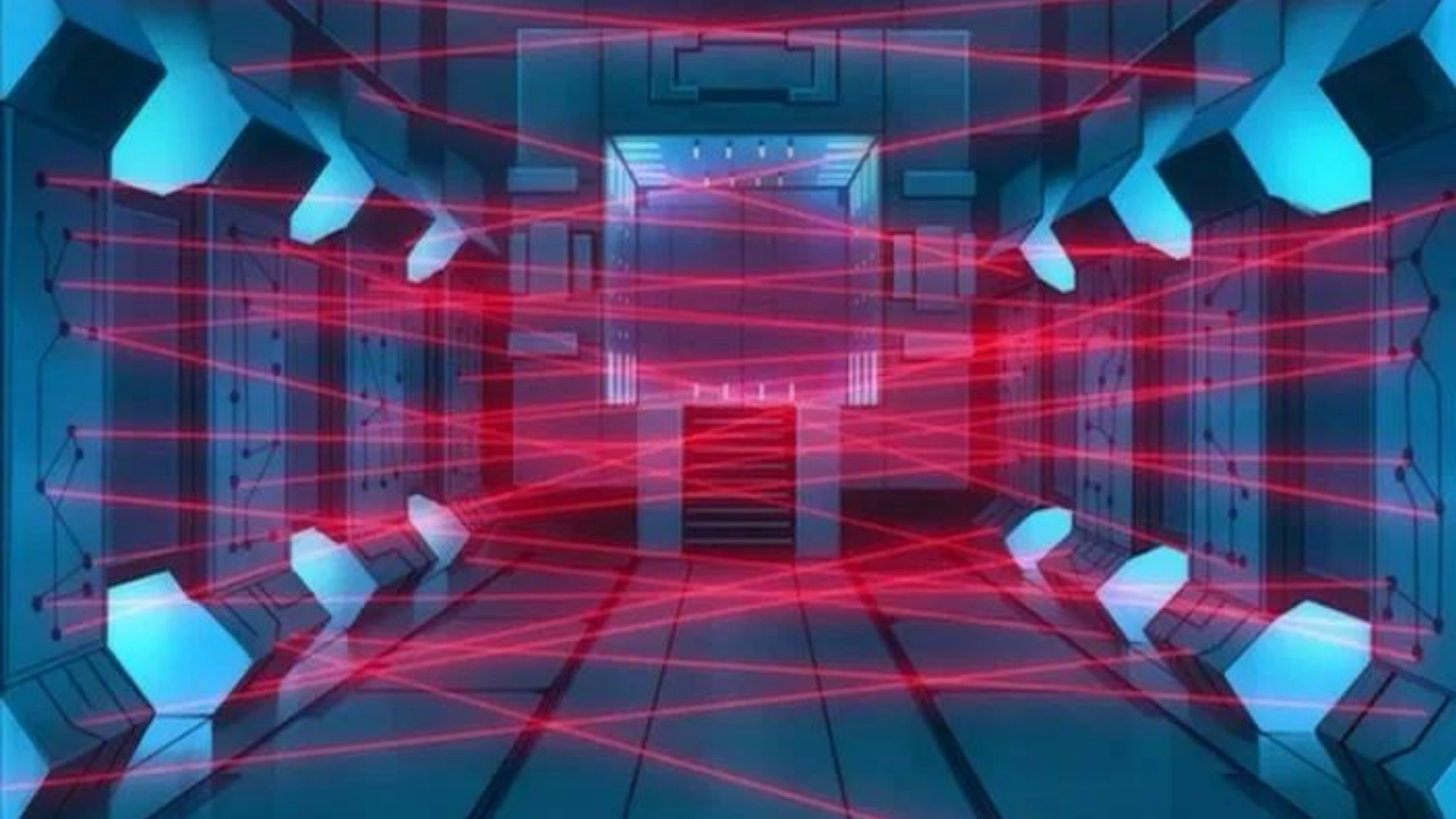
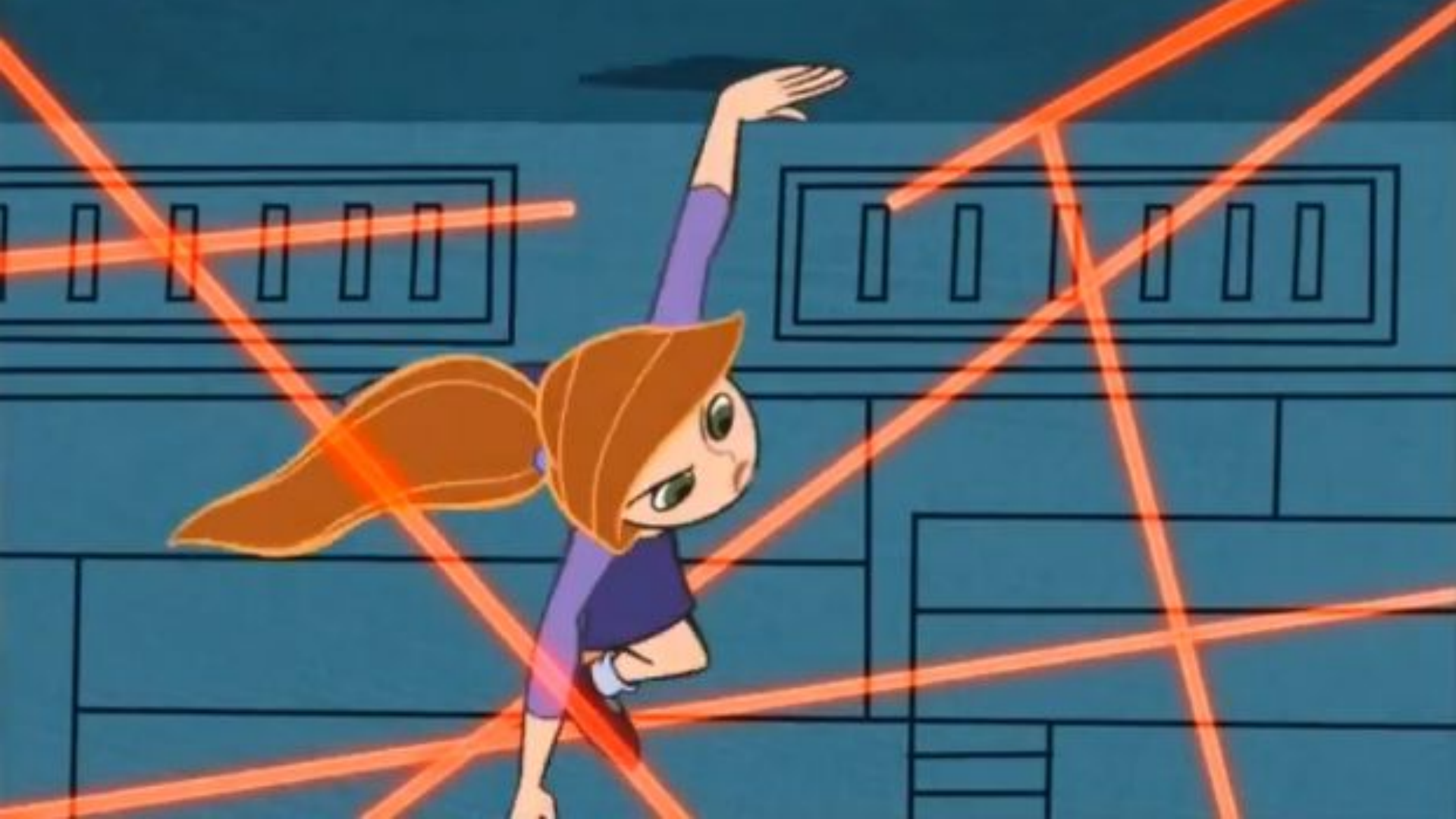
Defeating Physical Intrusion Detection Alarm Wires

Bill Graydon

@access_ctrl
b.graydon@ggrsecurity.com
github.com/bgraydon

GGR
SECURITY CONSULTANTS



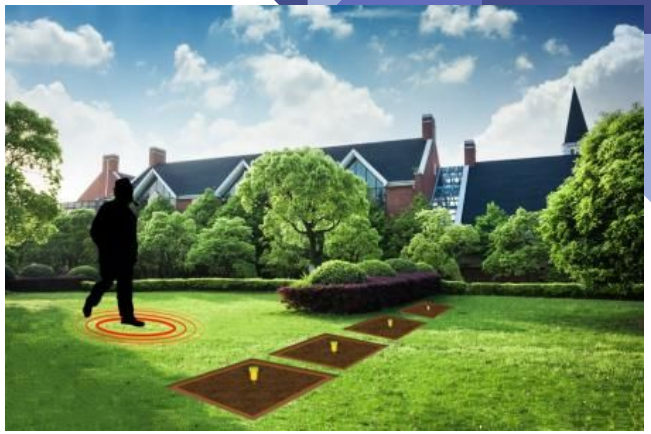


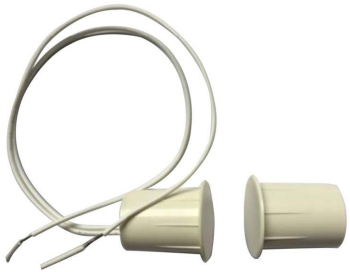
This is a talk about sensor communication wires.

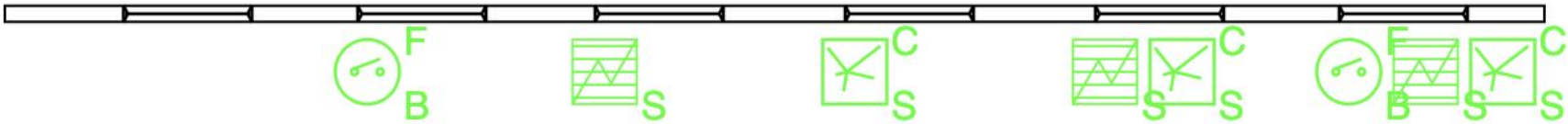
- Alarm systems and access control first
- Defeating line supervision and end-of-line resistors
  - Surrogate Resistor
  - Voltage Regulation
- Defenses

Go try it in the Lock Bypass Village!

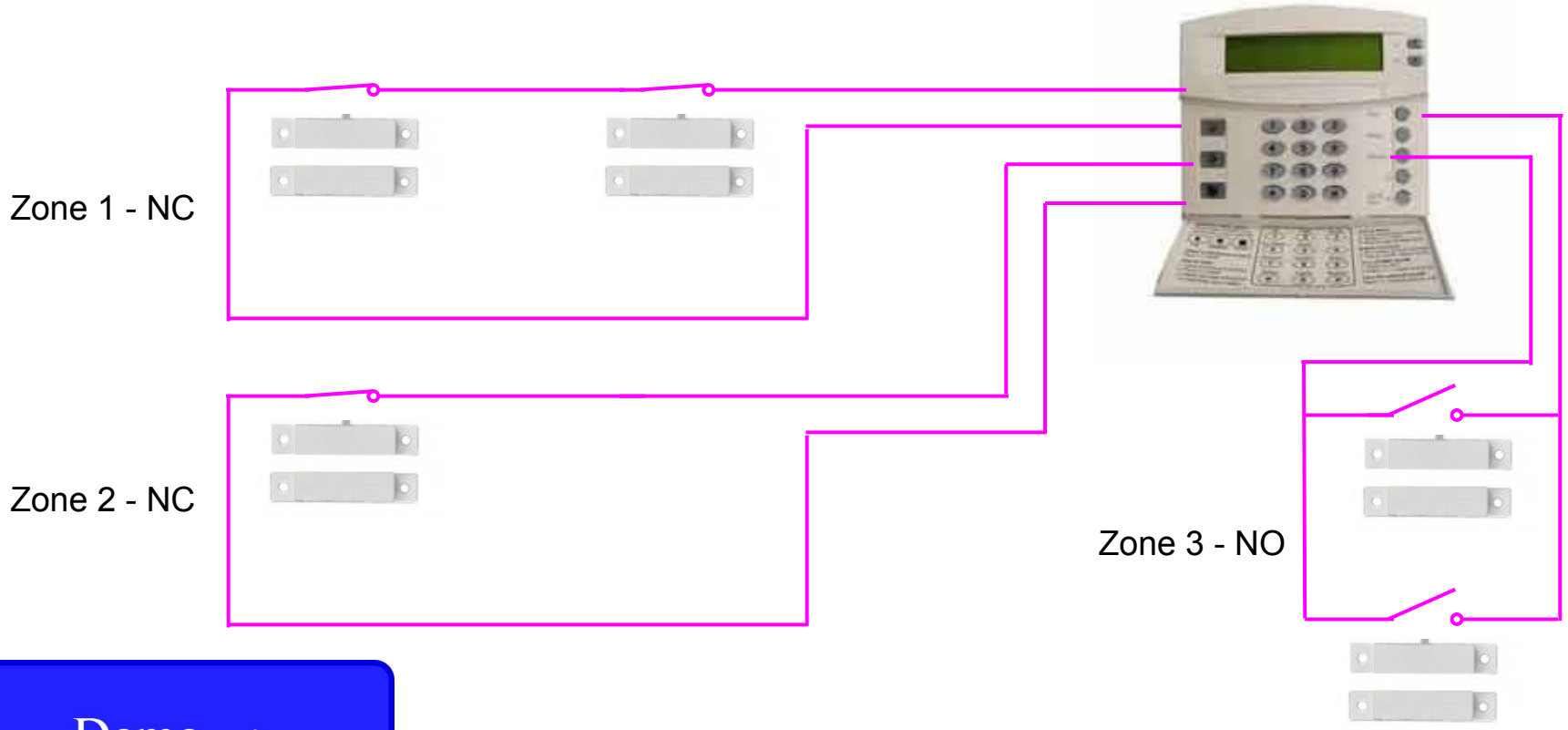
https://www.bypassvillage.org/games/alarm_wire/






