQTT-based messages.

Hardware Components

The WM8311 contains a Yocto-based Linux microcontroller. It performs the logical operations based on the state of the door, input from the reader and component

configuration. The WM8311 uses an inertial-based tamper to detect any unexpected movement. Five general-purpose LEDs, on the front of the WM8311, provide troubleshooting for power, Ethernet, tamper, etc.

- Power requirements
 - The WM8311 is powered from Power over Ethernet (PoE) and/or a 10VDC – 15 VDC DC Power. For UL, a UL294 approved Power Supply with Class 2 limited output is necessary.
- Inputs and Outputs
 - DSM - Door Sensor is a supervised input to determine if the door is open or closed.
 - AUX – Auxiliary supervised input (not currently used).
 - REX – Request to Exit supervised input (not currently used).
 - Form-C Relay is used for maglock control.
 - Reader uses RS485 +/-, GND and 12V Power Out.
- Permanent storage
 - The WM8311 maintains a local database for residents, staff and other information relative to the management of the door.

< WM8311 pictures to be added >

The reader attaches to the WM8311 via a serial bus that uses the OSDP protocol. It will come in three different styles: WM4321 Keypad, WM4322 single-gang and WM4323 mullion. The WM4321 Keypad version will be necessary for those installations that will have staff use a PIN to bypass the wander door control. All three styles will detect commonly used 125 kHz RFID access cards (if used by staff) and the WM1320 tags used by residents. Communication is performed using a negotiated key to encrypt communications between the reader and the WM8311. The reader uses an inertial-based tamper to detect any unexpected movement.

< 3 reader pictures to be added >

Each reader has an LED and sounder that provide local audio/visual feedback at the door and will reflect the state of the door and WM8311. After handling each event, the WM8311 will set the reader audio/visual feedback based on the state of the door. See Appendix A for more detail. Each AV feedback state has default settings for the LED and sounder, but the Host E-Call System can change those settings, as necessary.

The WM1320 is worn by a resident using a tamper-resistant band and is IP54 water-resistant. Initial development by Inovonics will provide a BLE-only device. Battery level will be reported with every detection notification. < more battery info TBD > The detection distance will be configurable for each monitored door to better handle different door proximity requirements. The WM1320 will not have an integrated help button.

< picture of tag to be added >

An Inovonics WM4324 enrollment unit can be used to register new WM1320 Wander Tags and staff access card into the system.

< picture of enrollment unit to be added >

Data Components

Each resident that is to be monitored as a wander risk, will wear a unique WM1320 with a tamper-resistant band. This is a Bluetooth Low Energy (BLE) tag that advertises multiple times a second and will be detected by the reader when its signal strength reaches an adjustable threshold. Once detected by the reader, an event message will be sent to alert the Host E-Call System of the wander risk and the maglock will be activated for a set duration. If the resident remains near the door, a loiter event message will be sent. This will give the Host E-Call System the chance to alert staff at the assisted-living facility, to redirect the resident away from the door area. If the WM1320 signal strength goes below an adjustable threshold or is not heard from for a prescribed period, the resident is considered to have left the door area and an exit event message is sent.

Staff can escort monitored residents through a managed door by using their credentials that securely authenticates the staff. This is known as bypass mode. Credentials can be entered as a PIN, when a WM4321 keypad reader is in use at the door or by use of a pre-registered staff access card held in front of the reader. Once the credentials are authenticated, the door will unlock, and the WM8311 will send an event message to the Host E-Call System of the bypass event. The staff member must open the door before the bypass duration has expired. Once the door closes the bypass mode is canceled and an event message is sent indicating that the bypass event has concluded.

Wander management of residents, staff bypass and door control can be scheduled. This will allow residents that might only have a tendency to wander during certain times of day, to affect managed door locks. Also, staff might only be allowed to escort a resident (bypass the door locks) on certain days or specific times of the day. Doors can be scheduled to be managed when necessary. For example, the front door may only be managed when staff is reduced during night hours. Schedules will need to be established before they can be assigned to residents, staff, and doors. Two schedules are built into the system: ID 1 for always active and ID 0 for never active.

When referencing non-singleton resources, you will need to associate an ID to the resource. So, for example, for each resident and staff resource to be established in the WM8311, you will need to associate an integer identifier that you can correlate to the Host E-Call System resource.

