Breaking Bulbs Briskly
By
Bogus Broadcasts

Joe Hall and Ben Ramsey

Goals

- Release some Z-Wave recon tools
- Break some fluorescent bulbs

Z-Wave

- Low-rate wireless network protocol
- Proprietary: no SDK without NDA!
- Big in automation & security systems

NEXIA
Logitech
LOWE'S
verizon
SAMSUNG
ADT
HUAWEI
D-Link
Kwikset
Honeywell

Z-Wave


FORTREZZ
WV-01, Wireless Z-Wave® Water Valve
Fortrezz LLC. MI 48309 www.fortrezz.com Made in U.S.A.


First Alert
SMOKE ALARM
SMOKE
WIRELESS
DO NOT PAINT


Wed, Aug 28
4:24 PM
Indoor Temp
75°
Cooling
Following Schedule: HOME
Outdoor Temp L 72° H 88°
85°
Indoor Humidity
50%
Away
75°
68°
Status
Menu
Auto
System Mode
Auto
Fan Mode
Auto
Air Cleaner
TRANE

What's Out There?

- Open-ZWave
  - Open source libraries
  - Control devices via Z-Wave USB stick
- Z-Force (BH '13 – Fouladi & Ghanoun)
  - Commodity radio
  - Custom firmware, closed-source software
- Scapy-radio (BH '14 – Picod et al.)
  - Generic wireless sniffer/injector using software-defined radios
  - Open source, uses GNU Radio and Scapy

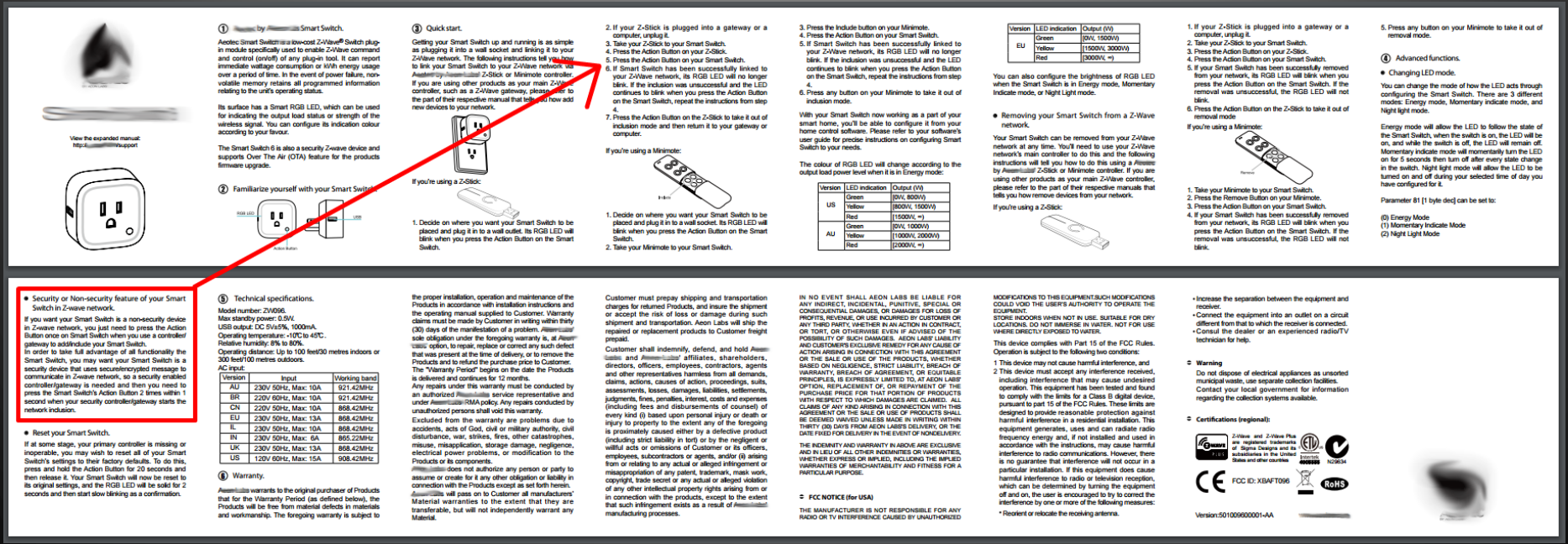
EZ-Wave

- Built on top of Scapy-radio
  - Extended support for Z-Wave protocol
- Includes 3 tools:
  1. ezstumbler: network discovery & enumeration
  2. ezrecon: device interrogation
     - Manufacturer / product name
     - Software versions
     - Supported command classes
     - Current state
     - Configuration settings