F
B
S
C
S
S
C
S
F
B
S
C
S

Alarm Zones



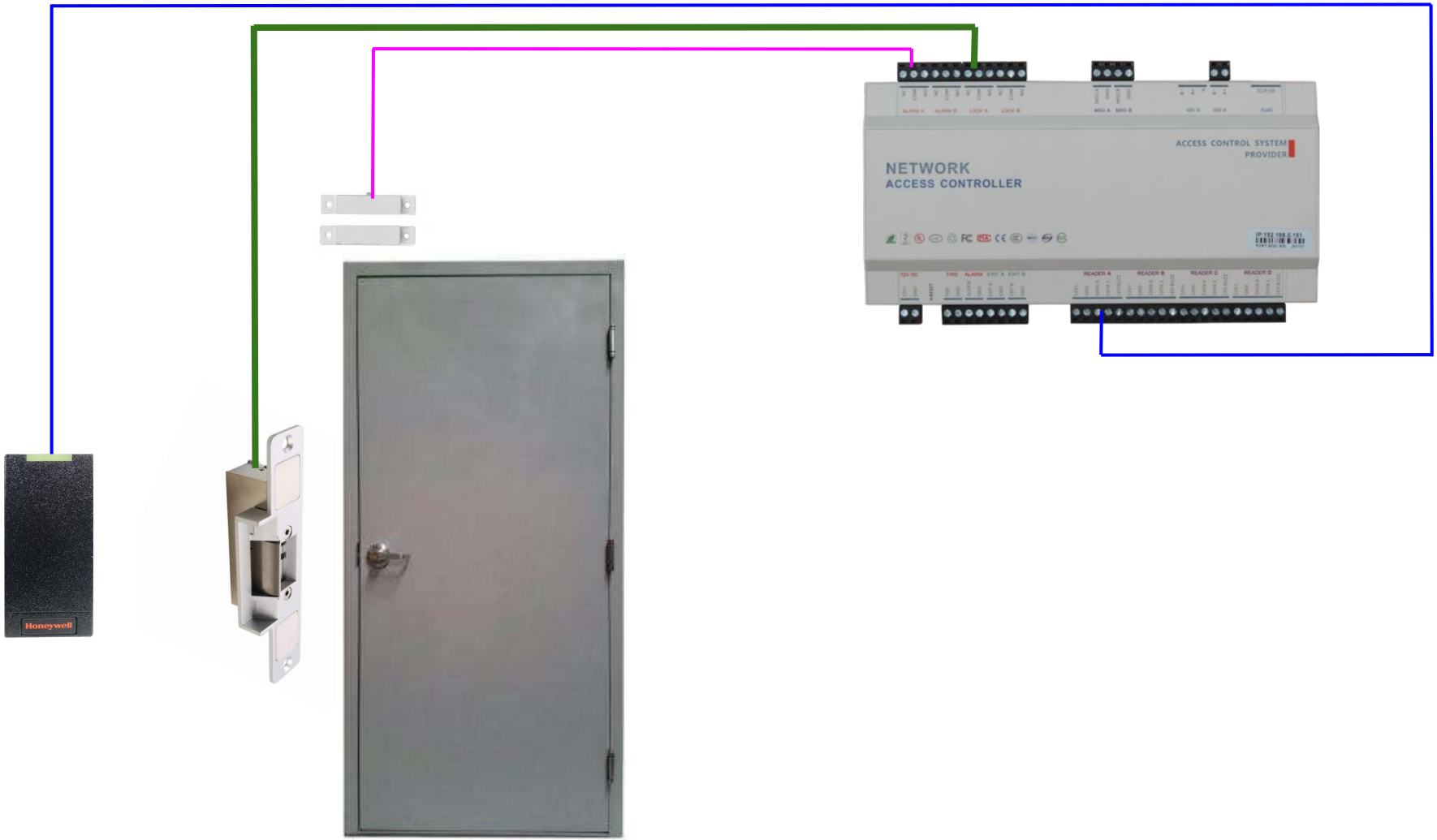
Demo →

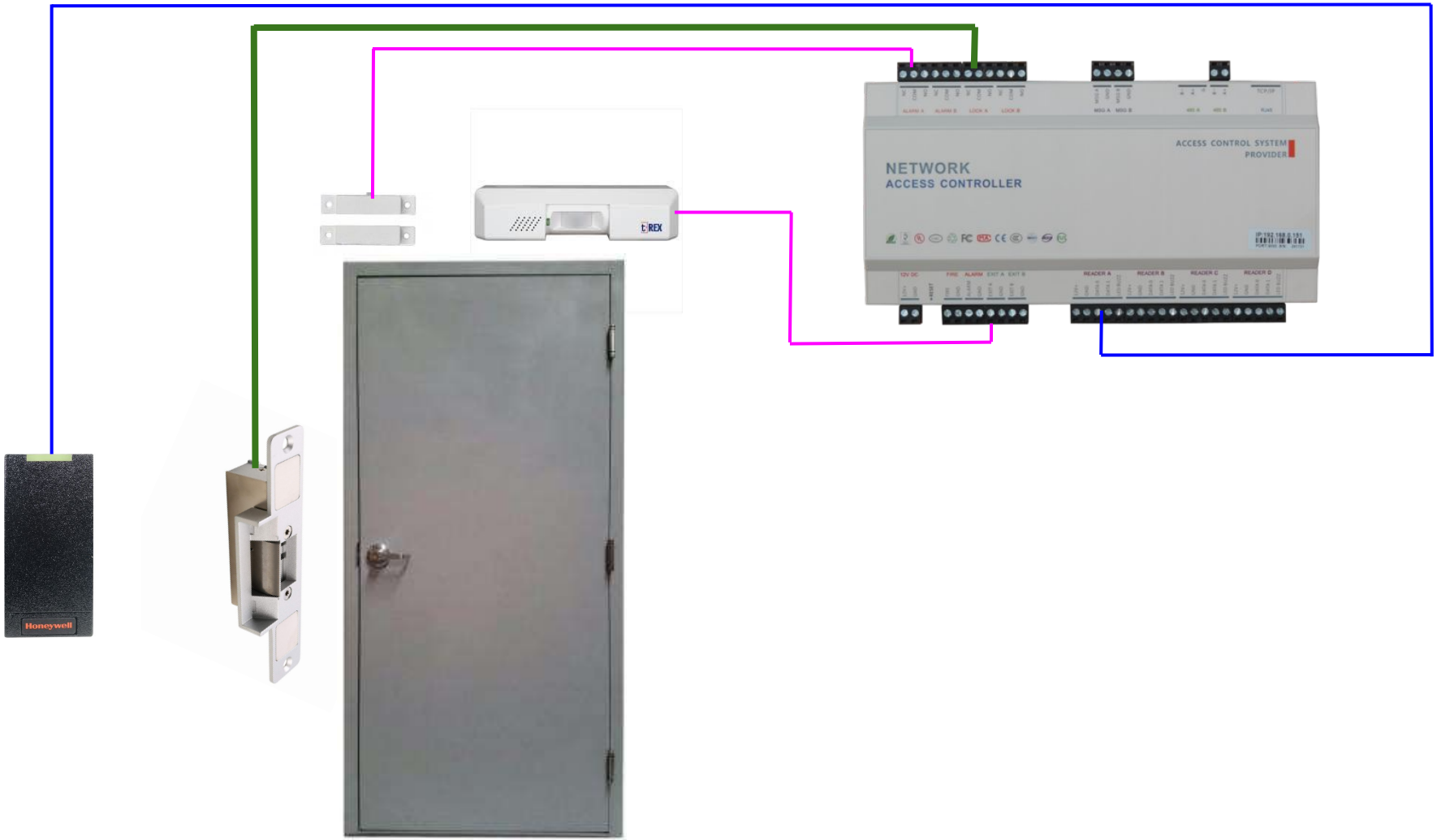

NIGHT BELL
DAY BELL
DAY ENTRY (9AM TO 5PM)
AFTER HOURS ENTRY (5PM)
WELCOME
PLEASE USE OTHER DOOR
What you need to know to help you and your family stay healthy
STOP
OUTBREAK ALERT
AUTOMATIC CAUTION DOOR
PULL
NO SMOKING
NO VAPING
If you need assistance while accessing our services, please see the Receptionist.
Service Animals Welcome
NOTICE
Property Protection System
These Premises are under 24 HOUR Video Surveillance
740


FIRE PANEL
FIRE PANEL RESET
LOCATED IN B-2


Ack/Lamp Tes
AUX. RELAY BY-PASS
BELL BY-PASS
STAIRWELL #3
ELEVATOR MACHINE ROOM
ELEVATOR SHAFT #1
ELEVATOR SHAFT #2
TRANSFORMER VAULT
MAIN ELECTRICAL ROOM
2ND FLOOR CENTRE STAIRWELL
PH GENERATOR ROOM
WET SPRINKLER FLOW
On Line
GENERATOR RUNNING
GENERATOR TROUBLE


Honeywell
NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER


Honeywell
NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER


Honeywell
tREX
NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER

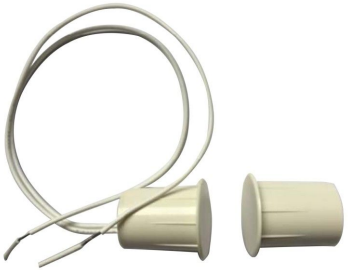

Honeywell
tREX


Honeywell
HID
IEI
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PRS
8 TUV
9 WXY
* 0 OPER #
ACTi


Honeywell


tREX


Honeywell
tREX



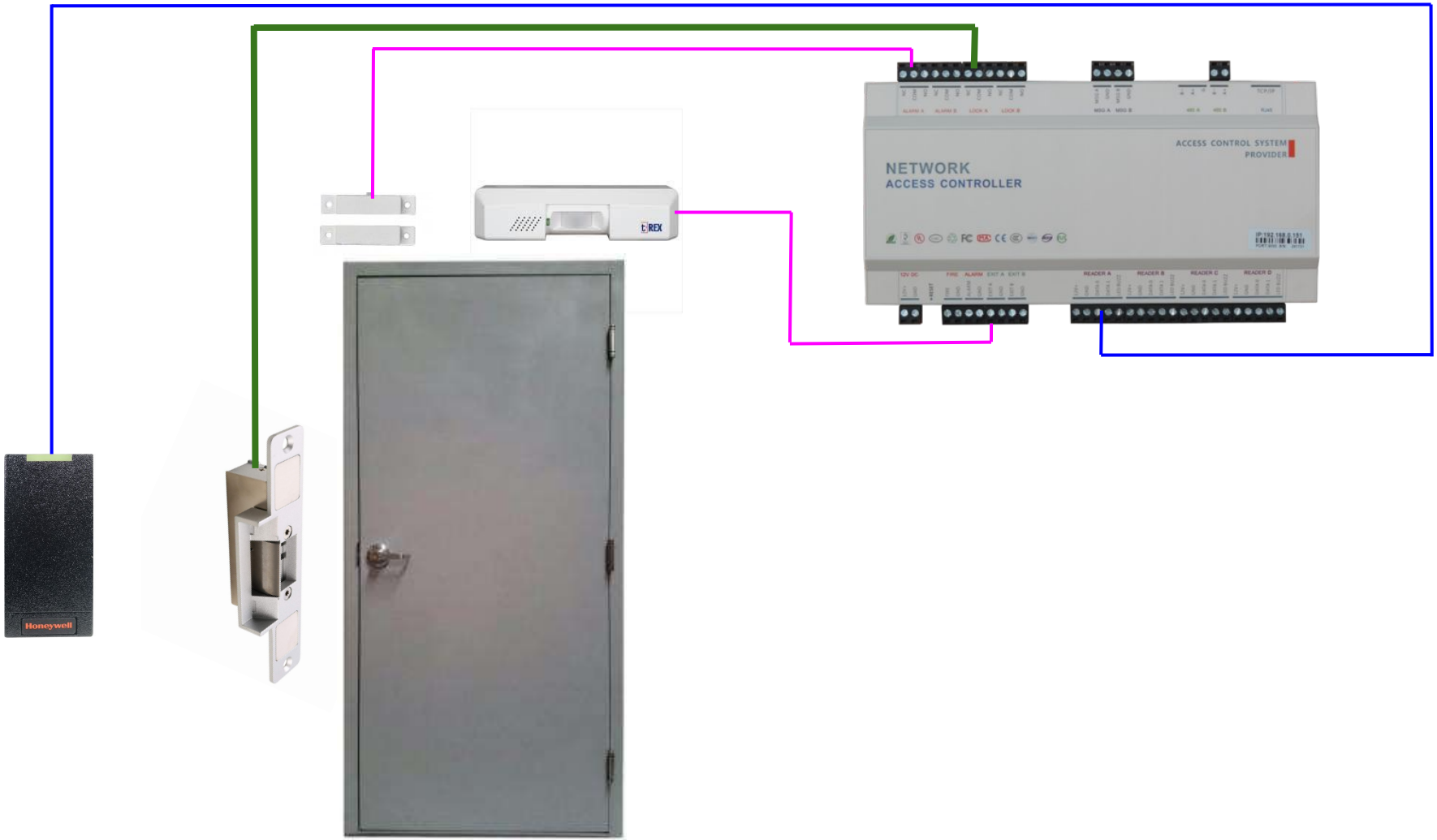

Honeywell
tREX
tREX

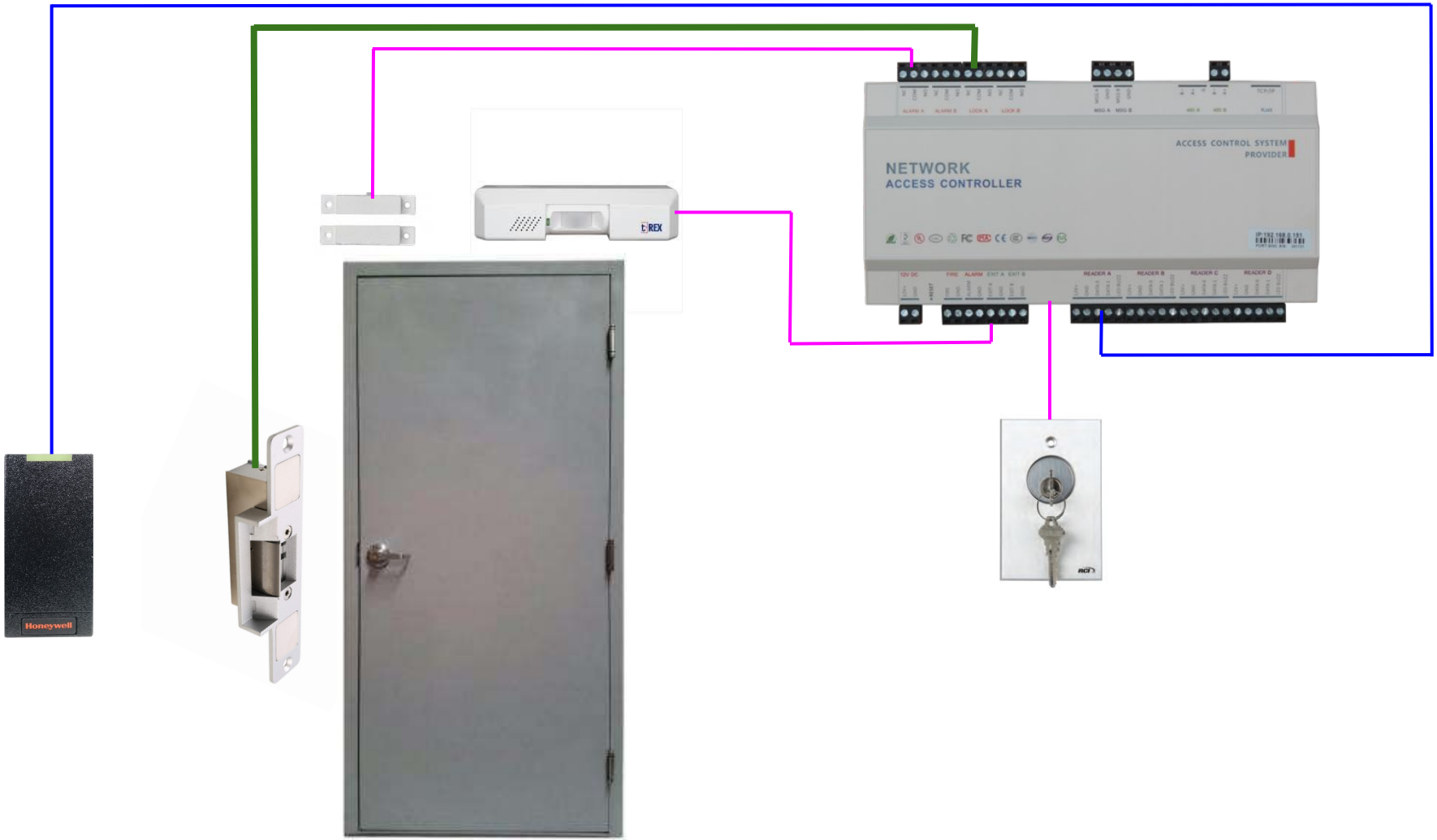

tREX


PUSH
TO
EXIT


PUSH TO EXIT


Honeywell


Honeywell
tREX
NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER


Honeywell
tREX
ACCESS CONTROL SYSTEM
PROVIDER
NETWORK
ACCESS CONTROLLER


NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER
tREX
PRESS
TO OPEN
PRESS
TO OPEN
Honeywell