Communication

- REST concepts followed
 - HTTP verbs are used to perform the associated commands. So, to add a resident, the Host E-Call System would send an HTTP POST request to the WM8311. To remove the resident, the Host E-Call System would send HTTP DELETE request. To change something about a resident, the Host E-Call System would send an HTTP PUT request and to get information, the Host E-Call System would send an HTTP GET request. PUT and POST request bodies are in the JSON format and therefore should include the HTTP header Content-Type: application/json. Response bodies are also in the JSON format.
 - In general, the responses will follow the standard HTTP protocol. For example, if a resource doesn't exist, a 404 NOT FOUND response will be returned. For a GET request where that resident doesn't exist, a 404 response will be returned. If a PUT or POST is made and the request body

contains invalid content, a 400 BAD REQUEST response will be returned. If trying to create a resource that already exists, 409 CONFLICT will be the expected response (there are exceptions though). If everything is correct a response of 200, 201 or 204 is returned, depending on the circumstances. The response body will contain the details of the request. A GET response will contain the data related to the requested resource. A DELETE response body is usually empty and returns a 204 code.

- Port 8080 will be the port used by default when making HTTP requests.
- < Setting up secure HTTP communication – TLS >
- MQTT concepts
 - Events are communicated as messages using MQTT, a lightweight publish / subscribe protocol. Events occurring at the WM8311 are published to a broker. The broker then relays those messages to the Host E-Call System subscribing to the event message(s).
 - The event message payload will be formatted as JSON unless otherwise specified.
 - All event messages are sent with a QOS of "1". This means that the broker is guaranteed to get the event message but could possibly also receive duplicates. When subscribing to these event messages, you probably want to use a QOS of "1" as well.
 - The WM8311 will send out a ping (PINGREQ) periodically to the broker. If the broker does not hear this ping when expected, it will consider the WM8311 as down and publish a Last-Will message. <LWT to be completed > The Host E-Call System should subscribe to these Last-Will messages to handle the situation where the WM8311 stops communicating (network failure, power issue, etc).
 - A UTC timestamp ("date") will be in each published message. This helps deal with the situation where the subscriber gets a retained message from the broker when it connects.
 - The <door id> used in the example event message topics below corresponds to the controller_id which is the WM8311 serial number. The serial number is visible on the side label of the WM8311 below the QR code.
< Image depicting serial number on label >
- Inovonics will provide an MQTT broker residing on the Google Cloud. Currently the connection can be made with the following:
 - < address >
 - < port >
 - < TLS version >
 - < username >
 - < password >
- You can use the MQTT client of your choice. Some of the more popular open-source implementations are available from the "Eclipse Paho Project" (<https://www.eclipse.org/paho/>).
- We're currently using MQTT version 3.1.1 but are investigating upgrading to 5.0

Operations

- Setup (HW installation covered in separate document)
 - This default configuration of the WM8311 uses DHCP to resolve its network address. The address can be determined by subscribing to

network event messages for that WM8311. So, for example, if the serial number of the WM8311 is 0119-0000-0000-2314, you would subscribe to the topic "`<MQTT username>/door/0119-0000-0000-2314/event/network`". The network event message is published when the WM8311 starts up (or if the network configuration changes). In the payload of the event message, the resolved IP address will appear in the "ip_address" JSON value. You can also listen for Gratuitous ARPs using a utility like WireShark (Add display filter "`eth.src[0:3]==5C:26:23 || eth.dst[0:3]==5C:26:23`" to ease finding of Gratuitous ARPs). Or if the network supports it, you can PING the WM8311's hostname. The default hostname is "`inovonics-wander-{last 6 MAC digits}`". So, for example, if the WM8311's MAC address (printed on a label below the serial number) is "`5C:26:23:00:33:0C`", you would `ping inovonics-wander-00330c`.