     Not available when encryption is used
  3. ezfingerprint
     - Determines Z-Wave module generation
     - PHY manipulation to exploit differences in transceivers

A Note About Security

- The protocol *supports* AES-128
  - Up to the device manufacturer to use it…
  - Only 9 of 33 devices we tested support encryption
    - 5 door locks & 4 newer devices
    - 3 of the 4 were 'opt-in' security…



View the expanded manual:
http://[redacted]/support

① [redacted] by [redacted] Smart Switch.

Aeotec Smart Switch is a low-cost Z-Wave® Switch plug-in module specifically used to enable Z-Wave command and control (on/off) of any plug-in tool. It can report immediate wattage consumption or kWh energy usage over a period of time. In the event of power failure, non-volatile memory retains all programmed information relating to the unit's operating status.

Its surface has a Smart RGB LED, which can be used for indicating the output load status or strength of the wireless signal. You can configure its indication colour according to your favour.

The Smart Switch 6 is also a security Z-wave device and supports Over The Air (OTA) feature for the products firmware upgrade.

② Familiarize yourself with your Smart Switch.

RGB LED
USB
Action Button

③ Quick start.

Getting your Smart Switch up and running is as simple as plugging it into a wall socket and linking it to your Z-Wave network. The following instructions tell you how to link your Smart Switch to your Z-Wave network via [redacted] Z-Stick or Minimote controller. If you are using other products as your main Z-Wave controller, such as a Z-Wave gateway, please refer to the part of their respective manual that tells you how add new devices to your network.

If you're using a Z-Stick:

1. Decide on where you want your Smart Switch to be placed and plug it in to a wall outlet. Its RGB LED will blink when you press the Action Button on the Smart Switch.
2. If your Z-Stick is plugged into a gateway or a computer, unplug it.
3. Take your Z-Stick to your Smart Switch.
4. Press the Action Button on your Z-Stick.
5. Press the Action Button on your Smart Switch.
6. If Smart Switch has been successfully linked to your Z-Wave network, its RGB LED will no longer blink. If the inclusion was unsuccessful and the LED continues to blink when you press the Action Button on the Smart Switch, repeat the instructions from step 4.
7. Press the Action Button on the Z-Stick to take it out of inclusion mode and then return it to your gateway or computer.

If you're using a Minimote:

Index

1. Decide on where you want your Smart Switch to be placed and plug it in to a wall socket. Its RGB LED will blink when you press the Action Button on the Smart Switch.
2. Take your Minimote to your Smart Switch.
3. Press the Include button on your Minimote.
4. Press the Action Button on your Smart Switch.
5. If Smart Switch has been successfully linked to your Z-Wave network, its RGB LED will no longer blink. If the inclusion was unsuccessful and the LED continues to blink when you press the Action Button on the Smart Switch, repeat the instructions from step 4.
6. Press any button on your Minimote to take it out of inclusion mode.

With your Smart Switch now working as a part of your smart home, you'll be able to configure it from your home control software. Please refer to your software's user guide for precise instructions on configuring Smart Switch to your needs.

The colour of RGB LED will change according to the output load power level when it is in Energy mode:

Version	LED indication	Output (W)
US	Green	(0W, 800W)
	Yellow	(800W, 1500W)
	Red	(1500W, ∞)
AU	Green	(0W, 1000W)
	Yellow	(1000W, 2000W)
	Red	(2000W, ∞)

Version	LED indication	Output (W)
EU	Green	(0W, 1500W)
	Yellow	(1500W, 3000W)
	Red	(3000W, ∞)

You can also configure the brightness of RGB LED when the Smart Switch is in Energy mode, Momentary Indicate mode, or Night Light mode.

● Removing your Smart Switch from a Z-Wave network.

Your Smart Switch can be removed from your Z-Wave network at any time. You'll need to use your Z-Wave network's main controller to do this and the following instructions will tell you how to do this using a [redacted] by [redacted] Z-Stick or Minimote controller. If you are using other products as your main Z-Wave controller, please refer to the part of their respective manuals that tells you how remove devices from your network.