ACCESS CONTROL SYSTEM
PROVIDER
NETWORK
ACCESS CONTROLLER
tREX
PRESS
TO OPEN
PRESS
TO OPEN
PULL
IN CASE
OF
FIRE
FIRE ALARM CONTROL PANEL
Honeywell


NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER
PRESS
TO OPEN
PRESS
TO OPEN
PULL
IN CASE
OF
FIRE
FIRE ALARM CONTROL PANEL
Honeywell


NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER
PRESS
TO OPEN
PRESS
TO OPEN
PULL
IN CASE
OF
FIRE
FIRE ALARM CONTROL PANEL
Honeywell


NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER
PRESS
TO OPEN
PRESS
TO OPEN
PULL
IN CASE
OF
FIRE
FIRE ALARM CONTROL PANEL
Honeywell


NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER
PRESS
TO OPEN
PRESS
TO OPEN
PULL
IN CASE
OF
FIRE
FIRE ALARM CONTROL PANEL
Honeywell


NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER
PRESS
TO OPEN
PRESS
TO OPEN
PULL
IN CASE
OF
FIRE
FIRE ALARM CONTROL PANEL
Honeywell


NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER
tREX
PRESS
TO OPEN
PRESS
TO OPEN
PULL
IN CASE
OF
FIRE
FIRE ALARM CONTROL PANEL
Honeywell


PUSH
TO OPEN


F/A


F/A
DOOR CONTACTS
SEC JB


BELL PHONE
ONLY
ALARM SYSTEM
DO NOT UNPLUG
IBERVILLE
BC52-C


SECURITY SYSTEM RM.


PUSH
TO OPEN


OKS
DOORKING

Red Team Attacks - Binary Sensor Comms Lines - Normally Closed

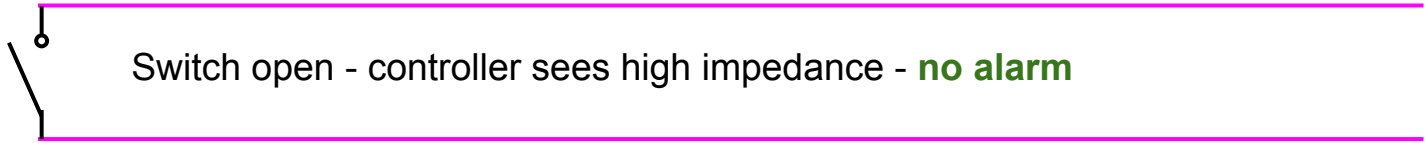
Switch closed - controller sees low impedance - **no alarm**

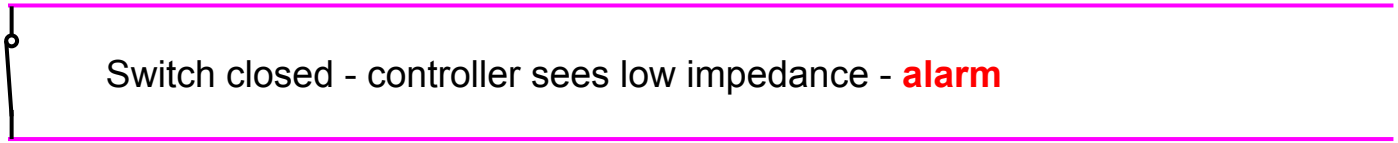
Switch open - controller sees high impedance - **alarm**

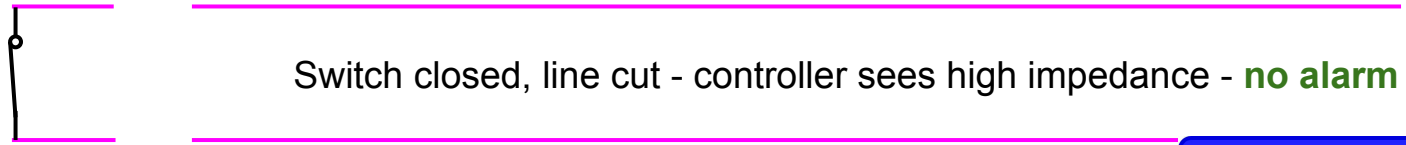
Switch open, line jumpered - controller sees low impedance - **no alarm**

Demo →

Red Team Attacks - Binary Sensor Comms Lines - Normally Open

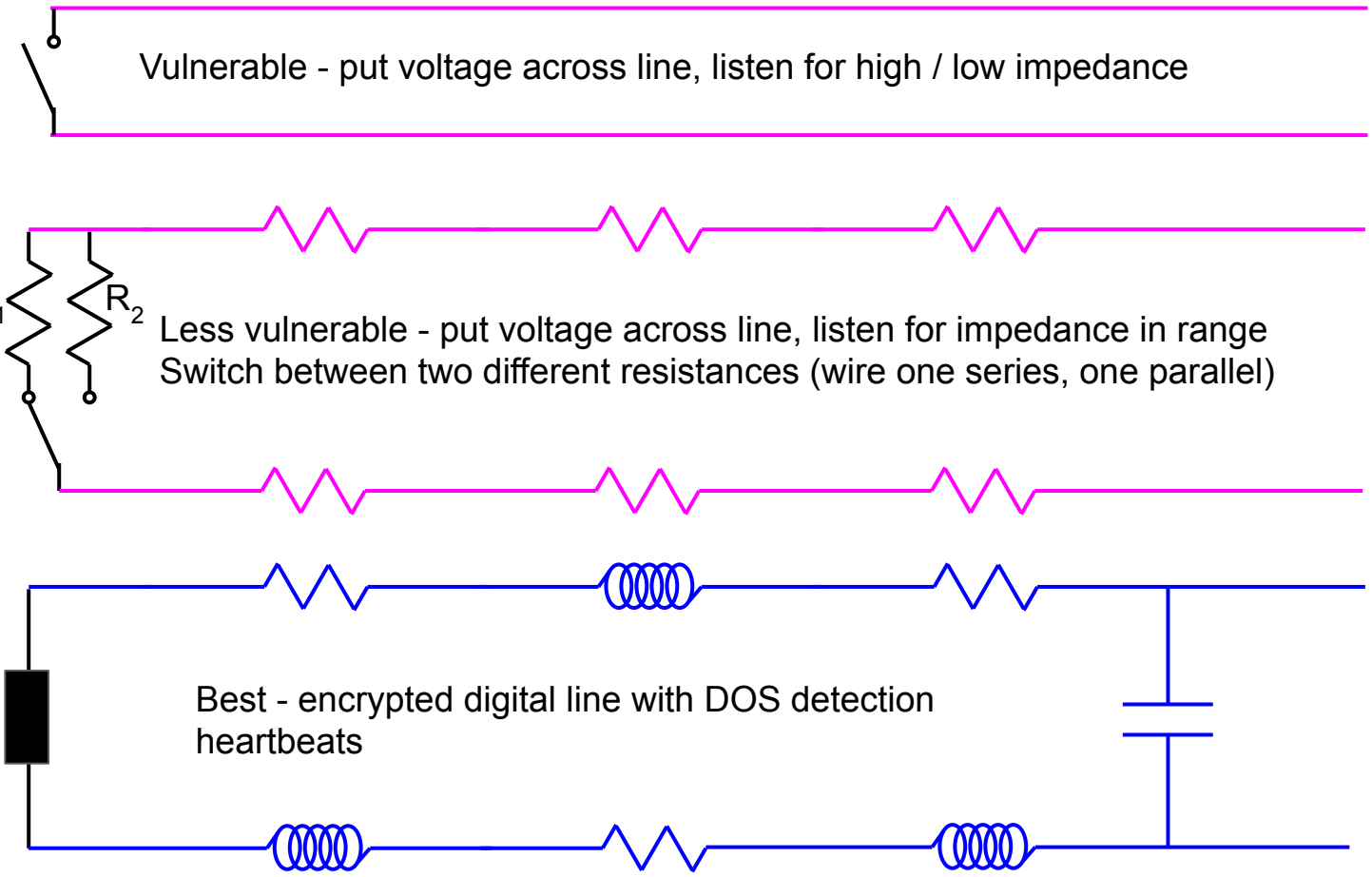






Demo →

Blue Team Defense - Binary Sensor Comms Lines



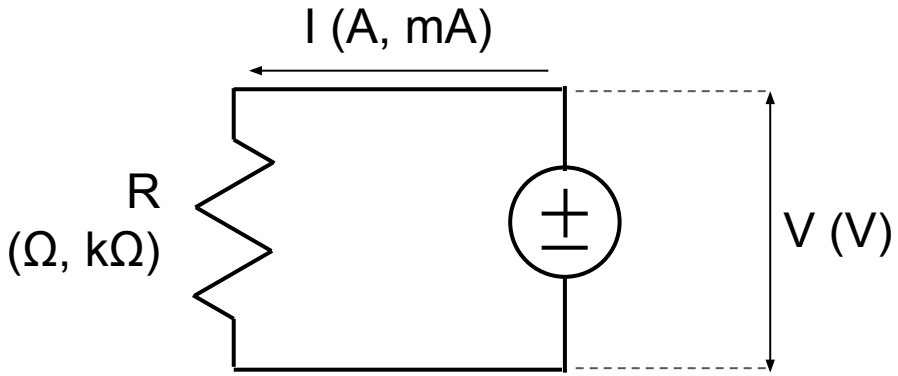
EOLR

End-of-line Resistors

Two Approaches

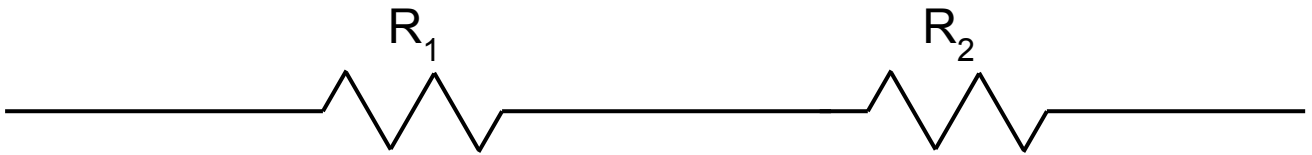
1) Surrogate Resistor
2) Voltage Regulation

Resistor Review (Slide 1 of 3)



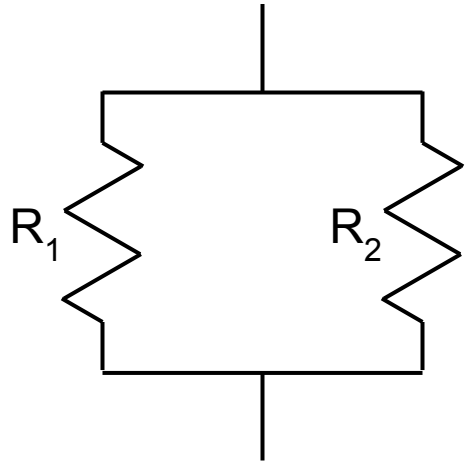
$$R = \frac{V}{I}$$

Resistor Review (Slide 2 of 3)

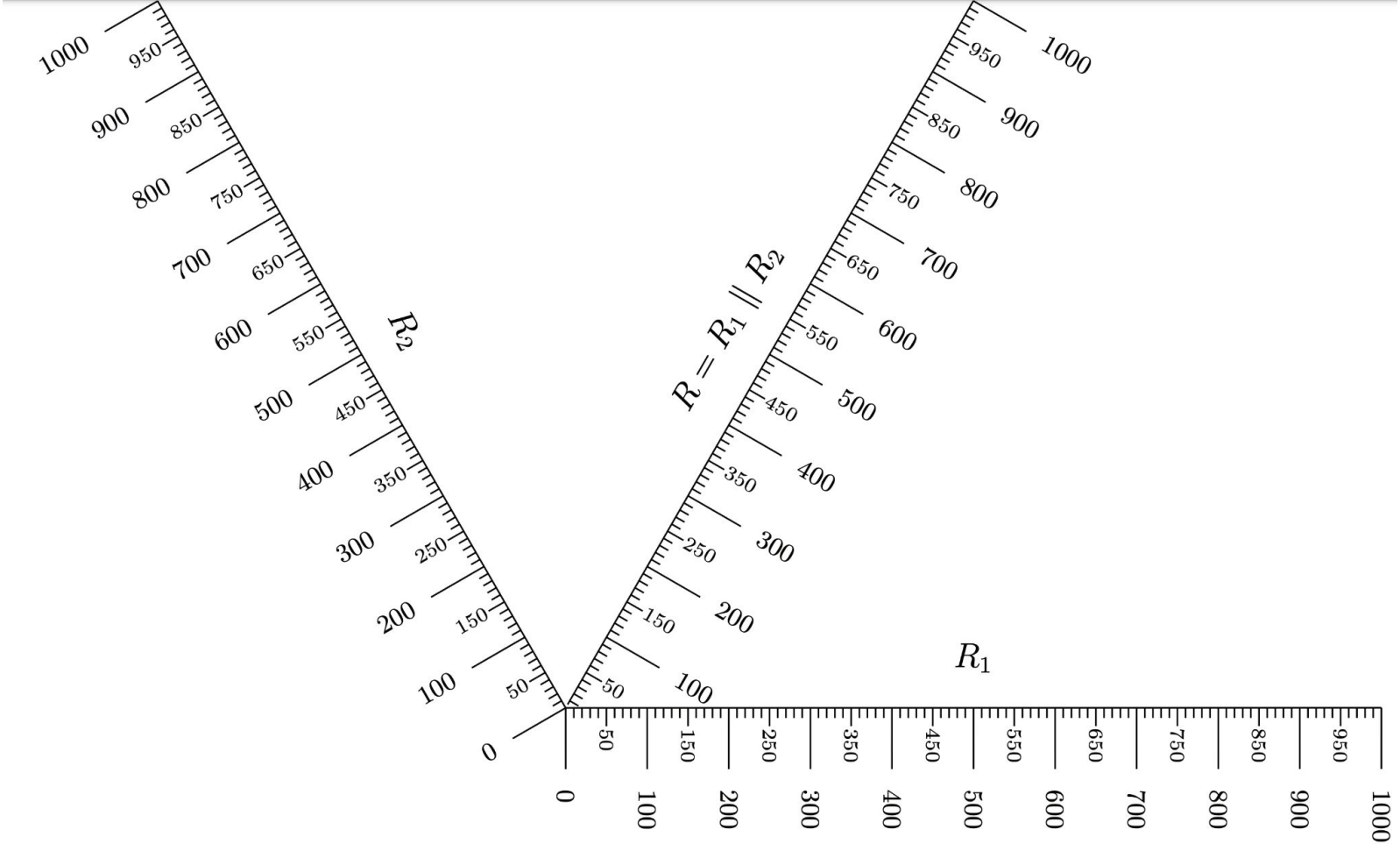


$$R_{equivalent} = R_1 + R_2$$

Resistor Review (Slide 3 of 3)