- Once the IP address is determined, the WM8311 can be configured as necessary through HTTP REST requests.
- The network addressing scheme can be adjusted through a PUT `http://<IP address:port>/network/` request.
- Data components, like schedules, staff, and residents, can be added via HTTP POST requests.
- Door inputs and time durations can be adjusted using a PUT `http://<IP address:port>/controller/` request.
- Once the door is completely configured, test the door management with staff credentials and WM1320 tags to verify the operation is correct. Adjustments may need to be made to the WM1320 detection and exit level sensitivity based on the resident area surrounding the door.
- System Startup
 - Five "Gratuitous" ARPs are sent out once the network configuration is determined.
 - The following event messages are published upon a normal startup: online (with health status), door schedule status (in-schedule or out-of-schedule) and network (with network configuration). Then the WM8311 tamper state is published. This is followed by the state of the inputs: door sensor, rex and aux.
 - A reader firmware check is performed to determine if the reader needs to be updated. If the WM8311 has a newer firmware version, that file will be transferred to the reader upon startup.
- Creating Schedules
 - Schedules can be used to define when residents, staff and the door control is actively managed in the Wander Management system. Two schedules are built-in: 0 (never managed) and 1 (always managed). They cannot be changed or deleted.
 - Up to seven schedules can be added with a POST `http://<IP address:port>/schedules/<schedule id>/` request where the schedule id is 2 through 8. Schedules are made up of an array of two intervals. Each interval contains a start time and period of length to define the time when the schedule is active and an array of weekdays to which the time period applies. Schedules must be created before they can be associated with residents, staff, and the door.
 - Schedules can be modified using the PUT request, retrieved with a GET request and removed with a DELETE request. Schedules must be removed from each component that uses it before it can be deleted from the

system. So, if resident #2 uses schedule #4, you must update resident #2 to use a different schedule before deleting schedule #4.

- Enrolling a Resident

- Create an integer ID of the resident in the Host E-Call System and use that ID to associate with the resident resource in the WM8311.
- Determine the loiter duration and schedule for the resident. The loiter duration is the period in tenths of a second after the resident is first detected at the door and a loiter event message is published.
- Insert battery into a WM1320
- Using a WM4324 enrollment unit, get the unique id of the WM1320 and verify the battery level < currently reported in millivolts – this may change in the future >.
- Send a POST request of that resident to each door that will be managed.
- For example, a staff member creates a resident with an ID of 28934972 in the Host E-Call System. They retrieve a WM1320 and insert the battery. Next the staff passes the WM1320 in front of the WM4324 enrollment unit. This will cause the WM4324 enrollment unit to generate a wander event message with that tag ID (and a resident ID of -1 since that WM1320 is not yet registered). Let's say in this case, it reports a tag ID of "0C:F3:EE:E4:00:0F". The staff then places the WM1320 on the resident's wrist. They want to be notified if that resident loiters more than 30 seconds and that resident is to be monitored 24/7. The Host E-Call System would then send the following POST request to all doors where that resident needs to be monitored:

```
POST /residents/28934972/
{ "loiter_duration": 300, "tag_id": "0C:F3:EE:E4:00:0F",
  "schedule_id": 1 }
```

- Enrolling Staff

- Create an integer ID of the staff member in the Host E-Call System and use that ID to associate with the staff resource in the WM8311.
- Determine credentials to use. A PIN can be used at doors where WM4321 keypad readers are available. If staff have access cards, they can be used at all readers. If you want to uniquely identify and manage staff that have the permission to escort residents, each staff member should have a unique PIN and/or access card.
- If staff access cards will be used for credentials, use the WM4324 enrollment unit to determine the card id. Watch for the "unknown-card" event message. In the JSON payload of that event message will be the "card" property which is the card id.
- Send a POST request of that staff resource to each WM8311 where that staff member will be able to escort residents.
- For example, a new staff member is hired at the assisted-living community. Another staff member creates the staff resource with an ID of 8801347 in the Host E-Call System. The new staff member's access card is placed in front of the WM4324 enrollment unit. This will cause the WM4324 enrollment unit to generate an unknown-card event message. Let's say, in this case, it reports a card ID of 46662071. The new staff member was also given a PIN of "0044" and is allowed to escort residents 24/7. The Host E-Call System would then send the following POST request to all doors that the staff member has bypass privileges:

```
POST /staff/8801347/
{ "bypass_card_number": 46662071, "bypass_pin": "0044",
```



```
"schedule_id": 1 }
```