If you're using a Z-Stick:

1. If your Z-Stick is plugged into a gateway or a computer, unplug it.
2. Take your Z-Stick to your Smart Switch.
3. Press the Action Button on your Z-Stick.
4. Press the Action Button on your Smart Switch.
5. If your Smart Switch has been successfully removed from your network, its RGB LED will blink when you press the Action Button on the Smart Switch. If the removal was unsuccessful, the RGB LED will not blink.
6. Press the Action Button on the Z-Stick to take it out of removal mode

If you're using a Minimote:

Remove

1. Take your Minimote to your Smart Switch.
2. Press the Remove Button on your Minimote.
3. Press the Action Button on your Smart Switch.
4. If your Smart Switch has been successfully removed from your network, its RGB LED will blink when you press the Action Button on the Smart Switch. If the removal was unsuccessful, the RGB LED will not blink.
5. Press any button on your Minimote to take it out of removal mode.

④ Advanced functions.

● Changing LED mode.

You can change the mode of how the LED acts through configuring the Smart Switch. There are 3 different modes: Energy mode, Momentary indicate mode, and Night light mode.

Energy mode will allow the LED to follow the state of the Smart Switch, when the switch is on, the LED will be on, and while the switch is off, the LED will remain off. Momentary indicate mode will momentarily turn the LED on for 5 seconds then turn off after every state change in the switch. Night light mode will allow the LED to be turned on and off during your selected time of day you have configured for it.

Parameter 81 [1 byte dec] can be set to:

(0) Energy Mode
(1) Momentary Indicate Mode
(2) Night Light Mode

● Security or Non-security feature of your Smart Switch in Z-wave network.

If you want your Smart Switch is a non-security device in Z-wave network, you just need to press the Action Button once on Smart Switch when you use a controller/gateway to add/include your Smart Switch.
In order to take full advantage of all functionality the Smart Switch, you may want your Smart Switch is a security device that uses secure/encrypted message to communicate in Z-wave network, so a security enabled controller/gateway is needed and then you need to press the Smart Switch's Action Button 2 times within 1 second when your security controller/gateway starts the network inclusion.

● Reset your Smart Switch.

If at some stage, your primary controller is missing or inoperable, you may wish to reset all of your Smart Switch's settings to their factory defaults. To do this, press and hold the Action Button for 20 seconds and then release it. Your Smart Switch will now be reset to its original settings, and the RGB LED will be solid for 2 seconds and then start slow blinking as a confirmation.

⑤ Technical specifications.

Model number: ZW096
Max standby power: 0.5W
USB output: DC 5V±5%, 1000mA
Operating temperature: -10℃ to 45℃.
Relative humidity: 8% to 80%
Operating distance: Up to 100 feet/30 metres indoors or 300 feet/100 metres outdoors.
AC input:

Version	Input	Working band
AU	230V 50Hz, Max: 10A	921.42MHz
BR	220V 60Hz, Max: 10A	921.42MHz
CN	220V 50Hz, Max: 10A	868.42MHz
EU	230V 50Hz, Max: 13A	868.42MHz
IL	230V 50Hz, Max: 10A	868.42MHz
IN	230V 50Hz, Max: 6A	865.22MHz
UK	230V 50Hz, Max: 13A	868.42MHz
US	120V 60Hz, Max: 15A	908.42MHz

⑥ Warranty.

[redacted] warrants to the original purchaser of Products that for the Warranty Period (as defined below), the Products will be free from material defects in materials and workmanship. The foregoing warranty is subject to the proper installation, operation and maintenance of the Products in accordance with installation instructions and the operating manual supplied to Customer. Warranty claims must be made by Customer in writing within thirty (30) days of the manifestation of a problem. [redacted] sole obligation under the foregoing warranty is, at [redacted] option, to repair, replace or correct any such defect that was present at the time of delivery, or to remove the Products and to refund the purchase price to Customer. The "Warranty Period" begins on the date the Products is delivered and continues for 12 months.
Any repairs under this warranty must be conducted by an authorized [redacted] service representative and under [redacted] RMA policy. Any repairs conducted by unauthorized persons shall void this warranty.
Excluded from the warranty are problems due to accidents, acts of God, civil or military authority, civil disturbance, war, strikes, fires, other catastrophes, misuse, misapplication, storage damage, negligence, electrical power problems, or modification to the Products or its components.
[redacted] does not authorize any person or party to assume or create for it any other obligation or liability in connection with the Products except as set forth herein.
[redacted] will pass on to Customer all manufacturers' Material warranties to the extent that they are transferable, but will not independently warrant any Material.