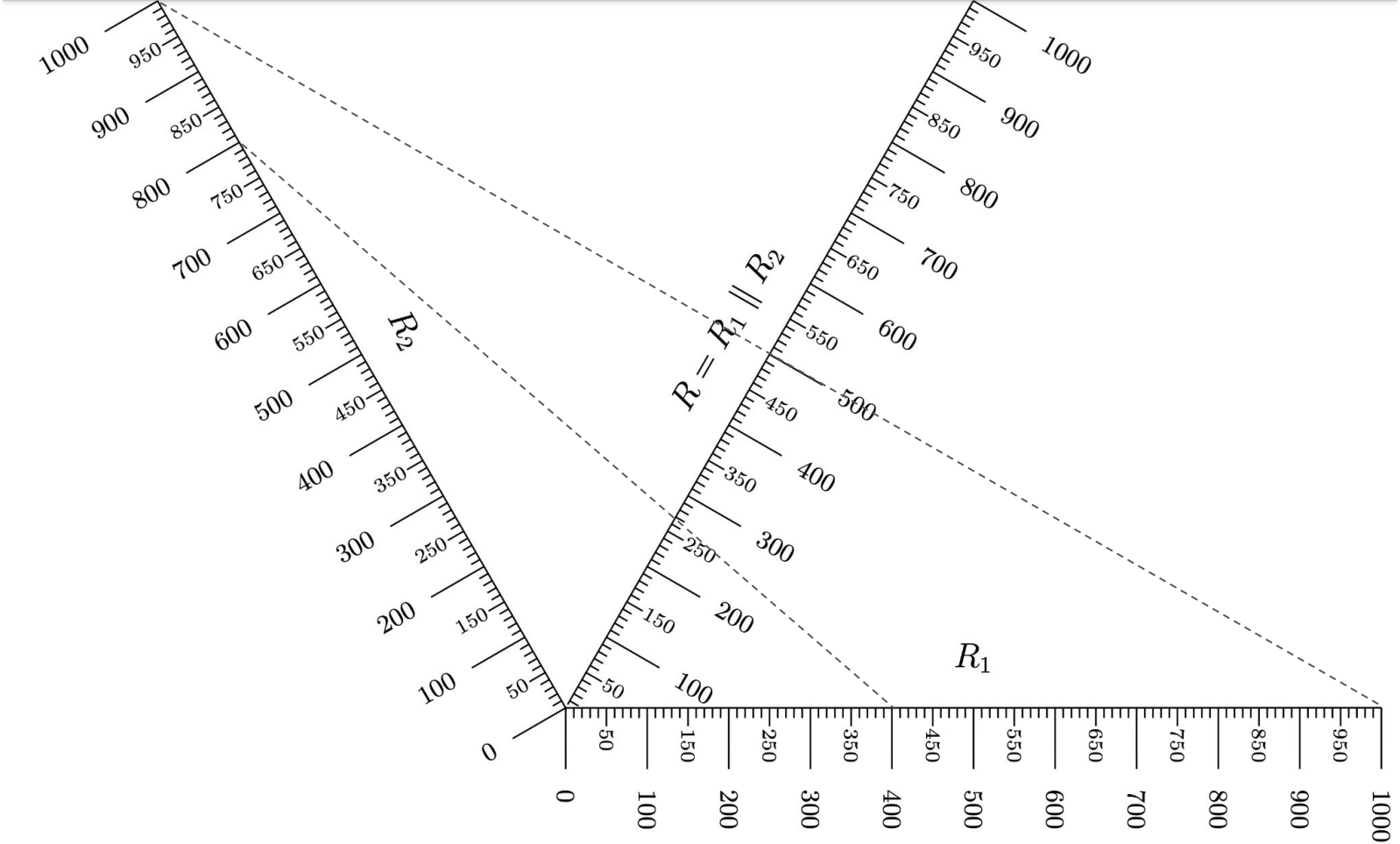


$$\frac{1}{R_{equivalent}} = \frac{1}{R_1} + \frac{1}{R_2}$$



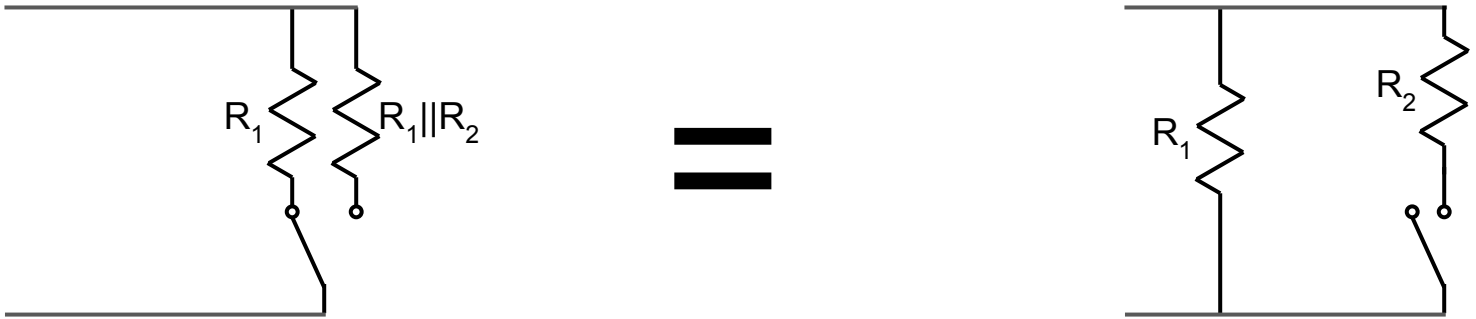
Equivalent Resistance of Two Resistors in Parallel

$$1/R = 1/R_1 + 1/R_2$$

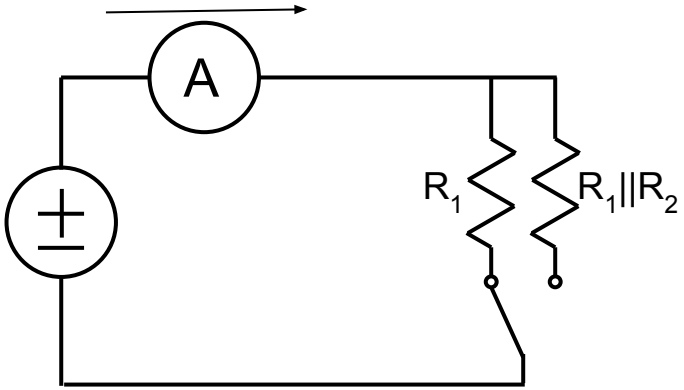


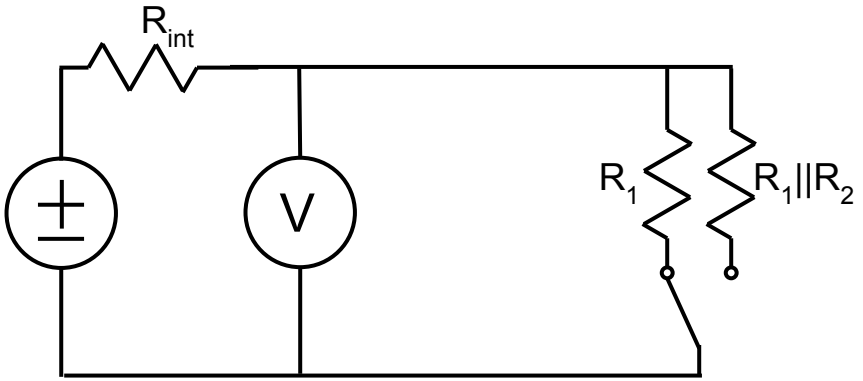
Equivalent Resistance of Two Resistors in Parallel

$$1/R = 1/R_1 + 1/R_2$$

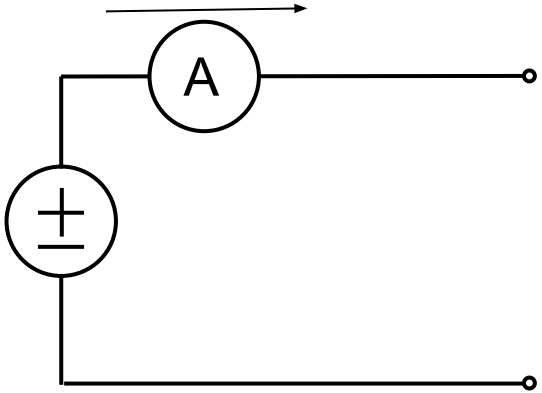

R1
R1||R2
=
R1
R2

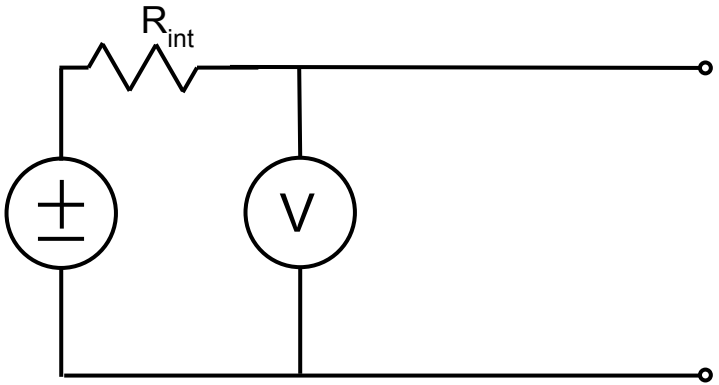
How does the controller measure resistance?



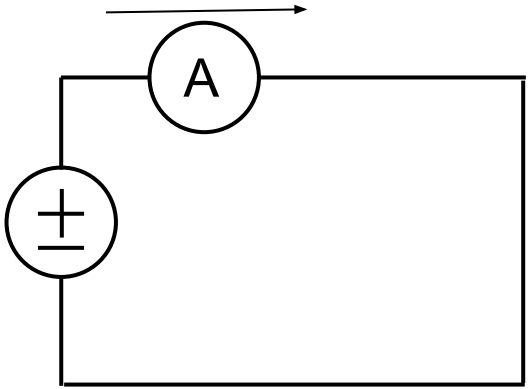


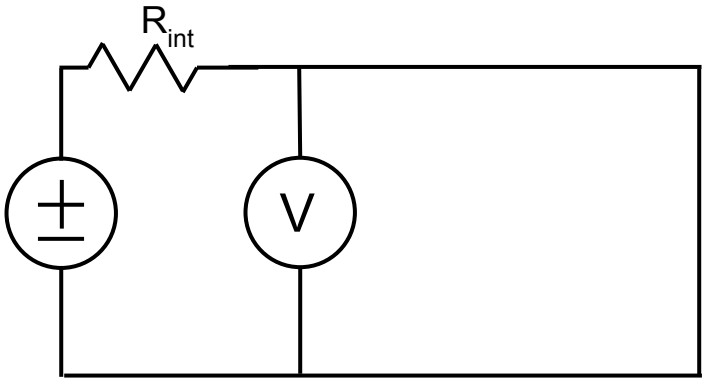
Special case: open circuit (line cut)



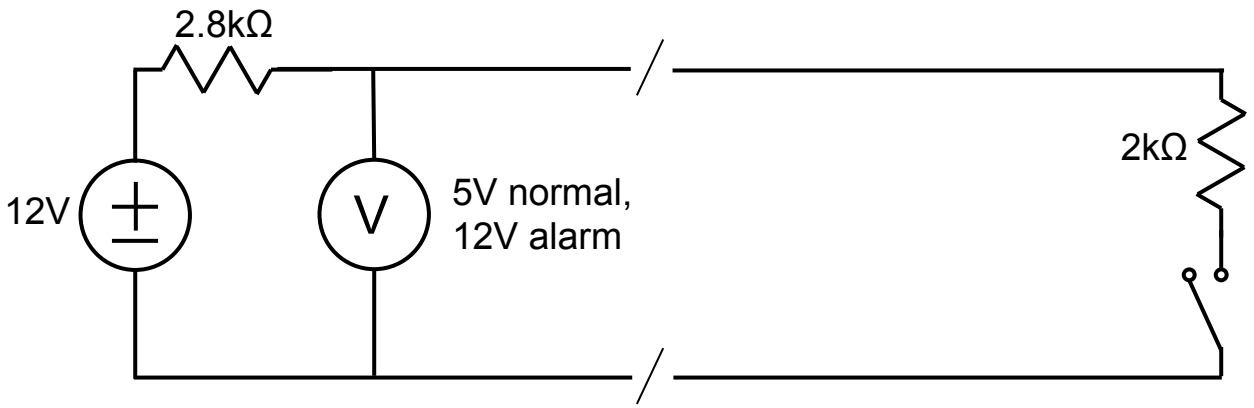


Special case: short circuit (line jumpered)





E.g. Honeywell




Simplex
SIG-51
EOL
Simplex
SIG-76
EOL
Simplex


END - OF - LINE
DEVICE
END - OF - LINE
DEVICE


H/S P2 EOL
FIRE FIGHTER'S TELEPHONE
TÉLÉPHONE DE POMPIER
IN CASE OF FIRE
DO NOT USE ELEVA
REMAIN CAL


DO NOT PAINT
H/S P2 EOL

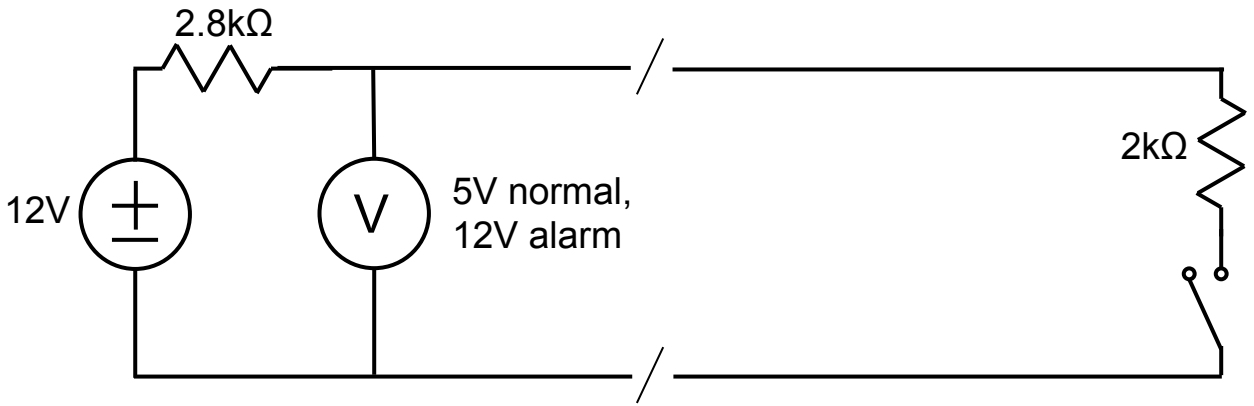
T.P.
+
–
12VDC
RELAY
N.C.
TAMPER
N.C.