- **Monitoring Door Events and Errors**
 - After the WM8311 and associated resources have been configured, you'll need to monitor for state changes by listening for event messages (i.e., subscribing to MQTT messages).
 - Whenever a resident is detected in proximity to a door, a wander enter event message is sent.
`<MQTT username>/door/<door id>/event/wander/<resident id>/enter`
 - After a specified period of time where no WM1320 is detected (subsequent to a detection event) or outside the BLE exit level, a wander exit event message is sent. This time period can be adjusted on the controller "ble_exit_duration" property. The BLE exit level can be adjusted on the controller "ble_exit_level" property.
`<MQTT username>/door/<door id>/event/wander/<resident id>/exit`
 - Both the enter and exit event messages includes the battery level that should be monitored. If the battery level reaches < TBD > level it should be replaced.
 - Loitering event messages are sent for residents that remain in close proximity to the door for lengthy period of time (i.e., loiter_duration).
`<MQTT username>/door/<door id>/event/wander/<resident id>/loiter`
 - When the door is opened or closed a corresponding event message is sent.
`<MQTT username>/door/<door id>/event/open`
`<MQTT username>/door/<door id>/event/closed`
 Likewise, when the door is locked or unlocked, an event message is sent to indicate the lock state changed.
`<MQTT username>/door/<door id>/event/locked`
`<MQTT username>/door/<door id>/event/unlocked`
 - When a staff member enters a PIN or swipes a staff access card at the reader to escort a resident through the doorway, a staff enter event message is sent.
`<MQTT username>/door/<door id>/event/staff/<staff_id>/enter`
 - When a door is detected to be opened longer than a configured duration (i.e., door_ajar_duration), a door ajar event is sent.
`<MQTT username>/door/<door id>/event/ajar`
 - Error event messages should be monitored to manage the proper operation of the WM8311. For example, if the average CPU load exceeds a specified threshold, an error event is sent.
`<MQTT username>/door/<door id>/error/5/detected`
- **Overriding Controller Management**

Normally the WM8311, once set up with the wander configuration (residents, staff, schedules, etc.), will run independently of the Host E-Call System and reporting any state changes as they occur. However, the Host E-Call System can take control away from the WM8311 and manage the door lock, reader LED and reader sounder directly. This is called an "override". When the lock, LED or sounder is in an override state, the WM8311 will not make any independent

changes to that component. Caution should be used when overriding these components, since the WM8311 will no longer be in active control but will relinquish management to the Host E-Call System. We don't recommend overriding under normal circumstances. If necessary, an override can be performed for a specified duration. The Host E-Call System can also cancel an override at any time.

- Factory Reset

Upon power up, with the WM8311 reset pushbutton pressed for 15 or more seconds, the network configuration will be set to factory default of DHCP. This does not affect any of the permanent storage, only the network settings. A full factory reset (network and permanent storage) can only be performed through the REST API.

<picture showing WM8311 and reset button>

- Design Considerations

- < Two close doors – cases >
- < Multi-floor issues >
- < Opposite side of door (coming in from outside) detection >

- Error Messages

- < Walk through errors and possible debugging >

```
err_NONE           = 0,           // No error
err_API_COMM_LOST  = 1,           // Lost internal communications
err_RDR_COMM_LOST  = 2,           // Lost communications to the reader
err_UNMATCHED_SCBK = 3,           // Unmatched OSDP (reader comm) key
err_HIGH_TEMP      = 4,           // CPU temperature high
err_HIGH_LOAD      = 5,           // CPU average load high
err_HIGH_FLASH     = 6,           // Flash usage high
err_HIGH_MEMORY    = 7,           // Memory usage high
err_API_ERROR      = 8,           // Internal error
err_CTL_ERROR      = 9            // Application error
```

- System Health

- If movement is detected by the accelerometer on the WM8311 or reader, an active tamper event message is sent.
- Input supervision issues (opens and shorts) on the door sensor (and AUX and REX if using) can be monitored by listening for (i.e., subscribing to) "fault-short" and "fault-open" event messages. See [Appendix C \(WM8311 Contact Supervision\)](#): for more information on input supervision.
- The system comes preconfigured with default settings for health thresholds. However, these can be adjusted as necessary using a PUT request. For example, changing the alarm limit for the CPU load percentage to 80 :
PUT /health/thresholds/

- ```

{
 "high_load_alarm": 80,
 "high_load_clear": 70
}