Customer must prepay shipping and transportation charges for returned Products, and insure the shipment or accept the risk of loss or damage during such shipment and transportation. Aeon Labs will ship the repaired or replacement products to Customer freight prepaid.

Customer shall indemnify, defend, and hold [redacted] and [redacted] affiliates, shareholders, directors, officers, employees, contractors, agents and other representatives harmless from all demands, claims, actions, causes of action, proceedings, suits, assessments, losses, damages, liabilities, settlements, judgments, fines, penalties, interest, costs and expenses (including fees and disbursements of counsel) of every kind (i) based upon personal injury or death or injury to property to the extent any of the foregoing is proximately caused either by a defective product (including strict liability in tort) or by the negligent or willful acts or omissions of Customer or its officers, employees, subcontractors or agents, and/or (ii) arising from or relating to any actual or alleged infringement or misappropriation of any patent, trademark, mask work, copyright, trade secret or any actual or alleged violation of any other intellectual property rights arising from or in connection with the products, except to the extent that such infringement exists as a result of [redacted] manufacturing processes.

IN NO EVENT SHALL AEON LABS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, OR USE INCURRED BY CUSTOMER OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT, OR TORT, OR OTHERWISE EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. AEON LABS' LIABILITY AND CUSTOMER'S EXCLUSIVE REMEDY FOR ANY CAUSE OF ACTION ARISING IN CONNECTION WITH THIS AGREEMENT OR THE SALE OR USE OF THE PRODUCTS, WHETHER BASED ON NEGLIGENCE, STRICT LIABILITY, BREACH OF WARRANTY, BREACH OF AGREEMENT, OR EQUITABLE PRINCIPLES, IS EXPRESSLY LIMITED TO, AT AEON LABS' OPTION, REPLACEMENT OF, OR REPAYMENT OF THE PURCHASE PRICE FOR THAT PORTION OF PRODUCTS WITH RESPECT TO WHICH DAMAGES ARE CLAIMED. ALL CLAIMS OF ANY KIND ARISING IN CONNECTION WITH THIS AGREEMENT OR THE SALE OR USE OF PRODUCTS SHALL BE DEEMED WAIVED UNLESS MADE IN WRITING WITHIN THIRTY (30) DAYS FROM AEON LABS'S DELIVERY, OR THE DATE FIXED FOR DELIVERY IN THE EVENT OF NONDELIVERY.

THE INDEMNITY AND WARRANTY IN ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER INDEMNITIES OR WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

FCC NOTICE (for USA)

THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT.SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.
STORE INDOORS WHEN NOT IN USE. SUITABLE FOR DRY LOCATIONS. DO NOT IMMERSE IN WATER. NOT FOR USE WHERE DIRECTLY EXPOSED TO WATER.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1 This device may not cause harmful interference, and
2 This device must accept any interference received, including interference that may cause undesired operation. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

* Reorient or relocate the receiving antenna.
* Increase the separation between the equipment and receiver.
* Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
* Consult the dealer or an experienced radio/TV technician for help.

Warning

Do not dispose of electrical appliances as unsorted municipal waste, use separate collection facilities. Contact your local government for information regarding the collection systems available.

Certifications (regional):

Z-Wave and Z-Wave Plus are registered trademarks of Sigma Designs and its subsidiaries in the United States and other countries

FCC ID: XBAFT096

RoHS

Version:501009000001-AA

Demo

Breaking Bulbs

- Z-Wave is not the only smart energy protocol!
- 2.4 GHz
  - Wi-Fi
  - ZigBee
  - 6LoWPAN
  - WirelessHART
  - Bluetooth
- < 1 GHz
  - Z-Wave
  - Insteon
  - Lutron
  - Xodus
  - …