SRN-2000/S
LED
SUPER
R.F.
PROTECTION
pattern
min
max
TAMPER
N.O
12V
TP

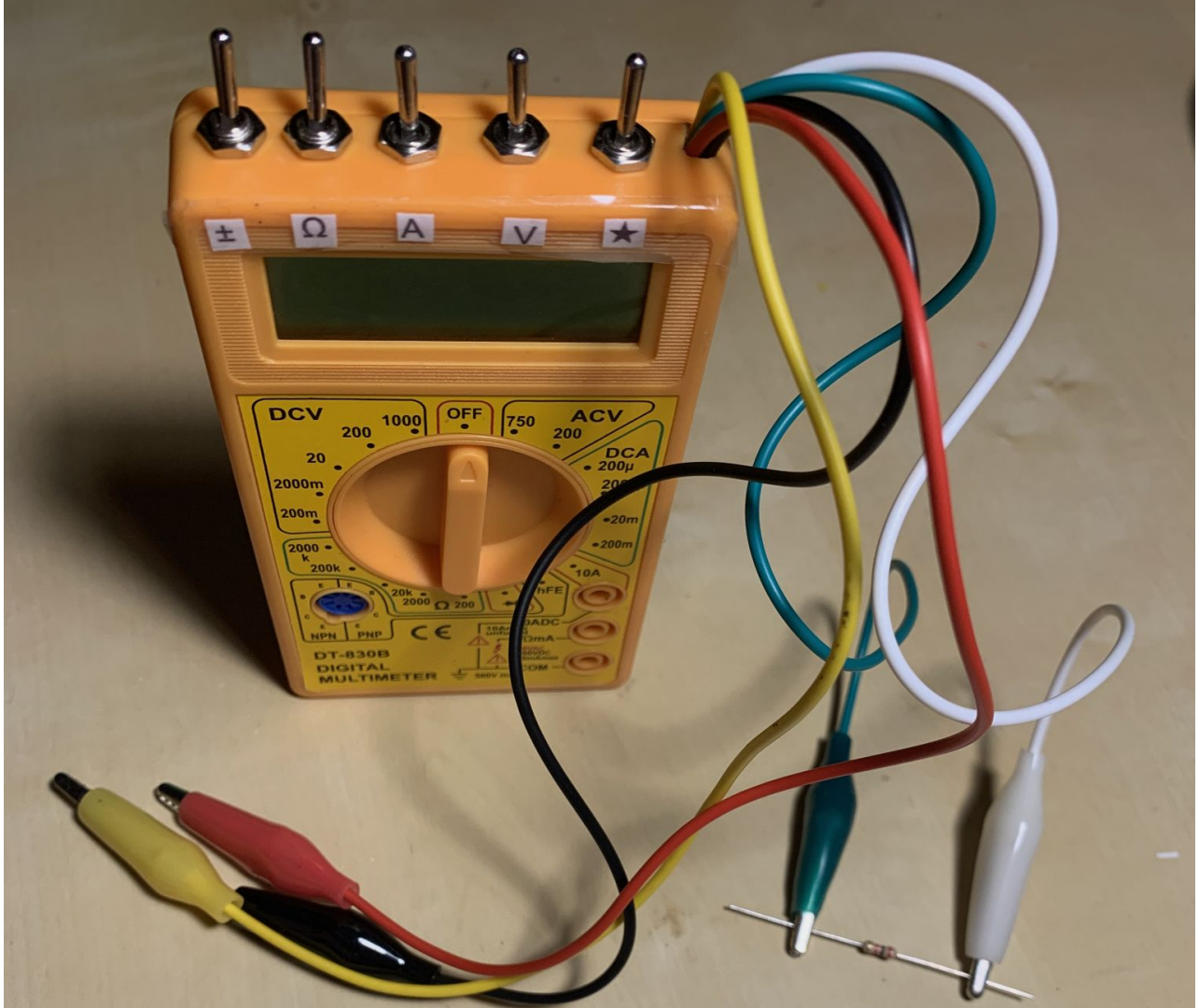
T.P.
+
−
12VDC
RELAY
N.C.
TAMPER
N.C.

SRN-2000/S
TAMPER
N.O
12V
TP

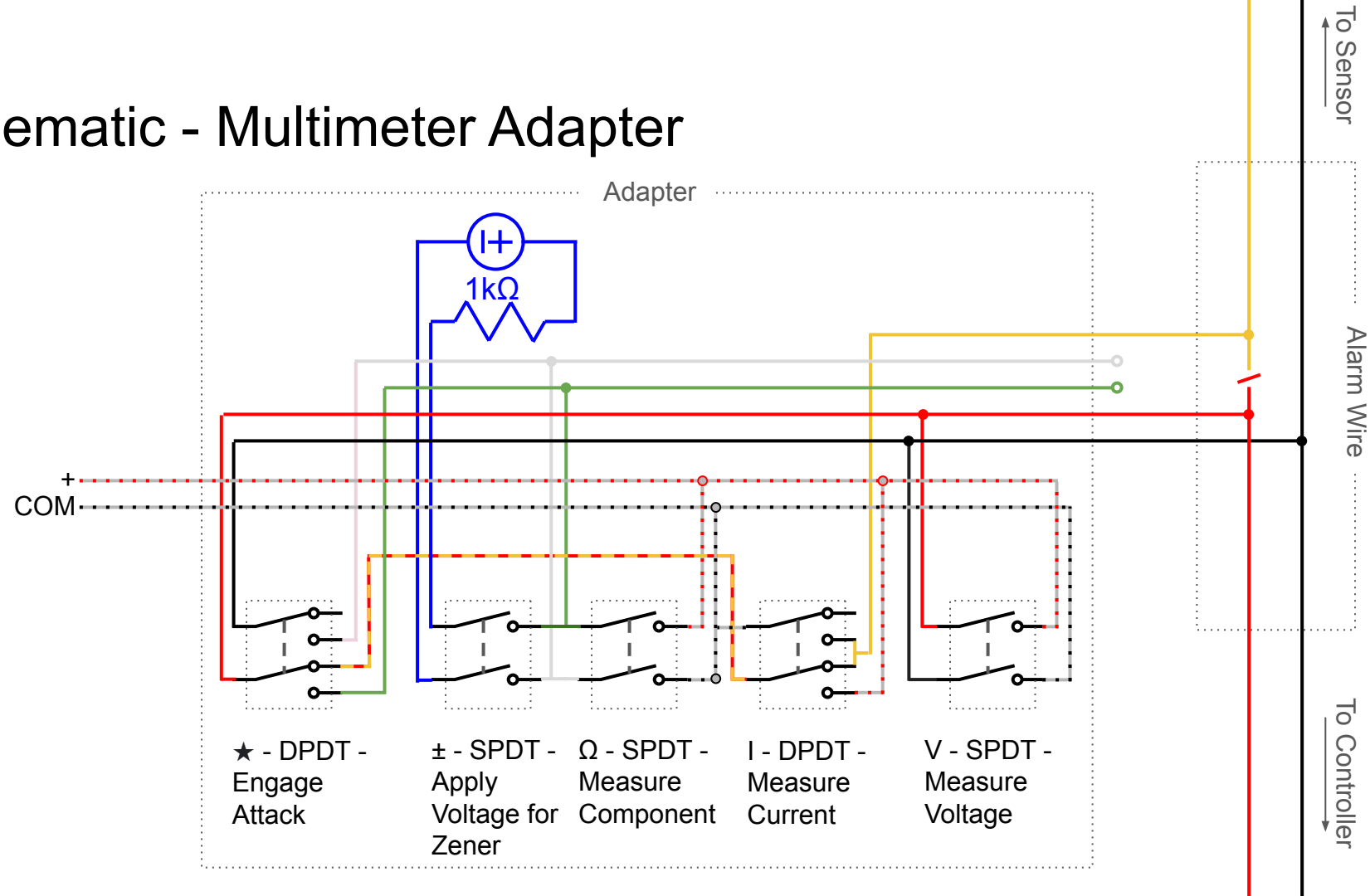
Attacking the EOLRs

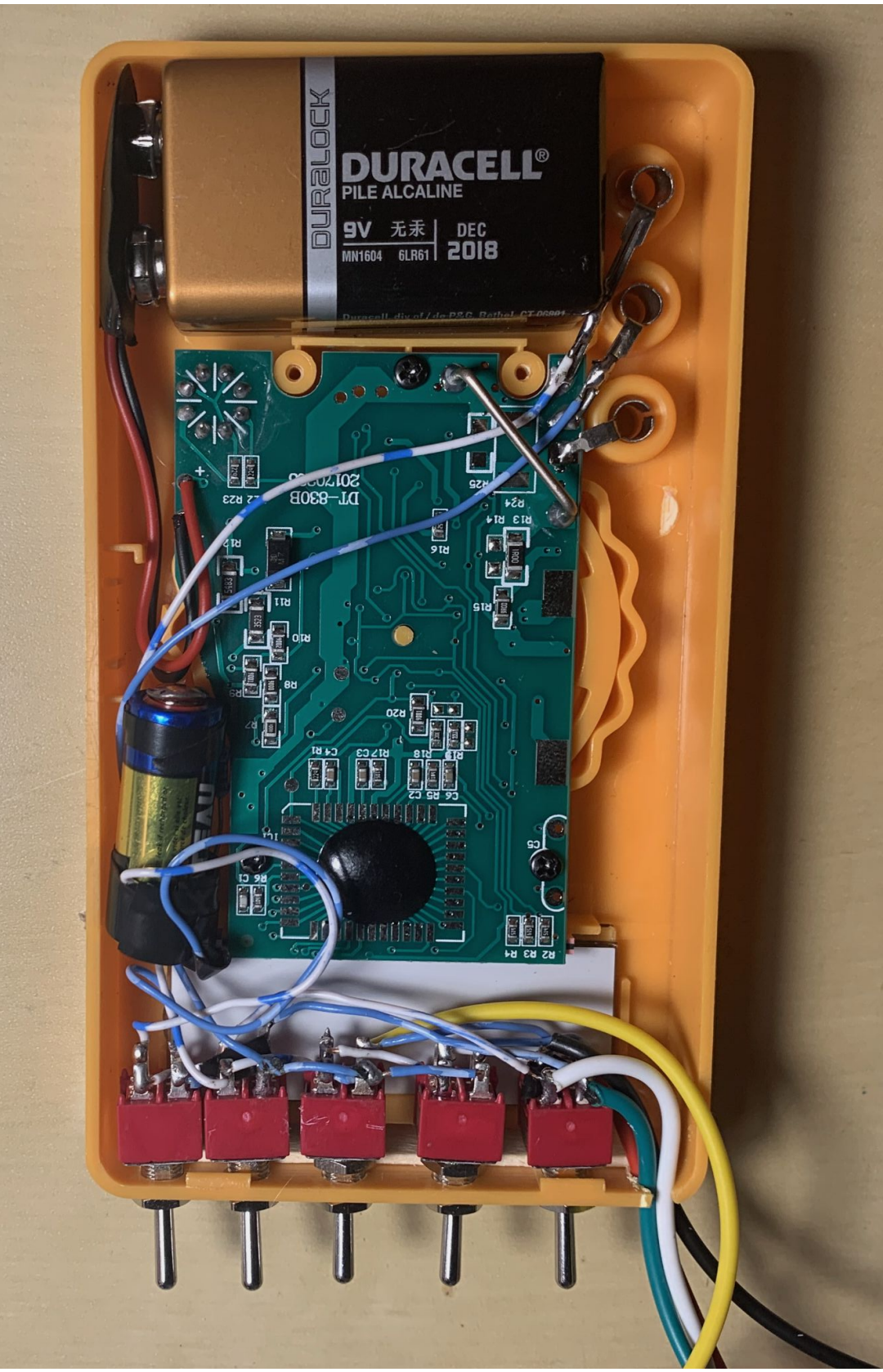


Demo →


±
Ω
A
V
★
DCV
1000
200
20
2000m
200m
OFF
750
ACV
200
DCA
200µ
20m
200m
10A
2000
k
200k
20k
2000
200
hFE
NPN
PNP
DT-830B
DIGITAL
MULTIMETER