```
- If the alarm threshold is exceeded, an error message will be sent. See Error Messages above. In the case of the CPU load being exceeded, you'll see an error/5/detected message with the current CPU load in the message payload. Thresholds can be set and monitored for flash and memory usage as well as, CPU load and temperature. Once the value being monitored goes below the clear value, a "cleared" message is sent.
  - Firmware updates
    - Periodically, the WM8311 (and/or reader) firmware will be updated, over-the-air, via a Mender server maintained by Inovonics. Mender is a system that allows Inovonics to update the firmware remotely whenever there are bug fixes or feature updates to deploy. The WM8311 will poll the Mender server and download any updates found into a reserve partition on the WM8311. Once loaded, the WM8311 will boot into that partition. If that all goes as expected, that partition will become the active partition. If there is any issue, the WM8311 will boot up into the previous working partition.
    - < Update coordination / schedule >
  - Field Demo Test app (maybe tag-detection-test)
    - To get up to speed quickly, we have created a Python-based GUI application that demonstrates using the Wander REST API and MQTT messages. This can be used out of the box to get a general understanding of how the wander system works. It can also be used as a stand-alone test of the operation as you develop your Host E-Call System. So, you can compare the functionality side-by-side. Also, you can peruse the code to see how it works.
    - < Picture of GUI >
  - Regulatory
    - < UL >

## Appendix A (A/V States):

The proper audio/visual feedback is evaluated in priority order from AV ID 0 to AV ID 8. So, for example, if a resident approaches a closed door that's currently locked, the audio/visual feedback will be AV ID 6.

|                | AV ID 0                 | AV ID 1          | AV ID 2           | AV ID 3               | AV ID 4                          | AV ID 5                          | AV ID 6                        | AV ID 7                 | AV ID 8     |
|----------------|-------------------------|------------------|-------------------|-----------------------|----------------------------------|----------------------------------|--------------------------------|-------------------------|-------------|
|                | Controller Error        | Door Not managed | Bypass Mode       | Resident at Open Door | Loiterer at Unlocked Closed Door | Resident at Unlocked Closed Door | Resident at Locked Closed Door | Door Ajar (No Resident) | No Resident |
| LED Output     | Rapid Blink red / amber | Off              | Blink green / off | Rapid Blink red / off | Blink red / off                  | Blink amber / off                | Solid amber                    | Blink green / amber     | Solid green |
| Sounder Output | Off                     | Off              | Off               | Chirping              | Off                              | Off                              | Off                            | Off                     | Off         |

NOTES:

1. If the LED state is blink, the LED will blink the first color for 500ms and second for 500ms.
2. If the LED state is rapid blink, the LED will blink the first color for 100ms and second for 100ms.
3. If the sounder state is chirp, the sounder will beep for 100ms and be silent for 100ms.

CONTROLLER ERROR (A/V ID 0)

There may be cases where the WM8311 cannot be sure that it can control the door properly. These cases may arise from improper configuration, low memory, other internal errors, etc. In these cases, the WM8311 will revert to the controller error audio/visual state to call attention to the error.

DOOR UNMANAGED (A/V ID 1)

This is the case where, because of the door schedule, the WM8311 is not monitoring for residents.

BYPASS MODE (A/V ID 2)

This is the case where a staff member has presented a valid credential to allow resident(s) egress through a normally locked door.

RESIDENT AT OPEN DOOR (A/V ID 3)

This is the case where a resident has been detected near an open door.

LOITERER AT UNLOCKED CLOSED DOOR (A/V ID 4)

This is the case where a resident has been near the door for a period of time greater than the loiter time assigned to that resident.

RESIDENT AT UNLOCKED CLOSED DOOR (A/V ID 5)

This is the case where a resident is near a closed door that has been unlocked due to expiration of the door lock timer.

RESIDENT AT LOCKED CLOSED DOOR (A/V ID 6)

This is the case where a resident in proximity to a locked door.

DOOR AJAR (A/V ID 7)

This is the case where the door has been held open for period of time greater than the door ajar duration.

NO RESIDENT PRESENT (A/V ID 8)

This is the case where there are no monitored residents near the door. Residents are monitored based on the time scheduled associated with that resident.