Breaking Bulbs

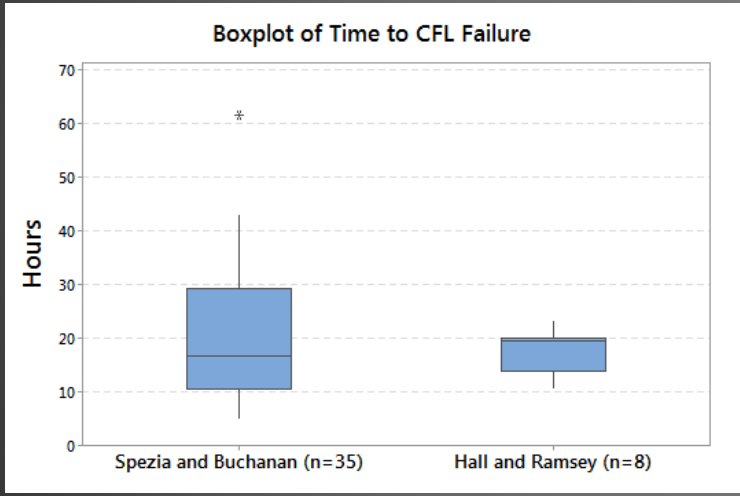
- How do you quickly break fluorescent bulbs?
  - Turn them on and off rapidly.

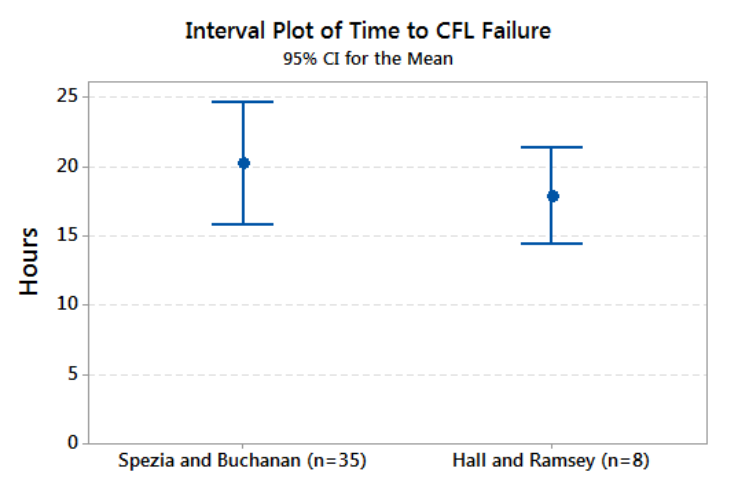
- C. Spezia and J. Buchanan, "Maximizing the Economic Benefits of Compact Fluorescent Lamps," *J. of Industrial Tech,* vol. 27, no. 2, *2011.*

- At 2 seconds on, 8 seconds off they report:
  - *Mean CFL failure: 7,300 cycles (20.3 hrs)*
  - *Wide range: 2,000-22,000 cycles (5.6-61.1 hrs)*