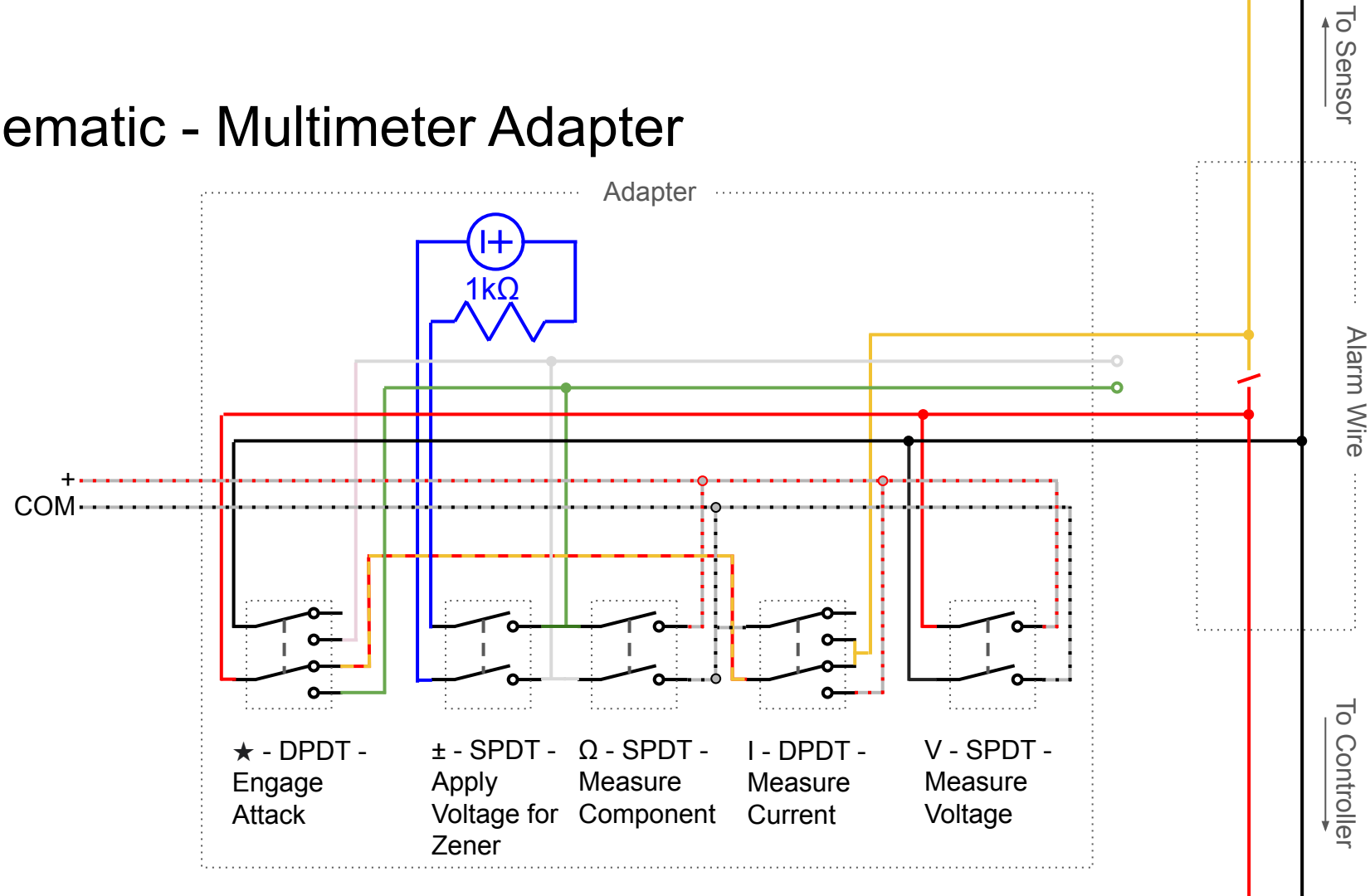
Schematic - Multimeter Adapter




DURALOCK
DURACELL®
PILE ALCALINE
9V 无汞
MN1604 6LR61
DEC
2018
DT-830B

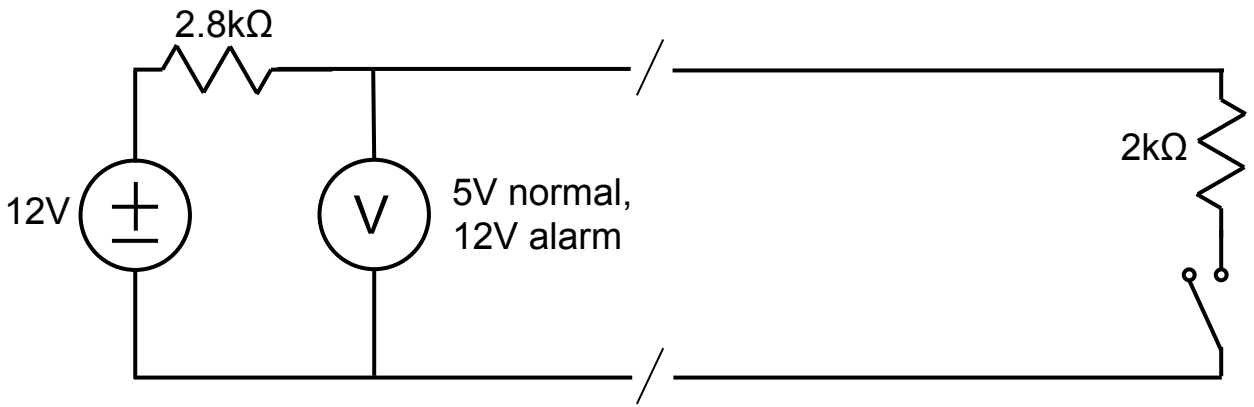
Demo →
DURACELL
PILE ALCALINE
9V
DEC
2018
DURALOCK
DT-830B

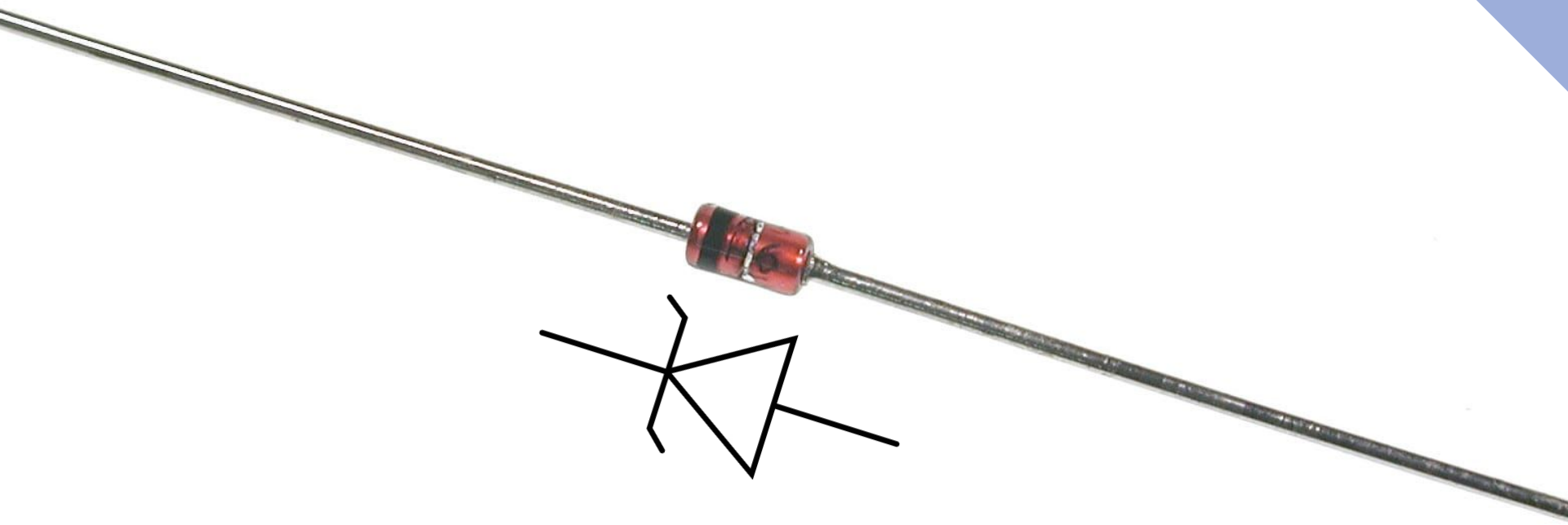
Schematic - Multimeter Adapter

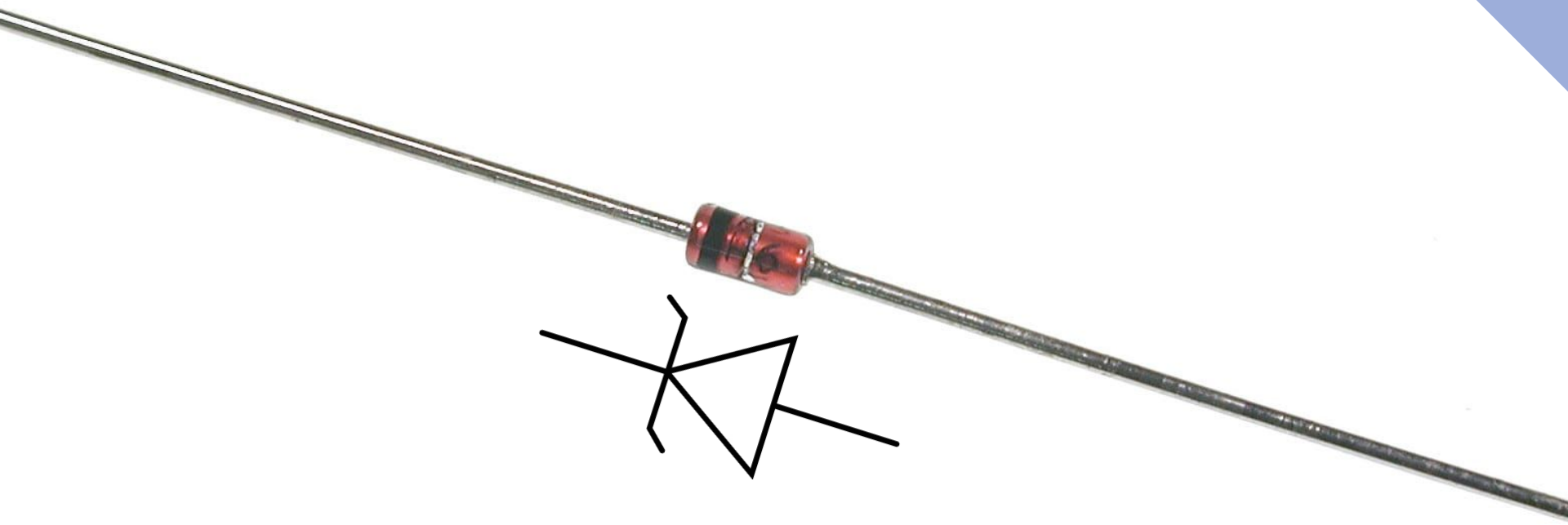


Can we do Better?

Can we do Better?







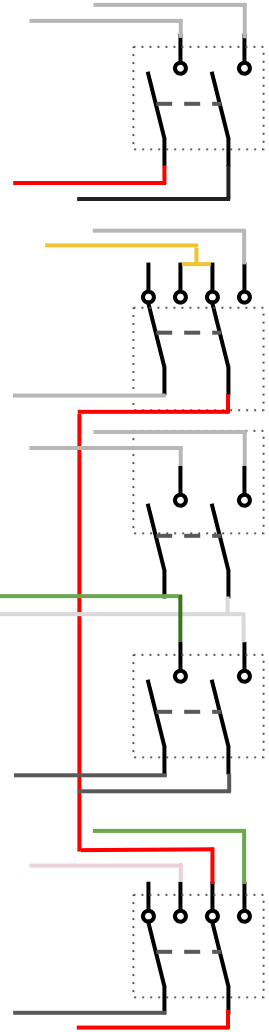
Demo →

Zener: effect changes with temperature; not well suited for outdoor applications if a high breakdown voltage (Avalanche effect dominates)

5.6V breakdown: Zener and Avalanche effect approximately equal, temperature coefficients cancel.

Low breakdown voltage: Zener effect dominates; much more rounded knee at breakdown. Less well suited - use resistive if possible.

Schematic - Multimeter Adapter



1 - SPDT - Measure Voltage

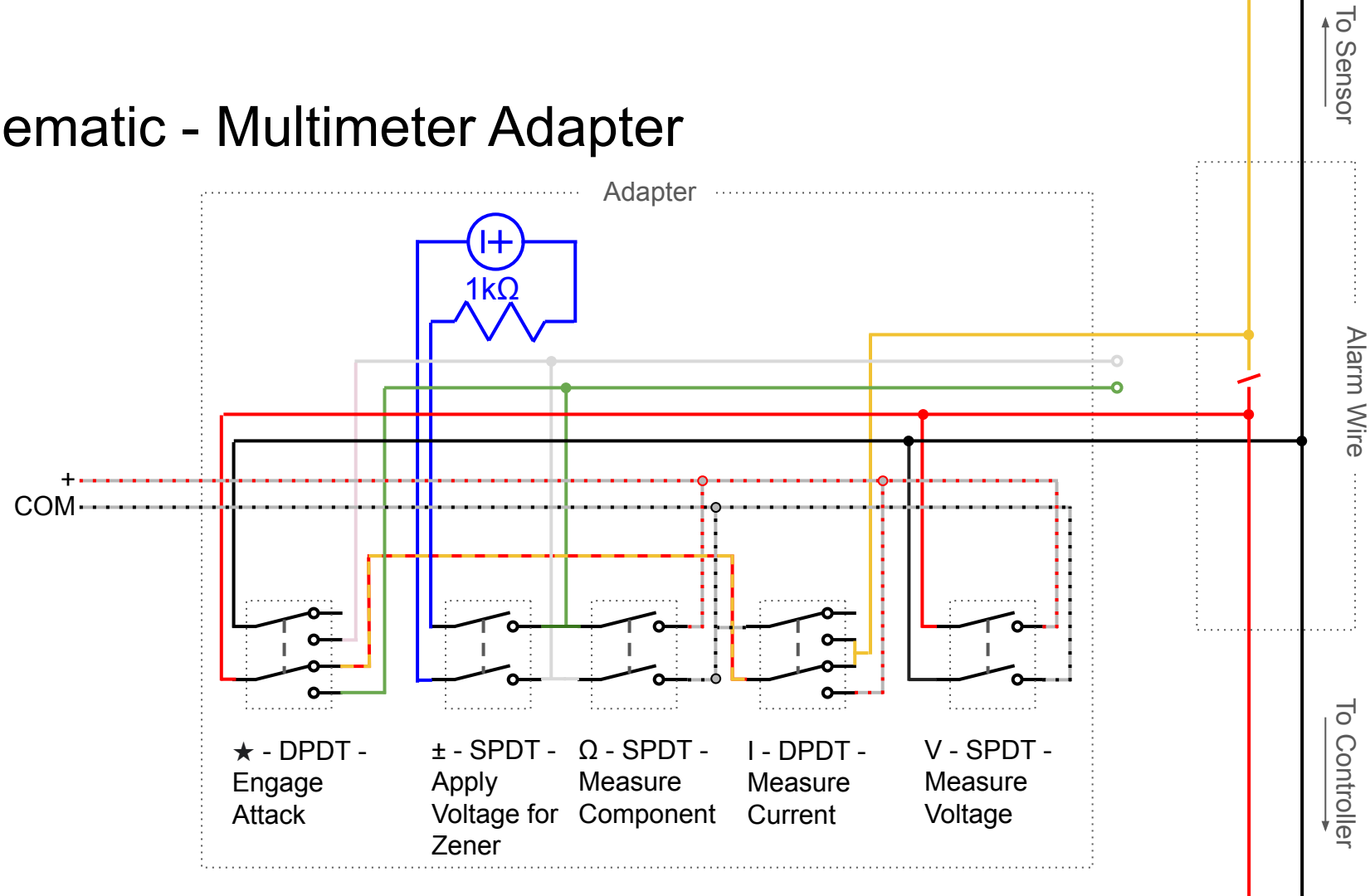
2 - DPDT - Measure Current

3 - SPDT - Measure Component

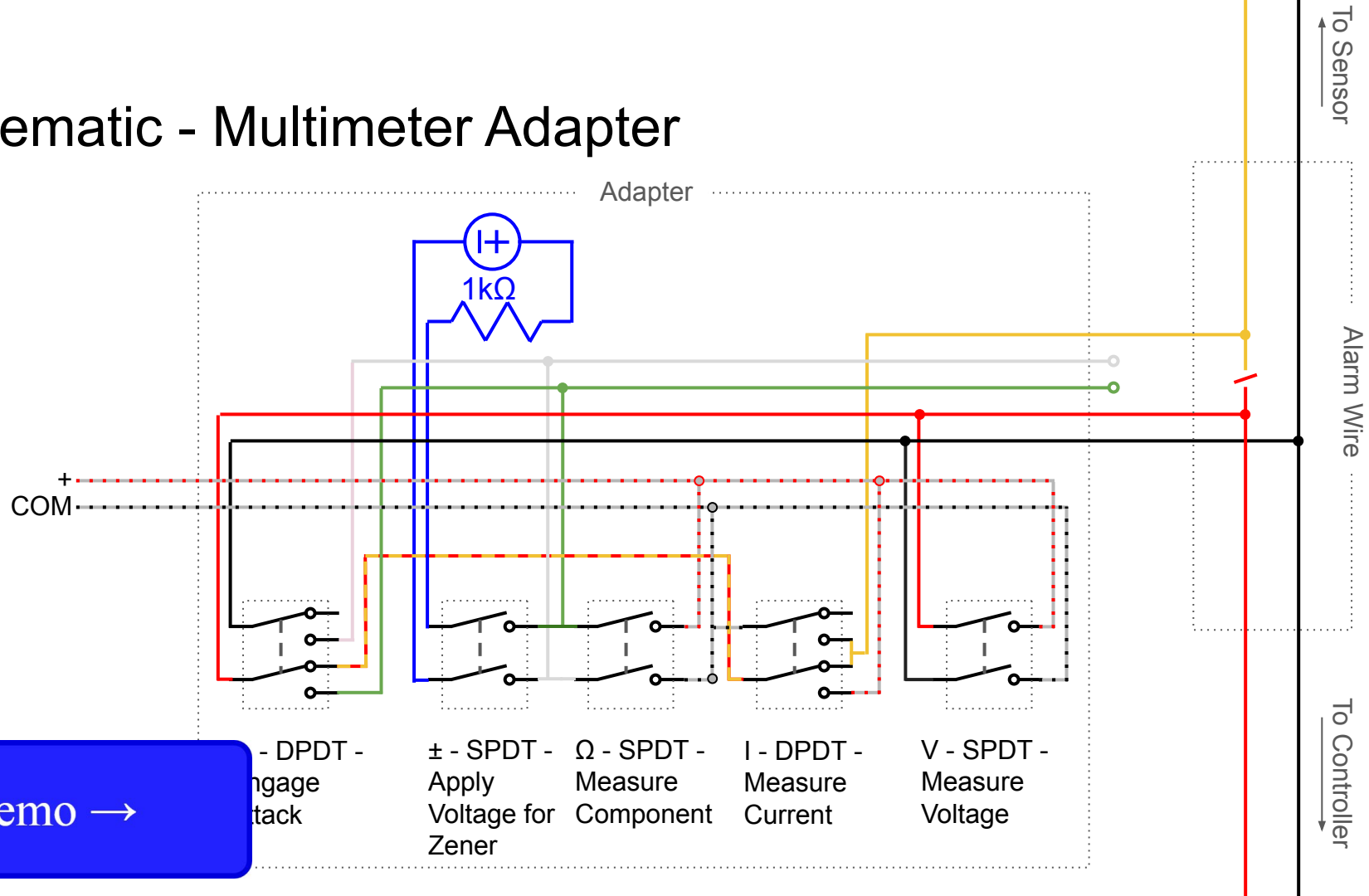
4 - SPDT - Apply Voltage for Zener Breakdown