The WM8311 will check for the appropriate state using the priorities listed above. It will set the A/V state of the Reader LED and sounder as mentioned for the first state found. For example, if there is a loiterer at a closed door when a valid bypass

credential is presented, the A/V state will change from solid amber LED to blinking green LED.

The table above represents the default (factory set) A/V states. The WM8311 will support an HTTP PUT request allowing the Host E-Call System to update these defaults to the host-defined values.

## Appendix B (Glossary):

- Resident – occupant at an assisted-living senior care facility that is a risk to wander from the premises.
- WM1320 Wander Tag – a BLE (Bluetooth Low-Energy) device worn by a resident that will be detected upon approaching monitored doors.
- WM8311 Door Controller - Yocto-based Linux microcontroller that performs the logical operations based on the state of the door, input from the reader and component configuration
- Reader – Detects Wander Tags as well as staff access cards and communicates that information to the WM8311 over RS-485/OSDP. It comes in three varieties: WM4321 Keypad, WM4322 single-gang and WM4323 mullion.
- Host E-Call System - Application used to manage assisted-living senior care.
- Staff – Personnel responsible for senior care at the facility.
- Staff access card – RFID 125 KHz access badge used by many access control systems.
- Door sensor – Contact sensor to provide feedback as to the state of the door (open / closed).
- Sounder – Audible feedback integrated into reader to alert to specified state of wander system.
- Signal strength – Strength of BLE signal of Wander Tag as received by the reader.
- Event message – MQTT message published by WM8311 upon detecting state change of wander system.
- Bypass – The act of escorting a resident through a monitored door by a staff member.

## Appendix C (WM8311 Contact Supervision):

### Introduction

The WM8311 supports three supervised inputs: Door Sensor (DSM), Request to Exit (REX) and an Auxiliary input (AUX). All contact point samples are performed by the WM8311 and only contact states (normal, alarm, opened, shorted) are reported to the controller. This document is intended to describe the contact sampling as performed by the WM8311. The DSM, REX and AUX inputs are identical in nature. The following paragraphs apply equally to each input.

## Implementation

The WM8311 associates a contact state with a voltage range as measured through a 12-bit A/D converter. The WM8311 accommodates at most 8 of these associations although, in practice, seldom will you see more than 4 in use. These range definitions must be consecutive and ascending. An example is shown below:

| Index | A/D Low Value | A/D High Value | Contact State |
|-------|---------------|----------------|---------------|
| 0     | 0             | 1317           | Short (2)     |
| 1     | 1318          | 2328           | Alarm (1)     |
| 2     | 2329          | 3148           | Normal (0)    |
| 3     | 3149          | 3790           | Alarm (1)     |
| 4     | 3791          | 4095           | Open (3)      |

Note that the ranges are not allowed to overlap as a contact sample can only relate to a single state. The values are represented as 12-bit unsigned integers.

## Contact Sampling

Contact points are sampled every 70ms. When the contact changes state, the WM8311 requires eight consecutive samples to be within a 32 ADC bit window. This sampling method provides reliable debounce on the contact.

Hysteresis is not supported as, using the state association scheme described above, there cannot be overlap of the voltage ranges.

## Associating the Contact State with a Voltage Range

The WM8311 receives a configuration message from the Host E-Call System that contains the series and parallel resistor values for each of DSM, REX and Aux. Using these resistor values, the WM8311 calculates the contact open and contact closed values using the equations in section [Supervised Inputs](#). The WM8311 then sets the range to be the calculated sample value plus and minus 511 ADC bits. For example, consider a normally closed DSM contact with a 330 $\Omega$  series resistor,  $R_s$ , and a 660 $\Omega$  parallel resistor  $R_p$ .