Breaking Bulbs

- Trust but replicate
  - 2 seconds on, 8 seconds off



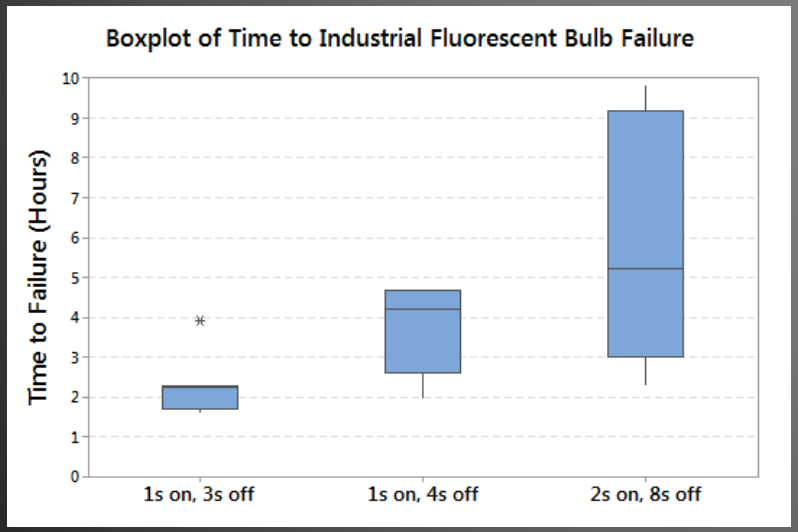


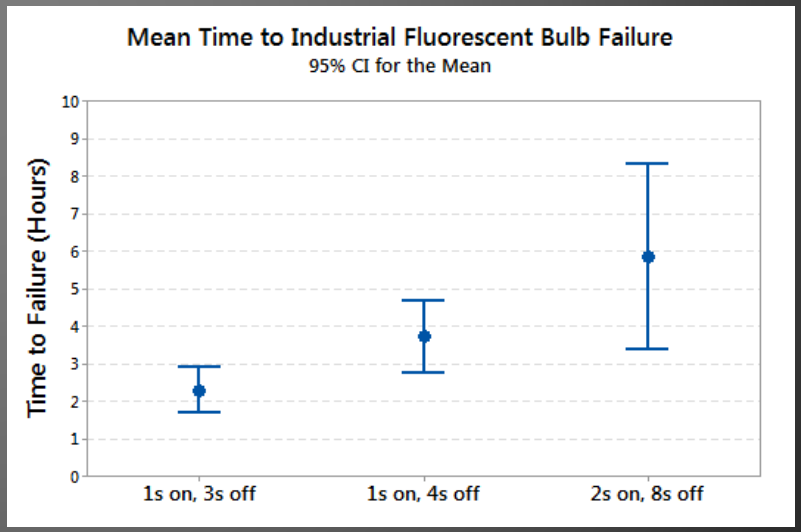
- What about industrial lighting?

Breaking Bulbs

- We can break industrial bulbs faster!
- *1 second on, 3 seconds off is fastest to fail*

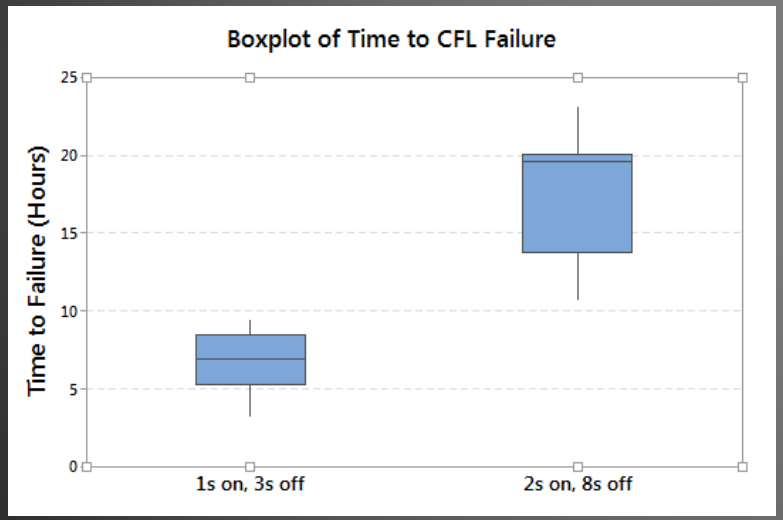
(Faster cycles do not provide enough thermal stress)

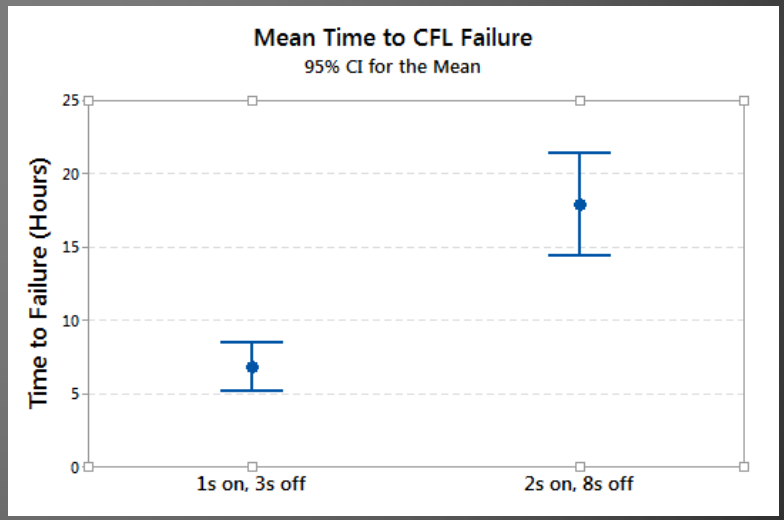




Breaking Bulbs

- Does 1 sec on, 3 secs off also work for residential CFLs?
  - Yes!





Takeaways

- Users:
  - Be mindful when wireless systems control the real world
  - As always… RTFM!
- Device Manufacturers:
  - Support encryption already…
    - We're tired of waiting!
  - Make it the default…
    - Let me decide if I don't want my stuff secure

Questions

EZ-Wave available @

https://github.com/AFITWiSec/EZ-Wave

Let The Forking Begin!