5 - DPDT - Engage Attack

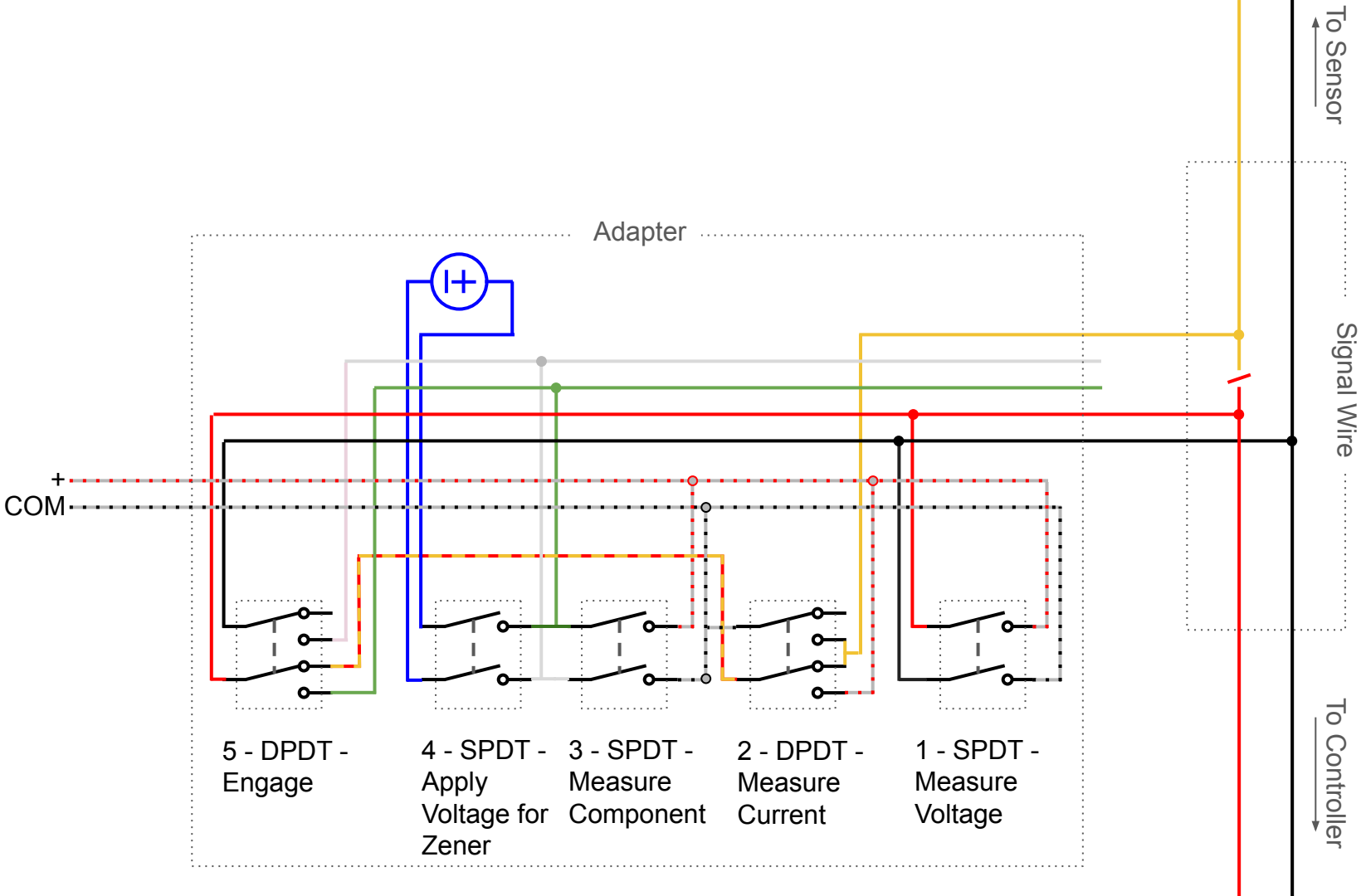
Schematic - Multimeter Adapter



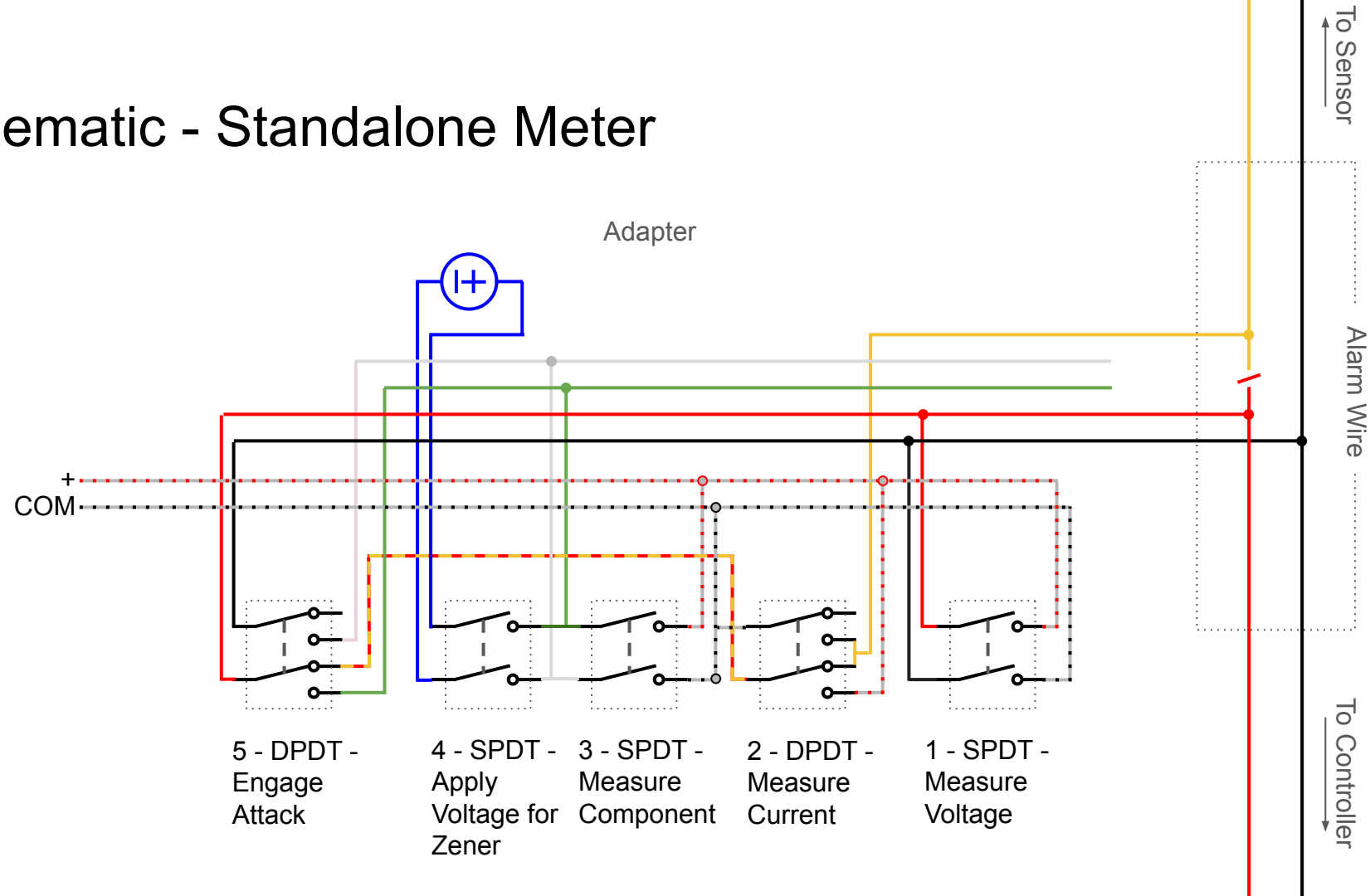
Schematic - Multimeter Adapter



Demo →

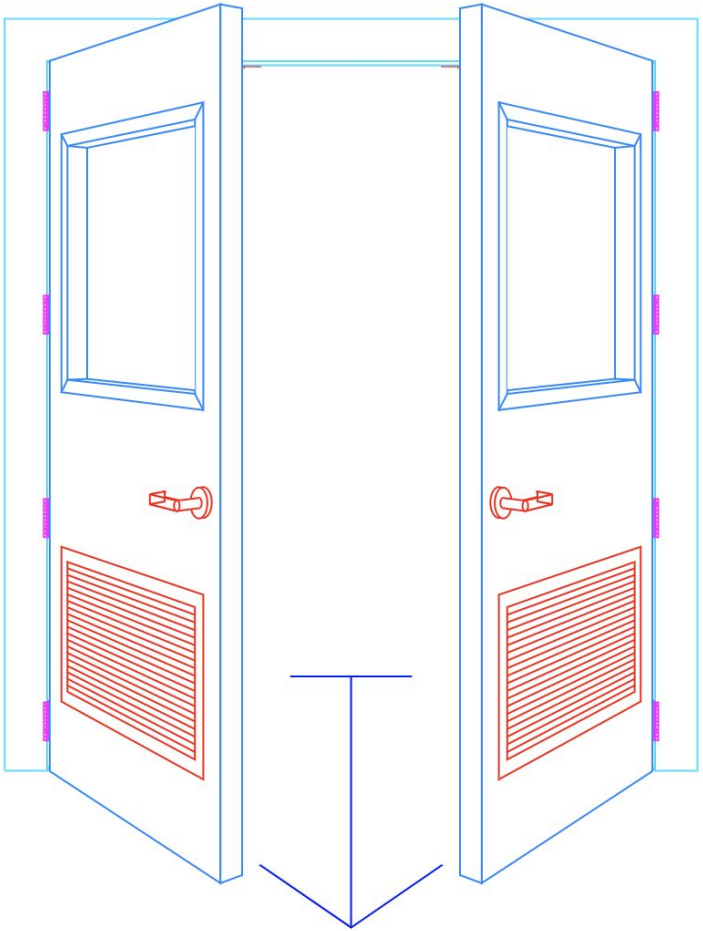

To Sensor
Signal Wire
To Controller
Adapter
+
COM
5 - DPDT - Engage
4 - SPDT - Apply Voltage for Zener
3 - SPDT - Measure Component
2 - DPDT - Measure Current
1 - SPDT - Measure Voltage