Given these resistor values, the contact open ADC value calculates to be 2690 while the contact closed value calculates to 1308. A window is calculated about the nominal sample points by adding and subtracting 511 from each. The range for contact open would be 2179 to 3201 while the range for contact closed would be 797 to 1819. From these, we set the Contact Setup ranges as:

| Index | A/D Low Value | A/D High Value | Contact State |
|-------|---------------|----------------|---------------|
| 0     | 0             | 796            | Short (2)     |
| 1     | 797           | 1819           | Normal (1)    |
| 2     | 2179          | 3201           | Alarm (0)     |
| 3     | 3202          | 4095           | Open (3)      |

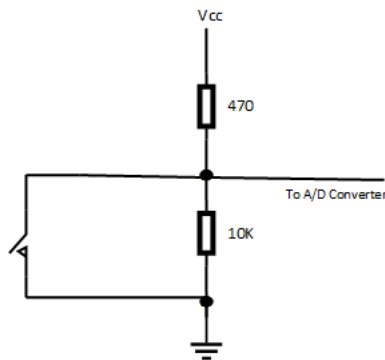
Note that the unspecified range of 1820 to 2178 is left undefined. Undefined ranges are not reported by the WM8311.

### Supervised inputs

End of line resistors are used to enable the detection of attempts to compromise the security by either shorting a normally closed circuit or by opening a normally open circuit. The following paragraphs describe each of these options. For each option resistors  $R_s$  and  $R_p$  reside at the contact.

### Unsupervised

This is the case where no end-of-line resistors are in used.

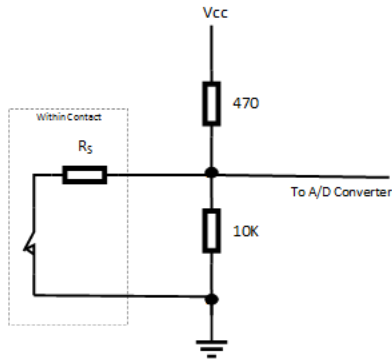


In this case, an open contact sample would be 95% of the 12-bit ADC range while a switch closed would register approximately 0x0000 on the ADC.

### Single serial resistor used with normally closed contact

This is the case where an alarm is generated whenever the normally closed switch is opened. The series resistor  $R_s$  is used to distinguish between a short circuit and switch closed. The short would cause the A/D converter to see zero volts while a switch closed causes the A/D converter to see a value as defined by the formula below. An alarm is generated whenever the line is cut, or the switch is open – no distinction is made between these two conditions.

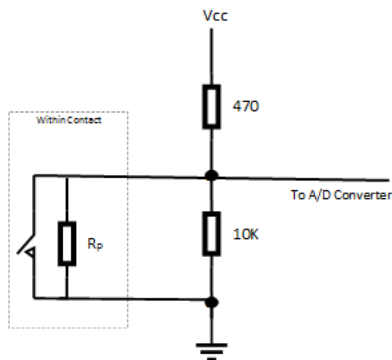
- Switch Open:  $ADC \cong 0.95 * 4095$
- Switch Closed:  $Rt = \frac{Rs * 10K}{Rs + 10K}$ ;  $ADC \cong 4095 * \frac{Rt}{470 + Rt}$
- Line Short:  $ADC \cong 0x0000$
- Line Open:  $ADC \cong 0.95 * 4095$



### Single parallel resistor used with normally open contact

This is the case where an alarm is generated whenever the normally open switch is closed. The parallel resistor  $R_p$  is used to distinguish between an open circuit and switch open. An open circuit causes the A/D converter to see  $V_{cc}$  while a switch open causes the A/D converter to see value as defined by the formula below. An alarm is generated whenever the line is shorted, or the switch is closed – no distinction is made between these two conditions.

- Switch Open:  $R_t = \frac{R_p * 10K}{R_p + 10K}$ ;  $ADC \cong 4095 * \frac{R_t}{470 + R_t}$
- 
- Switch Closed:  $ADC \cong 0x0000$
- Line Short:  $ADC \cong 0x0000$
- Line Open:  $ADC \cong 0.95 * 4095$



### Standard two-resistor configuration

This is the case where both line short and line open can be distinguished from switch closed and switch open. The diagram below is described using resistors of equal value. In practice, resistors  $R_s$  and  $R_p$  are chosen to increase the difference between switch closed and switch open.

- Switch Open:  $R_t = \frac{(R_s + R_p) * 10K}{R_s + R_p + 10K}$ ;  $ADC \cong 4095 * \frac{R_t}{470 + R_t}$
- Switch Closed:  $R_t = \frac{R_s * 10K}{R_s + 10K}$ ;  $ADC \cong 4095 * \frac{R_t}{470 + R_t}$



- Line Short:  $ADC \cong 0x0000$
- Line Open:  $ADC \cong 0.95 * 4095$