Schematic - Standalone Meter

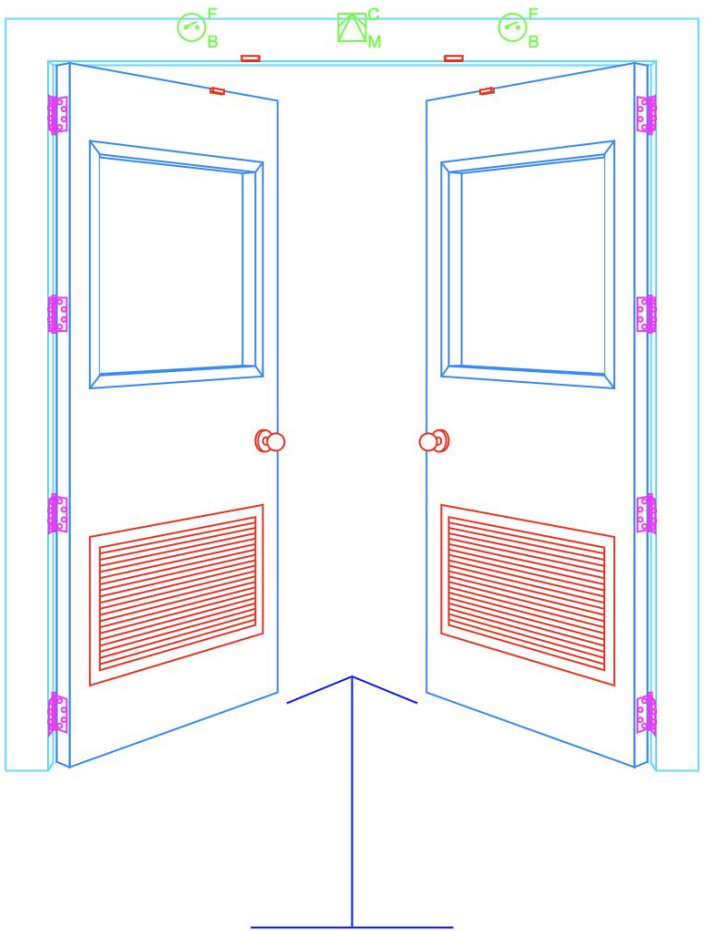


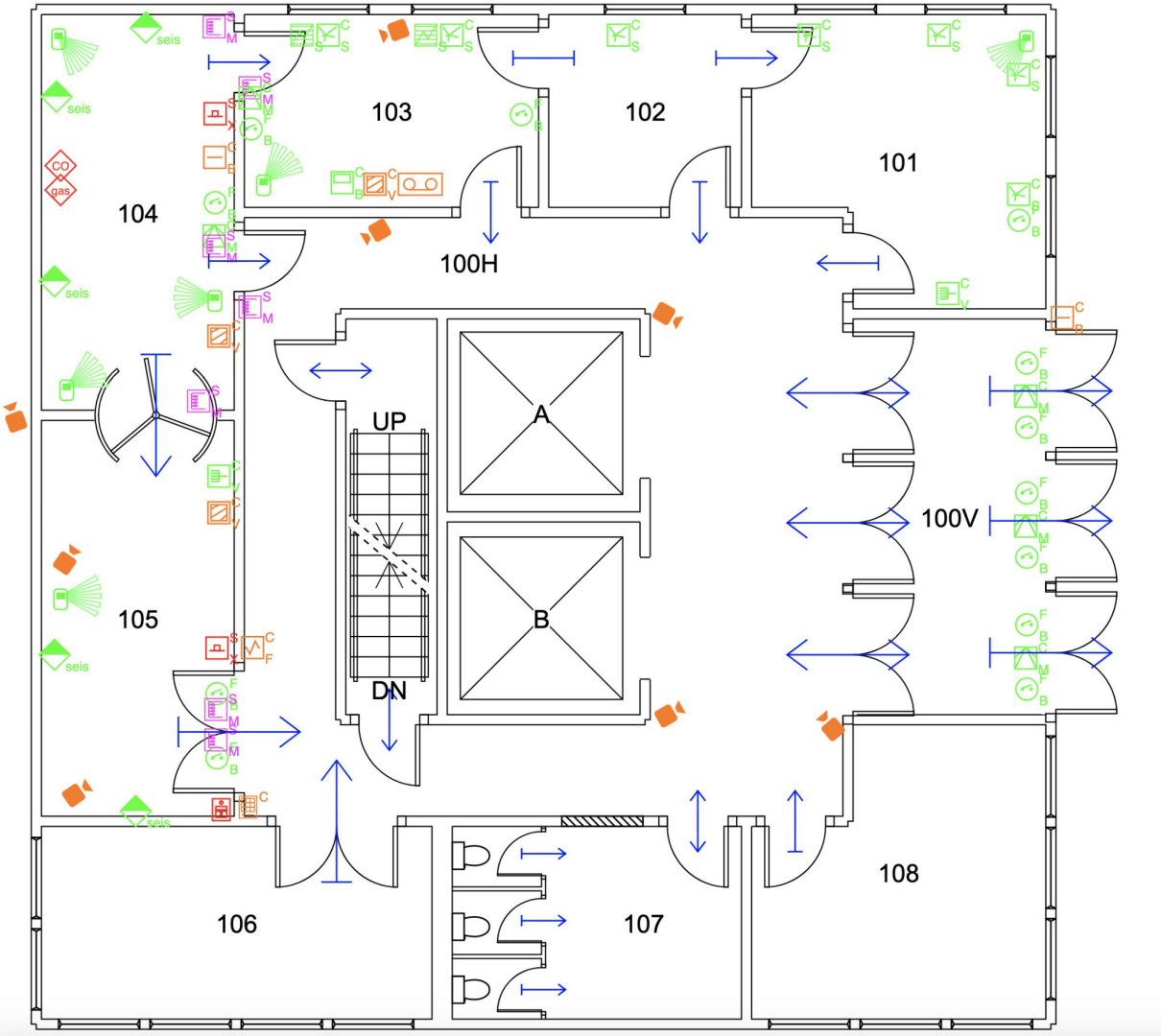
Defences

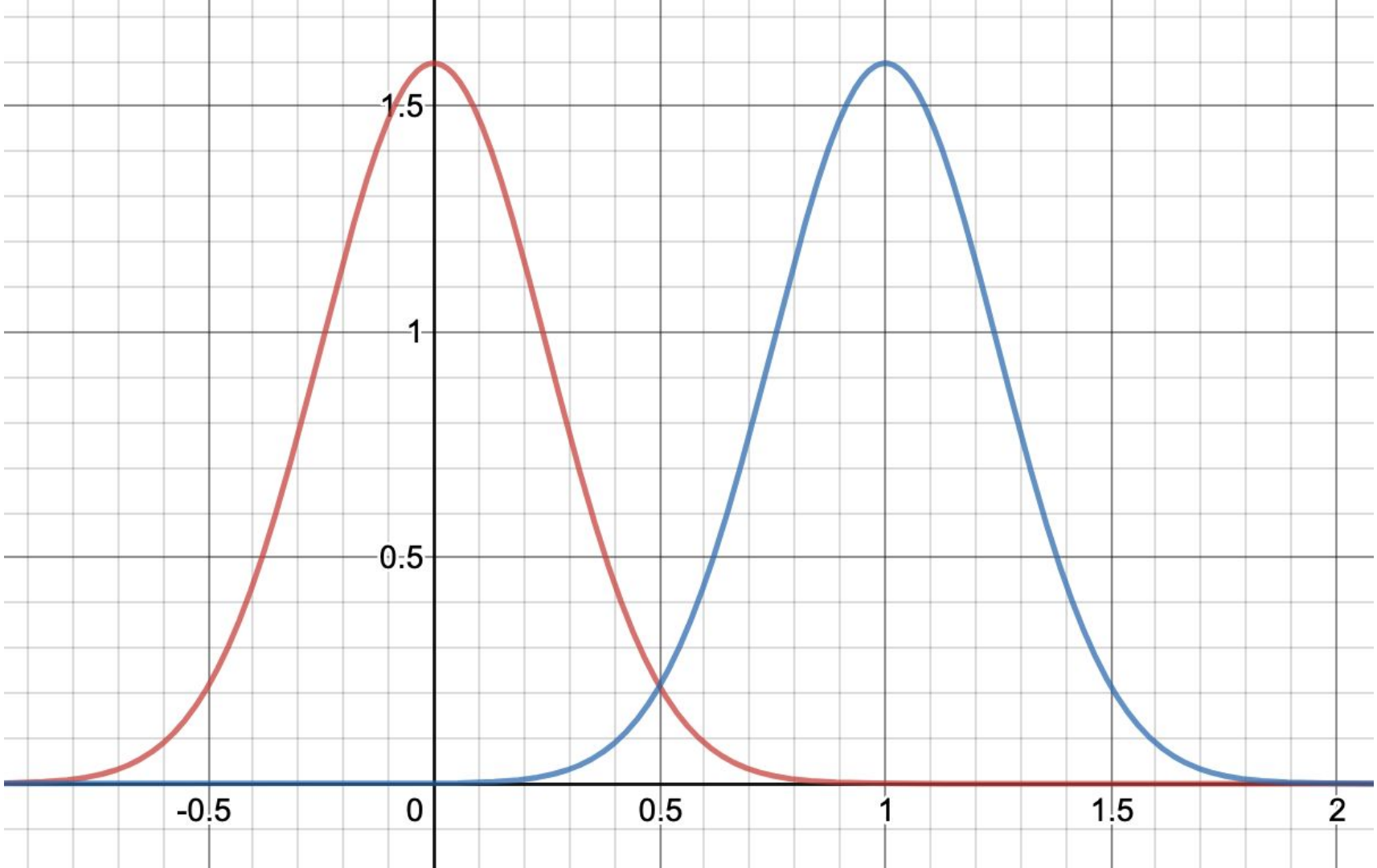
Side A



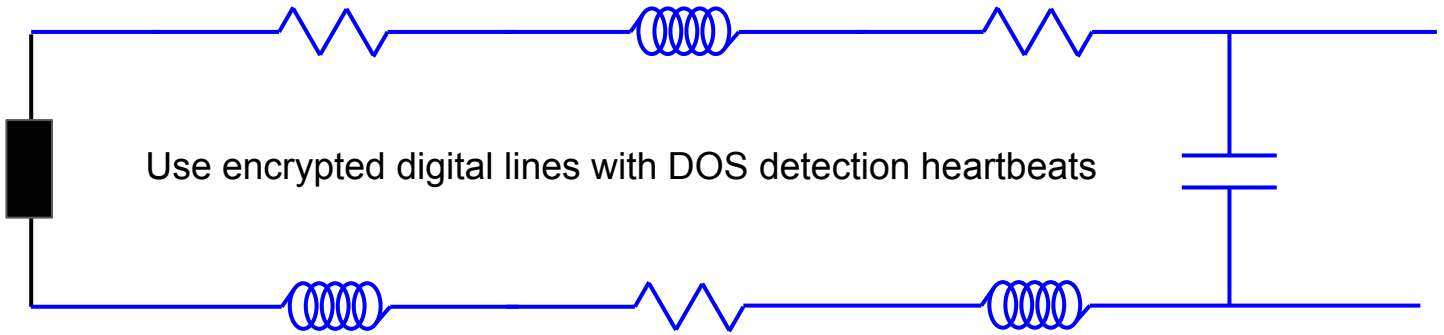
Side B




103
102
101
104
100H
UP
A
100V
105
B
DN
106
107
108


1.5
1
0.5
-0.5
0
0.5
1
1.5
2

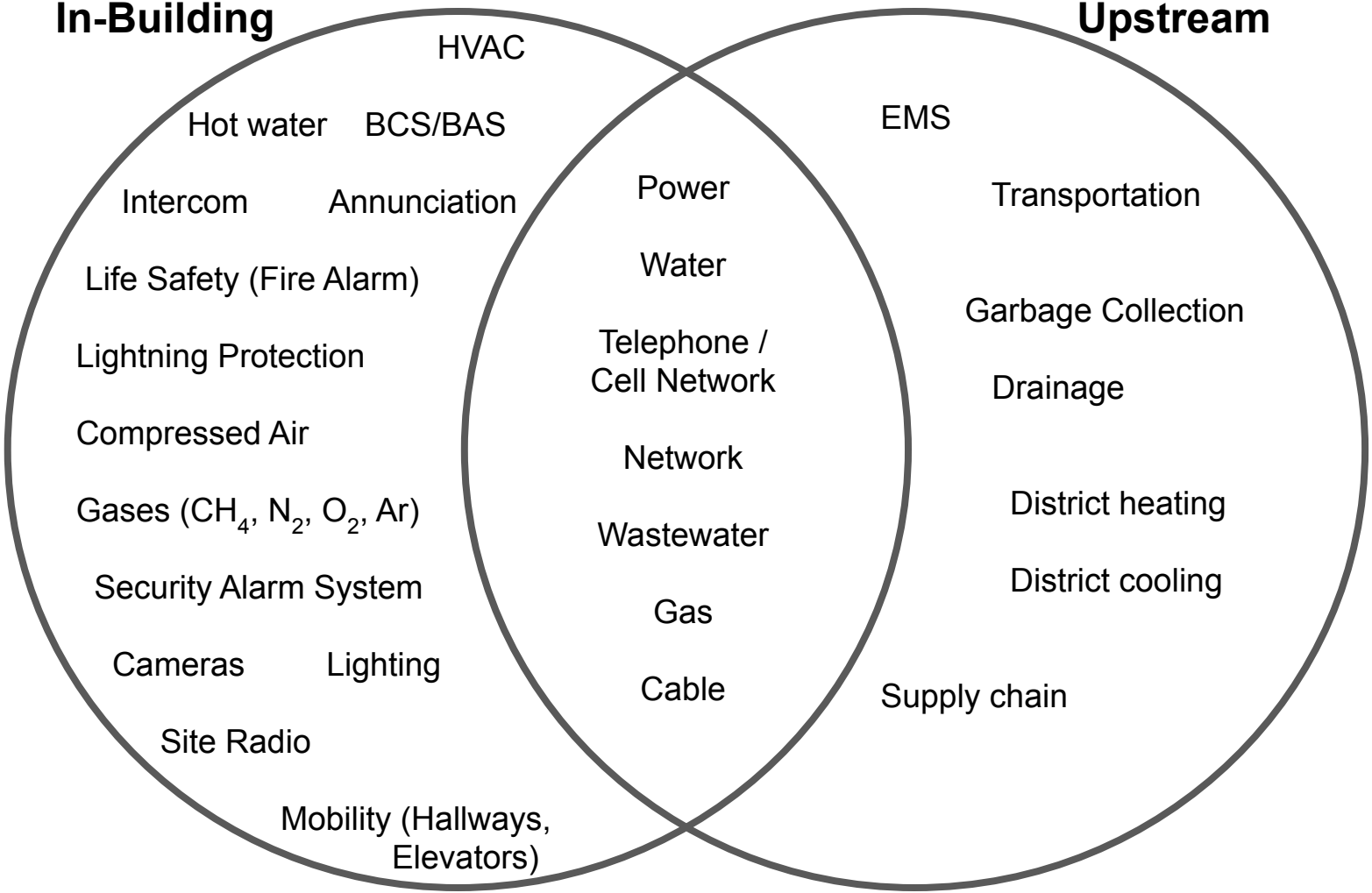
Encrypted Digital Lines



Operating Environment

What do you rely on? What can change?


VAL. to $50 Now $10 · $15 · $25


In-Building
HVAC
Hot water
BCS/BAS
Intercom
Annunciation
Life Safety (Fire Alarm)
Lightning Protection
Compressed Air
Gases (CH_4, N_2, O_2, Ar)
Security Alarm System
Cameras
Lighting
Site Radio
Mobility (Hallways, Elevators)
Power
Water
Telephone / Cell Network
Network
Wastewater
Gas
Cable
Upstream
EMS
Transportation
Garbage Collection
Drainage
District heating
District cooling
Supply chain

References

[1] B. Graydon, *Alarms and Access Controlled Doors*: DEF CON Safe Mode - Lock Bypass Village, August 6-9, 2020, Las Vegas, NV, USA. Available: https://www.youtube.com/watch?v=hGUMUG9VLKU

[2] N. Koch, *Inside Job: Exploiting Alarm Systems and the People Who Monitor Them*: HOPE 2020, July 25-August 2, 2020, New York, NY, USA. Available: https://www.youtube.com/watch?v=Rt_9dok3d_Q

[3] Physical Security, FM 19-30, Department of the Army, Washington, DC, USA, Mar. 1, 1979. [Online]. Available: https://www.jumpjet.info/Emergency-Preparedness/Disaster-Mitigation/Civil/Physical_Security.pdf

[4] R. Antunes, Intruder Alarm Systems: The State of the Art: Submitted to CEE'07 - 2nd International Conference on Electrical Engineering. Available: https://www.researchgate.net/profile/Rui-Azevedo-Antunes/publication/236982377_Intruder_Alarm_Systems_The_State_of_the_Art/links/5ec2c54492851c11a870c1ff/Intruder-Alarm-Systems-The-State-of-the-Art.pdf

[5] D. J. Brooks, Intruder alarm systems: Is the security industry installing and maintaining alarm systems in compliance to Australian Standard AS2201?: Secur J 24, 101–117 (2011). https://doi.org/10.1057/sj.2009.12

[6] B. A. Nadel, *Building Security*, New York, NY: McGraw Hill, 2004

[7] B. Graydon, *OSINT of Facilities by Physical Reconnaissance*: HOPE 2020, July 25-August 2, 2020, New York, NY, USA. Available: https://www.youtube.com/watch?v=BgovHNKh_fU

[8] K. Ng, *Bypass 101*: DEF CON Safe Mode - Lock Bypass Village, August 6-9, 2020, Las Vegas, NV, USA. Available: https://www.youtube.com/watch?v=3yKZqiYGYnA

[9] B. Phillips, *The Complete Book of Locks and Locksmithing, 7th ed.*, New York: McGraw-Hill Professional, 2017.

Questions?

b.graydon@ggrsecurity.com
@access_ctrl

Go try it!
https://www.bypassvillage.org/games/alarm_wire/

Or just: bypassvillage.org

Source:
https://github.com/bgraydon/alarm_wire

A huge thank you to Paul Robichaud, Karen Ng and Jenny & Bobby Graydon for their help in preparing this talk.